

AGREEMENT

OF [*DATE*]

ON THE PARTICIPATION OF

[*NCB*]

IN

TARGET2-SECURITIES

Currency Participation Agreement

THIS AGREEMENT IS ENTERED INTO ON [DATE] BETWEEN:

The European Central Bank

Kaiserstraße 29

60311 Frankfurt am Main

Germany

and

Nationale Bank van België/Banque Nationale de Belgique

de Berlaimontlaan/Boulevard de Berlaimont 14

1000 Brussels

Belgium

Deutsche Bundesbank

Wilhelm-Epstein-Str. 14

60431 Frankfurt am Main

Germany

Eesti Pank

Estonia pst. 13

15095 Tallinn

Estonia

Central Bank of Ireland

PO Box 559

Dame Street

Dublin 2

Ireland

Currency Participation Agreement

Bank of Greece

21, E. Venizelos Avenue

P.O. Box 3105

102 50 Athens

Greece

Banco de España

Alcalá 48

28014 Madrid

Spain

Banque de France

31, rue Croix-des-Petits-Champs

75001 Paris

France

Banca d'Italia

Via Nazionale, 91

00184 Rome

Italy

Central Bank of Cyprus

80, Kennedy Avenue

1076 Nicosia

Cyprus

Banque centrale du Luxembourg

2, boulevard Royal

2983 Luxembourg

Luxembourg

Currency Participation Agreement

Central Bank of Malta

Pjazza Kastilja

Valletta VLT 1060

Malta

De Nederlandsche Bank

Westeinde 1

1017 ZN Amsterdam

Netherlands

Oesterreichische Nationalbank

Otto-Wagner-Platz 3

1090 Vienna

Austria

Banco de Portugal

Rua do Comercio, 27

1100-150 Lisbon

Portugal

Banka Slovenije

Slovenska 35

1505 Ljubljana

Slovenia

Národná banka Slovenska

Imricha Karvaša 1

813 25 Bratislava

Slovakia

Currency Participation Agreement

Suomen Pankki

Snellmaninaukio

00170 Helsinki

Finland

(hereinafter collectively referred to as '**Eurosystem**' or '**Eurosystem Central Banks**')

and

[**NCB**]

[*address*]

The parties to this Agreement are referred to collectively as the '**Parties**' or individually as a '**Party**'.

Currency Participation Agreement

TABLE OF CONTENTS

LIST OF SCHEDULES.....	1
PREAMBLE	2
CHAPTER 1 SCOPE, DEFINITIONS AND INTERPRETATION OF THE AGREEMENT	4
Article 1 Subject matter and scope	4
Article 2 Definitions and interpretation.....	4
CHAPTER 2 RIGHTS AND OBLIGATIONS OF THE PARTIES	6
Article 3 Multilateral Character of T2S.....	6
Article 4 Duty of loyal cooperation and information	7
Article 5 Compliance with eligibility conditions for inclusion in T2S	8
Article 6 Contracts with CSDs	8
Article 7 Availability of expert personnel	9
Article 8 Compliance with Information Security requirements	9
Article 9 Obligations of the Eurosystem related to the development of T2S	10
Article 10 Obligations of the [NCB] related to the development of T2S	11
Article 11 Obligations of the Eurosystem related to testing	12
Article 12 Obligations of the [NCB] related to testing.....	13
Article 13 [NCB] Acceptance Tests of T2S	13
Article 14 Obligations of the Eurosystem related to Migration	14
Article 15 Obligations of the [NCB] related to Migration	15
Article 16 Obligations of the Eurosystem related to the provision and use of the T2S Services ..	15
Article 17 Obligations of the [NCB] related to the provision and use of the T2S Services	17
Article 18 Monetary policy operations in [currency]	18
Article 19 Obligations of the Parties related to the DCA balances	18
Article 20 Good governance.....	19
CHAPTER 3 GOVERNANCE AND CHANGE MANAGEMENT.....	19
Article 21 Governance of T2S.....	19
Article 22 Scope of participation rights.....	22
Article 23 Change and Release Management.....	23
Article 24 External Examiner	25
Article 25 Crisis management	28
Article 26 Amendments.....	29

Currency Participation Agreement

CHAPTER 4 LIABILITY REGIME, COSTS AND NETWORK SERVICE PROVIDER	31
Article 27 Standard of liability	31
Article 28 Liability rules	31
Article 29 Indemnification obligations of the [NCB] for acts of Third Parties	33
Article 30 Force Majeure and acts by Third Parties	34
Article 31 Costs and Pricing.....	34
Article 32 T2S Network Service Provider.....	35
CHAPTER 5 INTELLECTUAL PROPERTY RIGHTS, CONFIDENTIALITY AND DATA PROTECTION.....	37
Article 33 Intellectual Property Rights.....	37
Article 34 Confidentiality	39
Article 35 Data protection	40
CHAPTER 6 MISCELLANEOUS.....	41
Article 36 Governing law	41
Article 37 Dispute Resolution and Escalation Procedure.....	41
Article 38 Governors' Forum	43
Article 39 Duration, suspension and termination	44
Article 40 Own fees and costs	46
Article 41 Entire agreement.....	46
Article 42 No waiver	47
Article 43 Survival	47
Article 44 Notices.....	48
Article 45 Invalid or incomplete provisions	48
Article 46 Subcontracting.....	48
Article 47 Court proceedings.....	49
Article 48 Extension to other Parties.....	50

Currency Participation Agreement

LIST OF SCHEDULES

Schedule 1.	Definitions
Schedule 2.	T2S Programme Planning and Monitoring
Schedule 3.	User Testing
Schedule 4.	Migration
Schedule 5.	T2S Service Description
Schedule 6.	T2S Service Level Agreement
Schedule 7.	Pricing
Schedule 8.	Governance
Schedule 9.	Change and Release Management
Schedule 10.	Information Security
Schedule 11.	Exit Management
Schedule 12.	Procedure for Payment of Claims
[where applicable: Schedule 13.]	NCB-specific Requirements]

Currency Participation Agreement

PREAMBLE

Whereas:

A) On 6 July 2006, the Governing Council decided to explore, in cooperation with the Central Securities Depositories (hereinafter the ‘CSDs’) and other market participants, the possibility of setting up a new Eurosystem service for securities settlement in Central Bank Money, to be called TARGET2-Securities. As part of the Eurosystem’s tasks in accordance with Articles 17, 18 and 22 of the Statute of the European System of Central Banks and of the European Central Bank (hereinafter the ‘Statute of the ESCB’), T2S aims to facilitate post-trading integration by supporting core, neutral and borderless pan-European cash and securities settlement in Central Bank Money so that CSDs can provide their customers with harmonised and commoditised settlement services in an integrated technical environment with cross-border capabilities. As the provision of Central Bank Money is a core task of the Eurosystem, T2S has the nature of a public service. The Eurosystem will provide collateral management services and settlement in Central Bank Money in T2S in euro.

B) Settlement in Central Bank Money avoids liquidity risks and is therefore essential for sound post-trading of securities, and for the financial market in general.

C) On 17 July 2008, the Governing Council decided to launch the T2S project and to provide the resources required until its completion. On the basis of an offer made by the Deutsche Bundesbank, the Banco de España, the Banque de France and the Banca d’Italia (hereinafter the ‘4CB’), the Governing Council also decided that T2S would be developed and operated by the 4CB.

D) On 21 April 2010, the Governing Council adopted the Guideline ECB/2010/2 on TARGET2-Securities of 21 April 2010 (hereinafter the ‘T2S Guideline’)¹, which lays down the basic foundations of the T2S Programme in its Development Phase and further specifies the governance procedures of the Eurosystem applicable in this context. On the same day, the Governing Council endorsed the Second T2S Protocol on the granting by the Eurosystem Central Banks to each other of a power of attorney to sign the Framework Agreement with the CSDs, in the name and on behalf of all Eurosystem Central Banks.

E) Article 3 of the T2S Guideline provides that the governance of the T2S Programme within the Eurosystem is based on three levels. Level 1 (Governing Council) is responsible for the direction, overall management and control of the T2S Programme, has responsibility for the ultimate decision-making in this thereto and decides on the allocation of tasks not specifically attributed to Levels 2 and 3. Level 2 (T2S Board) is in charge of the tasks assigned to Level 2 within the gen-

¹ OJ L 118, 12.5.2010, p. 65.

Currency Participation Agreement

eral framework defined by the Governing Council. Level 3 (4CB) develops and operates T2S. The [NCB] has full and exclusive authority, in particular, to make available, set-up, monitor, block and close the DCAs in [currency] in T2S and shall be closely involved in the governance related to all matters of relevance for Connected NCBs in T2S as further specified in this Agreement.

F) General Principle [10] of T2S provides that T2S will be technically capable of settling currencies other than the euro. As regards the wish of the [NCB] to make the [currency] available for Central Bank Money settlement in T2S, and subject to the signing of this Agreement, including its Schedules ('Agreement'), the Governing Council has approved its eligibility on [date].

G) The Parties recognise that each Party to this Agreement has responsibility for retaining full control over its currency and maintaining its ability to implement monetary policy, exert efficient oversight of its market infrastructure and carry out its obligations for financial stability.

H) The Eurosystem and the [NCB] will exchange sensitive information pursuant to the terms of this Agreement. Moreover, T2S will also process sensitive data stemming from either of the Parties. Therefore, it is the common interest of the Parties to maintain the confidentiality of any such data according to applicable law. Pursuant to Article 37 of the Statute of the ESCB, national legislation or other principles of law, members of the governing bodies and the staff of the Central Banks are required, even after their duties have ceased, not to disclose information of the kind covered by the obligation of professional secrecy.

I) The Parties also acknowledge the importance of cooperating closely with respect to oversight and supervisory requirements that may apply in relation to this Agreement.

J) Notwithstanding the provisions on governance and dispute resolution set out in this Agreement, it is the common understanding of the Parties that they will use their best efforts and act in good faith to prevent any dispute arising out of this Agreement. In the event of any such a dispute, the Parties agree to settle it in an amicable way taking into particular account their respective roles as public authorities in respect of certain rights and obligations to be performed under this Agreement, and will use all possible technical means to resolve any such dispute to the extent they comply with the General Principles of T2S, the Multilateral Character of T2S and the eligibility conditions as set out in [Article 18(1)] OR [Article 18(2)] of the T2S Guideline.

Now, therefore, the Parties agree as follows:

CHAPTER 1

SCOPE, DEFINITIONS AND INTERPRETATION OF THE AGREEMENT

Article 1

Subject matter and scope

1. T2S shall be based on a single technical platform integrated with Central Bank RTGS Systems. It is a service provided by the Eurosystem to Participating CSDs allowing for the core, neutral and borderless settlement of securities transactions in Central Bank Money. T2S shall support not only settlement of securities transactions in euro, but will also be open to Eligible NCBs that wish to participate by making their currencies available for Central Bank Money settlement in T2S.
2. The [NCB] shall have no contractual relationship with the 4CB in relation to T2S, other than with each of these four Central Banks as members of the Eurosystem, and shall waive any recourse against the 4CB in connection with matters covered by this Agreement to the extent permissible by applicable law.
3. The Eurosystem shall have no contractual relationship with the Connected NCBs' Dedicated Cash Account Holders related to the use of [currency] for securities settlement in T2S.
4. This Agreement and the General Principles of T2S set out the scope of the T2S Services for the NCBs.
5. This Agreement sets out the Parties' rights and obligations for the Development Phase and the Operational Phase.

Article 2

Definitions and interpretation

1. In this Agreement references:
 - (a) to applicable laws, Schedules, Annexes or other documents shall be deemed to refer, unless specified otherwise, to the respective applicable laws, Schedules, Annexes or other documents;
 - (b) to this Agreement (whether included in the Articles of the Agreement or in a Schedule or an Annex) shall include the Schedules and the Annexes;
 - (c) to 'include', 'includes', 'including', 'in particular' or 'e.g.' means 'without limitation';

Currency Participation Agreement

- (d) to persons shall include natural and legal persons and shall include the permitted transferees and assignees of such individuals and legal entities;
 - (e) to the holder of any office or position of responsibility include references to such person as is from time to time appointed to exercise the functions of the holder;
 - (f) to any service or other matter or item as described, listed or specified in this Agreement shall include references to such service or other matter or item as removed, replaced, amended or edited from time to time under the terms of this Agreement;
 - (g) words in the plural shall have the same meaning when used in the singular and *vice versa*.
2. The heading and table of contents in this Agreement shall not affect its interpretation.
3. This Agreement is composed of the Preamble and of Articles 1 to [48] as well as **Schedules 1 to [12] OR [13]**. The Schedules and the Annexes to the Schedules form part of this Agreement and shall have the same force and effect as if expressly set out in Articles 1 to [48]. **Schedule 1** (Definitions) sets out the meaning of terms in this Agreement, which are written with initial capital letters, other than proper nouns or titles of the Schedules to the Agreement. In the event of any conflict or inconsistency between Articles 1 to [48], a Schedule or an Annex, [*for NCBs with such a Schedule 13 only*; and without prejudice to the NCB-specific Requirements as set out in **Schedule 13**], Articles 1 to [48] shall prevail. In the event of a conflict or inconsistency between **Schedule 1** and the other Schedules [*for NCBs with such a Schedule 13 only*; (other than **Schedule 13**)], or between such other Schedules themselves, **Schedule 1** shall prevail over the other Schedules [*for NCBs with such a Schedule 13 only*; other than **Schedule 13**] and shall be used to resolve conflicts or inconsistencies between such other Schedules except in the instances detailed here. In the event of a conflict between a Schedule and an Annex, the terms of the Schedule shall prevail. In the event of a conflict or inconsistency between this Agreement and any other document referenced or referred to it, this Agreement shall prevail.
4. Where this Agreement contains a German term as a translation of an English term, the German term shall be binding for the interpretation of this Agreement.
5. The T2S Scope Defining Set of Documents shall be part of this Agreement, unless and to the extent expressly specified to the contrary therein or in this Agreement. In case of such specification, the relevant part of the T2S Scope Defining Set of Documents shall have only interpretative value. The T2S Scope Defining Set of Documents may be complemented from time to time in accordance with **Schedule 9**. The Eurosystem shall aim at ensuring consistency between the T2S Scope Defining Set of Documents and **Schedule 5** at all times. In the event of inconsistencies between documents, the last version of the most detailed document reviewed by the Parties in accordance with Chapter 3 of Annex 8 to **Schedule 2** concerning the issue

shall prevail. If a requirement or function is not specified in the GFS or the UDFS, the URD shall prevail. The T2S Documentation that is not part of the T2S Scope Defining Set of Documents is not part of this Agreement unless and insofar expressly specified to the contrary in this Agreement. The T2S Documentation may be complemented from time to time by the Eurosystem in accordance with Annex 8 to **Schedule 2**. The Eurosystem shall make the T2S Documentation available to the [NCB]. The T2S Documentation is not to be understood as amending, being part of, or supplementing this Agreement unless specifically provided for in this Agreement.

CHAPTER 2

RIGHTS AND OBLIGATIONS OF THE PARTIES

Article 3

Multilateral Character of T2S

1. The Parties acknowledge that T2S is multilateral in character in that it aims at facilitating European post-trading integration by supporting securities settlement in Central Bank Money, thereby combining the interests of Central Banks, Participating CSDs and all other T2S Actors. The Parties agree that actions that would have a material negative impact on any of the Connected NCBs or would not be in line with the aim of achieving securities settlement in Central Bank Money are incompatible with the Multilateral Character of T2S. The T2S Services shall be provided to Connected NCBs on the basis of uniform requirements and Governance rules, which include a framework for Specific Changes.
2. The Parties acknowledge that this Agreement shall not cover nor affect or prejudice any current or future role or policy or the exercise of any rights and discretions or obligations of the [NCB] and the Eurosystem, or require the disclosure of any information in the possession of the [NCB] and the Eurosystem in its capacity as operator of a Securities Settlement System or as a T2S User or T2S Actor, except where otherwise provided in this Agreement.
3. The Parties also acknowledge that this Agreement does not cover or affect or prejudice any current or future role or policy or the exercise of any rights and discretions or obligations of the [NCB] or the Eurosystem, or require the disclosure of any information in the possession of the [NCB] or the Eurosystem, with respect to its tasks or responsibilities under the Treaty or applicable law (including, for monetary policy, the supervision or oversight of payment and securities settlement or clearing systems and financial stability).

Currency Participation Agreement

4. The [NCB] shall take, to the extent within the powers of the [NCB], all reasonable measures in relation to Legal and Regulatory Requirements, so that securities transactions in [currency] can be settled in T2S in Central Bank Money in accordance with the process specified in **Schedule 4** and by the time stipulated in **Schedule 2**, as further specified in Article 15, as well as in order to make efficient use of T2S Services and to maintain the Multilateral Character of T2S.
5. The [NCB] shall not prevent the Eurosystem from entering into one or more Parallel CPAs.
6. The Eurosystem shall inform the [NCB] reasonably in advance whenever an Eligible NCB enters into a CPA with the Eurosystem or a CSD enters into a Framework Agreement with the Eurosystem.
7. Notwithstanding the common understanding of the Parties to this Agreement, that its main substantive terms are uniform with regard to all Connected NCBs, and the Multilateral Character of T2S, all rights and obligations of the [NCB] under this Agreement are exercised independently from the other Connected NCBs except where otherwise provided in this Agreement.

Article 4

Duty of loyal cooperation and information

1. In the exercise of its rights and the performance of its obligations under this Agreement each Party shall:
 - (a) act in good faith and cooperate with the other Party closely and transparently in their contractual relations; and
 - (b) promptly give to the other Party notice of facts and information of which it is aware that may reasonably affect its own or the other Party's ability to perform obligations under this Agreement in any material respect.
2. The Eurosystem shall maintain contact with the relevant Union institutions and bodies, and to the extent necessary under this Agreement with national authorities, including the Relevant Competent Authorities.
3. Notwithstanding that General Principle 9 of T2S provides that the primary focus of the Eurosystem is to ensure efficient and sound settlement services in euro, as well as any relevant provisions of the Statute of the ESCB or the Treaty on the Functioning of the European Union, and in line with General Principle 10 of T2S the Eurosystem is committed to treating the [NCB] in the same manner as the Eurosystem, to treating settlement in [currency] in the same manner as settlement in euro, to treating the RTGS System for [currency] in the same manner

Currency Participation Agreement

as TARGET2 and to treating the [NCB's] CMS in the same manner as the CMS(s) of the Eurosystem Central Banks.

Article 5

Compliance with eligibility conditions for inclusion in T2S

1. [For EEA NCB: Pursuant to Article 18(1) of the T2S Guideline, an EEA currency is eligible for use in T2S provided that the Non-euro Area NCB, Other Central Bank or other authority responsible for such currency enters into a CPA with the Eurosystem, and before signing the CPA, the Governing Council has approved the eligibility of the currency.]

OR [For non-EEA NCB: Pursuant to Article 18(2) of the T2S Guideline, a currency other than an EEA currency is eligible for use in T2S provided that the Governing Council has approved the eligibility of such currency, if all the following conditions are met:

- (a) the legal, regulatory and oversight framework applicable to settlement in that currency provides substantially the same or a higher degree of legal certainty as that in force in the Union;
 - (b) the inclusion of such currency in T2S would have a positive impact on the contribution of T2S to the Union securities settlement market;
 - (c) the Other Central Bank or other authority responsible for such currency enters into a mutually satisfactory CPA with the Eurosystem.]
2. [For non-EEA NCB: The [NCB] shall ensure that the eligibility conditions of the [currency] as set out in Article 18(2)(a) of the T2S Guideline are met on an ongoing basis.]

Article 6

Contracts with CSDs

For the avoidance of doubt, the [NCB] acknowledges that pursuant to Article 16(3) of the T2S Guideline contracts with CSDs shall be approved by the Governing Council and subsequently signed by the Eurosystem Central Bank of the country where the seat of the CSD is located, or by the ECB for CSDs located outside the euro area, in either case acting in the name and on behalf of all Eurosystem Central Banks, and that, in relation to Ireland, the contract shall be signed by the Eurosystem Central Bank of the Member State that has notified the Securities Settlement System to ESMA in accordance with Article 10 of the Settlement Finality Directive.

Currency Participation Agreement

Article 7

Availability of expert personnel

Each Party shall ensure that sufficient and qualified personnel with appropriate expertise and training for the tasks in which they are engaged, are used to perform the duties and obligations under this Agreement.

Article 8

Compliance with Information Security requirements

1. The Eurosystem shall in accordance with and as described in **Schedule 10**:
 - (a) implement the Information Security framework for T2S;
 - (b) implement a process to manage Information Security in T2S by: (i) regularly reviewing the implementation and (ii) regularly aligning the T2S Security Requirements with technical developments;
 - (c) maintain the T2S Threat Catalogue;
 - (d) perform all activities related to Information Security in accordance with **Schedule 10**;
 - (e) report the results of Information Security reviews and provide additional information on request to the [NCB];
 - (f) report Information Security incidents to the [NCB] in accordance with the provisions set out in **Schedule 10**;
 - (g) provide all other relevant information to the [NCB] to allow the latter to fulfil its own risk management obligations and in particular inform the [NCB] if the Eurosystem decides to change its Information Security policy.
2. In view of ensuring Information Security for T2S, the [NCB] shall:
 - (a) ensure its own compliance with Information Security requirements in relation to T2S according to its internal standards, Legal and Regulatory Requirements and/or best practices;
 - (b) report Information Security incidents to the Eurosystem, if T2S or other T2S Actors might be impacted by such incidents; and
 - (c) report to the Eurosystem newly identified threats or detected gaps that might threaten T2S Information Security.
3. The Parties shall cooperate as follows:

Currency Participation Agreement

- (a) The Eurosystem shall at least on a yearly basis deliver for review to the [NCB] the T2S Information Security Risk Evaluation Table and the T2S Information Security Risk Treatment plan, as further specified in Section 4.2 of **Schedule 10**.
 - (b) The Eurosystem shall maintain a consolidated action plan for all risks appearing in a T2S Information Security Risk Treatment plan which require follow-up, and shall deliver for review to the [NCB] an updated version of the action plan at least on an annual basis, as further specified in Section 4.2.2 of **Schedule 10**.
 - (c) The Eurosystem shall set up a multilateral coordination substructure, in accordance with the Governance, to coordinate and monitor the T2S Information Security Risk Management activities, as further specified in Section 4.3 of **Schedule 10**.
 - (d) If a disagreement arises in the substructure, each Party may escalate the issue to the Steering Level and, if the disagreement persists, may initiate the Dispute Resolution and Escalation Procedure, as further specified in Section 4.3 of **Schedule 10**.
 - (e) If a new Information Security risk is identified, or if an existing Information Security risk obtains a higher likelihood or impact score, the Eurosystem shall communicate such changes to the [NCB] in accordance with the incident response times specified in **Schedule 6**, as further specified in Section 4.3 of **Schedule 10**.
- 4. Any matters related to operational risk, which are not covered by this Article or in **Schedule 10**, shall be managed directly by the Steering Level.
 - 5. The Eurosystem will implement an appropriate risk management framework and inform the [NCB] monthly about the risk situation.

Article 9

Obligations of the Eurosystem related to the development of T2S

The Eurosystem shall:

- (a) establish T2S in performance of its public tasks and in accordance with the T2S Scope Defining Set of Documents and **Schedule 5** and use reasonable efforts to allocate appropriate resources to its implementation and to respect the milestone deliverables set out in **Schedule 2** in line with the agreed procedure for modifications as defined in **Schedule 2**;
- (b) set up and maintain the T2S Programme Plan as well as assess and adjust the T2S Programme Plan, with a view to ensuring effective implementation of the T2S Services;
- (c) report to and inform the [NCB] in accordance with **Schedule 2** on the progress achieved;

Currency Participation Agreement

- (d) make available T2S Documentation to the [NCB] in line with **Schedule 2**;
- (e) implement Common and Specific Changes to the T2S Services as requested by the [NCB] and managed by the Eurosystem in accordance with Article 23 and **Schedule 9**;
- (f) provide reasonable support to the [NCB] during the Development Phase on request by the [NCB]; and
- (g) submit processes and reasonable timelines in line with **Schedule 9** to allow the [NCB] to review and agree on the preparation of the T2S Documentation as provided for in Article 10.

Article 10

Obligations of the [NCB] related to the development of T2S

As further specified in the relevant Schedules, the [NCB] shall participate in and contribute to the development of T2S as follows:

- (a) it shall cooperate with the Eurosystem by adapting its own systems and processes, especially by ensuring adequate system interfaces and, to the extent within the power of the [NCB], reliable connections, and allocate appropriate resources to the implementation of its project plan, assess and adjust such project plan, to allow for the [NCB's] operational and technical readiness for the use of the T2S Services and for the timely initiation of provision of such T2S Services. For the avoidance of doubt, such obligation of the [NCB] to adapt its own systems does not include an obligation to develop a full interface allowing Payment Banks to connect indirectly to T2S via the [NCB];
- (b) it shall support the Eurosystem in the preparation of the T2S Documentation in accordance with Annex 8 to **Schedule 2**,
- (c) it shall inform the Eurosystem whenever it has in its possession material information, whether of a technical or operational nature or in relation to Legal and Regulatory Requirements, that would in the absence of any action by the Eurosystem lead to a material adverse effect on the effective and harmonised functioning of the T2S Programme and/or T2S Services [for non-EEA currency: (including compliance with the eligibility conditions set out in Article 18(2)(a) of the T2S Guideline)];
- (d) it shall use reasonable efforts to respect the milestone deliverables set out in **Schedule 2**, as applicable, set up its own project plan for the implementation of the T2S Programme, allocate resources to successive versions of the T2S Documentation, with the view to ensuring effective use of the T2S Services in accordance with the timelines referred to in

Currency Participation Agreement

Article 9[(g)], and report on the progress of its project plan and its readiness for the effective implementation of the T2S Services;

- (e) it shall provide appropriate support to the Eurosystem in its relationship with the Relevant Competent Authorities responsible for Legal and Regulatory Requirements;
- (f) it shall cooperate with the Eurosystem and a Participating CSD located in the same country as the [NCB] as regards that Participating CSD's implementation of the T2S Programme; and
- (g) the [NCB] shall participate in and contribute to the work of the relevant groups set up or supported by the Eurosystem in relation to the Governance.

Article 11

Obligations of the Eurosystem related to testing

As further specified in **Schedule 3**, the Eurosystem shall:

- (a) coordinate the User Testing activities and communication between the [NCB] and the Central Banks whose respective currencies are available for settlement in T2S, as well as between the [NCB] and Participating CSDs participating in the User Testing activities;
- (b) inform the [NCB] about the results of User Testing as defined in **Schedule 3**;
- (c) prepare and execute the EAT, and provide regular progress reporting as well as an assessment report confirming the compliance of T2S with **Schedule 5** and the T2S Scope Defining Set of Documents before the start of User Testing;
- (d) define the NCB certification tests required to assess that the [NCB's] systems cannot harm T2S due to an inappropriate technical communication or operational procedure;
- (e) define the DCA Holder Certification Tests for those DCA Holders which [NCB] has authorised to connect to T2S with an A2A connection and for those DCA Holders which [NCB] has authorised to connect to T2S with a U2A connection which are required to assess that the systems of the directly connected DCA Holders of the [NCB] cannot harm T2S due to an inappropriate technical communication or operational procedure;
- (f) for all directly connected DCA Holders of [NCB], the Eurosystem shall undertake the DCA Holder Certification process; the Eurosystem shall upon request provide [NCB] with the results of such DCA Holder Certification process.
- (g) prepare the necessary non-functional tests and execute these non-functional tests in order for the Eurosystem to confirm the non-functional compliance of T2S;
- (h) remedy any material deficiency defined as critical defect (priority 1) and, for any defect defined as high defect (priority 2), either directly resolve the defect or, if agreed with the [NCB], as a first step, provide a technical or procedural workaround and, as a second

Currency Participation Agreement

step, resolve the defect within a specific timeframe to be defined along with the work-around to ensure that the T2S Services are established in accordance with the principles set out in **Schedule 5** and the T2S Scope Defining Set of Documents;

- (i) provide reasonable support for testing activities of the [NCB] in the different stages of User Testing; and
- (j) cooperate with the [NCB] in respect of its own acceptance tests of the relevant T2S Services in accordance with Article 13.

Article 12

Obligations of the [NCB] related to testing

As further specified in **Schedule 3**, the [NCB] shall:

- (a) support the Eurosystem in the preparation of the overall User Testing calendar by providing the Eurosystem with its proposed test plan and User Testing calendar of its activities;
- (b) execute the mandatory test cases and test scenarios for NCB certification within the period foreseen in **Schedule 2** for the migration wave in which it is participating;
- (c) in good time before the period foreseen in Schedule 2 for the migration wave in which it is participating, provide the Eurosystem with the necessary information about those DCA Holders which have been authorised to connect to T2S with an A2A connection and those which have been authorised to connect to T2S via a U2A connection. For the avoidance of doubt, the [NCB] is not responsible for the certification of its DCA Holders.
- (d) cooperate with the Eurosystem in respect of its acceptance tests for the relevant T2S Services in accordance with Article 13.

Article 13

[NCB] Acceptance Tests of T2S

1. Following the Eurosystem's notification of its readiness to fulfil synchronisation point 8 (start bilateral interoperability testing) according to Annex 9 to **Schedule 2**, the [NCB] shall be entitled to test the compliance of the relevant T2S Services with **Schedule 5** and the T2S Scope Defining Set of Documents in accordance with the methodology stated in this Article and in **Schedule 3**.
2. In case the [NCB] chooses to perform the tests defined in paragraph 1, the [NCB] shall finalise such tests within six months following the Eurosystem's notification of its readiness to

Currency Participation Agreement

fulfil synchronisation point 8 (start bilateral interoperability testing), unless provided otherwise in **Schedule 2**. If the [NCB] discovers that the relevant T2S Services do not comply with **Schedule 5** and/or the T2S Scope Defining Set of Documents, it shall follow the procedures laid down in Section 5.3 of **Schedule 3**.

3. Notwithstanding the [NCB]'s decision to perform the tests as described in paragraphs 1 and 2, the [NCB] shall provide to the Eurosystem in writing and within six months following the Eurosystem's notification of its readiness to fulfil synchronisation point 8 (start bilateral interoperability testing), whether or not it accepts the relevant T2S Services as compliant with **Schedule 5** and the T2S Scope Defining Set of Documents.
4. If the [NCB] notifies the Eurosystem that it does not accept the relevant T2S Services as compliant with **Schedule 5** and the T2S Scope Defining Set of Documents, it shall promptly, and in no case later than within five working days following such notification deliver a report to the Eurosystem describing all cases of non-compliance it has identified (non-compliance notification).
5. Following a Eurosystem's notice to the [NCB] that the Eurosystem has remedied individual or all cases of material non-compliance, the [NCB] shall test the error correction.
6. When the [NCB] finds that none of the reported cases of material non-compliance continues to exist, it shall provide a confirmation that it accepts the relevant T2S Services as compliant with **Schedule 5** and the T2S Scope Defining Set of Documents (compliance confirmation) in writing without undue delay.
7. This Article does not affect the [NCB's] termination rights according to Article 39.

Article 14

Obligations of the Eurosystem related to Migration

As further specified in **Schedule 4**, the Eurosystem shall:

- (a) establish the necessary procedures and tools for Migration which will, *inter alia*, support the [NCB] in suspending or reversing its Migration if the conditions for Migration, as defined in **Schedule 4**, cannot be satisfied; and
- (b) provide the [NCB] with support related to its activities necessary for completing Migration or suspending Migration, if necessary.

Currency Participation Agreement

Article 15

Obligations of the [NCB] related to Migration

As further specified in **Schedule 4**, the [NCB] shall:

- (a) adjust its internal systems, processes, interfaces and connections to enable its Migration to T2S in compliance with the T2S Documentation, and to achieve operational and technical readiness for the use of the T2S Services;
- (b) set up its own project plan for the Migration and do what is reasonably required to ensure that its Dedicated Cash Account Holders are able to migrate to the T2S-enabled Services within the timeframe specified in **Schedule 2**;
- (c) migrate to T2S in accordance with the process specified in **Schedule 4** and by the timeframe provided in **Schedule 2**, or, if it is unable to migrate by the scheduled date, at the latest it shall migrate by the date of the contingency migration wave, as specified in **Schedule 2**; and
- (d) cooperate with the Eurosystem in documenting that its Migration has been successfully completed.

Article 16

Obligations of the Eurosystem related to the provision and use of the T2S Services

1. For the provision and use of T2S Services, the Eurosystem shall:

- (a) provide the [NCB] with the T2S Services and system functionality as described in **Schedule 5**;
- (b) provide the [NCB] with all necessary rights to exclusively exercise full control in real time over the DCAs in [currency] in T2S, including the right to real-time blocking and unblocking with immediate effect and to the real-time initiation of their closure with effect on the next Settlement Day, however without prejudice to the finality and irrevocability of entries on such DCAs on the T2S Platform as set out in Article 19;
- (c) provide the [NCB] with the right to the real-time initiation of a change (being applicable in T2S on the next Settlement Day, except in special circumstances where specific manual procedures according to the MOP shall be foreseen for implementation in real-time) as regards the following:
 - (i) the usage of selected securities in its respective currency for auto-collateralisation,
 - (ii) the credits granted for securities settlement in [currency] in T2S,

Currency Participation Agreement

- (iii) the determination of the individual ISINs which may be used as collateral for individual credits in T2S,
 - (iv) the valuation of each ISIN, and
 - (v) the identification of the accounts on which the collateral may be held for credit with the [NCB],
- in each case if relevant for the [NCB's] collateral procedure;
- (d) implement Common and Specific Changes to the T2S Services as requested by the [NCB] and managed by the Eurosystem in accordance with Article 23 and **Schedule 9**;
 - (e) endeavour to maintain the T2S Services to support, in cooperation with the [NCB], ongoing compliance with Legal and Regulatory Requirements, without prejudice to the application of Article 23 and **Schedule 9** to changes that may need to be implemented as a result of such requirements;
 - (f) suspend the settlement in [currency] if so requested by the [NCB];
 - (g) reinstate operations to permit use of the T2S Services following a failure as specified in **Schedule 6**;
 - (h) provide the [NCB] with financial statements, reports and other information on T2S on a regular basis that fairly represent the business and financial conditions, results of operations and state of the cost recovery in relation to T2S on the respective dates or for the respective periods covered by such financial statements, reports and other information; and
 - (i) update the T2S Documentation in a timely manner.
2. Changes to the T2S Platform or T2S Business Application that need to be implemented urgently to restore or continue the provision of the T2S Services in accordance with the service levels specified in **Schedule 6**, may be autonomously decided and implemented by the Eurosystem in accordance with **Schedule 6** and the MOP, provided that such a change does not in any way diminish the right of the [NCB] to exclusively exercise control over its DCAs. The Eurosystem shall inform the [NCB] as soon as reasonably practicable on the nature and characteristics of the changes and the time in which the change shall be implemented.
3. The Eurosystem shall make available to the [NCB] a monthly Service Level Report to determine the degree of the Eurosystem's compliance with **Schedule 6**, in particular as regards the KPIs. If the Eurosystem fails to meet any of the KPIs, it shall in cooperation with the [NCB]:
- (a) investigate the underlying cause of the failure;
 - (b) take necessary measures to minimise the impact of the failure;

Currency Participation Agreement

- (c) take necessary measures to prevent the failure from recurring; and/or report on the cause, the status and the remedies required to prevent recurrence of the failure.

Article 17

Obligations of the [NCB] related to the provision and use of the T2S Services

1. The [NCB] shall use the T2S Services, once (a) the User Testing is completed as specified in Article 15 and **Schedule 3** and (b) Migration has been successfully completed as specified in Article 15 and **Schedule 4**.
2. In pursuance of its obligations to use the T2S Services, the [NCB] shall, in particular:
 - (a) perform the duties and responsibilities assigned to it in **Schedule 6**, and in particular:
 - (i) according to its rules applicable to its RTGS Participants, make available, set up and close DCAs of its RTGS Participants in [currency] for all securities-related payment transactions in [currency] in T2S; for the avoidance of doubt the Parties agree that the Eurosystem is not responsible for monitoring the DCAs;
 - (ii) set up and manage static data, access rights and configuration data pertaining to its Dedicated Cash Account Holders and its own participation in T2S;
 - (iii) provide for the interoperability of its own RTGS System in accordance with the timing provisions specified in **Schedule 2** and, where applicable, its Collateral Management System with T2S to ensure the smooth functioning of the relevant connections;
 - (iv) based on the operational decision of the [NCB], provide auto-collateralisation in [currency] to its Dedicated Cash Account Holders according to its own terms and conditions;[and]
 - (v) if the auto-collateralisation functionality is used, provide to the Eurosystem a list of eligible securities and the Collateral Value for the securities identified as eligible for auto-collateralisation as well as any other data necessary for the Eurosystem to judge the eligibility of securities for a specific participant (including, in relation to close links and the identification of the accounts on which the collateral may be held, if relevant for the [NCB's] collateral procedure) [.][]; and]
 - (vi) [for non-EEA currency: inform the Eurosystem without delay after having gained knowledge of Legal or Regulatory Requirements that might have a material impact on the participation of the [NCB] in T2S (including compliance with the eligibility conditions set out in Article 18(2)(a) of the T2S Guideline).]

Currency Participation Agreement

- (b) ensure that the agreements with its Dedicated Cash Account Holders, to the extent that they are not directly connected to T2S and use Connectivity Services via the [NCB] if the [NCB] chooses to offer such services, contain provisions that are consistent with Article 28 and Article 32 regarding the use of Connectivity Services by the [NCB]; and
 - (c) support the resumption of the T2S Services following an event of a failure as specified in **Schedule 6**.
3. The [NCB] shall review, comment on, and accept or reject the Eurosystem report referred to in paragraph 3 of Article 16. If the [NCB] rejects the report in whole or in part, or the remedies proposed by the Eurosystem for preventing recurrence of not meeting the KPIs, it may revert to the Dispute Resolution and Escalation Procedure.

Article 18

Monetary policy operations in [currency]

The [NCB] shall be entitled to undertake settlement of monetary policy transactions in Central Bank Money in [currency] outside T2S provided that: (i) the Eurosystem has received all relevant information on the technical functioning of such settlement; and (ii) such settlement neither requires changes to nor negatively affects, the T2S functionality as described in the T2S Scope Defining Set of Documents. The Eurosystem shall grant to the Participating CSD(s) designated by the [NCB] a derogation from the eligibility criterion set out in Article 15(1)(e) of the T2S Guideline in relation to such monetary policy transactions in line with the Decision ECB/2011/20, the procedure of granting such derogation shall be finalised as soon as possible after the Eurosystem has received all relevant information set out under (i). Such derogation shall not be unreasonably withheld by the Eurosystem.

Article 19

Obligations of the Parties related to the DCA balances

1. DCA balances of the [NCB] operated on the T2S Platform shall only be changed in T2S. The [NCB] shall ensure as regards its operational processes and contractual terms that entries on the DCAs on the T2S Platform have immediate legal effect, with regard to the finality and irrevocability of the settlement and shall make all necessary arrangements to this effect. Moreover, with regard of the moment of entry of Transfer Orders into a system and their irrevocability, in accordance with the Settlement Finality Directive, the Eurosystem shall inform the [NCB] and take into account the [NCB's] views as regards the harmonisation efforts to which

Currency Participation Agreement

Participating CSDs are committed under the respective Framework Agreement related to harmonisation of the different rules applicable in the systems of the different CSDs.

2. The Parties agree that all matters relating to the DCAs (including the validity and enforceability of any debits and credits to the DCAs) are governed by the law of the [NCB].

Article 20

Good governance

In order to avoid conflicts of interest between the [NCB's] operating and regulatory functions in relation to T2S, the [NCB] shall ensure that members of the T2S Board do not participate in any oversight or other activity that could create a conflict of interest, as specified in the rules of procedures of the T2S Board.

CHAPTER 3

GOVERNANCE AND CHANGE MANAGEMENT

Article 21

Governance of T2S

1. Without prejudice to Article 37 the governance framework applicable during the development and operation of the T2S Services is specified in this Article and **Schedule 8**. In particular the following principles of relevance to Connected NCBs shall apply:
2. Based on Article 127 of the Treaty on the Functioning of the European Union and Article 3 of the Statute of the ESCB, in the T2S context, the Eurosystem shall in particular:
 - (a) exclusively exercise full control over all cash accounts in euro in T2S, i.e. operate the cash accounts it holds for its banks and safeguard the integrity of the euro which, for the purposes of this Agreement, includes the implementation of monetary policy including all central bank credit operations as well as settlement in Central Bank Money in the euro;
 - (b) contribute to the smooth conduct of policies pursued by the competent authorities relating to the prudential supervision of credit institutions and the stability of the financial system;
 - (c) ensure that it does not distort a level playing field for market participants; and
 - (d) exert efficient oversight of market infrastructure while preserving the separation of this function from its operational activities of T2S.

Currency Participation Agreement

3. Subject to **Schedule 8**, Connected NCBs shall have the same rights in T2S as the Eurosystem in relation to their respective currencies.
4. The Eurosystem shall have control and participation rights in the Governance of T2S in the performance of its tasks under the Treaty on the Functioning of the European Union and the Statute of the ESCB and in its capacity as owner and operator of T2S. In particular, this includes the ability to recover its costs and to operate T2S in a safe and efficient manner with due consideration of the rights, interests, prerogatives and obligations of the T2S Stakeholders in line with the Multilateral Character of T2S. The Governing Council shall have ultimate decision making powers.
5. The Connected NCBs shall have control and participation rights in accordance with the Governance framework of T2S, in particular through their participation in the relevant Governance bodies as set out in this Article and the decision-making process as outlined in **Schedule 8**.
6. Without prejudice to the ultimate decision-making powers of the Governing Council as set out in **Schedule 8**, and the decision-making bodies of the Connected NCBs, the T2S Governance bodies shall comprise:
 - (a) the T2S Board, which replaces the T2S Programme Board established by Decision ECB/2009/6;
 - (b) the CSD Steering Group (CSG), whose mandate and composition are annexed to Schedule 8 of the Framework Agreement;
 - (c) the Non-euro Currencies Steering Group (NECSG), whose mandate and composition are set out in **Schedule 8**;
 - (d) the Governors' Forum, whose mandate and composition are set out in **Schedule 8**;
 - (e) the T2S Advisory Group (AG), whose mandate and composition are set out in the Annex to the T2S Guideline; and
 - (f) the National User Groups (NUGs), whose mandate and composition are set out in the Annex to the T2S Guideline.

These T2S Governance Bodies shall draft their respective rules of procedure once they have been established.
7. The [NCB] shall have all necessary rights to exclusively exercise full control in real time over the DCAs in [currency] in T2S, including the right to real-time blocking and unblocking with immediate effect and to close them with immediate effect.

Currency Participation Agreement

8. The [NCB] shall have the right of the real-time initiation of a change being applicable in T2S on the next Settlement Day, except in special circumstances where the MOP provides for specific manual procedures for implementation in real-time as regards:
 - (a) the usage of selected securities in its respective currency for auto-collateralisation,
 - (b) the credits granted for securities settlement in [currency] in T2S,
 - (c) the determination of the individual ISINs which may be used as collateral for individual credits in T2S,
 - (d) the valuation of each ISIN, and
 - (e) the identification of the accounts on which the collateral may be held for credit with the [NCB],in each case if relevant for the [NCB's] collateral procedure.
9. Any amendment to this Agreement or a system change shall be without prejudice to the rights specified in paragraph 8.
10. The refusal of a Change Request by the Connected NCB(s) shall be justified by the need to safeguard central bank functions, i.e. the Connected NCB(s) shall consider the Change Request inappropriate for reasons linked to their responsibilities in terms of safeguarding the integrity of the respective currency or in relation to financial stability.
11. In case of disagreement between the Governing Council and the Connected NCB(s) over the latter's refusal of a Change Request or over any other decision by the T2S Board, the Governors' Forum shall be asked to find an amicable solution for this matter in line with Article 37 and Article 38.
12. If the dispute in the Governors' Forum is based on the refusal of a Change Request by Connected NCB(s) for one of the reasons set out in paragraph 10, the Eurosystem shall have to justify overruling the refusal either (i) with the need to safeguard general Eurosystem central bank functions (safeguarding the euro, financial stability, no distortion of competition) or (ii) with the need to preserve the integrity of the T2S Platform for economic, functional or technical reasons.
13. If no amicable solution can be found, then the concerned Connected NCB(s) shall have the right to exit T2S within 24 months in line with paragraph 4 of Article 38.

Currency Participation Agreement

Article 22

Scope of participation rights

1. The participation rights of the [NCB] during the Development Phase shall include the following:
 - (a) the right to submit Change Requests in accordance with the Change and Release Management procedure as described in Article 23 and **Schedule 9**;
 - (b) the right to be represented and to participate in the Governance as specified in Article 21 and in **Schedule 8**; and
 - (c) the right to obtain information as otherwise provided for in this Agreement.
2. The participation and controlling rights of the [NCB] during the Operational Phase shall include the following:
 - (a) the right to submit Change Requests in accordance with the Change and Release Management procedure set out in Article 23 and **Schedule 9**;
 - (b) the right to receive a report on the technical and operational examinations by the External Examiner in line with the multi-year T2S examination plan and the [NCB's] right to request special examinations by the External Examiner, and to have access to the underlying documentation in accordance with Article 24 [if relevant for a Connected NCB: "and Schedule 13"];
 - (c) the right to receive on request and without delay all information, related to the administration and bookings on the DCAs opened by the [NCB], related to the associated intra-day credit, collateral and accounts where the collateral is held, including but not limited to all relevant manual and system-generated reports, routine descriptions and material allowing for the tracing of errors of administration;
 - (d) the right to be represented and to participate in the Governance as specified in Article 21 and in **Schedule 8**;
 - (e) the right to obtain information as otherwise provided for in this Agreement; and
 - (f) other rights granted by this Agreement.
3. The rights set out in paragraphs 1 and 2 shall be exercised without prejudice to the Multilateral Character of T2S and the principle of central bank independence set out in Article 130 and Article 282(3) of the Treaty on the Functioning of the European Union and Article 7 of the Statute of the ESCB as well as in relevant national legislation.

Article 23

Change and Release Management

1. The Parties may propose Change Requests for the T2S Business Application and the T2S Scope Defining Set of Documents, requirements for T2S Network Service Providers and specifications for the Value-added Connectivity Services. Such proposal shall be made and dealt with in accordance with **Schedule 9**.
2. The Change and Release Management process shall adhere to the following principles:
 - (a) T2S is aimed at accommodating market evolution and supporting innovation;
 - (b) without prejudice to the right of the [NCB] to submit a request for the implementation of Specific Changes, new or changed services within T2S shall be provided with the objective of being available to all Central Banks and Participating CSDs in T2S, and through them to T2S Users;
 - (c) without prejudice to the powers of the Central Banks as specified in **Schedule 8**, no individual Central Bank or Participating CSD shall have a veto right with respect to the approval of a Change Request;
 - (d) T2S shall endeavour to support the [NCB's] compliance with its Legal and Regulatory Requirements, to the extent that the Eurosystem is informed by the [NCB] about such requirements and to the extent that they are compatible with the Multilateral Character of T2S;
 - (e) it is the [NCB's] responsibility to involve its user communities throughout the whole Change and Release Management;
 - (f) the Eurosystem shall continue to be committed to communicating information in a transparent manner towards the market in line with established T2S practices;
 - (g) the development of specific functionalities to accommodate national specificities shall be limited as much as possible. Instead, where applicable, building the necessary interfaces to let the Central Banks and Participating CSDs offer these national specificities on their platforms, with no impact on T2S, shall be favoured;
 - (h) in the case of changes in respect of Legal and Regulatory Requirements which apply only to one or a few Central Banks or Participating CSDs, Specific Changes in accordance with paragraph 3 shall be available; and
 - (i) sufficient time shall be allotted for implementing any change needed by the Eurosystem to develop the T2S Services on a consistent basis and provide enough lead time for the Central Banks and Participating CSDs to change their own internal systems, processes, interfaces and connections accordingly.

Currency Participation Agreement

3. The following principles are applicable to Specific Changes:
 - (a) a Central Bank or a Participating CSD which has a specific need triggered by Legal and Regulatory Requirements or by innovation/improvements has the possibility to propose a new functionality provided that it does not endanger the Lean Scope of T2S and is not incompatible with the Multilateral Character of T2S; and
 - (b) the requesting Central Bank or Participating CSD shall formally commit itself to bear the financial consequences of the Specific Change in accordance with **Schedule 7**; and/or
 - (c) the associated costs shall be shared among all Central Banks and Participating CSDs making use of the functionality in accordance with **Schedule 7**; and
 - (d) the Specific Changes shall be approved in accordance with **Schedule 9**; and
 - (e) no Specific Change may be implemented if this imposes changes to existing features, functionalities, processes or interfaces, or a deterioration of the service level of other Central Banks or Participating CSDs which have not approved such Specific Change, unless such other Central Banks or Participating CSDs agree to it.
4. In accordance with paragraph 2 of Article 33, but subject to paragraph 3 of Article 33, the [NCB] shall waive any IPRs that it may have acquired in connection with the proposed T2S Services or that may have arisen in the context of the Change and Release Management process. If any other legal or natural person directly or indirectly with the Change and Release Management process has acquired IPRs in connection with the proposed changes, the [NCB] shall: (i) inform the Eurosystem as soon as it becomes aware of potential IPRs vested in such a legal or natural person; and (ii) use its best endeavours to ensure that such a legal or natural person also waives any IPRs acquired in the abovementioned context.
5. The full financial consequences related to Common Changes and Specific Changes shall be recovered in accordance with **Schedule 7**.
6. Subject to paragraph 3, as regards a Specific Change requested by the [NCB] related to safeguarding the currency and/or financial stability as part of crisis management measures, the Eurosystem shall make such Change Request only transparent to Connected Central Banks and Participating CSDs on request of the [NCB] until no later than the point in time the change has been formally taken up in a release, provided that the [NCB] has formally committed to bear the financial consequences of the change.
7. In the case of refusal to implement changes triggered by Legal and Regulatory Requirements, the Governing Council shall provide a full written explanation of the reasons for the refusal.
8. Authorised changes and defect resolutions the implementation of which is pending are prioritised based on a scoring mechanism. The definition of the release is based on this priority rat-

Currency Participation Agreement

ing taking into account the business and legal criticality of changes, the associated risks, budgetary implications and the capacity for Common Changes and Specific Changes. The approval of the content of the release and the final prioritisation are carried out as described in **Schedule 8**.

Article 24

External Examiner

1. Without prejudice to the principle of central bank independence in the performance of its public tasks, as established under Article 130 and Article 282(3) of the Treaty on the Functioning of the European Union and in the relevant national legislation, the Eurosystem shall facilitate the [NCB's] and its auditors' (meaning any auditor which has the right to audit the [NCB] pursuant to national legislation or central bank policy) compliance with applicable national legal requirements in relation to the [NCB's] connection to T2S under this Agreement. The Parties agree that without prejudice to the abovementioned principle to the extent legally possible recourse would be made to the External Examiner in line with the following provisions[.], *only relevant for Connected NCB having a Schedule 13 to that effect*: provided that nothing in this article shall be interpreted as diminishing the rights granted to the [NCB's] auditors in **Schedule 13**.]
2. The performance of the T2S Services shall be subject to technical and operational examinations performed by the External Examiner appointed by the Governing Council on the proposal of the CSG and after having consulted the NECSG on this proposal. The [NCB] shall not bear any of the costs of the External Examiner for these regular examinations or the special examinations due to incidents specified in paragraph 5.
3. The External Examiner shall perform its services within the scope set by the Governing Council and in accordance with internationally recognised audit standards including but not limited to the Statement on Standards for Attestation Engagement (SSAE) No 16 or International Standards for Assurance Engagements (ISAE) No 3402 or any replacement of these standards. The External Examiner shall be changed every four years.
4. The Governing Council shall set the External Examiner's mission statement and a multi-year examination plan, taking into account examination items proposed by the NECSG. Without prejudice to paragraph 5, the scope of the regular and any special examinations shall be limited to the provision of T2S Services or directly related aspects. The objective of these examinations is to give to the NECSG reasonable assurance about whether (i) the organisation set by the Eurosystem meets the obligations established in this Agreement and (ii) the controls implemented by the Eurosystem are suitably designed to meet the security objectives.

Currency Participation Agreement

Moreover, the External Examiner shall deliver an opinion on the effectiveness of the controls performed by the Eurosystem on the basis of the results of the compliance check reviews and of the risks assessment and related treatment plans managed by the Eurosystem. A Connected NCB – to the extent feasible, as coordinated through the NECSG – may also propose to the Governing Council special examinations to be conducted by the External Examiner outside the multi-year examination plan.

5. Where a special examination is necessary because of a severe incident or a material and ongoing problem which has disrupted the proper functioning of the T2S Platform or the provision of T2S Services, the External Examiner shall have access to all relevant documentation.
6. Following the submission of the External Examiner's report of its regular examination, the NECSG shall hold with the External Examiner an annual meeting, or in case of a special examination, an extraordinary meeting, to review the submitted report and to discuss the solutions to the identified issues. The report and recommended solutions for the identified issues shall then be submitted to the Governing Council. Within three months of receiving the report, the Governing Council shall reply whether it accepts or rejects each of the recommended solutions. If it accepts a recommendation, the Governing Council shall describe how it intends to implement such recommendation and in what timeframe. The External Examiner shall then monitor the Eurosystem's progress on implementing the accepted recommendations and report back to the NECSG at the annual meeting. If a recommendation is rejected, the Governing Council shall communicate the reasons to the NECSG.
7. Without prejudice to paragraphs 4, the [NCB] shall have the right to: (i) propose to the NECSG items for the regular examinations and for special examinations to be conducted by the External Examiner; (ii) for the avoidance of doubt subject to the confidentiality requirements of Article 34 receive all of the External Examiner's reports and supporting documentation relevant to the [NCB's] use of T2S Services; and (iii) request the External Examiner to provide additional explanations to the NECSG in the course of meetings referred to in paragraph 6 or in written form following such meetings and falling within its remit. The [NCB] and/or its auditors may propose directly to the Governing Council special examinations to be conducted by the External Examiner provided that the [NCB] bear the costs associated with such special examinations.
8. The Governing Council shall communicate to the NECSG, to the [NCB] and/or to its auditors the reasons for refusing to include items for regular or special examination to be conducted by the External Examiner on the proposal of the NECSG, the [NCB] and/or its auditors as provided for in paragraph 7. The NECSG, the [NCB] and/or its auditors may make new proposals to the Governing Council with the understanding that the Connected NCBs and the Eurosystem would use their best efforts to come to a mutually agreeable solution.

Currency Participation Agreement

9. The Eurosystem shall ensure that the External Examiner has the following rights and obligations related to the performance of its examinations:
- (a) the External Examiner shall contact the Eurosystem through the indicated contact persons. The External Examiner shall give the Eurosystem 14 calendar days prior notice before starting the regular or special examination and shall notify to the Eurosystem the following: (i) the object of the examination; (ii) the names of the authorised representatives of the External Examiner who will carry out the examination; (iii) the Eurosystem offices at which the examination is to be conducted; (iv) the methods to be applied; and (v) the timescale;
 - (b) the External Examiner may examine technical and operational documentation and records, whether in written or electronic form, directly relevant for assessing the performance of the T2S Services, setting the T2S pricing policy and implementing budgetary aspects of T2S. Such technical and operational documentation and records shall be made available, on request, to the authorised representatives of the External Examiner during normal business hours at the relevant Eurosystem offices. The External Examiner may, for its own internal use only, make copies and excerpts from the documentation and records made available by the Eurosystem. Such copies and excerpts shall be listed in a transmission protocol and returned to the Eurosystem on completion of the examination or check and on confirmation from the External Examiner that no other unauthorised copies or transcripts exist; and
 - (c) the External Examiner shall ensure that the authorised representatives who carry out the examinations comply with: (i) internal rules of the relevant Eurosystem member, as communicated to such authorised representatives before the commencement of their activity; and (ii) the confidentiality rules set out in Article 34. The authorised representatives of the External Examiner shall not enter areas or offices and shall not use physical or electronic resources of the Eurosystem other than those which are strictly needed for the performance of the examination.
10. The Eurosystem shall maintain documentation and records documenting the performance of this Agreement, for at least 10 years after their creation and, in respect of documents and records that are maintained at the date of the termination of this Agreement, for at least 10 years following termination. Such documentation and records shall include any financial records relating to costs and expenses directly related to the performance of this Agreement, as incurred by the Eurosystem on its own behalf or on behalf of the [NCB]. In the event that the [NCB] notifies the Eurosystem of a legal action requiring the preservation of certain records or a change in the law establishing longer records preservation periods the Eurosystem shall:
- (i) suspend the destruction of documentation or records, as requested by the [NCB]; and (ii)

Currency Participation Agreement

give the [NCB] 60 calendar days prior notice before destroying the documentation or records subject to such suspension, during which notice period the [NCB] may submit a reasoned request for their further maintenance, with the Eurosystem being entitled to the reimbursement of reasonable costs incurred as a result of such further maintenance.

11. Nothing in paragraph 10 shall relieve the [NCB] or the Eurosystem from their statutory or contractual obligations related to the storage of records and documents.

Article 25

Crisis management

1. The Eurosystem shall manage and resolve any operational disturbances in T2S. In addition, due to the central role which T2S plays in securities settlement in connected markets, the Eurosystem shall assume a coordinating role. In particular, it shall coordinate, initiate and lead activities in connection with any event of an operational or financial nature which may impact the functioning and performance of T2S. The Eurosystem shall use its best efforts to protect the functioning of T2S and to operate T2S in a way that supports the financial stability of all connected markets.
2. The principles of crisis management are laid down in **Schedules 5 and 6**, and the procedural aspects of the crisis management framework are set out in the MOP.
3. The details of the assistance to be provided by the Eurosystem in the case of a crisis are specified in **Schedule 6** and are based on the following principles:
 - (a) the Eurosystem shall have adequate organisational and personnel capacities to deal with a crisis;
 - (b) the Eurosystem shall fully cooperate with the Connected NCBs, the Participating CSDs, the Relevant Competent Authorities and ESMA to manage a crisis, including investigating the feasibility of and implementing reasonable workarounds;
 - (c) the Eurosystem shall prepare and maintain a crisis management plan, and shall test its appropriateness on a regular basis together with the Connected NCBs, the Participating CSDs, the Relevant Competent Authorities and ESMA; and
 - (d) the Eurosystem shall provide a report to the Connected NCBs and the Participating CSDs, the Relevant Competent Authorities and ESMA on the effective handling of a crisis within a reasonable period of time after such a crisis has occurred.
4. The details of the assistance to be provided by the [NCB] in the case of a crisis are specified in **Schedule 6** and are based on the following principles:

Currency Participation Agreement

- (a) the [NCB] shall use its best efforts to fully cooperate with the Eurosystem in order to manage a crisis;
 - (b) the [NCB] shall use its best efforts to inform the Eurosystem about any potential market disturbances that may have an impact on T2S without delay;
 - (c) the [NCB] shall use its best efforts to ensure that its own crisis management plans cover T2S crisis scenarios;
 - (d) the [NCB] shall without undue delay inform and involve its Dedicated Cash Account Holders about any T2S crisis that could impact them; and
 - (e) the [NCB] shall use its best efforts to assist in the preparation and maintenance of a crisis management plan by the Eurosystem.
5. If the [NCB] deems that financial stability of its country or the safeguarding of its currency is threatened, the [NCB] may unilaterally and to the extent possible after informing the Eurosystem reasonably in advance of any such event, invoke its own crisis management plan, which may include the settlement of transactions in [currency] outside T2S, if necessary for reasons of financial stability or the safeguarding of its currency and to the extent the invocation of crisis management measures does not have a negative impact on the settlement of transactions in other currencies in T2S. In such circumstances, the Eurosystem shall, in line with the Decision ECB/2011/20 grant to the Participating CSD(s) designated by the [NCB] a derogation from the eligibility criterion set out in Article 15(1)(e) of the T2S Guideline in relation to such transactions settled outside of T2S to preserve financial stability and to safeguard its currency. The Eurosystem shall use its best efforts to support the [NCB] in moving to crisis management measures and in returning to normal activities in T2S. Without prejudice to the Eurosystem's own crisis management responsibilities, the Eurosystem shall not take action to hinder the efficient crisis management of the [NCB].
6. The Eurosystem shall, to the extent possible, endeavour to: (i) provide reasonable notice prior to the suspension of the provision of T2S Services to a Participating CSD or a Directly Connected Party and (ii) involve the [NCB] in the crisis management in relation to the Participating CSD or a Directly Connected Party as specified in **Schedule 6** and the MOP.

Article 26

Amendments

1. Any amendment of, or supplement to, this Agreement shall be executed in writing and agreed by the Parties unless provided otherwise in this Article. Subject to paragraphs 4 to 6 of this

Currency Participation Agreement

Article, the Parties need to agree on an amendment and neither Party shall unreasonably withhold its agreement to such amendment.

2. Each Party shall inform the other Party of any amendment it proposes to this Agreement as soon as practicable.
3. The Eurosystem may on 30 days' prior notice unilaterally amend this Agreement in respect of non-material amendments of technical or operational nature, such as, changes in contact details of either Party, unless the [NCB], within 30 days following receipt of the notice of any such proposed amendment and subject to confirmation of delivery of the notice by the [NCB], notifies the Eurosystem that it does not agree that the changes are minor.
4. Any amendment to this Agreement required due to a system change pursuant to Article 23 and **Schedule 9** shall be incorporated in this Agreement as soon as practicable. The scope of system changes is further defined in **Schedule 9**.
5. The Eurosystem may amend the Annexes to **Schedule 2** pursuant to the process detailed therein, Furthermore, the Eurosystem may amend **Schedule 7** with prior notice of 180 calendar days to the [NCB], in accordance with the T2S pricing policy decided by the Governing Council and published on the T2S website or if the actual use of T2S Services that have an initial zero price is not within an expected consumption pattern.
6. Without prejudice to either Party's rights and prerogatives, the Parties agree to negotiate in good faith to amend this Agreement to the extent required, in the event that:
 - (a) any of the legal acts or instruments forming an element of the Overall Legal Framework for T2S or for the participation of the [NCB] in T2S, including for the avoidance of doubt such legal acts or instruments that apply in the jurisdiction of the [NCB], is amended and in the event any such amendment has a material effect on this Agreement, in the reasonable opinion of the Eurosystem or the [NCB]; or
 - (b) an objection is received by the Eurosystem in accordance with paragraph 3; or
 - (c) an envisaged amendment to Parallel CPAs, which does not fall under the scope of Article 23 and **Schedule 9**, also necessitates an amendment to this Agreement due to the uniform character of the CPAs and/or the Multilateral Character of T2S; or
 - (d) an envisaged amendment to one or more Framework Agreements with Participating CSDs, which does not fall under the scope of Article 23 and **Schedule 9**, also necessitates an amendment to this Agreement due to the Multilateral Character of T2S.

CHAPTER 4

LIABILITY REGIME, COSTS AND NETWORK SERVICE PROVIDER

Article 27

Standard of liability

1. Except as otherwise provided in this Agreement, the Parties shall be bound by a general duty of reasonable care in relation to each other in performing their respective duties and obligations under this Agreement.
2. Each Party shall be obliged to perform only the duties and obligations specifically attributed to it in this Agreement and shall be liable only in respect of those duties and obligations as provided for in this Agreement.
3. Each Party shall take all reasonable and practical actions or measures to mitigate any loss, damage or adverse consequence that it may cause to the other Party or that it may suffer by reason of the acts or omissions of the other Party.

Article 28

Liability rules

1. Each Party shall be liable to the other Party without limitation for any loss or damage resulting from fraud or wilful misconduct in performing its duties and obligations under this Agreement.
2. Subject to paragraphs 4 and 6, each Party shall be liable to the other Party for any Direct Loss incurred resulting from its gross or ordinary negligence in performing its duties and obligations under this Agreement. Without prejudice to paragraph 3, liability for indirect loss and damages not qualifying as Direct Loss is excluded to the extent permitted by German law.
3. The Eurosystem shall also be liable to the [NCB] for a claim of the [NCB's] DCA Holder against the [NCB] in connection with T2S Services (hereinafter a 'Customer Claim'), resulting from the Eurosystem's gross or ordinary negligence in performing its duties and obligations under this Agreement, if and to the extent that all of the following criteria are satisfied: (a) the [NCB] is held legally liable for the Customer Claim pursuant to an Enforceable Judgement, or has, with the approval of the Eurosystem (such approval shall not be unreasonably withheld or delayed), settled the Customer Claim; (b) the loss or damage of a DCA Holder is the direct result of an act or omission of the Eurosystem; and (c) the Customer Claim would have been settled by the [NCB] in favour of a DCA Holder according to local market practice. For the avoidance of doubt, the liability under this paragraph shall include

Currency Participation Agreement

claims for loss of interest. If there is a difference between the Customer Claim for which the [NCB] is held liable pursuant to an Enforceable Judgement and the amount due according to local market practice, the Parties shall use their best efforts to settle the issue in an amicable way. The [NCB] shall reimburse to the Eurosystem a Customer Claim (i) for which the condition(s) outlined above are not fulfilled or are reversed or (ii) which is paid twice on the basis of this Agreement as well as on another basis, such as an insurance policy or through a claim paid by a Central Bank based on the same facts and circumstances. For the avoidance of doubt, no Customer Claim shall be paid directly to the NCB's DCA Holders.

4. Each Party shall be liable to the other Party in proportion of the contribution of its fraud, wilful misconduct, gross or ordinary negligence in the loss or damage of the other Party.
5. Without prejudice to paragraph 1, the Eurosystem's liability according to this Article shall be limited or excluded as follows:
 - (a) a maximum total amount per calendar year for all losses and damages suffered by the [NCB] and all Connected NCBs that were caused by events that occurred in the same calendar year;
 - (i) for the Eurosystem's ordinary negligence, the liability of the Eurosystem vis-à-vis, combined, the [NCB] and all Connected NCBs shall be limited to a maximum total amount of EUR 20 000 000 for the relevant calendar year.
 - (ii) for the Eurosystem's gross negligence, the liability of the Eurosystem vis-à-vis, combined, the [NCB] and all Connected NCBs shall be limited to a maximum total amount of EUR 100 000 000 for the relevant calendar year.

If the aggregate amount of losses or damages suffered by the [NCB] and all Connected NCBs in any calendar year exceeds the maximum set out in this subparagraph, then the amount due to the [NCB] shall be calculated and paid by the Eurosystem pro rata, i.e. having regard to the total amount of all losses or damages suffered by the [NCB] and all Connected NCBs;

 - (b) the Eurosystem shall not be liable for losses or damages suffered by the [NCB] related to the early termination of any Parallel CPA or any Framework Agreement by any relevant party; and
 - (c) a Party shall not be liable for any delay in meeting a relevant synchronisation point as specified in **Schedule 2**.
6. Without prejudice to paragraph 1, the [NCB's] liability vis-à-vis the Eurosystem in accordance with this Article shall be limited, in the following way:

Currency Participation Agreement

- (i) for the [NCB's] ordinary negligence, the liability of the [NCB] shall be limited to EUR 2 000 000 per calendar year; and
 - (ii) for the [NCB's] gross negligence, the liability of the [NCB] shall be limited to EUR 10 000 000 per calendar year.
7. The procedures for the exercise, allocation and payment of liability claims are set out in **Schedule 12**.
8. For the avoidance of doubt, the circumstances specified in paragraphs 1 and 2 of Article 30 shall apply as grounds for exclusion of the liability under this Article.
9. As part of the Eurosystem's tasks in accordance with Articles 17, 18 and 22 of the Statute of the ESCB, T2S has the nature of a public service. All obligations of the Eurosystem arising under this Agreement may only be performed jointly by all members of the Eurosystem and qualify as joint liability. All rights and claims of the [NCB] under this Agreement are therefore always rights and/or claims that may be exercised only against all members of the Eurosystem jointly.

Article 29

Indemnification obligations of the [NCB] for acts of Third Parties

1. The [NCB] shall indemnify and hold harmless the Eurosystem from any direct loss incurred as a result of the acts and omissions of one of the [NCB's] DCA Holders in relation to T2S to the extent that such loss is not caused by (i) the Eurosystem's negligence; or (ii) any malfunction or failure in the technical infrastructure of the T2S Business Application to the extent the Eurosystem has not adopted those measures that are reasonably necessary to protect the infrastructure against such malfunction or failure, and in proportion to the Eurosystem's contribution to such loss or damage. The circumstances specified in paragraphs 1 and 2 of Article 30 shall apply as grounds for exclusion of the liability under this Article. In case the Eurosystem and the [NCB] do not agree on the extent and/or proportion of the Eurosystem's contribution to the Eurosystem's loss under sub-paragraphs (i) and (ii), the Dispute Resolution and Escalation Procedure pursuant to Article 37 shall be initiated in order to settle the issue in an amicable way. Any net reimbursement to be paid by the [NCB] to the Eurosystem under this paragraph shall only be due once the dispute has been settled and shall be limited to EUR 10 000 000 per calendar year for all events that occurred in that calendar year. If a dispute under this paragraph cannot be settled pursuant to Article 37, a Party may initiate the court proceedings set out in

Currency Participation Agreement

Article 47. The procedures for the exercise and payment of claims of the Eurosystem against the [NCB] under this paragraph are set out in **Schedule 12**.

2. The obligations of the [NCB] pursuant to paragraph 1 shall not be construed as a limitation of any claim for loss or damage the [NCB] may have against the Eurosystem under this Agreement, in particular pursuant to Article 28.
3. To the extent legally feasible under the law applicable to the [NCB], the [NCB] shall procure that its legal and contractual arrangements with a Third Party contain provisions that (i) prevent such Third Parties from asserting a claim directly or indirectly against the Eurosystem in relation to the T2S Services used by the [NCB] and/or (ii) do not provide for a liability regime to such Third Parties which is more favourable than the liability regime applying between the Eurosystem and the NCB under this Agreement.

Article 30

Force Majeure and acts by Third Parties

1. Each Party shall under no circumstances be obliged to perform or have any liability for its failure to perform any of its duties and obligations under this Agreement to the extent that such failure results from any act, fault, or omission of the other Party or a Third Party for which it is not responsible, or a Force Majeure event.
2. Without prejudice to Article 32, the Eurosystem shall not be responsible for the acts and omissions of communication, network and connectivity service providers, and in particular not for the performance of the Connectivity Services or any performance failures of a T2S Network Service Provider.
3. Each Party shall give notice to the other Party without undue delay upon becoming aware of any actual or imminent failure referred to in paragraph 1, and use its reasonable efforts to resolve such failure as soon as is reasonably possible.

Article 31

Costs and Pricing

1. Without prejudice to the Change and Release Management procedure and unless otherwise provided in this Agreement, neither Party shall bear any of the costs related to the development of T2S or the rights and obligations under this Agreement which the other Party incurs during the Development Phase and/or the Operational Phase, and the [NCB] shall not bear any of the costs related to the development of T2S or the rights and obligations under this

Currency Participation Agreement

Agreement which the Eurosystem incurs during the Development Phase and/or the Operational Phase.

2. The [NCB] acknowledges that **Schedule 7** shall, to the extent relevant for this Agreement, apply to all T2S Services, including the services provided by the [NCB] to its Dedicated Cash Account Holders in [currency].

Article 32

T2S Network Service Provider

1. The Eurosystem shall allow the [NCB] to connect its IT systems to the T2S Platform, either via a Value-Added Connection or via a Dedicated Link Connection.
2. The [NCB] shall inform the Eurosystem about the solution it has chosen for its connection to T2S at least six months prior to the intended start date of its testing activities.
3. The [NCB] shall use reasonable efforts to ensure that its connectivity with the T2S Platform functions properly at all times. The [NCB] shall provide in its rules or contractual terms for an obligation to be imposed on its Dedicated Cash Account Holders to use reasonable efforts to ensure that their connectivity with the T2S Platform functions properly at all times.
4. The [NCB] shall inform the Eurosystem of its intention to change its T2S Network Service Provider(s) as soon as reasonably possible.
5. As far as the Value-Added Connections are concerned, the following provisions shall apply:
 - (a) The Eurosystem shall communicate to the [NCB] during the Development Phase in accordance with **Schedule 2** which T2S Network Service Provider(s) that it has selected for the provision of Connectivity Services to the [NCB]. The requirements according to which the T2S Network Service Provider(s) have been selected, and which they need to comply with are specified in attachments 1 (technical requirements) and 2 (business requirements) to the Licence Agreement, available on the Banca d'Italia's website. Changes to these requirements shall be managed in accordance with **Schedule 9** and the Licence Agreement.
 - (b) The Eurosystem shall exercise due care in coordinating the Connected NCBs' monitoring of the compliance of the T2S Network Service Provider(s) with those requirements pursuant to sub-paragraph [a] which the [NCB] can monitor itself. The Eurosystem shall exercise due care in the monitoring of the compliance of the T2S Network Service Provider(s) with those requirements pursuant to sub-paragraph [a] which the [NCB] cannot monitor itself. The Eurosystem shall address material breaches of such requirements in accordance with the relevant contractual provisions with the T2S Network Service Pro-

Currency Participation Agreement

viders. If the [NCB] connects to the T2S Platform via a T2S Network Service Provider in respect of which the Eurosystem has identified a material breach or a potential material breach of the requirements, the Eurosystem shall inform the [NCB] about the (potential) material breach it has identified, as well as about the steps it has undertaken to remedy (or avoid) such a (potential) material breach. Should the material breach by the T2S Network Service Provider(s) not be remedied within a reasonable timeframe, the Eurosystem shall take the appropriate measures towards the T2S Network Service Provider(s), subject to the Eurosystem's arrangements with the T2S Network Service Provider(s), and provide support to the [NCB].

- (c) The [NCB] shall carry out its own due assessment as regards the ability of the selected T2S Network Service Provider(s) to offer a Value-Added Connection to the [NCB] and as regards the reliability of these T2S Network Service Provider(s) (financially, operationally, technically or otherwise) towards the [NCB]. The [NCB] may not rely solely on the results of the selection process undertaken by the Eurosystem regarding the selection of the T2S Network Service Provider(s).
- (d) The Eurosystem shall not be responsible for any cost or loss that the [NCB] may incur as a result of a need to transition to a different T2S Network Service Provider, if the T2S Network Service Provider with which the [NCB] has contracted the Connectivity Services loses, for whatever reason, its status as a T2S Network Service Provider.
- (e) For the avoidance of doubt and notwithstanding paragraph 1 of Article 30, the [NCB] shall not be responsible to the Eurosystem for the acts and omissions of its Network Service Provider(s). The [NCB] shall inform the Eurosystem and the other Connected NCBs about any concerns it may have regarding the, financial, operational or technical reliability of the T2S Network Service Provider(s) as well as any performance issues regarding the delivery of the Value-Added Connection provided by its T2S Network Service Provider(s). The Eurosystem shall assess whether or not the information provided by the [NCB] could reasonably indicate non-compliance by the T2S Network Service Provider(s) with the requirements referred to in sub-paragraph a. If the Eurosystem, acting reasonably, decides that the T2S Network Service Provider does not comply with the relevant requirements, the Eurosystem shall forthwith take appropriate steps against the T2S Network Service Provider, subject to the Eurosystem's arrangements with the T2S Network Service Provider. At all times, the Eurosystem shall keep the [NCB] informed of the steps it takes and discuss the proposed actions with the [NCB] in advance.
- (f) The Parties shall monitor the risk situation of the T2S Network Service Provider(s) within their respective contractual relationships with their T2S Network Service Provider(s) and discuss them as appropriate within the Information Security framework.

Currency Participation Agreement

- (g) The Parties shall analyse the impact on the T2S Programme Plan in accordance with **Schedule 2**, whenever the Eurosystem starts a new selection process of a T2S Network Service Provider.
 - (h) The provision of Connectivity Services is outside of the scope of the T2S Services and the Eurosystem is not responsible to the [NCB] for the acts and omissions of the T2S Network Service Provider(s).
6. The Eurosystem shall communicate to the [NCB] in accordance with **Schedule 2** the entity that will offer the necessary Physical Connectivity Services for the Dedicated Link Connection, as well as the necessary specifications for the Value-added Connectivity Services, which the [NCB] has to implement, in order to establish a Dedicated Link Connection with the T2S Platform. The rights and obligations of the Parties related to the Dedicated Link Connection will be specified outside this Agreement.

CHAPTER 5 INTELLECTUAL PROPERTY RIGHTS, CONFIDENTIALITY AND DATA PROTECTION

Article 33 Intellectual Property Rights

1. Each Party and, where applicable, its licensors, shall retain all rights and titles in their Background IPRs. In particular, the Eurosystem shall not acquire any right, title or interest in or to the IPRs of the [NCB] or its licensors (including but not limited to software, data, documentation, processes and procedures of the [NCB]), save to the extent required for the performance of this Agreement.
2. The Parties agree that no IPRs developed or created before or during the course of this Agreement by or for the benefit of the Eurosystem or its subcontractors shall be transferred, licensed or otherwise conveyed to the [NCB], save as expressly set out in this Agreement. This includes without limitation (i) all IPRs developed or created in connection with the development of T2S or the establishing or provision of T2S Services (ii) changes to T2S or to the T2S Scope Defining Set of Documents implemented pursuant to Article 23 and **Schedule 9**, and (iii) the T2S Documentation and any other documents created or used for the development and operations of T2S.

Currency Participation Agreement

3. Notwithstanding paragraph 2 above, the Parties may use general project know-how acquired in connection with T2S, in particular in connection with **Schedule 9**, including after the termination of this Agreement.
4. The Eurosystem shall provide the T2S Services in a manner which shall ensure that no IPR of any Third Party is infringed through the use of T2S Services by the [NCB] in line with this Agreement. If legal action is commenced or threatened against the [NCB] based on an alleged infringement of the IPR of any Third Party through the use of the T2S Services by the [NCB], the [NCB] shall (a) notify the Eurosystem in accordance with Article 44 as soon as reasonably practicable, (b) allow the Eurosystem, at its expense, control of the defence of the claim (without prejudice to the [NCB's] right to take an active role in the proceedings at its own expense); (c) not make admissions, agree to any settlement or otherwise compromise the defence of the claim without the prior written consent of the Eurosystem, such consent not being unreasonably withheld; and (d) give, at the Eurosystem's request, reasonable assistance in connection with the conduct of the defence. If the [NCB] is held liable for the infringement of the Third Party's IPR according to an Enforceable Judgement or has, with the prior written consent of the Eurosystem, settled the claim, the Eurosystem shall reimburse the [NCB] in accordance with **Schedule 12** for all payments that the [NCB] has to make to the relevant Third Party. The consent referred to in the previous sentence shall not be unreasonably withheld. This reimbursement obligation shall not apply with regard to any Third Party claim asserted before a court outside (i) the Union or (ii) the home country of any Connected NCB. In this case, the liability rules pursuant to Article 28 shall apply
5. The Eurosystem grants to the [NCB] a non-exclusive and non-transferable licence to copy the T2S Documentation and any other document made available to the [NCB] for any purpose connected to the use of the T2S Services or other purpose that is incidental to the rights granted to the [NCB] under this Agreement.
6. The T2S Trademarks and Logos remain the sole property of the Eurosystem. The Eurosystem grants to the [NCB] the non-exclusive, non-transferable right to use the T2S Trademarks and Logos in the territories, in which they are protected, for the T2S Services in conformity with applicable law.
7. The [NCB's] trade marks and logos remain its (or its Affiliates') sole property. The [NCB] grants to the Eurosystem the non-exclusive, non-transferable right to use the [NCB's] trade-marks and logos in the territories, in which they are protected, for the T2S Services in conformity with applicable law.

Currency Participation Agreement

Article 34 Confidentiality

1. The Parties acknowledge and agree that they have received and will receive Confidential Information in connection with this Agreement.
2. The Parties agree that all Confidential Information shall be used only for the purpose of exercising rights or complying with obligations under this Agreement and the receiving Party shall ensure that only such personnel to whom disclosure of the Confidential Information is required for the purpose of exercising any rights or the performance of the receiving Party's obligations under this Agreement shall have access to the Confidential Information and only to the extent necessary to exercise these rights or perform these obligations.
3. Without prejudice to paragraph 2 and Article 35, to the extent that Confidential Information disclosed by the [NCB] consists of statistical or personal data, such data may only be disclosed by the Eurosystem with the [NCB's] consent. The [NCB] shall cooperate in developing efficient procedures for obtaining this consent both for single and regular use of this data.
4. The receiving Party of each item of Confidential Information shall use all reasonable efforts, taking into account the materiality and proprietary nature of the particular Confidential Information, to protect such Confidential Information from unauthorised use or intentional, inadvertent or otherwise disclosure and, in any event, shall exercise at least the same reasonable level of care to avoid any such unauthorised use or disclosure as it uses to protect its Confidential Information.
5. Notwithstanding the foregoing, a Party may disclose Confidential Information to third parties with the prior written consent of the other Party, and each Party shall be free to disclose Confidential Information without the consent of the other Party:
 - (a) as required by a court of competent jurisdiction or a Relevant Competent Authority or an administrative body of a competent jurisdiction, or otherwise required by applicable laws, but only to the extent legally required; or
 - (b) in any potential or actual litigation among the Parties arising in connection with the T2S Programme, to the extent required to establish, exercise or defend a legal claim; or
 - (c) to their directors, officers, personnel, attorneys, consultants, auditors, subcontractors, insurers and agents on a strict need-to-know basis in connection with their duties, as long as such persons are advised of the confidential nature of such information and their obligation to protect it as confidential and are bound by confidentiality undertakings consistent with those contained in this Agreement, or pursuant to national legislation,

Currency Participation Agreement

provided that, with respect to paragraph (a) above, the Party shall, subject to applicable laws, inform the other Party reasonably in advance in order to enable it to take precautionary actions.

If this Agreement is terminated or expires for any reason, the receiving Party of each item of Confidential Information, including but not limited to documents, contracts, records or properties, shall return it to the disclosing Party and/or, at the disclosing Party's discretion, destroy it and provide a corresponding certificate to the disclosing Party, except to the extent that retention of any Confidential Information is required by applicable laws or expressly permitted under this Agreement. A receiving Party may keep one copy of the Confidential Information for backup, audit and compliance purposes, subject to the obligation to keep this copy confidential and not use the information for any other purpose. The same shall apply where the [NCB] withdraws or is excluded from this Agreement as between the [NCB] and the Eurosystem. This confidentiality obligation shall remain in force following the termination or expiration of this Agreement.

6. Nothing in this Article limits the ability of the Parties to provide the text of this Agreement to the relevant Union institutions and bodies, and national authorities, including the Relevant Competent Authorities, for purposes related to receiving regulatory assessments or approvals necessary for provision and use of the T2S Services or establishing the tax status of the T2S Services, in line with the division of responsibilities in this respect.
7. The Parties acknowledge and agree that this Agreement may be published (including publication on the T2S website) once the Governing Council has approved it and decided to offer this Agreement to Eligible NCBs.

Article 35

Data protection

1. Each Party shall comply with the data protection laws applicable to it and in particular [for EEA NCBs: the relevant transposition of Directive 95/46/EC] [OR] [for non-EEA NCBs: legislation applicable to the [NCB] which is at least equivalent to Directive 95/46/EC] or, as applicable, Regulation (EC) No 45/2001.
2. The Eurosystem shall use personal data solely for the purpose of providing and using the T2S Services. Within these limits, the Eurosystem may transfer personal data to Third Parties including T2S Network Service Providers. Where the Eurosystem receives personal data from the [NCB] under this Agreement, and where the Eurosystem (and/or any of its subcontractors and/or Third Parties used to provide the T2S Services) transfers such personal data to a country outside the European Union which does not provide an adequate level of protection, as the

Currency Participation Agreement

level of protection in the European Union, the Parties shall agree on the terms and conditions for the data transfer which shall be based on the standard contractual clauses for the transfer of personal data to processors established in third countries as approved by Decision 2010/87/EU.

3. The [NCB] shall acquaint itself with the respective T2S Network Service Provider's data retrieval policy prior to entering into a contractual relationship with such T2S Network Service Provider. The [NCB] shall, to the extent required under applicable law, have obtained or shall obtain all necessary authorisations and approvals from or shall make the necessary notifications to the relevant regulatory or administrative authorities as well as other interested parties required for the Eurosystem to use and store data as contemplated under this Agreement.

CHAPTER 6 MISCELLANEOUS

Article 36 Governing law

This Agreement shall be governed by the laws of Germany with the exception of its conflict of laws principles.

Article 37 Dispute Resolution and Escalation Procedure

1. The Parties shall attempt to resolve disputes between them arising out of or relating to this Agreement in a constructive manner that reflects the concerns and legitimate interests of each Party at the appropriate levels of authority within each Party prior to the initiation of judicial proceedings. In particular, the Parties shall aim to settle a dispute already at the appropriate level and within the appropriate framework with the objective of avoiding the need to invoke this Dispute Resolution and Escalation Procedure.
2. Either Party may initiate the Dispute Resolution and Escalation Procedure by giving written notice to the other Party as specified below, except where a specific dispute resolution procedure is specified in the relevant documentation. It is the expectation of the Parties that each step as follows is completed within a reasonable timeframe:

Currency Participation Agreement

- (a) Step 1: if the parties to the dispute cannot find a mutually agreeable solution to a dispute at working level, a party to the dispute may escalate the issue to the NECSG and the T2S Board;
 - (b) Step 2: the NECSG and the T2S Board shall discuss the issue within the respective body. If the dispute has not been resolved and if the initiator belongs to the NECSG, the NECSG may propose to the T2S Board that the dispute is escalated to Step 3(a) or 3(b), or if the initiator belongs to the T2S Board, the T2S Board may propose that the dispute is escalated to Step 3(a) or 3(b);
 - (c) Step 3(a): the NECSG shall meet with the chairperson of the T2S Board. In considering the issue, the NECSG may request the advice of the CSG and/or the AG. If the NECSG and the chairperson of the T2S Board come to a mutually agreeable solution, the proposed solution must be submitted to the T2S Board for endorsement. Where the NECSG and the chairperson of the T2S Board have not found a mutually agreeable solution, the issue may be escalated to Step 3(b);

Step 3(b): the T2S Board shall meet with the NECSG member of the Connected NCB(s) in dispute with the Eurosystem or, if deemed appropriate considering the subject-matter of the dispute, with all NECSG members. Following agreement of the parties, one or more expert panels may be established on an ad hoc basis which shall provide advice on technical issues relevant to a dispute. In addition, the T2S Board may seek advice from the CSG and/or the AG. If a mutually agreeable solution cannot be found, the issue may be escalated to the Governors' Forum by any Party without delay;
 - (d) Step 4: if a dispute is escalated to the Governors' Forum, it may seek advice of the CSG and/or the AG. Following agreement of the Governors' Forum, one or more expert panels may be established on an ad hoc basis which shall provide advice especially on technical issues relevant to a dispute in order to assist in finding a solution to the dispute. If the Governors' Forum agrees on a solution, the proposed solution must be submitted to the Governing Council and the governing bodies of the respective Connected NCBs for endorsement;
 - (e) Step 5: where despite the Eurosystem's commitment to settle disputes in an amicable way and to facilitate that all Connected NCBs can fulfil their statutory, legal and regulatory responsibilities within the Lean Scope of T2S in a technically viable way, there is an insurmountable obstacle to a consensual solution, the Governing Council and the relevant Connected NCB may terminate the CPA in accordance with the relevant provisions of Article 39.
3. At each stage of the escalation process and without prejudice to the mandate of the Governors' Forum, adequate consideration shall be given to related matters that are the subject of

Currency Participation Agreement

similar escalation procedures between the Eurosystem and a Participating CSD in relation to T2S.

4. The details of the NECSG's mandate are specified in Annex 1 to **Schedule 8**.

Article 38

Governors' Forum

1. The Governors' Forum is mandated to discuss in exceptional circumstances T2S matters relevant to Connected NCBs that could not be resolved through the Dispute Resolution and Escalation Procedure with the objective that the Governors' Forum shall aim at discussing and settling such disputes by agreeing on a common resolution by way of consensus. Any such resolution of the Governors' Forum shall be submitted to the Governing Council for endorsement after the governing bodies of the Connected NCBs concerned have endorsed any such resolution. The details of its mandate are specified in Annex 2 to **Schedule 8**.
2. The Governors' Forum shall be composed of the governors of the Connected NCBs and an equal number of members of the Governing Council.
3. The President of the ECB shall call for a meeting of the Governors' Forum if:
 - (a) one or more members of the NECSG consider that a decision of the T2S Board negatively affects the concerned Connected NCBs ability to safeguard the integrity of the respective currencies, (which includes the implementation of monetary policy including all credit operations as well as the settlement in Central Bank Money in the respective currencies) or financial stability; or
 - (b) one or more governors of the respective Connected NCB(s) wish to discuss any matter in relation to T2S; or
 - (c) the Governing Council wishes to consult the Governor's Forum before taking a decision in relation to T2S or to discuss any matter in relation to T2S.
4. The Eurosystem may reject a Connected NCB's refusal of a Change Request for the following reasons:
 - (a) the need to safeguard the general Eurosystem central bank functions of safeguarding the integrity of the euro or of financial stability or of preventing the distortion of competition between private market participants; or
 - (b) the need to preserve the integrity of T2S for economic, functional or technical reasons.

If the issue has been escalated to the Governors' Forum, where no agreement on an amicable solution of the issue can be found or such a solution is not endorsed by the Governing Coun-

Currency Participation Agreement

cil or the governing body of the Connected NCB concerned, the Connected NCB concerned may terminate this Agreement and may require that it exits within a maximum period of 24 months from the date of the Governing Council's decision to implement the change. The Connected NCB concerned shall endeavour to exit from T2S as soon as reasonably possible already before the expiry of that period. During the exit period and to the extent relevant for the operation of T2S, the Connected NCB shall not be affected by the Change it rejected.

Article 39

Duration, suspension and termination

1. This Agreement shall become effective on the Agreement Date and shall, subject to Article 23 and, Article 26 as well as this Article, continue in full force and effect for an indefinite period of time, unless in the event that T2S as a whole is terminated by the Eurosystem, in which case the Agreement shall be terminated with a minimum notice period of 365 days.
2. The provisions of this Agreement shall not have any retroactive effect except for Article 4, Article 33 and Article 34, which shall apply retroactively.
3. The [NCB] may unilaterally terminate this Agreement with six months' prior notice thereof, unless otherwise agreed in this Agreement or between the Eurosystem and the [NCB]. Without prejudice to paragraph [11] **OR** [10], the [NCB] shall coordinate all exit activities with its Dedicated Cash Account Holders, so that all necessary arrangements are made when the [NCB] will have exited T2S.
4. Each Party may terminate this Agreement:
 - (a) if the other Party is in material breach of any provisions of this Agreement and such breach has not been remedied within 90 calendar days of a written warning notice of such breach with immediate effect; or
 - (b) if the right of termination for cause (*Kündigung aus wichtigem Grund*), which is not covered by sub-paragraph (a), is provided for under mandatory rules of German statutory law with a notice period of 365 days, except where another notice period is provided by applicable law.
5. If due to a major technical threat to the security or integrity of T2S stemming from the [NCB's] technical connection to or use of T2S, the [NCB] remains unable to perform its obligations, and such a threat cannot be resolved by a temporary disconnection of the [NCB] or any of its Dedicated Cash Account Holders in accordance with **Schedule 6**, the Eurosystem may suspend its obligations under this Agreement immediately. The Eurosystem shall also, to the extent possible, give reasonable prior notice to the [NCB] of the planned suspension, and,

Currency Participation Agreement

to the extent possible, consult the [NCB] prior to the planned suspension or provide all relevant information related to the suspension to the [NCB] after the [NCB] has been suspended. A suspension shall be terminated as soon as the reason for suspension has ended.

6. If, due to a Force Majeure event, one of the Parties remains unable to perform its obligations, the other Party may suspend the obligations of this Agreement immediately or, to the extent possible, with reasonable prior notice. Neither Party shall have any liability to the other as a result of such suspension, but any such suspension shall be without prejudice to any rights which may have arisen prior to suspension. A suspension shall be terminated as soon as the reason for suspension has ended.
7. [For non-EEA NCB relevant only: The Eurosystem may terminate this Agreement with reasonable prior notice to the [NCB], where the eligibility conditions for the [currency] pursuant to paragraph (1)(a) of Article 5 are not met and such default is not remedied within a reasonable period of time.]
8. If the [NCB] considers that its rights and obligations under this Agreement would be materially and adversely affected by a change pursuant to Article 23, or such a change would be in conflict with Legal and Regulatory Requirements, and any such change cannot be implemented as a Specific Change, it may with at least 90 calendar days prior notice to the Eurosystem unilaterally terminate this Agreement.
9. Without prejudice to either Party's rights and prerogatives and prior to giving notice to the respective other Party, any request to terminate this Agreement shall be subject to the prior Dispute Resolution and Escalation Procedure with a view to attempting in good faith to reach a resolution to the need for such termination, except if the Parties agree that the Dispute Resolution and Escalation Procedure is unlikely to result in an amicable resolution of the issue or if the [NCB] has renounced its right to resort to the Dispute Resolution and Escalation Procedure.
10. All notices under this Article shall be subject to confirmation of delivery of the notice by the Party receiving the notice.
11. The details of the cooperation and assistance to be provided by the Eurosystem in case of termination are specified in **Schedule 11** and are based on the following principles:
 - (a) the [NCB] shall be responsible for the set up and execution of the exit plan;
 - (b) without prejudice to paragraph 4 of Article 38, if the [NCB] terminates this Agreement pursuant to paragraph 2, until its exit it shall maintain its internal systems sufficiently compatible with the T2S functionality and with agreed Service Levels until its exit, so as to allow T2S to provide the agreed services to other T2S Actors, which may imply that the [NCB] is required to implement authorised changes, in particular in case of Fast-track

Currency Participation Agreement

Changes, as specified in **Schedule 9**. Irrespective of the cause of termination, the [NCB] shall continue to participate in the Change and Release Management procedures until its exit;

(c) irrespective of the cause of termination and subject to paragraph 4 of Article 38, the Eurosystem shall continue to provide T2S Services to the [NCB] for a period of up to 24 months, following the date of the notice of termination on request of the [NCB];

(d) irrespective of the cause of termination, the Eurosystem shall provide the required assistance, as reasonably necessary, to the [NCB] and, except in case of termination for cause by the [NCB], the [NCB] shall reimburse the costs for planning, coordination and execution of exit activities beyond the normal operational support to the Eurosystem; and

(e) the Eurosystem shall maintain at the disposal of the [NCB] the relevant documents, data and archives related to T2S Services provided to the [NCB].

12. To the extent required, the Eurosystem and the [NCB] shall continue to cooperate in good faith on any remaining issues deriving from the [NCB's] participation in T2S

13. [Only for Non-euro Area NCBs of the EU: This Agreement shall expire on the date that the Member State of the Union of the [NCB] adopts the euro.]

Article 40

Own fees and costs

Each Party shall bear its own costs and expenses connected with the preparation, execution, operation and termination of this Agreement, including the costs of its legal and other advisors, without prejudice to other provisions of this Agreement.

Article 41

Entire agreement

Without prejudice to Article 2, this Agreement and the Schedules represent the complete agreement regarding the subject-matter hereof and replace any prior oral or written communications between the Eurosystem and the [NCB].

Currency Participation Agreement

Article 42

No waiver

1. The exercise or waiver, in whole or in part, of any right, remedy, or duty provided for in this Agreement shall not constitute the waiver of any prior, concurrent or subsequent right, remedy, or duty within this Agreement.
2. In relation to disputes between the Parties arising out of or in connection with this Agreement, the [NCB] and the Eurosystem irrevocably and unconditionally waive their respective privileges and immunities in relation to the jurisdiction of the Court of Justice pursuant to Article 47 and irrevocably agree that either Party will not claim any such immunity in proceedings before the Court of Justice. Nothing in or relating to this Agreement shall be deemed to be or shall constitute a waiver of any of the privileges and immunities of the [NCB] or the Eurosystem in relation to immunity from execution or enforcement and attachment or arrest of property.

OR [for non-euro area NCBs outside EU opting for jurisdiction of courts of Frankfurt instead of Court of Justice – with corresponding amendment in Article 47]

2. In relation to disputes between the Parties arising out of or in connection with this Agreement, the [NCB] and the Eurosystem irrevocably and unconditionally waive their respective privileges and immunities in relation to the jurisdiction of the courts of Frankfurt am Main pursuant to Article 47 and irrevocably agree that either Party will not claim any such immunity in proceedings before the courts of Frankfurt am Main. Nothing in or relating to this Agreement shall be deemed to be or shall constitute a waiver of any of the privileges and immunities of the [NCB] or the Eurosystem in relation to immunity from execution or enforcement and attachment or arrest of property.

Article 43

Survival

Any terms of this Agreement that by their nature extend beyond the termination or expiration of this Agreement shall remain in effect until fulfilled, including examination, Confidential Information, court proceedings, data protection, governing law and jurisdiction, indemnification, Intellectual Property Rights, limitation of liability, charges and survival.

[where applicable: **Schedule 13** shall remain in full force and effect until the end of the calendar year following the calendar year of termination or expiry of this Agreement.]

Currency Participation Agreement

Article 44

Notices

1. Except where otherwise provided for in this Agreement, all notices required or permitted pursuant to this Agreement shall be in writing delivered by hand or sent by registered post, facsimile or otherwise or by an authenticated message through a T2S Network Service Provider to the authorised person notified as such by the other Party. Except as otherwise provided for in the MOP, all notices of the [NCB] to the Eurosystem in relation to this Agreement shall be submitted to the Chairperson of the T2S Board and all notices of the Eurosystem to the [NCB] in relation to this Agreement shall be submitted to: [xxx].
2. Except as otherwise provided in this Agreement, to prove that a notice has been sent, it shall be sufficient to prove that the notice was delivered to the relevant address or that the envelope containing such notice was properly addressed and posted except that confirmation of receipt shall be required for notices in relation to Articles [21, 24, 25, 34, 36 and 44] and for all notices in relation to **Schedule 8**.
3. All notices shall be given in English.

Article 45

Invalid or incomplete provisions

If a provision of this Agreement is or becomes invalid or is inadvertently incomplete, the validity of the other provisions of this Agreement shall not be affected thereby. The invalid or incomplete provision shall be replaced or supplemented by a legally valid arrangement which is consistent with the intentions of the Parties' intentions or with what would have been the Parties' intention according to the aims of this Agreement had they recognised the invalidity or incompleteness. It is the intention of the Parties that this Article shall not merely result in a reversal of the burden of proof but that Section 139 of the BGB is contracted out in its entirety.

Article 46

Subcontracting

1. The [NCB] shall inform the Eurosystem reasonably in advance when it plans to outsource or subcontract any part of its obligations or to assign or transfer any rights or obligations arising out of or in connection with the performance of this Agreement to any Third Party.
2. Due to the public nature of T2S, the operation and running of T2S can only be entrusted to one or more Eurosystem Central Banks. The development and operation of T2S is performed

Currency Participation Agreement

by the 4CB or by an Affiliate of the 4CB or by one or more Euro Area NCBs pertaining to the 4CB, as part of an internal distribution of work within the Eurosystem and is not to be considered as outsourcing, subcontracting, assigning or transferring within the meaning of this Article.

3. Without prejudice to paragraph 2, the Eurosystem may only outsource or subcontract its tasks under this Agreement to a Third Party that have or may have a material impact on the performance of its obligations under this Agreement, if it has the express, prior written consent of the [NCB] which shall not be unreasonably withheld or delayed. No such consent is needed if the Third Party is an Affiliate of one or more of the 4CB and if the rights and obligations of the Parties remain materially unchanged. Outsourcing and subcontracting within the meaning of this Article do not include the procurement of services and/or components necessary for the 4CB to build, upgrade and maintain T2S and the procurement of services by the Eurosystem, and therefore no consent of the [NCB] is needed.
4. Any request for consent under paragraph 3 shall be answered within four weeks after the Eurosystem has received a confirmation of receipt of the request. Any refusal of consent shall give reasons for the refusal. If there is no response within four weeks, the Eurosystem may reiterate its request. The [NCB] shall from that point have two weeks within which to respond to the Eurosystem. If there is no response within these two weeks, the [NCB] shall be deemed to have given its consent.
5. In any case of outsourcing or subcontracting undertaken by a Party, it shall remain liable to the other Party for the performance of its duties and obligations under this Agreement. The Party concerned shall cause its subcontractors to be bound by confidentiality obligations similar to the ones provided by this Agreement.

Article 47

Court proceedings

1. The Parties agree that any dispute between the Parties arising out of or in connection with this Agreement shall be decided through proceedings between all Parties to this Agreement and that any such dispute, subject to the prior completion of the Dispute Resolution and Escalation Procedure set out in Article 37 (except for issues that have undergone the decision-making process in Section 1.2. and 1.3 of **Schedule 8** after which the Dispute Resolution and Escalation Procedure does not have to be initiated) and without prejudice to a Party's termination rights set out in this Agreement, shall be brought before [the Court of Justice of the European Union by either of the Parties] OR [*For Norges Bank and Icelandic CB*] [the courts of Frankfurt].

Currency Participation Agreement

2. The members of the Eurosystem have authorised the European Central Bank to act in the name and on behalf of all other members of the Eurosystem in all matters related to arbitration and court proceedings arising under this Article.

Article 48

Extension to other Parties

The [NCB] shall accept adhesion to this Agreement as Party of any national central bank of a Member State adopting the euro as its currency, provided that any such national central bank confirms in writing that it is bound by the terms of this Agreement as if it had signed this Agreement. The [NCB] shall be given no less than three months' prior written notice of adhesion of any such national central bank to this Agreement, and any such national central bank shall confirm in writing that it is bound by the terms of this Agreement as if it had signed this Agreement.

Done at Frankfurt am Main on [DATE]. The [NCB] and the ECB shall receive one original copy each. Each Eurosystem Central Bank shall receive a certified copy of the original copy deposited at the ECB.

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 1

DEFINITIONS

Currency Participation Agreement

Schedule 1 – Definitions

1. Definitions

In this Agreement, unless the context requires otherwise, terms defined in singular have the same meaning in plural, and vice versa.

In this Agreement, references to Union legislation are intended as referring to the most recent version of that legal act.

In this Agreement, unless the context requires otherwise, terms with initial capital letter have the following meanings:

‘4CB’	means the Deutsche Bundesbank, the Banco de España, the Banque de France and the Banca d’Italia, collectively, in their capacity as national central bank [NCBs] responsible for building, maintaining and running the T2S Platform based on the relevant contractual arrangements and on decisions of the Governing Council.
‘Acceptance Tests of T2S’	means that the [NCB] shall have the right to test T2S’ compliance with Schedule 5 and the T2S Scope Defining Set of Documents.
‘Advisory Group (AG)’	means the T2S Advisory Group, the mandate and composition of which is set out in the Annex to Guideline ECB/2010/2.
‘Affiliate’	means a legal entity which, with respect to any person, directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with the person in question. For the purposes of this definition, ‘control’ means the possession, directly or indirectly, of more than 50% of the equity interests of a person or the power to direct or cause the direction of the management and policies of a person, in whole or in part, whether through ownership of voting interests, by contract or otherwise.
‘Agreement’	means this Currency Participation Agreement, including the Schedules and Annexes.
‘Agreement Date’	means the date on which both Parties signed this Agreement.
‘Annex’	means an Annex to one of the Schedules to this Agreement.
‘Application-to-Application (‘A2A’)	means a connectivity mode to exchange information between the T2S software application and the application at the T2S Actor.
‘Background IPRs’	means all IPRs owned by or licensed to the [NCB] or to the Eurosystem prior to the Agreement Date.

Currency Participation Agreement

Schedule 1 – Definitions

‘Basic Custody Services’	means the holding and administration, by an entity entrusted with such tasks, of securities and other financial instruments owned by a Third Party. Basic Custody Services include the safekeeping of securities, the distribution of interest and dividends on the securities in safekeeping, and the processing of corporate actions on the said securities.
‘Batch Settlement’	means the set of sequenced, scheduled processes in T2S that settle or attempt to settle all instructions that are eligible for settlement on an transaction-by-transaction basis.
‘BGB’	means the Bürgerliches Gesetzbuch, i.e., the German Civil Code.
‘Business Continuity and Disaster Recovery’	means the set of rules and procedures aimed at resuming normal T2S Services, in compliance with the Service Levels as described in Schedule 6 , after the occurrence of an incident, as well as at mitigating the impact of such an incident.
‘Central Bank (CB)’	means the European Central Bank (ECB), each Euro Area NCB and each Connected NCB.
‘Central Bank Money (CeBM)’	means the liabilities of a Central Bank, in the form of either banknotes or bank deposits held at a Central Bank, which can be used for settlement purposes.
‘Central Bank Static Data’	means the set of business objects, specific to a Central Bank in T2S and owned by that Central Bank, that T2S requires to process the transactional data related to that Central Bank.
‘Central Securities Depository (CSD)’	means an entity that a) enables securities to be established and settled in book entry form, and/or maintains and administers securities on behalf of others through the provision or maintenance of securities accounts; and b) operates or provides for a Securities Settlement System in accordance with Article 2(a) of Directive 98/26/EC or for entities not located in the EEA in accordance with the relevant national legislation equivalent with Directive 98/26/EC and/or that is regulated by Central Bank; and c) is recognised as a CSD by national regulation and/or legislation and/or authorised or regulated as such by the Relevant Competent Authority.
‘CESR/ESCB Recommendations for Securities Settlement Systems’	means Committee of European Securities Regulators (CESR)/European System of Central Banks (ESCB) Recommendations for Securities Settlement Systems and Recommendations for Central Counterparties in the European Union.
‘Change and Release Management (CRM)’	means the set of rules used and the activities performed when a Change Request as described in, Schedule 9 is initiated and until it is rejected or the change is implemented into the production environment.
‘Change Management’	means the processes used and the activities performed when a Change Request as described in, Schedule 9 is initiated and until it is rejected or authorised for implementation.

Currency Participation Agreement

Schedule 1 – Definitions

‘Change Request’	means a request of a Party for a change that is subject to the Change and Release Management process, as described in Schedule 9 .
‘Change Review Group (CRG)’	means the group established by the Steering Level and composed of the relevant T2S Actors mandated to analyse Change Requests and make proposals on the content of T2S releases, as further specified in Schedule 9 .
‘Collateral Management System (CMS)’	means a system to manage collateral (i.e. assets, pledged as a guarantee for repayment of loans or sold as part of repurchase agreements) for Central Banks, CSDs and Directly Connected Parties.
‘Collateral Value’	means price of collateral including accrued interest, adjusted with appropriate haircuts and, if applicable, with the pool factor or public index.
‘Common Change’	means a change implemented for the benefit of all T2S Actors as described in Schedule 9 .
‘Common Static Data’	means the business information, which is available to all T2S Actors and which T2S requires to process business operations. This includes but is not limited to processing schedules, system entities, the SWIFT BIC Directory, system configuration data, attribute domains that are not specific to a CSD or central bank and standardised roles and privileges from which CSDs and Central Banks can configure their specific roles and access rights for their system users.

Currency Participation Agreement

Schedule 1 – Definitions

‘Confidential Information’	means any information, data, documentation or material that includes trade and business secrets, know how and information regarding the business, financial situation, products and prospects, processes and methodologies, customers, suppliers and employees, systems, programmes, algorithms, source codes, technical and security requirements and specifications (including any information that any party is obliged to keep confidential according to a contractual agreement or by law), and any other information, data, material or documentation (in each case to the extent marked as confidential or with a similar designation, or which a reasonable person would consider as confidential) related to a Party or its Affiliates, which such a Party has disclosed (in whatever form) to the other Party in connection with this Agreement. Confidential Information does not include information that: (a) has been designated by a Party as being intended for disclosure to Third Parties and does not reveal Confidential Information received by another Party; (b) becomes generally available to the public other than as a result of a breach of the confidentiality obligations under this Agreement; or (c) is received from a Third Party not bound by an obligation of confidentiality with respect to such information (while the receiving Party is aware or made aware by the other Party of this fact); (d) was known to or legally in a Party's possession without obligations of confidentiality prior to such information being provided as Confidential Information in accordance with this Agreement; or (e) is developed by either Party (or its Affiliates or their employees or representatives) independently without the use of Confidential Information of the other Party.
‘Connected NCB’	means an Eligible NCB having signed a CPA.
‘Connectivity Services’	means the combination of Physical Connectivity Services and Value-added Connectivity Services.
‘Crisis’ or ‘Crisis Situation’	means a situation that requires the involvement of the senior manager of the [NCB] (referred to as NCB crisis manager in Schedule 6), in order to manage a severe technical incident or market disturbance, either in accordance with the requirements specified in the MOP or because the procedures described in the MOP are not sufficient to effectively handle the situation.
‘CSD Steering Group (CSG)’	means the T2S governance body which, with respect to a set of matters stipulated in the Framework Agreement, makes resolutions and delivers opinions on behalf of the Contracting CSD and Participating CSDs. The CSG mandate is annexed to Schedule 8 of the FA.
‘Currency Participation Agreement (CPA)’	means each of the contractual agreement to be entered into by the Eurosystem and an Eligible NCB to allow for securities settlement in Central Bank Money in the non-euro currency they are responsible for.

Currency Participation Agreement

Schedule 1 – Definitions

‘Decision (2010/87/EU)’	means Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5).
‘Decision ECB/2009/6’	means Decision ECB/2009/6 of 19 March 2009 on the establishment of the TARGET2-Securities Programme Board (ECB/2009/6) (OJ L 102, 22.4.2009, p. 12).
‘Decision ECB/2011/20’	means Decision ECB/2011/20 of 16 November 2011 establishing detailed rules and procedures for implementing the eligibility criteria for central securities depositories to access TARGET2-Securities services (OJ L 319, 02.12.2011, p. 117).
‘Dedicated Cash Account (DCA)’	means a cash account in T2S operated by a Central Bank.
‘Dedicated Cash Account Holder (DCA Holder)’	means a holder of a DCA which is directly connected to T2S (i.e. through A2A and/or U2A).
‘Dedicated Link Connection’	means a solution to connect the T2S data centres with the data centres of the Directly Connected T2S Actors, whereby the Value-added Connectivity Services are implemented in T2S and in the systems of the Directly Connected T2S Actors.
‘Delivery-versus-Payment (DvP)’	means a securities settlement mechanism which links a securities transfer and a funds transfer in such a way as to ensure that delivery occurs if – and only if – the corresponding payment occurs.
‘Development Phase’	means the period, during which the Eurosystem specifies, develops and tests T2S and establishes its operational framework; this period ends on the date that the Governing Council decides that the full scope of T2S Services as documented in Schedule 5 are operational in the T2S production environment, as depicted in Annex 1 to Schedule 1 .
‘Directive 95/46/EC’	means Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).
‘Directive 98/26/EC’	means Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems (OJ L166, 11.6.1998, p. 45).
‘Direct Loss’	means loss or damage directly caused to the damaged Party as a result of the gross or ordinary negligence of the other Party in performing its duties and obligations under this Agreement. Lost revenues, lost profits, lost savings and reputational damage shall not qualify as Direct Loss, instead they shall qualify as indirect losses.

Currency Participation Agreement

Schedule 1 – Definitions

‘Directly Connected Party (DCP)’	means a T2S User, which has been authorised by its Contracting CSD or Central Bank to access T2S directly to use T2S Services (e.g. directly connected DCA Holder).
‘Directly Connected T2S Actor’	means either any of the Participating CSDs, or any of the Connected NCBs, or any of the DCPs or directly connected DCA Holders.
‘Dispute Resolution and Escalation Procedure’	means the procedure described in Article [35] of this Agreement for resolving disputes between the Parties.
‘Dynamic Data’	see ‘Transactional Data’.
‘ECB’	means the European Central Bank.
‘Eligible NCB’	means (i) each Non-euro Area NCB, and (ii) each Other Central Bank from the country belonging to the European Economic Area, or from another country in the case where it is deemed eligible pursuant to the Governing Council decision referred to in [recital F] of the Currency Participation Agreement.
‘Enforceable Judgement’	means a binding and enforceable judgment or equivalent type of decision rendered by a court or award rendered by an arbitral tribunal
‘ESMA’	means European Securities and Markets Authority
‘Euro Area NCB’	means the NCB of a Union Member State whose currency is the euro.
‘Eurosysteem’	means, in accordance with Article 1 of the Statute of the ESCB and of the European Central Bank, the ECB and the NCBs of the Union Member States whose currency is the euro..
‘Eurosysteem Acceptance Testing (EAT)’	means the formal testing conducted by the Eurosysteem to determine whether the T2S Platform is compliant with the T2S Scope Defining Set of Documents.
‘Eurosysteem Central Bank’	means either the ECB or the Euro Area NCB, as the case may be.
‘Exit Management’	means a set of rules and procedures applied on termination of the Agreement, howsoever caused, as described in Schedule 11 .
‘External Examiner’	means a well-reputed, internationally active auditing firm that has the tasks set out in Article [24] of this Agreement assigned to it.
‘Fast-track Change’	means a change that is imposed by Legal and Regulatory Requirements, or by CSG resolutions related to risk management, or changes that are critical for the stability of the T2S Platform or by Central Bank decisions related to safeguarding the currency/-ies or related to crisis management measures to ensure financial stability and that, owing to the time constraints, has to be implemented in a shorter timeframe than normal, which will be decided on an ad-hoc basis, as specified in Schedule 9 .

Currency Participation Agreement

Schedule 1 – Definitions

‘Force Majeure’	means any circumstances beyond the reasonable control of the non-performing Party, including, without limitation, an element of nature or an act of God, earthquake, fire, flood, war, terrorism, civil, industrial or military disturbance, sabotage, labour strike or lock-outs, pandemic, epidemic, riot, loss or malfunction of utilities or communication services, court order, act of civil or military authority, or governmental, judicial or regulatory action.
‘Framework Agreement (FA)’	means the contractual framework between a CSD and the Eurosystem for the Development Phase and the Operational Phase of T2S.
‘Free of Payment (FoP)’	means the delivery of securities with no corresponding payment.
‘General Specifications (GS)’	means together with the GFS and the GTD, the document that describes how the Eurosystem envisages implementing the URD. In particular, the General Specifications focus on those user requirements that do not have a functional or technical dimension, such as operational support, testing, migration and Information Security.
‘General Functional Specifications (GFS)’	means a general functional description of the T2S Business Application to be developed to comply with the T2S user requirements. It will include elements such as the functional architecture (domains, modules and interactions), the conceptual models, the data model or the data flow process.
‘General Principles of T2S’	means the general principles approved by the Governing Council to define the main cornerstones of T2S, as referenced to in the URD.
‘General Technical Design (GTD)’	means the document that details the solution envisaged for the T2S non-functional requirements, more specifically with regard to the application design and the infrastructure design
‘Governors’ Forum’	has the meaning set out in Article [38] and Schedule 8 .
‘Governance’	means the set of rules and procedures concerning the management of T2S Services, including the related decision-making of the parties involved in T2S, as specified in Schedule 8 .
‘Governance Bodies’	means the bodies specified in Article [21 (6)] of this Agreement and involved in the decision-making process with final decisions being taken by the Governing Council in accordance with Article [21] of this Agreement and in accordance with Schedule 8 .
‘Governing Council’	means the decision-making body of the ECB comprising the members of the Executive Board of the ECB and the governors of the Euro Area NCBs, as provided for in Article 10 of the Statute of the ESCB.
‘Graphical User Interface (GUI)’	means the interface that allows a user to interact with a software application through the use of graphical elements (e.g. windows, menus, buttons and icons) on a computer screen using the keyboard and the mouse.

Currency Participation Agreement

Schedule 1 – Definitions

‘Guideline ECB/2010/2’	means Guideline ECB/2010/2 of 21 April 2010 on TARGET2-Securities (OJ L 118, 12.5.2010, p. 65).
‘Information Security’	means a set of requirements and procedures, described in Schedule 10 and based on International Organisation for Standardisation (‘ISO’) Standard 27002:2005, aimed at safeguarding the integrity, confidentiality and availability of the T2S information and T2S Services.
‘Information Technology Infrastructure Library (ITIL)’	means the set of best practices for managing IT infrastructure, development and operations, maintained under the auspices of the Office of Government Commerce, an office of the UK Treasury.
‘Insolvency Event’	means a collective judicial or administrative proceeding, including an interim proceeding, in which the assets and affairs of the Contracting CSD are subject to control or supervision by a court or other competent authority for the purpose of reorganisation or liquidation.
‘Intellectual Property Rights (IPRs)’	means any patents, utility models, designs, trademarks, copyrights (each of the foregoing, to the extent applicable, registered, applied for or unregistered), inventions whether or not patentable, database rights, know-how and all rights having equivalent or similar effect in any jurisdiction.
‘Intended Settlement Date (ISD)’	means the date on which the parties to a securities transaction agree that settlement is to take place. The ISD is also referred to as the contractual settlement date or value date.
‘International Securities Identification Number (‘ISIN’)	means the number, which uniquely identifies a security. Its structure is defined in ISO 6166.
‘Investor CSD’	means a CSD that holds a security for which it is not the/an Issuer CSD. It holds these securities either directly or indirectly, via one or more intermediaries, at the/an Issuer CSD
‘Issuer CSD’	means a CSD, which holds a primary deposit in the relevant securities, either in dematerialised or physical form.
‘Key Performance Indicator(s) (KPI(s))’	means a metric used to quantify the expected performance of the Eurosystem and to monitor compliance with the Service Level Agreement.
‘Lean Scope of T2S’	means the scope of T2S defined by the URD resulting from the market involvement and is restricted by the General Principles of T2S, as referenced in the URD.
‘Legal and Regulatory Requirements’	means all applicable requirements (as may be amended from time to time) that a Connected NCB must comply with, including those of a legal, regulatory (including fiscal), supervisory and oversight nature and that are relevant in the context of T2S.

Currency Participation Agreement

Schedule 1 – Definitions

‘Licence Agreement’	means the contract signed by the Banca d'Italia, in the name and on behalf of the Eurosystem, and each NSP, which contains the requirements which the latter has to fulfil to be entitled to deliver the Connectivity Services to the Eurosystem and to the Directly Connected T2S Actors.
‘Maintenance Window’	means the period for system maintenance, during which T2S is planned to be unavailable, as defined in Schedule 6 .
‘Manual of Operational Procedures (MOP)’	means the document that describes the procedures to be applied by all T2S Actors, aimed at ensuring the smooth conduct of daily operations and at minimizing the duration and impact of service interruptions or deteriorations.
‘Matching’	means the process used for comparing the settlement details provided by parties in order to ensure that they agree on the terms of the transaction.
‘Member State’	means a country that is a member of the Union.
‘Migration’	means a set of rules and procedures concerning the [NCB’s] migration to T2S, as described in Schedule 4 .
‘Migration Period’	means the time period beginning on the date on which the T2S Board confirms that the T2S production environment is ready for CSDs and Central Banks to connect (SP14) and ending on the date on which [all CSDs and Central Banks] that have signed the FA and the CPA, respectively, have migrated on T2S in accordance with the conditions applicable to Synchronisation Point 16.
‘Multilateral Character of T2S’	has the meaning set out in Article [3] of this Agreement.
‘National User Group (NUG)’	has the meaning set out in the Annex to the T2S Guideline and link the respective national market with the AG.
‘NCB-specific Requirements’	means features affecting the design, functionality and/or operational or legal requirements of T2S or Legal and Regulatory Requirements, that are specific to the [NCB] and that are described in Schedule 13 .
‘NCBs’ Acceptance Tests of the T2S Services’	means the process whereby the Connected NCB assesses the compliance of the relevant T2S Services with Schedule 5 and the T2S Scope Defining Set of Documents as further specified in Article [13] of this Agreement and in Schedule 3 .
‘Non-euro Currencies Steering Group (NECSG)’	means the T2S governance body which, with respect of a set of matters stipulated in the CPA, makes resolutions and delivers opinions on behalf of the non-euro area NCBs having signed the CPA. The NECSG mandate is annexed to Schedule 8 of the CPA.
‘Non-euro Area NCB’	means the NCB of a Union Member State, whose currency is not the euro.

Currency Participation Agreement

Schedule 1 – Definitions

‘Operations Managers Group (OMG)’	means the group established by the Steering Level and composed of the relevant T2S Actors that develops and maintains the Manual of Operational Procedures, meets to review the T2S service performance against the Service Level Agreement and coordinates the management of operational incidents, as specified in Schedule 6.
‘Operational Phase’	means the time period when the full scope of T2S Services are operational in the T2S production environment and beginning on the T2S Go-Live Date, as depicted in Annex 1 to Schedule 1 .
‘Other Central Bank’	means the Central Bank of a country outside the EU.
‘Parallel Currency Participation Agreement’	means an agreement essentially identical, save for the identity of the Parties, to this Agreement, entered into between a Connected NCB (other than the [NCB]) and the Eurosystem.
‘Participating CSD(s)’	means the CSD(s) that have signed the Framework Agreement.
‘Party’ or ‘Parties’	means the Connected NCB and the Eurosystem or either of them (as required by context).
‘Payment Bank’	means a commercial bank used to affect money settlements. In the context of securities settlement, a Payment Bank provides cash on behalf of a CSD participant to support the settlement of securities.
‘Payment Free of Delivery (PFoD)’	means a transfer of cash without the delivery of securities.
‘Physical Connectivity Services’	means the implementing, maintaining and keeping available of a data communication network for the purpose of exchanging files and messages between the Directly Connected T2S Actors and T2S, as more specifically described in the Licence Agreement.
‘Pricing’	means a set of rules and procedures that is applied to price the T2S Services and T2S-related services provided by the Eurosystem, as described in Schedule 7 .
‘Project Managers Group (PMG)’	means the group established by the Steering Level and composed of the relevant T2S Actors that coordinates and monitors activities to ensure that the initial release as well as subsequent releases of T2S go live, as specified in Schedule 2, 3 and 4 .
‘Real-time Settlement’	means the continuous process in T2S that settles or attempts to settle instructions that are eligible for settlement on a transaction-by-transaction basis.
‘Regulation (EC) No 45/2001’	means Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

Currency Participation Agreement

Schedule 1 – Definitions

‘Release Management’	means the set of rules used and the activities performed to implement a set of authorised changes and defect corrections in a new version of the T2S Business Application, as set out in Schedule 9 .
‘Relevant Competent Authority’	means any organisation having regulatory, supervisory or oversight authority over the [NCB], or a Connected NCB or a Participating CSD (as required by the context).
‘RTGS Participants’	means participants in the RTGS System that are considered as participants according to the national implementation of Article 2 of Settlement Finality Directive [OR <i>if the NCB is established outside the European Economic Area</i> : participants in the [NCB’s] RTGS System that enjoy an equivalent protection to that in force for ‘participants’ as defined in Article 2 of the Settlement Finality Directive].
‘RTGS System’	means a Real-Time Gross Settlement System operated by the [NCB] or by another Central Bank (as required by the context) which is connected to T2S to provide liquidity in [currency] to T2S.
‘Schedule’	means a Schedule to this Agreement.
‘Second T2S Protocol’	means the protocol signed by all Eurosystem CBs the purpose of which is for the Eurosystem CBs to grant each other a power of attorney to sign the Framework Agreement with the CSDs in the name and on behalf of all the Eurosystem CBs.
‘Securities Account’	means an account maintained by a CSD to which securities may be credited or debited.
‘Securities Settlement System’	means a system as defined in Article 2(a) of Directive 98/26/EC for the execution of transfer orders related to title to or interest in a security or securities by means of a book entry on a register, or otherwise.
‘Service Description’	means the description of the T2S Services, contained in Schedule 5 .
‘Service Level’	means level of performance of a T2S Service that Schedule 6 and that the Contracting CSD requires to deliver its services to its customers.
‘Service Level Agreement (SLA)’	means the agreement defining the Service Levels, measured against agreed KPIs where relevant, to be provided by the Eurosystem to the Connected NCBs, as specified in Schedule 6 and in relation to T2S Services.
‘Service Level Report’	means the monthly report made available by the Eurosystem to the [NCB] to determine the degree of the Eurosystem’s compliance with the Service Level Agreement, as specified in Schedule 6 , in particular as regards the KPIs.
‘Settlement Day’	means a day on which T2S settlement takes place according to the daily processing schedule.

Currency Participation Agreement

Schedule 1 – Definitions

‘Settlement Finality Directive’	means Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems (OJ L 166, 11.6.1998, p. 45).
‘Specific Change’	means any new feature, functionality or service – or any amendment of an existing feature, functionality or service – which is not implemented as a Common Change (within the applicable governance arrangements), but which some Participating CSDs and/or Central Banks wish to implement, provided that it is compliant with the Lean Scope of T2S, and for which they jointly accept to bear the investment and running costs.
‘Statute of the ESCB’	means the Statute of the European System of Central Banks and of the European Central Bank (Protocol No 4 to the Treaty on the Functioning of the European Union, OJ C 83, 30.3.2010, p. 230).
‘Steering Level’	means the level comprising the T2S Board for tasks delegated by the Governing Council, the NECSG and the CSG, as specified in Schedule 8 .
‘Suspension’	means the temporary freezing – possibly limited to the T2S Services relevant to the cause of suspension – of the rights and obligations of the Contracting [NCB] for a period of time to be determined by the Eurosystem, as described in Article [39].
‘T2S Actor’	means either the Participating CSDs, a CSD participant (a legal entity or, as the case may be, an individual) having a contractual relationship with the CSD for the processing of its securities settlement-related activities in T2S, or a Central Bank, whose currency is available for settlement-related processing in T2S, or a member of a Central Bank having a contractual relationship with the Central Bank for the processing of its settlement-related cash-processing activities in T2S.
‘T2S Board’	means the Eurosystem management body established pursuant to Decision ECB/2012/xx, which has the task of developing proposals for the Governing Council on key strategic issues and executing tasks of a purely technical nature in relation to T2S.
‘T2S Business Application’	means the software developed and operated by the 4CB on behalf of the Eurosystem with a view to enabling the Eurosystem to provide the T2S Services on the T2S Platform.
‘T2S Documentation’	means the T2S non-scope defining set of documents that consists of the T2S Specification, the T2S Operational Phase Documents and the T2S Project Documents as described in Schedule 2 Annex 8 (T2S Deliverables List and Management Process).
‘T2S-Enabled Services’	means the services of the [NCB] it provides to its Dedicated Cash Account Holders on the basis of the T2S Services.

Currency Participation Agreement

Schedule 1 – Definitions

‘T2S Go-Live Date’	means the first Settlement Day after which the first Participating CSD(s)/NCB(s) have migrated to T2S.
‘T2S Memorandum of Understanding’	means the Memorandum of Understanding concluded on 16 July 2009 between the Eurosystem and the Contracting CSDs as well as other European CSDs, showing the commitment towards T2S and setting out the mutual obligations and responsibilities for the time period up to the conclusion of a definitive agreement.
‘T2S Network Service Provider (T2S NSP)’	means a network service provider (NSP) that has concluded a Licence Agreement with the Eurosystem to provide Connectivity Services to T2S. It is a business or organisation providing the technical infrastructure, including hardware and software, to establish a secure and encrypted network connection that permits the exchange of information between T2S and T2S Actors.
‘T2S Operator’	means the legal and/or organisational entity/entities that operate/operates the T2S Platform. As part of an internal distribution of work within the Eurosystem, the Governing Council entrusted the 4CB with operating T2S, on behalf of the Eurosystem.
‘T2S Operational Phase Documents’	means the set of documents that describes how T2S provides its services when it is in production. It encompasses the documentation for T2S as a software application and the manuals describing the rules and procedures for operating T2S.
‘T2S Platform’ or ‘TARGET2-Securities (T2S)’	see ‘TARGET2-Securities (T2S)’
‘T2S Programme’	means the set of related activities and deliverables needed to develop T2S until the full Migration of all CSDs, which have signed the Framework Agreement and all Euro Area NCBs as well as all Connected NCBs.
‘T2S Programme Plan’	means the common Eurosystem-CSD-Central Bank plan, outlining the milestones, Key Milestones and timelines to deliver the T2S Programme as well as the respective actions and contributions required from the Eurosystem, the CSDs and other T2S Stakeholders, as described in Schedule 2 .
‘T2S Project Documents’	means the set of documents required for planning, monitoring and successfully completing the scheduled activities (e.g. User Testing, Migration, client readiness tracking) in the T2S project lifecycle but not during the operational part, i.e. from the start of the T2S Programme until T2S is live, or during any subsequent preparation for releases.
‘T2S Scope Defining Set of Documents’	means the set of documents defining the scope of T2S composed of the URD, the UDFS, the GUI Business Functionality, the GFS Functional Chapter, the Dedicated Link Connectivity Specifications and the Data Migration Tool Specifications and Related Procedures..

Currency Participation Agreement

Schedule 1 – Definitions

‘T2S Services’	means the services to be provided by the Eurosystem to the Contracting CSDs and Central Banks as specified in this Agreement and any other relevant agreement.
‘T2S Specifications’	means the set of documents, when added to the T2S Scope Defining Set of Documents, provide a full description of T2S. This includes the GFS non-Functional Chapters.
‘T2S Stakeholder’	means any organisation; legal entity or governmental entity; public or private interest groups; or individual that has a valid interest in the outcome of the T2S project and the governance and operation of T2S.
‘T2S Threat Catalogue’	means the information on relevant threats to the T2S Platform,, which serves as the basis for the specification of appropriate security controls and, at a later stage, the evaluation of residual risks in terms of impact and likelihood, as described in Schedule 10 (Information Security).
‘T2S Trademarks and Logo’	means all “T2S”-trademarks and / or the logo  owned by a Eurosystem Central Bank.
‘T2S User’ or ‘User’	see ‘User’
‘TARGET2’	means the payment system functioning in accordance with Guideline ECB/2007/2 of 26 April 2007 on a Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET2) (OJ L 237, 8.9.2007, p. 1).
‘TARGET2-Securities (T2S)’ or ‘T2S Platform’	means the set of hardware, software and other technical infrastructure components through which the Eurosystem provides the services to CSDs that allow core, neutral and borderless settlement of securities transactions on DvP basis in Central Bank Money.
‘Third Party’	means an individual or legal entity, which is not party to the contractual relationship, as defined in this Agreement. For the avoidance of doubt, a Third Party is a person or legal entity other than the [NCB], the European Central Bank, Euro Area NCB or the T2S Operator.
‘Transactional Data’	means the information that T2S creates and stores through the execution of a business process event where the content of the information defines that event. This includes but is not limited to inbound and outbound XML messages, all types of settlement instructions and all data that T2S generates for the life cycle of the instruction (e.g. securities positions) and static data maintenance instructions. This is also referred to as Dynamic Data in the Schedules and in other documentation.
‘Transfer Order’	has the meaning set out in Article 2(i) of Directive 98/26/CE.
‘Treaty on the Functioning of the European Union (TFEU)’ or ‘Treaty’	means the Treaty on the Functioning of the European Union (OJ C 83, 30.3.2010, p. 47).

Currency Participation Agreement

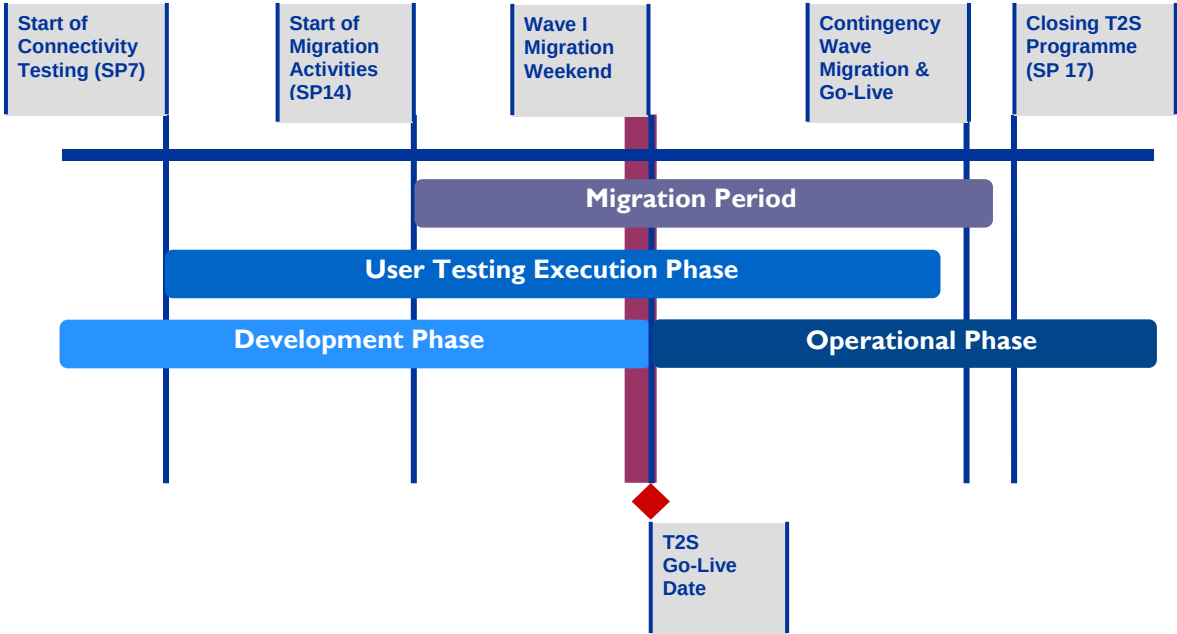
Schedule 1 – Definitions

‘User’ or ‘T2S User’	means a legal entity or, as the case may be, an individual, that has a contractual relationship with the Contracting CSD or another Participating CSD for the processing of its settlement-related activities in T2S, or a member of a CB (whose currency is available for settlement-related processing in T2S) having a contractual relationship with the CB for the processing of its securities settlement-related cash-processing activities in T2S.
‘User Detailed Functional Specifications (UDFS)’	means the a detailed description of the functions managing the T2S external data flows (from A2A). It will include the necessary information for the users to adjust or to develop their internal information systems with a view to connecting them to T2S.
‘User Handbook (UHB)’	means the document describing the way in which T2S Users can make use of a number of T2S software functions that are available in a U2A (screen- based) mode
‘User Requirements Document (URD)’	means document setting out the user requirements for T2S as published by the ECB on 3 July 2008 and as subsequently amended through the T2S change and release management procedure.
‘User Testing ‘ or ‘User Tests’	means a set of rules and procedures concerning the T2S’s testing by the Connected NCBs as described in Schedule 3 .
‘User-to-Application (U2A)’	means a connectivity mode to exchange information between software applications of T2S and a T2S Actor through the GUI.
‘Value-added Connection’	means a solution to connect the T2S data centres with the data centres of the Directly Connected T2S Actors, whereby both the Value-added Connectivity Services and the Physical Connectivity Services are provided by a NSP.
‘Value-added Connectivity Services’	means the set of messaging services, security services and operational services either provided by an NSP in accordance with the Licence Agreement, or implemented in T2S and in the systems of the Directly Connected T2S Actors.

Currency Participation Agreement

Schedule 1 – Annex 1 – Diagram of Phases/Periods

Annex 1 – Diagram of Phases/Periods



CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 2

T2S PROGRAMME PLANNING AND MONITORING

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

Table of contents

1	INTRODUCTION	1
1.1	Context	1
1.2	Structure of Schedule	2
2	SCOPE AND OBJECTIVES.....	4
2.1	Scope.....	4
2.2	Objectives	4
3	GENERAL RESPONSIBILITIES OF THE PARTIES TO THIS AGREEMENT ...	5
3.1	General Responsibilities of the Eurosystem	5
3.2	General Responsibilities of the Contracting National Central Banks (CBs).....	5
3.3	General responsibilities of the Project Manager Group (PMG).....	7
4	SUPPORTING DOCUMENTATION	8
4.1	T2S Programme Work Breakdown Structure	8
4.2	T2S Programme Deliverables	8
4.3	Milestones	9
5	T2S PROGRAMME PLAN.....	10
5.1	CB-relevance of planning items.....	10
5.2	T2S Programme Plan Views	11
5.3	T2S Critical Path.....	14
6	MONITORING FRAMEWORKS.....	15
6.1	T2S Programme Status Assessment Framework	15
6.2	T2S Risk and Issue Management and Monitoring Framework.....	17
6.3	T2S Monitoring of Client Readiness Framework	22
7	PROCESSES.....	27
7.1	Methodology and Conventions	27
7.2	Programme Plan Preparation, Adaptation and Assessment Review Process.....	29
7.3	Adaptation Process for updated Annexes without affecting the plan:	32
7.4	Disagreement Resolution process	34

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

1 Introduction

1.1 Context

T2S is a large-scale programme, involving a significant number of actors. Owing to this complexity, a successful development, implementation and production start of T2S requires agreement between the parties to this Agreement on their roles and responsibilities as well as the respective expectations and commitments during the programme. It is not sufficient for the parties to this Agreement to the T2S Programme to establish and monitor stand-alone project plans independently of each other. It requires a common programme plan that:

- is based upon clearly identified and scoped deliverables;
- takes into account all the respective constraints and dependencies of the parties to this Agreement; and
- undergoes regular, close monitoring over the life of the programme, with decisions committing all parties.

As the plan may evolve during the course of the T2S Programme, a comprehensive framework must exist to manage events that may affect the programme's deliverables and milestones, including a review and decision-making process for adapting the programme plan. This requires a regular dialogue between the parties to this Agreement to enable them to manage their own parts of the programme, and jointly make proposals on common tasks and activities affecting the other parties to this Agreement. Contracting National Central Banks (CBs) must be in the position to organise their planning and their internal resources. Conversely, the Eurosystem planning of the User Testing and Migration phases, as well as the start operations in T2S, requires the input of all T2S Actors.

A successful programme delivery requires a consistent and complete framework to plan, coordinate, monitor and report the activities of the T2S Actors. Article 25 of the CPA defines the process of updating this Schedule 2. This Schedule 2 specifies the process of updating Annexes of Schedule 2 (see Section 7).

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

1.2 Structure of Schedule

The Schedule 2 contains different sections and has several Annexes.

The third section presents the general responsibilities of the Eurosystem and the Contracting CBs.

The fourth section describes the main documents supporting the monitoring of the T2S Programme Plan.

The fifth section presents the three official views of the T2S Programme plan and their main features.

The sixth section presents the main principles and conventions used for progress monitoring, for risk monitoring and for the management of bilateral relations between the Eurosystem and each Contracting CB.

The seventh section documents the T2S Programme Plan monitoring process and includes the process for changing Schedule 2 Annexes.

The Annexes to Schedule 2 have three objectives:

- to provide the initial state of the T2S Programme planning documentation, which may evolve according to the processes defined in Schedule 2;
- to provide the templates used for programme reporting purposes; and
- to provide the initial state of the supporting documentation.

Schedule 2 includes the following Annexes:

Annexes with focus on the plan substance:

- Annex 1 - T2S Executive Summary Plan
- Annex 2 - T2S Operational Plan
- Annex 3 - T2S Detailed Plan
- Annex 4 - T2S Programme Plan assumptions

Annexes with focus on reporting templates:

- Annex 5 - T2S Programme Progress Reporting templates
- Annex 6 - T2S Risk and Issue Reporting templates

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

54 Annexes with focus on supporting documents:

- 55 ▪ Annex 7 - T2S Programme Work Breakdown Structure (WBS)
- 56 ▪ Annex 8 - T2S list of Deliverables
- 57 ▪ Annex 9 - T2S list of Synchronisation points
- 58 ▪ Annex 10 - T2S list of Milestones on the critical path

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

2 Scope and Objectives

2.1 Scope

This document on Programme Planning and Monitoring (Schedule 2 of the CPA) presents the commitment of the Eurosystem to establish and maintain a common programme plan (the T2S Programme Plan) and defines roles, responsibilities, processes and interactions of the parties to this Agreement.

2.2 Objectives

The objectives of Schedule 2 are:

- to document the baseline T2S Programme Plan and its underlying assumptions;
- to define the framework for coordinating, managing and attempting to resolve potential disagreement on the T2S Programme Plan;
- to provide all parties to this Agreement with the necessary information to develop, coordinate and manage their respective project plans in coordination with the T2S Programme Plan;
- to define a monitoring and reporting framework on the progress against the T2S Programme Plan, including risks and issues; and
- to define a monitoring framework for client readiness.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

3 General Responsibilities of the parties to this Agreement

3.1 General Responsibilities of the Eurosystem

The Eurosystem commits to deliver and maintain the documentation, frameworks and processes, as defined in this Schedule and its Annexes. This means that at any point in time there will be a valid programme plan and an agreed framework to provide all parties to this Agreement with relevant information on the programme status detailing the main principles, frameworks, processes and tools to support the programme monitoring. The Eurosystem commits to follow the framework and processes defined in this Schedule.

Furthermore, the responsibilities of the Eurosystem include:

- preparing and maintaining the T2S Programme Plan;
- organizing a close coordination with Contracting CBs for reviewing and proposing changes to the plan to the Steering Level;
- providing on a regular basis to Contracting CBs an accurate T2S Programme status assessment based on the T2S Programme Plan;
- preparing reports on, and response plans for, risks and issues pertaining to the T2S Programme Plan with emphasis on activities and deliverables that impact Contracting CBs;
- establishing and chairing the Project Managers Group (PMG) to review, discuss and agree on the T2S Operational Plan and the T2S Programme status for Contracting CBs relevant planning items with Contracting CSDs and Contracting CBs; and
- establishing and attending a bilateral forum between the Eurosystem and each Contracting CB to review and discuss the Contracting CB's individual status assessment for their activities within the T2S Programme Plan.

3.2 General Responsibilities of the Contracting National Central Banks (CBs)

Contracting CBs are responsible for ensuring their own readiness and for undertaking reasonable efforts to coordinate the readiness of their clients (including those who are directly connected to T2S) to start with T2S. Contracting CBs commit to follow the framework and processes defined in this Schedule and its Annexes.

Furthermore, the responsibilities of the Contracting CBs include:

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

- 103 ▪ establishing their own adaptation plans to start operations with T2S in synchronisation with
104 the T2S Programme Plan;
- 105 ▪ providing relevant and accurate information on progress and achievement of milestones,
106 deliverables and synchronisation points, as well as on risks and issues, including response
107 plans, potentially affecting the T2S Programme Plan. This is to enable the Eurosystem to
108 maintain the T2S Programme Plan and consolidate the information received in the context of
109 the monitoring of client readiness;
- 110 ▪ participating in the PMG to review, discuss and agree on the T2S Operational Plan and the
111 T2S Programme status for activities, deliverables and milestones affecting the plans of
112 Contracting CBs; and
- 113 ▪ participating in a bilateral forum between the Eurosystem and each Contracting CB to review
114 and discuss the Contracting CB's individual status assessment of its activities within the T2S
115 Programme Plan to become operational on T2S.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

3.3 General responsibilities of the Project Manager Group (PMG)

The PMG shall be composed of representatives of the Eurosystem, Contracting CSDs and Contracting CBs. Schedule 1 and Schedule 8 define the general role of the PMG. The following specifies the responsibilities of the PMG when supporting activities as defined in Schedule 2. The PMG shall:

- Meet (physically or via conference call) on a regular basis and on an ad hoc basis when requested by one of the members. The PMG determines the frequency of its meetings based on its needs.
- Assess the T2S Operational Plan and propose updates as detailed in Section 7.
- Assess the T2S Programme status report and propose changes.
- Identify risks and issues related to the execution of the T2S Plan
- Propose mitigation or resolution measures for all risks and issues identified.
- Discuss and propose solutions for multilateral issues related to the readiness of one of its members.
- Act proactively and in good faith to achieve agreement between PMG members.
- Prepare escalations on and escalate disagreements to the Steering Level.
- Be informed on a regular (e.g. quarterly) basis and identify the needs of the changes to the T2S Scope Defining Set of Documents.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

4 Supporting Documentation

The Eurosystem provides the documents described in this section as background information supporting programme planning and monitoring. The Annexes to Schedule 2 contain the baseline versions of these documents. These documents may evolve in the course of the programme as defined by the processes in Section 7.

The supporting documentation provides the reference that allows the reader to understand the content and construction of the plans and reports.

4.1 T2S Programme Work Breakdown Structure

The Eurosystem defines and maintains a *Work Breakdown Structure (WBS)* for the purpose of programme planning and monitoring. The WBS is a Deliverable-oriented hierarchical decomposition of the work that the T2S Programme needs to execute to deliver T2S successfully. The WBS is the basis for grouping, aggregating and classifying the activities and deliverables for the T2S Programme Plan as well as for T2S programme status monitoring.

4.2 T2S Programme Deliverables

A Deliverable is a unique and verifiable product, result, or capabilities to perform a service, required to complete a process or phase¹.

The specification of the Deliverable consists of the information documented in the introduction to Annex 8 (e.g. name of the Deliverable, its classification according to the WBS)

The Eurosystem defines and maintains the List of Deliverables.

¹ In line with the PMBOK®

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

4.3 Milestones

Milestones are significant points or events in the programme². In addition to this standard milestone definition, the T2S Programme Plan includes specific milestones as defined in the subsequent paragraphs.

4.3.1 Synchronisation Points

A synchronisation point is a point of time in the programme at which the T2S Programme is to reach a specific objective. The purpose of a synchronisation point is to monitor at foreseen time intervals that the progress of all parties to this Agreement is in line with the programme plan.

The Eurosystem provides the list of synchronisation points, which includes the list of the deliverables and milestones that require delivery or completion by the Eurosystem, Contracting CSDs and Contracting CBs in order to have successfully achieved the synchronisation point.

4.3.2 Critical Milestones

Critical milestones are milestones on the critical path of the T2S Programme Plan.

² In line with the PMBOK®

5 T2S Programme Plan

The T2S Programme Plan is the common Eurosystem-CSD-CB plan. This chapter describes the three views of the T2S Programme Plan that the Eurosystem provides in order to allow Contracting CSDs and Contracting CBs to monitor the progress of the T2S Programme and update their own plans.

The T2S Programme WBS, based on work streams, provides the organisational structure for activities, tasks, and milestones of the plans.

5.1 CB-relevance of planning items

The T2S Programme Plan differentiates between CB-relevant, non-CB-relevant and CB-internal planning items, specifically identified in the T2S Programme Plan.

5.1.1 CB-relevant planning items

These are planning items (e.g. deliverables, milestones and processes) affecting, or being affected by the Contracting CBs.

- Deliverables are CB-relevant if the Contracting CB is:
 - the assignee;
 - the addressee;
 - the reviewer; or
 - being consulted.
- Meetings, workshops are CB-relevant when:
 - the Contracting CB is participating (e.g. NECSG, PMG, AG, Sub Groups); or
 - feedback is expected on specific topics (e.g. planning workshops)
- Programme phases, activities and tasks are CB-relevant when the Contracting CB is involved as an actor, e.g. as a reviewer or an observer.
- Programme phases, activities and tasks affecting the successful and timely completion of the Synchronisation Points.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

The Eurosystem will provide status reporting on these items in the PMG. Contracting CBs can review/analyse, discuss, and envisage alternative solutions for these items.

5.1.2 Non CB-relevant planning items

These are planning items (e.g. deliverables, milestones and processes) that do not require any Contracting CB involvement. The T2S Programme Plan does not present the details of activities or steps leading to a deliverable, but it provides milestones and summary tasks to ease plan readability.

Some examples for these items:

- Internal Eurosystem activities or deliverables not impacting the critical path or the delivery of a Contracting CB deliverable (e.g. Internal Detailed Functional Specifications, Internal development process);
- predecessor of processes highlighted above (all the tasks preparatory to the deliverables, e.g. information security preparatory work related to the deliverable ‘risk assessment’); and
- independent processes (e.g. Internal Eurosystem governance).

The Eurosystem shall provide a status reporting and information on planning items that are not CB-relevant that are in the Operational Plan. However, Contracting CBs do not analyse and propose alternative solutions for these planning items.

5.1.3 Internal CB planning items

The T2S Programme Plan presents the main dependencies, relating to the completion process for specific milestones, called *Synchronisation Points*. Since Contracting CBs may be ready at various points in time, the T2S Programme Plan only presents the ultimate deadline before a delay could affect the critical path.

In the context of the monitoring of client readiness, Contracting CBs report progress on these items to their relationship manager, who in turn reports to the PMG. These items are under management responsibility of the Contracting CB. Therefore, the Eurosystem does not analyse or propose alternative solutions for these items.

5.2 T2S Programme Plan Views

The Eurosystem ensures the synchronisation of three different views of the T2S Programme Plan:

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

- the T2S Detailed Plan, which presents the most detailed level and is to be used as reference to support detailed discussions when issues arise at the level of the T2S Operational Plan;
- the T2S Operational Plan, which forms the baseline subject to monitoring at PMG level;
- the T2S Executive Summary Plan, which is the plan communicated externally and which contains the most important dates of the T2S Programme Plan.

The Eurosystem produces an initial version of the plans in June of each year. The Eurosystem reviews the draft plans with Contracting CBs, wherever CB-relevant, in order to deliver an agreed T2S Operational Plan in September following the process described in Section 7 of the present Schedule.

5.2.1 T2S Detailed Plan

The T2S Detailed Plan provides for the T2S Programme the accurate and detailed planning for all deliverables and activities, relevant for Contracting CBs as well as selected deliverables, milestones and activities not CB-relevant or CB-internal to ease readability. It also provides the necessary details until the end of the project, bearing in mind that the accuracy of the information decrease with time. The purpose of the T2S Detailed Plan is to provide the single point of reference and to support discussion within the PMG when the T2S Operational Plan does not provide sufficient detail.

The Eurosystem produces an updated version of this plan in June. The Eurosystem reviews a draft T2S Detailed Plan with Contracting CBs, wherever CB-relevant, to support the delivery of the T2S Operational Plan in September.

The T2S Detailed Plan specifies:

- all CB-relevant deliverables, milestones and activities (flagged as “CB-relevant”);
- selected deliverables, milestones and tasks that are not-CB-relevant or CB-internal, but required for the understanding of the plan and for a global overview of the programme;
- the synchronisation points for the monitoring of client readiness for Contracting CSDs and Contracting CBs; and
- a Schedule of meetings and workshops, requiring the participation of Contracting CSDs and/or Contracting CBs.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

The T2S Programme Office provides updates of this plan as references to support the bilateral meetings for monitoring of client readiness (MCR) and the meetings of the PMG.

Should a regular update relate to an internal Eurosystem activity (4CB or ECB) and have no impact on the T2S Operational Plan (e.g. critical path, readiness; review period, etc.), the Eurosystem amends the T2S Detailed Plan, without prior discussion at PMG level.

5.2.2 T2S Operational Plan (One-Year Rolling)

The T2S Operational Plan aggregates the detail of the T2S Detailed Plan for one calendar year, including all tasks starting and/or finishing in that year. It also provides summary tasks and activities for the subsequent years until completion of the programme. This plan forms the baseline and is the basis for the reporting of the T2S Programme status. The purpose of the T2S Operational plan is:

- to coordinate the activities and interactions on deliverables between the Eurosystem and Contracting CBs;
- to enable Contracting CBs to develop and to monitor their own internal plans for T2S and to determine their resource requirements; and
- to support Contracting CBs in performing their own assessment of the progress of the T2S Programme.

The T2S Operational Plan specifies for the one calendar year:

- all major deliverables, dependencies, milestones and aggregated tasks ;
- whether a planning item is CB-relevant;
- the synchronisation point for the monitoring of client readiness for Contracting CSDs and Contracting CBs; and
- a summary task of the period of time requiring the participation of Contracting CSDs and/or Contracting CBs.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

The Eurosystem provides updates of this plan to support the meetings for monitoring of client readiness and the meetings of the PMG. If a planning update affects another party (in the larger sense: readiness with external provider, review period, dependency Eurosystem, Contracting CSDs and Contracting CBs etc...) or influences the critical path, focussed information will be provided, including the explanation of the issue, the impact analysis and whenever relevant, the presentation of alternative solutions to be envisaged.

5.2.3 T2S Executive Summary Plan

The T2S Executive Summary Plan documents the milestones, synchronisation points and the duration of activities for the major deliverables and phases of the T2S Programme in order to provide a high-level summary view of the T2S Programme Plan.

5.3 T2S Critical Path

The critical path is the sequence of activities/tasks with the longest overall duration, determining the shortest time possible to complete the programme.

The T2S Detailed Plan documents the critical path for the Eurosystem activities and includes some external dependencies such as activities of Contracting CBs. Building the critical path for external dependencies requires a series of assumptions, as the plan cannot reflect detailed dependencies with each Contracting CB. The Eurosystem provides all such assumptions (Annex 4 to this Schedule) when providing the T2S Detailed Plan. The T2S Detailed and T2S Operational Plan highlights (MS Project) the tasks belonging at the critical path in red. The critical path may change because of updates of the T2S Detailed Plan.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

6 Monitoring frameworks

The next sections define supporting materials and the methodology followed to assess progress and report the risks and issues.

Section 7 describes the underlying process.

6.1 T2S Programme Status Assessment Framework

6.1.1 Objectives and Scope

The Eurosystem establishes a T2S Programme status assessment framework. The objectives of the framework are:

- Organise regular reporting to all parties to this Agreement at the various levels of governance about the progress of the T2S Programme against the T2S Operational Plan;
- to enable proper monitoring by providing a status report;
- to facilitate the coordination of activities and interactions on deliverables between the Eurosystem and the Contracting CBs; and
- to ensure that possible plan deviations against the Operational Plan are identified, discussed and addressed in a timely and appropriate manner.

In regularly scheduled (multilateral) assessment meetings with Contracting CBs, the Eurosystem reports on the progress against the T2S Operational Plan. Contracting CBs report their progress on deliverables pertaining to synchronisation points on a bilateral basis as part of the monitoring of client readiness.

6.1.2 Key Element of Programme Status Assessment and Monitoring

The process description for programme assessment and monitoring is Annex 5 to this Schedule.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

6.1.2.1 T2S Progress Dashboard

The T2S Programme WBS specifies the structure of the dashboard template, presented in Annex 5 and 6 to this Schedule. Using the WBS, the T2S dashboard presents a high-level overview of the progress achieved and the overall risk situation for the main streams of the programme (aggregation of activities and deliverables at work stream level).

The T2S Progress Dashboard presents the following elements:

- status, with colour coding;
- change (for status), compared to previous report;
- trend, expected in the next report;
- risk, with colour coding; and
- change, (for risk) compared to previous report.

6.1.2.2 T2S Programme Status Report

The Eurosystem provides a T2S Programme Status. The T2S Programme Status Report includes:

- the high-level T2S Progress Dashboard, as described in the previous Section;
- per work stream a status assessment for each CB-relevant deliverable with a status “green”, “yellow” or “red”;
- per work stream a detailed status assessment for each CB-relevant deliverable with a status “yellow” or “red”;
- per work stream a risk assessment for each CB-relevant deliverable. A detailed risk assessment is provided in case the risk criticality is “yellow” or “red”; and
- per work stream an issue description (incl. a response plan) for each issue pertaining to a CB-relevant Deliverable, in case a risk has materialised.

6.1.2.3 Conventions

The Eurosystem prepares a programme status assessment for each Deliverable, using colour coding (Green/Yellow/Red). This assessment evaluates the status of a Deliverable based on time, quality and scope.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

A specific colour, based on a three colours scheme, specifies the progress:

Colour	Description
Green	Deliverable is within the required scope and quality and is on time
Yellow	Deliverable will not have the required scope, will be delayed and/or not of the required quality if no corrective measures are taken
Red	Corrective measures have not delivered the expected effect or no corrective measures are possible. Deliverable will be delayed to achieve the required quality or scope if no extraordinary action is taken and requires escalation as described in section 7.2.

In addition to the colour reported for the progress assessment, the reporting of the Deliverable shows:

- the change from the previous progress assessment; and
- the expected trend for the next monitoring period.

The T2S Programme Status Report provides detailed information for each activity or Deliverable with a “yellow” or “red” status, including:

- the list of achievements;
- when relevant, the list of milestones missed or delayed; and
- the list of mitigating actions already started or envisaged to manage the situation.

6.2 T2S Risk and Issue Management and Monitoring Framework

6.2.1 Definitions, Scope and Objectives

The Eurosystem establishes a T2S Risk and Issue Management and Reporting Framework as comprehensive tool for the handling of risks and issues. The term ‘risk’ refers to a ‘threat’ to the successful delivery of the T2S Programme. The framework does not track and manage ‘opportunities’. ‘Issues’ define materialised risks.

The objectives of the framework that all parties to this Agreement are to follow are:

- to identify, manage and monitor risks and issues, potentially affecting the successful delivery of the T2S Programme;
- to inform and discuss between all parties to this Agreement in case of risks/issues, which may

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

potentially impact T2S Operational Plan;

- to ensure that potential risks are addressed in a timely and appropriate manner; and
- to ensure that planning issues are identified, discussed and addressed in a timely and appropriate manner.

6.2.2 Principles

The T2S Risk and Issue Management and Reporting Framework covers all risks, which may materialise during the programme's lifetime (i.e. from today until 'start operation') and all identified issues. The framework also foresees for each risk a root cause analysis, which identifies the underlying cause leading to the risk. The assumption is that one root cause will exist for each risk.

The assessment of programme risks applies a common grading scale for probability and impact. A probability/impact matrix is then applied to determine the criticality zone each risk is allocated to. The actual risk situation (reflecting the status of implementation of mitigation measures) is decisive for assessing the criticality.

The parties to this Agreement shall report:

- risks and the related risk response strategy as soon as possible following the formal risk assessment; and
- issues as soon as possible after their identification.

6.2.3 Risk and Issue Identification and Registration

All parties to this Agreement ensure that the appropriate risk and issue management functions as well as operational processes are in place for the registration of identified risks and issues, potentially affecting the various programme deliverables and milestones. All parties to this Agreement commit to share risks and issues in the appropriate forums, as defined hereafter in the Sections "T2S Monitoring of Client Readiness Framework" and "Processes".

6.2.4 Risk Assessment

The party to this Agreement identifying a risk (risk owner) shall evaluate the risk, based on:

- the impact on the T2S Programme; and

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

- the probability of the risk materialising.

6.2.4.1 Risk Impact Grading Scale

The T2S Risk and Issue Management Framework applies a five-level impact grading scale:

		Impact				
		5 Very Severe	4 Major	3 Significant	2 Low	1 Negligible
Project Objective	Scope	Project end item is effectively useless	Scope change unacceptable	Major areas of scope affected	Minor areas of scope affected	Scope impact barely noticeable
	Quality	Project end item is effectively useless	Quality reduction unacceptable	Quality reduction requires an approval	Only very demanding applications are affected	Quality degradation barely noticeable
	Cost	> 10 M euros	1M – 10M euros	100,000 – 1M euros	10,000 – 100,000 euros	<10,000 euros
	Time ³	> 20% time increase	10 - 20% time increase	5 - 10% time increase	1 - 5% time increase	< 1% time increase

Figure 1: Risk Impact Grading Scale

The programme objectives scope, quality, cost and time are the basis for evaluating the risk impact, following the international standard Project Management Book of Knowledge (PMBOK) with the exception of the cost dimension. The use of this standard facilitates the assessment of the risk by determining the effect of the materialisation of an identified risk on each project objective. The highest category of the risk's impact on a project objective defines the overall impact of the risk.

³ The percentages are calculated against the overall project duration.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

6.2.4.2 Risk Probability Grading Scale

The T2S Risk and Issue Management Framework applies a five-level probability grading scale.

Risk Probability				
1 Very Unlikely	2 Unlikely	3 Possible	4 Likely	5 Almost Certain

Figure 2: Risk Probability Grading Scale

The description of the risk probability level uses a percentage to classify the risk according to a probability that it materialises. When possible, the assessment of the probability of a risk eventuating is based on comparable large-scale programmes. However, the experience of management in similar programmes and projects and the experience in operating in similar complex environments and organisations are also factors in determining the probability for common risk programme risks.

6.2.4.3 Probability-Impact Matrix

The impact of a T2S-related risk and the probability of occurring determine its level of criticality. The T2S Programme uses the following probability/impact matrix for determining the criticality of a risk according to a three colour scheme.

Impact	5	Red	Red	Red	Red	Red
	4	Yellow	Yellow	Red	Red	Red
	3	Green	Yellow	Yellow	Yellow	Yellow
	2	Green	Green	Green	Green	Yellow
	1	Green	Green	Green	Green	Green
		1	2	3	4	5
Probability						

Figure 3: Probability-Impact Matrix

- The intersection between the impact of the risk and its probability in the matrix specifies the level of criticality of a risk to the T2S Programme (labelled with the colours green, yellow

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

and red). The level of criticality determines on how the risk is managed.

In case the criticality level of a work stream for which several risks have been identified needs to be determined, the most severe risk determines the criticality level of the entire work stream.

6.2.5 Risk Tolerance Policy

The T2S Programme risk tolerance policy defines the level of programme risk that the ECB (ESCB/Eurosystem) is prepared to accept. The T2S Programme risk tolerance policy stipulates that the criticality of a risk and determines the body responsible for accepting a non-mitigated risk. The framework considers risks allocated to the green criticality level as accepted ex ante. All risks allocated beyond the tolerated level, i.e. those in the yellow and red zone, are subject to further risk management measures. Risks allocated to the red zone have the highest priority for mitigation.

6.2.6 Risk Response Plan

Risk response plans address identified T2S risks. Unless exempted by the confidentiality rules, the PMG monitors the implementation of the risk response plan, as indicated in the risk identification form, based on status reports received from the risk owners. The T2S Programme Office informs the Steering Level of the status of mitigation via the regular status reports. In case the risk has been reported to the other parties to this Agreement, the respective status information is provided in the (multilateral) monitoring meetings as defined hereafter in the Sections “T2S Monitoring of Client Readiness Framework” and “Processes”.

6.2.7 Issue Response Plan

Issue Response Plans address identified issues affecting the successfully delivery of T2S. The implementation of the issue response plan and sharing of information on issues is analogous to the process for risk response plans.

6.2.8 Risk/Issue Reporting

Based on the information received via the risk/issue notification forms, the Eurosystem registers each identified risk/issue. A risk/issue sheet provides high-level information on the risk/issue and its background and forms part of the T2S Programme Status Report.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

6.3 T2S Monitoring of Client Readiness Framework

6.3.1 Definitions, Objectives and Scope

In the context of this Schedule, Client Readiness is defined as the capability of a Contracting CB (and their respective communities - including DCAH) to fulfil the legal, functional, technical and organisational requirements (i.e. all showstopper are resolved) to start operation in T2S relative to the synchronisation points (CB-relevant milestones), as specified in the T2S Programme Plan.

The term Monitoring of Client Readiness (MCR) defines the framework to ascertain the readiness of a Contracting CB (and their respective communities- including DCAH) to start operation in T2S based on the Contracting CBs' progress against the agreed milestones and deliverables of the T2S Operational Plan for the current phase of the T2S Programme. As a component of T2S Programme Planning and Monitoring, the parties to this Agreement agree to establish such a framework to allow the Eurosystem to monitor the readiness status of Contracting CBs to start operation with T2S.

The objectives of the MCR Framework are:

- to ensure accurate reporting on the progress of a Contracting CB regarding its readiness level relative to the T2S Programme Plan;
- to establish the necessary collaborative measures, rules, procedures and tools to support the monitoring process; and
- to foster the communication between individual Contracting CBs and the Eurosystem on programme-plan-related issues, with a view to ensure timely and proactive identification and notification of any event that would have a material effect on the T2S Programme Plan and the start operation of T2S.

The scope of the MCR includes activities that the Contracting CBs and their communities (including DCAH) must undertake to ensure the required readiness level relative to the T2S Operational Plan and to the successful and timely completion of the Synchronisation Points.

MCR covers all phases of the T2S Programme until start of full operation of T2S with the successful implementation of the last of the planned migration waves. It also includes the monitoring of and reporting on the readiness of the Contracting CB clients, indirectly and directly connected to T2S. It should be noted that the Contracting CBs are responsible for tracking their own community (including DCAH) and accurately reporting to the Eurosystem.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

MCR encompasses the following activities:

- the monitoring of the fulfilment of the mutual obligations, milestones and deliverables;
- the monitoring and review of the mutual obligations in regular intervals and for individual periods, as bilaterally agreed, to ascertain their status as compared to the T2S Programme Plan; and
- the identification and notification of delays or any event affecting the successful and timely completion of the Synchronisation Points.

6.3.2 Monitoring of Client Readiness and Reporting

6.3.2.1 Principles

Gathering client readiness relevant information from the Contracting CB and comparing the Contracting CB's adaptation and migration plan to the overall T2S Programme Plan ensures that all Contracting CBs consistently and jointly progress towards a successful start operation in T2S. At the synchronisation points, the parties to this Agreement can assess whether they remain aligned with the T2S Programme Plan. MCR identifies risks (incl. potential mitigation measures) as well as issues (incl. response plans), which potentially affect the Eurosystem, Contracting CSDs or Contracting CBs or the successful start operation of T2S. Between synchronisation points, the Contracting CBs and the Eurosystem collaborate closely to support each other in the timely achievement of the relevant assessments, deliverables and milestones.

The parties to this Agreement agree to meet bilaterally to review, assess and discuss the Contracting CB's progress at least once per synchronisation point, based on agreed assessment criteria and status reporting methodology of this Schedule. Contracting CBs agree to report for readiness monitoring:

- the progress against their adaptation plan and status of their deliverables; and
- their risks and issues pertaining to their adaptation and affecting the successful completion of synchronisation points.

6.3.2.2 Periodicity

The periodicity of meetings is dependent on the phase of the T2S Programme. Meetings will occur:

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

- on a quarterly basis from the signature of the CPA until the start of the User Testing;
- on a monthly basis from the start of User Testing; and
- on an ad hoc basis when requested by one of the parties to this Agreement.

6.3.2.3 Organisation

MCR includes all Contracting CBs participating in the T2S Programme. The Eurosystem monitors actively the degree of client readiness and asks the Contracting CBs for regular monitoring of the status of the different activities and of the preparedness level of their communities (including DCAH).

The Eurosystem monitors Client Readiness at three levels:

- The first level of monitoring is at the operational level of the client relationship management, with support provided by the other functions of the T2S Programme. The formal communication and exchange of information between the Contracting CB and the T2S Programme Office takes place by means of (a) written submissions or (b) bilateral meetings between representatives of the Contracting CB and representatives of the T2S Programme. Aiming at ensuring an efficient and effective communication, a Contracting CB has a single person of contact within the client relationship area of the T2S Programme. The role of the single person of contact is to bundle the issues, comments and questions of the Contracting CB, to coordinate and align these issues, comments and questions with other Contracting CSDs and Contracting CBs and to ensure final response and implementation;
- The second level of monitoring of client readiness is at the level of the PMG, which looks for common alternatives to resolve issues causing a delay or a risk of delay to a synchronisation point; and
- The third level of client readiness monitoring is at the Steering Level.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

6.3.3 Client Readiness Reporting

The Eurosystem regularly reports on the overall Client Readiness (Contracting CSDs and Contracting CBs) as part of the programme status assessment and discusses the status with the Contracting CBs in multilateral meetings. The status of a specific Contracting CB in the context of MCR is subject to the confidentiality and transparency rules (see Section 6.3.4). The Eurosystem intends to publish aggregated client readiness-relevant information on a regular basis to provide a summary of the T2S readiness status covering the entire community (including DCAH). The Eurosystem reviews this assessment with the Contracting CBs prior to publication.

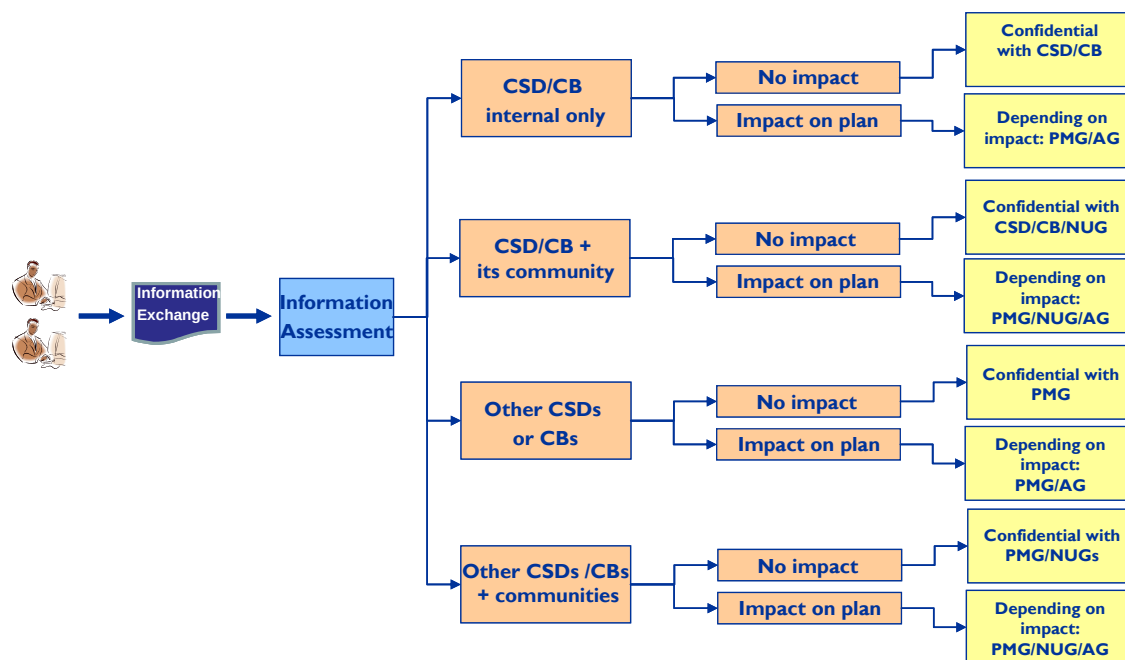
6.3.4 Confidentiality and Transparency Rules

The Eurosystem is committed to full transparency regarding T2S. T2S communication on client readiness addresses a wide spectrum of recipients, comprising individual Contracting CBs, various T2S governance bodies and the public.

Full transparency does not preclude confidentiality. As a matter of principle, and as reflected in the business rules below, Contracting CB readiness status and internal issues, discussed in the MCR bilateral meetings, remain confidential unless they affect the overall readiness, other Contracting CBs, the T2S Programme organisation and/or the T2S business case. Communication of any other topics to a third party shall require prior written mutual consent. The business rules, which govern the confidentiality versus transparency dimensions, are set out below:

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring



547

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

7 Processes

The below processes only cover topics related to Schedule 2; therefore, the process actors' roles, as described below, are only applicable to the Schedule 2 topics and should not be read as a limitation to their roles in other topics of the CPA.

7.1 Methodology and Conventions

The T2S monitoring process is represented in a diagram and supported by a high-level process description.

Individual sub-processes are described, but not supported by business diagrams.

There is no specific section to describe the individual activities, decision points or business rules.

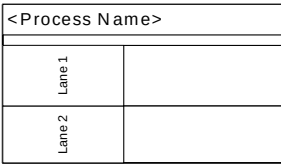
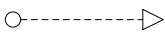
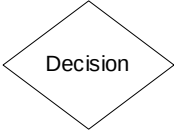
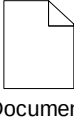
Likewise, the adaptation process for Schedule 2 Annexes is represented in a diagram and supported by a high-level process description.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

7.1.1 Standards

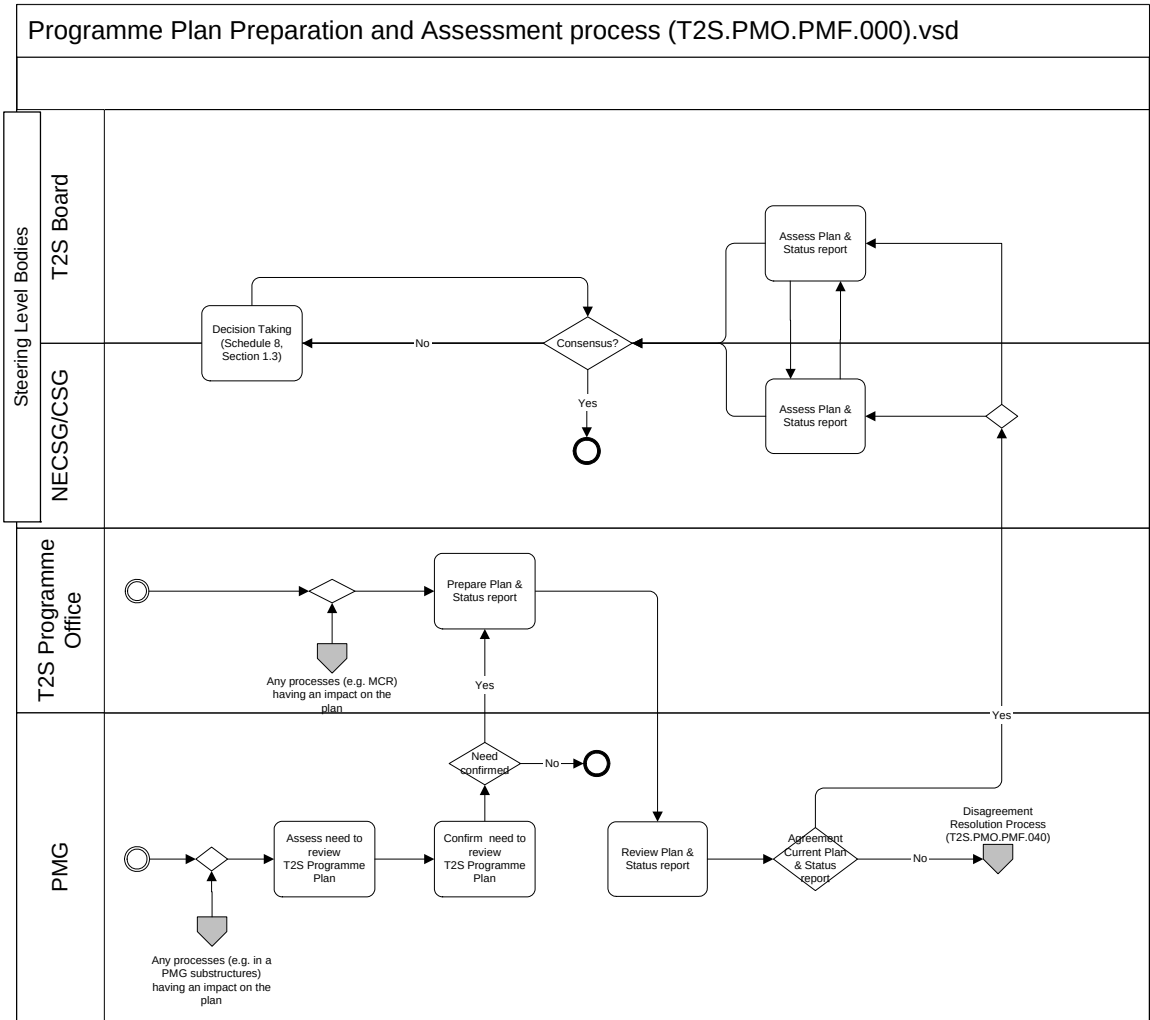
The document uses a simplified version of the Business Process Modelling Notation (BPMN) 2.0 notation, as documented below.

Convention	Description
	Pools (Participants) and lanes represent responsibilities of a business actor for activities in a process. A pool or a lane can be an organization, a role, or a system. Lanes may subdivide pools or other lanes hierarchically.
	This symbol represents the starting point for a process.
	This symbol represents the termination of a process.
	An Activity is a unit of work or action.
	This symbol defines the execution order of activities.
	This symbol defines an indirect execution of activity (e.g. sending/exchange of information).
	This symbol represents a decision, resulting in the triggering of different activities. It typically follows an activity.
	Gateway, used to ease the readability of the flow transfers
	A Data Object represents information flowing through the process, such as business documents, e-mails, or letters
	Indicates reference to an external process not described in the current business process map

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

7.2 Programme Plan Preparation, Adaptation and Assessment Review Process



Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

568 7.2.1 Process Actors and their Roles

Process Actor		Process Role
T2S Programme Office		The T2S Programme Office is responsible for collecting information from the Eurosystem, Contracting CSDs and Contracting CBs in order to prepare for PMG and Steering Level review: ▪ An updated T2S Programme Plan; ▪ A Programme Status Report (including progress, risks and issues). The T2S Programme Office sends the relevant information (T2S Programme Plan and Programme Status Report) to the PMG, at least 1 week before PMG meetings. The T2S Programme Office is responsible for organising and chairing the PMG meetings.
PMG		In this process, the PMG is responsible for : • Assessing and agreeing on the updates of the T2S Operational Plan • Assessing and agreeing on the T2S Programme status report. Its responsibility is to analyse the plan and the reporting packages, propose improvements or changes, and highlight risks and issues. When alternatives for solving an issue exist, the PMG will assess them and propose the best way forward. It is the responsibility of the PMG to act pro-actively and in good faith to try to achieve agreement between PMG members.
NECSG		The NECSG is responsible for assessing the programme plan and programme status, taking into account the recommendations supplied by the PMG and taking all necessary steps to reach a consensus at Steering Level.
T2S Board		The T2S Board is responsible for assessing the programme plan and programme status, taking into account the recommendations supplied by the PMG and taking all necessary steps to reach a consensus at Steering Level. The T2S Board also coordinates the work at Steering Level to reach a consensus following the process described in Schedule 8, Section 1.3.

569

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

7.2.2 High-Level Process Description

This section provides an overview of the process to monitor the T2S Programme Plan. This includes progress and risk reporting, and adaptation to the plan. This process encompasses the ongoing monitoring of the programme by the different actors. It applies to production of the programme status reports and to updates of the plan. It may also result in changes to the different supporting documents, e.g. to document changes in planning assumptions. This process does not apply to changing the layouts of plans and supporting documents, as described in the Annexes of this Schedule 2. Such changes follow the process for the adaptation of Schedules described in section 7.3.

The T2S Programme Office collects information from the Eurosystem, Contracting CSDs and Contracting CBs for plan updates and status reporting.

Based on the information received, the T2S Programme Office updates the T2S Operational Plan, prepares a Programme status reports.

When applicable, the T2S Programme Office prepares presentations on changes, impacts and alternative solutions.

The T2S Programme Office sends the various plans and the programme status report to the PMG at least one week before the meeting.

The T2S Programme office presents the overall programme plan and status during the PMG sessions for review and discussion.

Once the PMG has reviewed and agreed on the T2S Operational Plan and status reports, it forwards the plan and status reports to the Steering Level for endorsement. The T2S Board coordinates the work at Steering Level to reach a consensus following the process described in Schedule 8, Section 1.3.

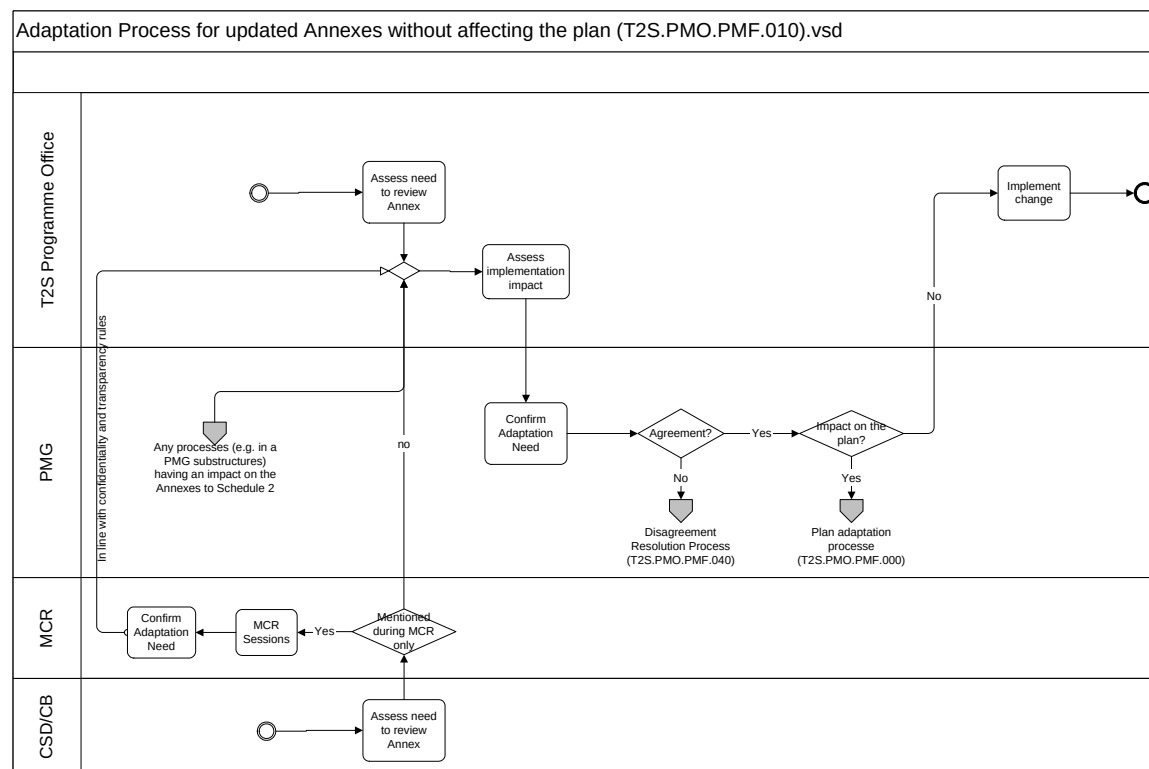
In case of disagreement on the implementation, the PMG may initiate the PMG disagreement resolution process in order to seek for guidance from the Steering Level.

The PMG meets at least quarterly or as agreed with the PMG members.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

7.3 Adaptation Process for updated Annexes without affecting the plan:



7.3.1 Process Actors and their Roles

Process Actor	Process Role
T2S Programme Office	The T2S Programme Office is responsible for: - identifying and raising adaptation requests; - collecting adaptation requests; - undertaking the impact assessment for the requested adaptation; - communicating the results of the impact analysis to the PMG; and - implementing the adaptation in the applicable processes and templates.
CB	The Contracting CBs are responsible identifying and raising adaptation requests, if relevant.
Monitoring of Client Readiness	The MCR is responsible for providing information on the reasons for the adaptation request to the T2S Programme Office to allow for an impact assessment.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

PMG	In this process, the PMG is responsible for: ▪ reviewing and discussing the adaptation requests; ▪ confirming the need of the adaptation or rejecting the request to the Steering Level; and ▪ escalating Disagreement on adaptation request to the Steering Level.

7.3.2 High Level Process Description

This section provides a process to adapt the Annexes to the present Schedule that do not affect the plan over time in a controlled way. This process is valid to change the layout of the plan and of the supporting documentation, but it does not apply for changing the plan (e.g. the Eurosystem and/or CBs may wish to review the Annexes to Schedule 2 of this CPA in order to improve reporting). Adaptations approved at Steering Level, do not need to go through this procedure, and should be directly implemented.

The T2S Programme Office and/or CBs may wish to change an Annex.

The T2S Programme Office collects the change(s) request. Thereafter, the T2S Programme Office assesses the change(s) request. The PMG reviews the change(s) request together with the T2S Programme Office assessment.

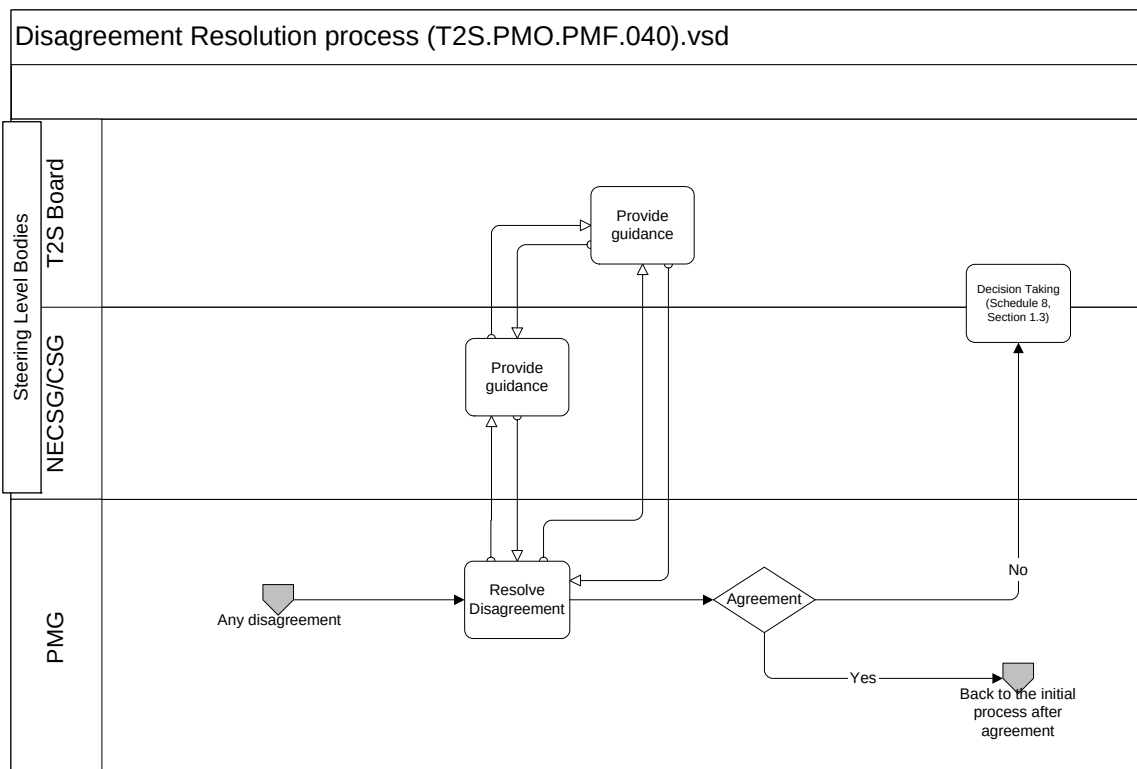
After agreement on the change(s) at PMG level, the T2S Programme Office implements the change(s).

In case of disagreement, the PMG may initiate the disagreement resolution process to get agreement on the proposed change(s).

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

7.4 Disagreement Resolution process



7.4.1 Process Actors and their Roles

Process Actor	Process Role
PMG	The PMG is responsible for taking all necessary actions to solve the disagreement.
NECSG	The NECSG is responsible for discussing with T2S Board any disagreement escalated by the PMG and for providing guidance to the PMG. In case of outstanding disagreement after escalation at PMG level, the NECSG takes all necessary steps to reach a consensus at Steering Level.
T2S Board	The T2S Board is responsible for discussing with NECSG any disagreement escalated by the PMG and for providing guidance to the PMG. In case of outstanding disagreement after escalation at PMG level, the T2S Board coordinates the work at Steering Level to reach a consensus following the process described in Schedule 8, Section 1.3.

Currency Participation Agreement

Schedule 2 – T2S Programme Planning and Monitoring

7.4.2 High Level Process Description

This Section describes the process to be followed in case of disagreement within the PMG.

In case of disagreement within the PMG, the PMG escalates to the Steering Level for guidance on how to mitigate the disagreement.

The Steering Level discussed the escalated issue in view of providing guidance to the PMG.

The Parties should aim to conducting the process of resolving disagreements within 2 weeks.

In case of outstanding disagreement after escalation at PMG level, the T2S Board coordinates the work at Steering Level to reach a consensus following the process described in Schedule 8, Section 1.3, before a potential escalation.

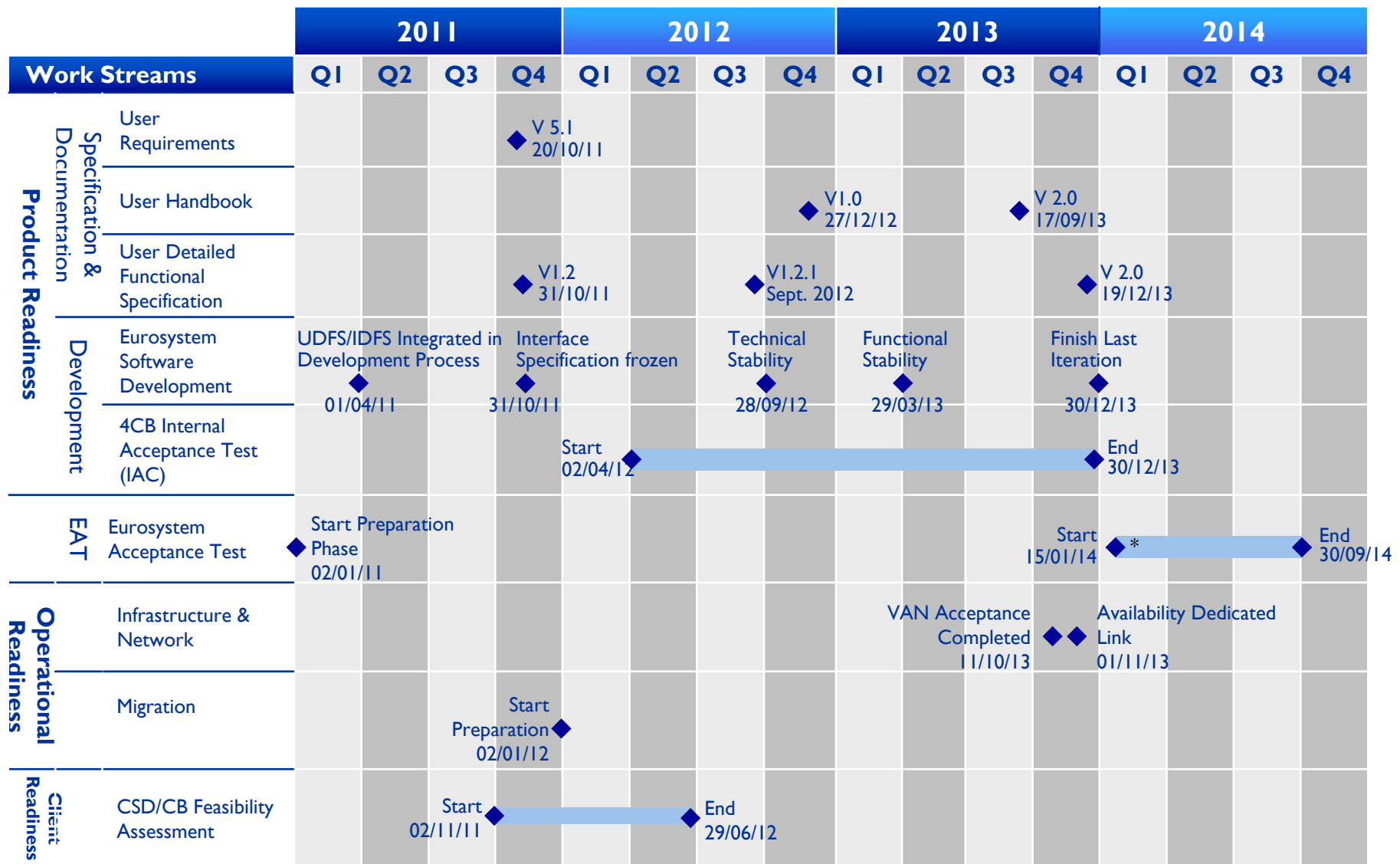
CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 2 – ANNEX 1

T2S EXECUTIVE SUMMARY PLAN

Executive Summary Plan

T2S Executive Summary Plan



* Including buffer

T2S Executive Summary Plan

		2014				2015				2016				2017
Work Streams		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Client Readiness	Pilot Testing		Start** JUL 2014	End SEP 2014										
	User Testing Wave I			Start** OCT 2014			End JUN 2015							
	User Testing (Remaining Waves 2-3)			OCT 2014								JUN 2016		
Operational Readiness	Infrastructure & Network					Production Environment Ready Mar 2015								
	Phased Migration until Contingency Wave						JUN 2015 Go-live wave I 22/06/15						Go-Live Contingency Wave JAN 2017 18 months after wave I	

** For simplicity reasons, connectivity's activities which could be performed prior to the start do not appear on this plan view

Client Readiness Tracking Synchronisation Points 1

	2011				2012				2013				2014			
Synchronisation Points	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
SP1 - Start Feasibility Confirmed			20/12/11	◆												
SP2 - Feasibility Confirmation						10/08/12	◆									
SP3 – T2S Programme Plan Comprehensiveness							17/12/12	◆								
SP4 - Network Providers Confirmed												24/04/14	◆			
SP5 - Eurosystem ready for EAT											15/01/14	◆				
SP6 - Eurosystem Ready for User Testing													02/09/14	◆		
SP7 - Start Connectivity Test													07/07/14	◆		
SP8 - Start Bilateral Interoperability Testing													01/10/14	◆		

Client Readiness Tracking Synchronisation Points 2

	2014				2015				2016				2017
Synchronisation Points	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
SP9 - Start Multilateral Interoperability Test (by Wave)			DEC 2014	◆				◆					
SP10 - Start Community Test (by Wave)				MAR 2015	◆			◆					
SP11 - Start Business Day Test (by Wave)					MAY 2015	◆			◆				
SP12 - End of User Testing (by Wave)					JUN 2015	◆			◆				
SP13 - Eurosystem Ready for Production (by Wave)			DEC 2014	◆					◆				
SP14 - Ready to Connect to Prod. Environment (by Wave)			FEB 2015	◆					◆				
SP15 - Ready to upload Static Data (by Wave)			APR 2015		◆				◆				
SP16 - Ready for Migration Weekend and Start Operations (by Wave)					JUN 2015	◆							Contingency Wave JAN 2017
SP17 - Closing of migration (after Contingency wave)												March 2017	◆



CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 2 – ANNEX 2

T2S OPERATIONAL PLAN

Disclaimer:

Planning is an ongoing process and Annexes with planning elements are subject to change during the lifetime of a project. Planning workshops with CSDs and CBs will continue to agree on the planning for Connectivity, User Testing and Migration. Subsequent plan updates follow the process, documented in the Schedule 2, Section 7.

Annexes 2, 3, 4, 7, 8, 9 and 10 document the planning status as at 7 Nov. 2011.

T2S Operational Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1
1	100	PRODUCT READINESS		1945d	Tue 01/04/08	Fri 02/10/15																										
2	500	SPECIFICATION AND DOCUMENTATION		1417d	Fri 28/11/08	Mon 19/05/14																										
3	1100	REQUIREMENTS		692d	Thu 26/03/09	Thu 17/11/11																										
35	16100	[Deliverable] - User Requirement Document (URD) 5.01		0d	Thu 17/11/11	Thu 17/11/11	Eurosystem	64 17/11/2011																								
36	18100	SPECIFICATIONS		1401d	Fri 28/11/08	Thu 24/04/14																										
37	18200	General Specification (GS)		1401d	Fri 28/11/08	Thu 24/04/14																										
45	26100	GS v. 2.0		257d	Wed 24/04/13	Thu 24/04/14																										
46	26200	Internal Eurosystem Preparation [General Specifications v. 2.0]		219d	Mon 10/06/13	Thu 17/04/14																										
55	34150	[Deliverable] - General Specification (GS) V. 2.0		0d	Wed 24/04/13	Wed 24/04/13	Eurosystem	51 24/04/2013																								
67	47100	General Functional Specifications (GFS)		1231d	Mon 19/01/09	Mon 14/10/13																										
81	60100	GFS 4.0 - aligned with URD 5.0		347d	Tue 02/02/10	Wed 01/06/11																										
99	74400	Feedback of the ECB T2S project team to the Market on GFS V4.0 13/04		15d	Mon 04/04/11	Fri 22/04/11	Eurosystem	4/2011 22/04/2011																								
101	74500	Delivery GFS Note		0d	Wed 01/06/11	Wed 01/06/11	Eurosystem	01/06/2011																								
102	73400	GFS 5.0		139d	Tue 02/04/13	Mon 14/10/13																										
103	73500	Internal Eurosystem Preparation [Production of the GFS V5.0]		134d	Tue 02/04/13	Mon 07/10/13																										
113	88150	[Deliverable] - General Function Specification (GFS) V 5.0		0d	Mon 14/10/13	Mon 14/10/13	Eurosystem	49 14/10/2013																								
132	155150	Internal Detailed Functional Specification (IDFS)		910d	Wed 16/12/09	Tue 18/06/13																										
133	156100	Settlement Algorithm Objectives Document		327d	Fri 15/01/10	Fri 15/04/11																										
148	165100	Production of IDFS		910d	Wed 16/12/09	Tue 18/06/13																										
156	172200	WS - Delivery IDFS V0.85 to the Development Coordination		0d	Tue 15/02/11	Tue 15/02/11	Eurosystem	15/02/2011																								
170	97100	User Detailed Functional Specifications (UDFS)		1300d	Thu 01/01/09	Tue 07/01/14																										
182	550200	Work on Messages Pillar I-III		1300d	Thu 01/01/09	Tue 07/01/14																										
183	105100	Message standardisation		1300d	Thu 01/01/09	Tue 07/01/14																										
194	116200	Production of UDFS V1.0, V1.1, V1.2 (in line with GFS V4.0)		560d	Mon 03/08/09	Fri 23/09/11																										
195	116300	Production of UDFS V1.0 [dialogue between T2S and Its users and detailed msg specification]		560d	Mon 03/08/09	Fri 23/09/11																										
231	190500	UDFS v1.0 - Messages		207.75d	Thu 01/04/10	Fri 14/01/11																										
232	190550	Pillar III (T2S specific messages)		207.75d	Thu 01/04/10	Fri 14/01/11																										
233	190580	Detailed T2S message specification, development and T2S documentation for UDFS		207.75d	Thu 01/04/10	Fri 14/01/11																										
239	192400	Production of first draft T2S customised schema files/documentation by 4CB		79.75d	Tue 28/09/10	Fri 14/01/11																										
241	134940	Validation of draft T2S customised files/docum. By SGMS (incl. Incorporation of		47d	Thu 11/11/10	Fri 14/01/11	SGMS	14/01/2011																								
242	190450	Validations of the version v0.3 to produce the UDFS V1.0		517d	Thu 01/10/09	Fri 23/09/11																										

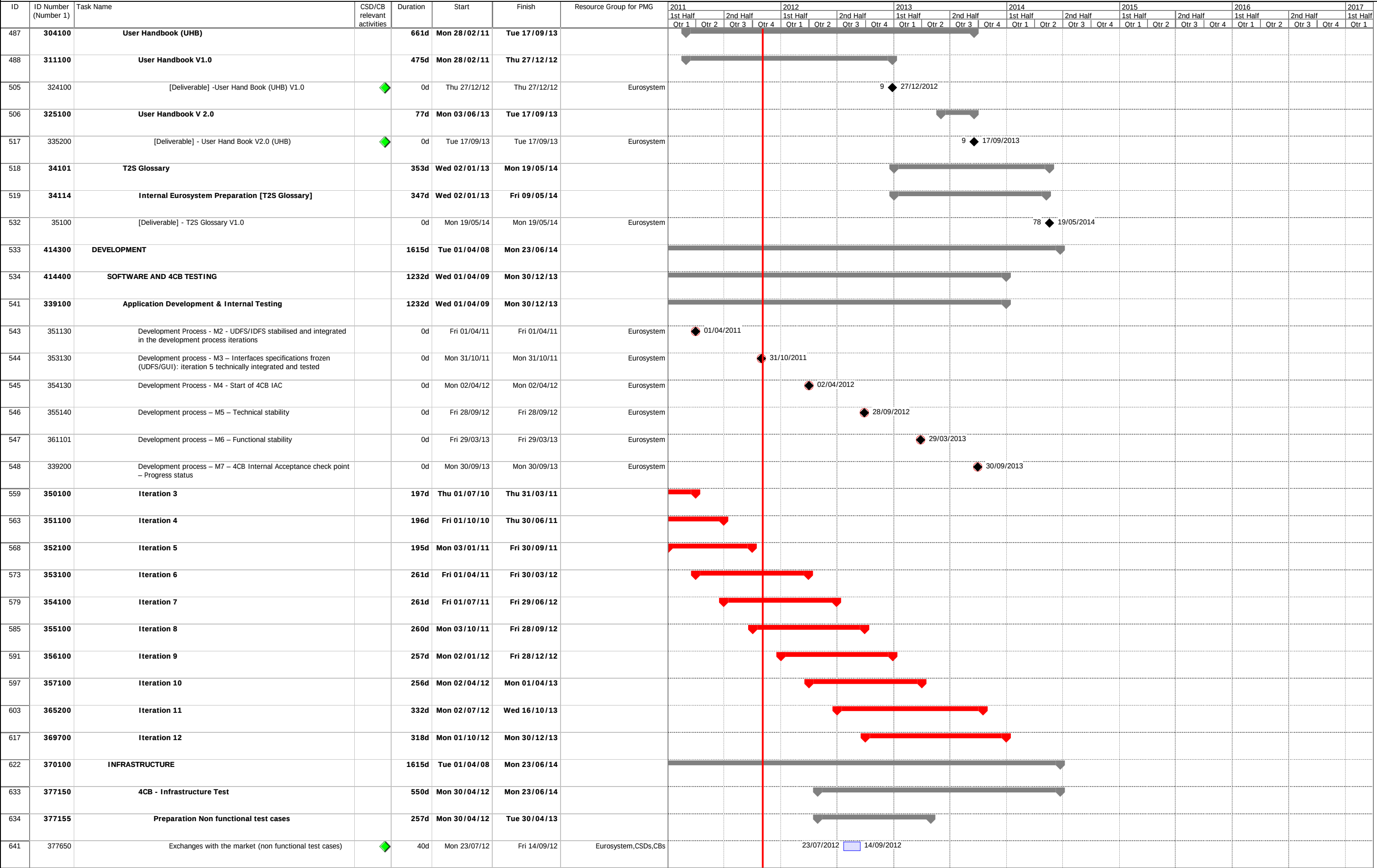
Task Task Critical Milestone Milestone Critical Task Project Summary Group By Summary

T2S Operational Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1
245	190470	ECB T2S programme Office /Market review of UDFS V0.3 (one month)		21d	Thu 30/12/10	Wed 26/01/11	Eurosystem																									
246	190490	Reception of consolidated ECB/Market feedback on UDFS v0.3 to FC		0d	Wed 26/01/11	Wed 26/01/11	Eurosystem																									
247	190560	Integration of PMC & ECB T2S Programme Office comments in v0.3 to produce the V1.0 of UDFS (1,5 month)		30d	Thu 27/01/11	Wed 09/03/11	Eurosystem																									
250	190700	Delivery of UDFS V1.0 to the Market by the ECB		1d	Fri 25/03/11	Fri 25/03/11	Eurosystem																									
251	190800	Validation of complete UDFS V1.0 by the Market		107d	Thu 10/03/11	Fri 05/08/11																										
254	195100	Feedback from the Market on the UDFS V1.0		45d	Mon 28/03/11	Fri 27/05/11	CSDs																									
256	196100	Consolidation of Market comments by the ECB		10d	Mon 30/05/11	Fri 10/06/11	Eurosystem																									
257	198100	Integration of Market comments in complete UDFS V1.0 (two months)		40d	Mon 13/06/11	Fri 05/08/11	Eurosystem																									
258	199100	Delivery to ECB T2S Programme Office of UDFS V1.1		0d	Fri 05/08/11	Fri 05/08/11	Eurosystem																									
259	199200	UDFS v1.2 - Messages		486d	Thu 01/10/09	Wed 10/08/11																										
260	134500	Pillar II (new standard)		288d	Thu 28/01/10	Fri 04/03/11																										
262	134570	Detailed T2S message specification and T2S documentation for UDFS		288d	Thu 28/01/10	Fri 04/03/11																										
263	134600	Customisation of draft ISO schema files (incl. definition of fields)/documentation,		288d	Thu 28/01/10	Fri 04/03/11																										
265	134670	Validation of draft T2S customised files/documentation by		288d	Thu 28/01/10	Fri 04/03/11	SGMS																									
266	124150	Final Validation Pillar II by the SGMS		0d	Fri 04/03/11	Fri 04/03/11	SGMS																									
267	134700	Pillar III (T2S specific messages)		486d	Thu 01/10/09	Wed 10/08/11																										
268	134730	Detailed T2S message specification, development and T2S documentation for UDFS		486d	Thu 01/10/09	Wed 10/08/11																										
269	134770	Creation of HLBR by 4CB for delivery to SWIFT; Validation by SGMS (as BVG)		371d	Thu 01/10/09	Wed 02/03/11																										
271	134830	SGMS Validate the HLBR (incl. Incorporation of comments by 4CB)		330d	Fri 27/11/09	Wed 02/03/11	SGMS																									
273	134900	Production of first draft T2S customised schema files/documentation by 4CB		100.75d	Wed 23/03/11	Wed 10/08/11																										
275	134950	Validation of draft T2S customised files/docum. By SGMS (incl. Incorporation		61d	Wed 18/05/11	Wed 10/08/11	SGMS																									
276	134150	Final Validation Pillar III by the SGMS		0d	Fri 01/07/11	Fri 01/07/11	SGMS																									
277	200100	Final validation of complete UDFS V1.1 by ECB T2S Programme Office		34d	Mon 08/08/11	Fri 23/09/11																										
288	211100	[Deliverable] - User Detailed Functional Specification (UDFS) V1.2		0d	Mon 31/10/11	Mon 31/10/11	Eurosystem																									
289	211200	Start feasibility study		0d	Wed 02/11/11	Wed 02/11/11	CSDs,CBs																									
290	211300	Production of UDFS V1.2.1 (CR and Architecture Issues)		290d	Mon 01/08/11	Fri 07/09/12																										
322	214800	[Deliverable] - User Detailed Functional Specification (UDFS) V1.2.1		0d	Fri 07/09/12	Fri 07/09/12	Eurosystem																									
323	215100	UDFS v 2.0		86d	Wed 21/08/13	Thu 19/12/13																										
326	217100	Validation and revision of UDFS v.2.0 after IAC		64d	Fri 20/09/13	Thu 19/12/13																										
327	217200	Internal Eurosystem Preparation [Validation and revision of UDFS v.2.0 after IAC]		62d	Fri 20/09/13	Tue 17/12/13																										
335	223150	[Deliverable] - UDFS v.2.0		0d	Thu 19/12/13	Thu 19/12/13	Eurosystem																									

	Task		Task		Critical Milestone		Milestone		Critical Task		Project Summary		Group By Summary	

T2S Operational Plan with Critical Path
31/10/2011



Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017	
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half	
								Otr 1	Otr 2	Otr 3	Otr 4	Otr 1	Otr 2	Otr 3	Otr 4	Otr 1	Otr 2	Otr 3	Otr 4	Otr 1	Otr 2	Otr 3	Otr 4	Otr 1	Otr 2	Otr 3	Otr 4	Otr 1	Otr 2	Otr 3	Otr 4	Otr 1	
648	380110	[Deliverable] - T2S Non-functional Testing Scenarios		0d	Wed 02/01/13	Wed 02/01/13	Eurosystem									111		02/01/2013															
651	380300	Execution Non functional test cases		214d	Tue 30/04/13	Mon 03/03/14																											
652	378101	Start Execution Infrastructure test		0d	Tue 30/04/13	Tue 30/04/13	Eurosystem																										
659	386100	[Deliverable] - Non Functional Testing Report		0d	Fri 28/02/14	Fri 28/02/14	Eurosystem																										
664	388100	EUROSYSTEM ACCEPTANCE TEST		1225d	Mon 03/01/11	Fri 02/10/15																											
665	389200	EAT PREPARATION		1225d	Mon 03/01/11	Fri 02/10/15																											
983	451300	[Deliverable] - CSDs Market specific test cases for EAT V1.0		0d	Thu 17/10/13	Thu 17/10/13	CSDs																										
984	451700	[Deliverable] - CBs Market specific test cases for EAT V1.0		0d	Thu 17/10/13	Thu 17/10/13	CBs																										
1045	451400	[Deliverable] - EAT Documentation V1.0 (EAT Test Sets)		0d	Thu 14/11/13	Thu 14/11/13	Eurosystem																										
1071	482300	EAT EXECUTION		265d	Mon 02/12/13	Mon 15/12/14																											
1074	485100	Execution Phase EAT Critical		236d	Wed 15/01/14	Fri 12/12/14																											
1075	464150	Synchronization Point [SP5: Start of Eurosystem Acceptance Test]		0d	Wed 15/01/14	Wed 15/01/14	Eurosystem																										
1076	486120	Start EAT - Eurosystem Acceptance Test (following the Entry Criteria)		0d	Wed 15/01/14	Wed 15/01/14	Eurosystem																										
1089	493130	[Deliverable] EAT Assessment Report		0d	Mon 01/09/14	Mon 01/09/14	Eurosystem																										
1090	493160	Go-no go decision with CSDs to start the User Testing		0d	Mon 15/09/14	Mon 15/09/14	T2SPB																										
1094	498100	EAT Status update (recurrent task during EAT phase until 1 month prior the start of UT)		23d	Wed 12/02/14	Fri 14/03/14																											
1099	451800	[Deliverable] - EAT Status update (recurrent task)		0d	Fri 14/03/14	Fri 14/03/14	Eurosystem																										
1194	524100	CLIENT READINESS		2134d	Mon 17/11/08	Mon 30/01/17																											
1195	524200	SYNCHRONISATION AND ON-BOARDING		2134d	Mon 17/11/08	Mon 30/01/17																											
1196	534200	CSD READINESS		1950d	Fri 31/07/09	Mon 30/01/17																											
1275	536000	CSDs Feasibility Assessment		280d	Mon 21/11/11	Mon 17/12/12																											
1276	536100	Preparation of impact assessment and adaptation plan by CSDs		160d	Mon 21/11/11	Fri 29/06/12	CSDs																										
1277	213100	[Deliverable] - CSD Feasibility Assessment		0d	Fri 29/06/12	Fri 29/06/12	CSDs																										
1281	214100	Synchronization Point [SP2 - Feasibility Confirmation by CSD/CB]		0d	Fri 10/08/12	Fri 10/08/12	Eurosystem																										
1284	553000	Update on CSD Feasibility Assessment		0d	Mon 17/12/12	Mon 17/12/12	CSDs																										
1285	553100	Synchronisation Point [SP3 - T2S Programme Plan Comprehensiveness]		0d	Mon 17/12/12	Mon 17/12/12	Eurosystem,CSD																										
1546	625200	Proof of Eligibility to Participate in T2S (Wave 1)		67d	Mon 10/11/14	Mon 16/02/15																											
1553	625600	[Deliverable] - Proof of Eligibility to Participate in T2S (Wave 1)		0d	Mon 19/01/15	Mon 19/01/15	CSDs																										
1556	625900	Proof of Eligibility to Participate in T2S (Wave 2)		67d	Mon 13/07/15	Tue 13/10/15																											
1563	626700	[Deliverable] - Proof of Eligibility to Participate in T2S (Wave 2)		0d	Tue 15/09/15	Tue 15/09/15	CSDs																										
1566	627000	Proof of Eligibility to Participate in T2S (Wave 3)		67d	Fri 01/01/16	Tue 29/03/16																											

T2S Operational Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017	
								1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	
1573	628000	[Deliverable] - Proof of Eligibility to Participate in T2S (Wave 3)	◆	0d	Thu 03/03/16	Thu 03/03/16	CSDs																										
1576	544100	CB READINESS		882d	Fri 31/07/09	Mon 17/12/12																											
1581	536300	CBs Feasibility Assessment		280d	Mon 21/11/11	Mon 17/12/12																											
1582	536310	Preparation of impact assessment and adaptation plan by CBs	◆	160d	Mon 21/11/11	Fri 29/06/12	CBs																										
1583	546500	[Deliverable] - CB Feasibility Assessment	◆	0d	Fri 29/06/12	Fri 29/06/12	CBs																										
1587	546600	Synchronization Point [SP2 - Feasibility Confirmation by CSD/CB]	◆	0d	Fri 10/08/12	Fri 10/08/12	Eurosystem																										
1590	553200	Update on CB Feasibility Assessment	◆	0d	Mon 17/12/12	Mon 17/12/12	CBs																										
1591	546800	Synchronisation Point [SP3 - T2S Programme Plan Comprehensiveness]	◆	0d	Mon 17/12/12	Mon 17/12/12	Eurosystem,CB																										
1633	516600	USER TRAINING AND TESTING		1953d	Fri 02/01/09	Wed 13/07/16																											
1634	555100	TRAINING PREPARATION		1119d	Mon 02/08/10	Mon 01/12/14																											
1635	556100	Preparation of the T2S Training Framework		480d	Mon 02/08/10	Thu 31/05/12																											
1645	558100	Training Framework Phase		436d	Thu 30/09/10	Thu 31/05/12																											
1654	559700	Consultation of Public Training Framework V0.1 with CSDs and CBs		35d	Mon 16/01/12	Fri 02/03/12																											
1655	559800	Delivery of Public Training Framework V0.1 to the CSDs and CBs for advice	◆	0d	Mon 16/01/12	Mon 16/01/12	Eurosystem																										
1656	559900	Feedback from CSDs and CBs on Public Training Framework v0.1	◆	20d	Mon 16/01/12	Fri 10/02/12	CSDs,CBs																										
1658	556500	Workshop with CSDs and CBs on Public Training Framework V0.1 (in case of need)	◆	1d	Fri 02/03/12	Fri 02/03/12	ECB,4CB,CSDs,CBs																										
1668	562100	[Deliverable] - T2S Public Training Framework V1.0	◆	0d	Thu 31/05/12	Thu 31/05/12	Eurosystem																										
1678	563100	Training Materials preparation		603d	Mon 23/07/12	Mon 01/12/14																											
1685	566400	Publication of T2S Training Calendar		0d	Mon 17/12/12	Mon 17/12/12	Eurosystem																										
1686	566500	Internal Eurosystem Preparation [Training Materials]		540d	Fri 28/09/12	Mon 10/11/14																											
1700	568100	[Deliverable] - Basic Training Materials	◆	0d	Mon 03/06/13	Mon 03/06/13	Eurosystem																										
1702	568400	[Deliverable] - Technical Training Materials	◆	0d	Tue 03/09/13	Tue 03/09/13	Eurosystem																										
1704	568600	[Deliverable] - Functional Training Materials	◆	0d	Tue 03/12/13	Tue 03/12/13	Eurosystem																										
1706	568800	[Deliverable] - Operational Training Materials	◆	0d	Fri 20/06/14	Fri 20/06/14	Eurosystem																										
1708	569000	[Deliverable] - Testing Training Materials	◆	0d	Tue 03/06/14	Tue 03/06/14	Eurosystem																										
1710	569200	[Deliverable] - Migration Training Materials	◆	0d	Mon 01/12/14	Mon 01/12/14	Eurosystem																										
1711	574200	TRAINING EXECUTION		786d	Mon 01/07/13	Wed 13/07/16																											
1712	575100	Training Session		471d	Mon 01/07/13	Wed 06/05/15																											
1713	575101	Start training session	◆	0d	Mon 01/07/13	Mon 01/07/13	Eurosystem,CSDs,CBs																										
1721	580150	CSDs and CBs training sessions finalised before wave 1	◆	0d	Wed 06/05/15	Wed 06/05/15	Eurosystem,CSDs,CBs																										
1722	581100	Refresh-training before go-live		300d	Thu 28/05/15	Wed 13/07/16																											

Task	Task	Critical Milestone	Milestone	Critical Task	Project Summary	Group By Summary

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
1726	583100	USER TESTING PREPARATION		1463d	Fri 02/01/09	Wed 27/08/14																										
1734	592200	T2S User Testing Calendar		224d	Mon 29/04/13	Thu 13/03/14																										
1735	592300	Internal Eurosystem Preparation [T2S User Testing Calendar]		90d	Mon 29/04/13	Fri 30/08/13																										
1739	593400	Market consultation on T2S User Testing calendar	🟢	134d	Mon 02/09/13	Thu 13/03/14																										
1756	597300	[Deliverable] - User Testing Calendar	🟢	0d	Thu 13/03/14	Thu 13/03/14	Eurosystem																									
1757	616200	Certification Test Sets		334d	Fri 01/03/13	Thu 19/06/14																										
1758	616300	Internal Eurosystem Preparation [Certification Test Sets]		334d	Fri 01/03/13	Thu 19/06/14																										
1762	616540	Market Consultation/Information on Certification test sets	🟢	164d	Mon 28/10/13	Thu 19/06/14																										
1780	634600	[Deliverable] - CSD Certification Test Cases	🟢	0d	Thu 19/06/14	Thu 19/06/14	Eurosystem																									
1781	634700	[Deliverable] - CB Certification Test Cases	🟢	0d	Thu 19/06/14	Thu 19/06/14	Eurosystem																									
1782	634800	[Deliverable] - DCP Certification Test Cases	🟢	0d	Thu 19/06/14	Thu 19/06/14	Eurosystem																									
1807	603100	UT Registration Guide		284d	Mon 04/03/13	Fri 11/04/14																										
1808	603200	Internal Eurosystem Preparation [UT Registration Guide]		100d	Mon 04/03/13	Fri 19/07/13																										
1812	606140	Market information on UT Registration Guide	🟢	128d	Mon 22/07/13	Wed 22/01/14																										
1827	607200	[Deliverable] - Registration Guide for User Testing	🟢	0d	Wed 22/01/14	Wed 22/01/14	Eurosystem																									
1828	627100	Completed UT Registration Guide for User Testing (network registration)	🟢	0d	Fri 11/04/14	Fri 11/04/14	CSDs,CBs																									
1829	611100	User Testing Guide		283d	Mon 04/02/13	Wed 12/03/14																										
1830	611200	Internal Eurosystem Preparation [User Testing Guide]		150d	Mon 04/02/13	Fri 30/08/13																										
1834	612240	Market consultation on User Testing Guide	🟢	133d	Mon 02/09/13	Wed 12/03/14																										
1849	616100	[Deliverable] - User Testing Guide	🟢	0d	Wed 12/03/14	Wed 12/03/14	Eurosystem																									
1865	630100	UT Environment Preparation		20d	Wed 11/06/14	Tue 08/07/14																										
1869	634200	UT environment ready	🟢	0d	Wed 11/06/14	Wed 11/06/14	Eurosystem																									
1870	634300	Delivery updated version of the EAT Status update	🟢	0d	Wed 27/08/14	Wed 27/08/14	Eurosystem																									
1871	497100	Synchronization Point [SP6 - Eurosystem Ready for User Testing]	🟢	0d	Tue 02/09/14	Tue 02/09/14	Eurosystem																									
1879	636100	USER TESTING EXECUTION		517d	Mon 07/07/14	Wed 29/06/16																										
1880	645100	Synchronization Point [SP7 - Start Connectivity Testing]	🟢	0d	Mon 07/07/14	Mon 07/07/14	Eurosystem,CSDs,CBs																									
1881	645150	Connectivity Testing for Interoperability wave 1		82d	Mon 07/07/14	Wed 29/10/14																										
1886	646160	[Deliverable] - User Testing Stage Report (Wave 1) V1.0 [Connectivity phase]	🟢	0d	Tue 30/09/14	Tue 30/09/14	Eurosystem																									
1890	649200	Synchronization Point [SP8 - Start Bilateral Interoperability Testing]	🟢	0d	Wed 01/10/14	Wed 01/10/14	Eurosystem,CSDs,CBs																									
1891	649250	Acceptance Phase		126d	Thu 02/10/14	Thu 02/04/15																										
1892	647200	CSD Acceptance phase wave 1	🟢	60d	Thu 02/10/14	Mon 29/12/14																										

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017	
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half	
								Otr 1	Otr 2	Otr 3	Otr 4	Otr 1	Otr 2	Otr 3	Otr 4	Otr 1	Otr 2	Otr 3	Otr 4	Otr 1	Otr 2	Otr 3	Otr 4	Otr 1	Otr 2	Otr 3	Otr 4	Otr 1	Otr 2	Otr 3	Otr 4	Otr 1	
1896	649000	CB Acceptance phase wave 1		60d	Thu 02/10/14	Mon 29/12/14																											
1900	647350	CSD Acceptance phase wave 2		126d	Thu 02/10/14	Thu 02/04/15																											
1904	649300	CB Acceptance phase wave 2		126d	Thu 02/10/14	Thu 02/04/15																											
1908	647450	CSD Acceptance phase wave 3		126d	Thu 02/10/14	Thu 02/04/15																											
1912	649700	CB Acceptance phase wave 3		126d	Thu 02/10/14	Thu 02/04/15																											
1916	647550	Certification Phase		184d	Thu 02/10/14	Mon 22/06/15																											
1917	647600	CSD Certification phase wave 1		60d	Thu 02/10/14	Mon 29/12/14																											
1921	647890	CB Certification phase wave 1		60d	Thu 02/10/14	Mon 29/12/14																											
1925	647990	CSD Certification phase wave 2		125d	Thu 02/10/14	Wed 01/04/15																											
1929	648290	CB Certification phase wave 2		125d	Thu 02/10/14	Wed 01/04/15																											
1933	648390	CSD Certification phase wave 3		184d	Thu 02/10/14	Mon 22/06/15																											
1937	648590	CB Certification phase wave 3		184d	Thu 02/10/14	Mon 22/06/15																											
1941	650100	Interoperability - Community - Business Day Testing Wave 1		447d	Mon 01/09/14	Wed 18/05/16																											
1942	652100	Interoperability Bilateral Testing Wave 1		55d	Wed 01/10/14	Thu 18/12/14																											
2001	714280	[Deliverable] - User Testing Stage Report (Wave 1) V1.1 Interoperability Bilateral phase]		0d	Thu 18/12/14	Thu 18/12/14	Eurosystem																										
2002	714300	Synchronization Point [SP9.1 - Start Multilateral Interoperability Testing (wave 1)]		0d	Mon 29/12/14	Mon 29/12/14	Eurosystem,CSDs,CBs																										
2003	722000	Interoperability Multilateral testing Wave 1		45d	Tue 30/12/14	Wed 04/03/15																											
2007	723100	[Deliverable] - User Testing Stage Report (Wave 1) V1.2 [Interoperability Multilateral phase]		0d	Wed 04/03/15	Wed 04/03/15	Eurosystem																										
2040	726400	Connectivity Testing for Migration wave 1		42d	Mon 01/09/14	Wed 29/10/14																											
2044	726800	Migration Wave 1		100d	Wed 03/09/14	Tue 27/01/15																											
2053	730100	Synchronization Point [SP10.1 - Start Community Testing Wave 1]		0d	Wed 04/03/15	Wed 04/03/15	Eurosystem,CSDs,CBs																										
2054	730200	Connectivity Testing for Community wave 1		20d	Thu 05/02/15	Wed 04/03/15																											
2057	731100	Community testing Wave 1		50d	Wed 04/03/15	Thu 14/05/15																											
2120	789400	[Deliverable] - User Testing Stage Report (Wave 1) V1.3 [Community phase]		0d	Thu 14/05/15	Thu 14/05/15	Eurosystem																										
2121	789500	DCP-DCAH Certification phase wave 1		30d	Thu 05/03/15	Wed 15/04/15																											
2124	789800	[Deliverable] - Certification report for DCPs (Wave 1)		0d	Wed 15/04/15	Wed 15/04/15	Eurosystem																										
2127	792000	[Deliverable] - Certification report for DCAH (Wave 1)		0d	Wed 15/04/15	Wed 15/04/15	Eurosystem																										
2128	796000	Synchronization Point [SP11.1 - Start Business Day Testing Wave 1]		0d	Mon 18/05/15	Mon 18/05/15	Eurosystem,CSDs,CBs																										
2129	796100	Business day test Wave 1		19d	Mon 18/05/15	Fri 12/06/15																											
2153	832300	[Deliverable] - User Testing Stage Report (Wave 1) V1.4 [Business day phase]		0d	Fri 12/06/15	Fri 12/06/15	Eurosystem																										
2154	832400	Progress Report Wave 1(recurrent task during UT phase until End of User Testing Wave 1)		10d	Fri 28/11/14	Thu 11/12/14																											

Task		Task		Critical Milestone		Milestone		Critical Task		Project Summary		Group By Summary	

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
2457	2273080	[Deliverable] - User Testing Stage Report (Wave 3) V3.1 Interoperability Bilateral phase]		0d	Tue 23/06/15	Tue 23/06/15	Eurosystem																									
2458	2273500	Synchronization Point [SP9.3 - Start Multilateral Interoperability Testing (wave 3)]		0d	Tue 23/06/15	Tue 23/06/15	Eurosystem,CSDs,CBs																									
2459	2273100	Interoperability Multilateral testing Wave 3		93d	Wed 24/06/15	Fri 30/10/15																										
2463	2275000	[Deliverable] - User Testing Stage Report(Wave 3) V3.2 [Interoperability Multilateral phase]		0d	Fri 30/10/15	Fri 30/10/15	Eurosystem																									
2496	2282050	Connectivity Testing for Migration wave 3		40d	Fri 10/04/15	Fri 05/06/15																										
2500	2282400	Migration Wave 3		148d	Fri 17/04/15	Mon 09/11/15																										
2510	2284000	Synchronization Point [SP10.3 - Start Community Testing Wave 3]		0d	Mon 09/11/15	Mon 09/11/15	Eurosystem,CSDs,CBs																									
2511	2284100	Connectivity Testing for Community wave 3		40d	Tue 13/10/15	Mon 07/12/15																										
2514	2285000	Community testing Wave 3		125d	Mon 09/11/15	Wed 27/04/16																										
2577	2345100	[Deliverable] - User Testing Stage Report (Wave 3) V3.3 [Community phase]		0d	Wed 27/04/16	Wed 27/04/16	Eurosystem																									
2578	2346000	DCP-DCAH Certification phase wave 3		135d	Tue 22/12/15	Wed 22/06/16																										
2581	2346300	[Deliverable] - Certification report for DCPs (Wave 3)		0d	Fri 18/03/16	Fri 18/03/16	Eurosystem																									
2584	2346700	[Deliverable] - Certification report for DCAH (Wave 3)		0d	Fri 18/03/16	Fri 18/03/16	Eurosystem																									
2585	2351100	Synchronization Point [SP11.3 - Start Business Day Testing Wave 3]		0d	Wed 27/04/16	Wed 27/04/16	Eurosystem,CSDs,CBs																									
2586	2352000	Business day test Wave 3		40d	Wed 27/04/16	Wed 22/06/16																										
2610	2390200	[Deliverable] - User Testing Stage Report (Wave 3) V3.4 [Business day phase]		0d	Wed 22/06/16	Wed 22/06/16	Eurosystem																									
2611	2391000	Progress Report Wave 3 (recurrent task during UT phase End of User Testing Wave 3)		10d	Fri 28/11/14	Thu 11/12/14																										
2613	2391200	[Deliverable] - Progress Report Wave 3 (recurrent task)		0d	Thu 11/12/14	Thu 11/12/14	CSDs,CBs																									
2614	2394400	Support Testing for other waves		161d	Thu 05/03/15	Wed 14/10/15																										
2617	2394200	Synchronization Point [SP12.3 - End of User Testing Execution Phase Wave 3]		0d	Wed 29/06/16	Wed 29/06/16	Eurosystem,CSDs,CBs																									
2619	1310100	CONTRACTUAL FRAMEWORK		602d	Tue 01/09/09	Wed 21/12/11																										
2748	1027100	OPERATIONAL READINESS		1984d	Mon 15/06/09	Mon 30/01/17																										
2749	1027200	NETWORK AND CONNECTIVITY		1260d	Mon 15/06/09	Thu 24/04/14																										
2750	1028100	NETWORK AND CONNECTIVITY		1260d	Mon 15/06/09	Thu 24/04/14																										
2809	1063480	Tender process for Value-Added Services (VA-NSPs)		147d	Fri 08/07/11	Tue 31/01/12																										
2811	1059100	[Deliverable] - Tender for Network Connectivity (VAN)		0d	Fri 08/07/11	Fri 08/07/11	Eurosystem																									
2814	1061100	Signature of Network Service Provider Agreement		0d	Tue 31/01/12	Tue 31/01/12	Eurosystem																									
2815	1062000	CSDs - Network Service Provider negotiations		543d	Tue 28/02/12	Fri 11/04/14																										
2818	1063120	CSD: Network Agreement Contract signed		0d	Fri 11/04/14	Fri 11/04/14	CSDs																									
2821	1063190	CB: Network Agreement Contract signed		0d	Fri 11/04/14	Fri 11/04/14	CBs																									
2822	1060500	Tender process for Dedicated line (DL-NSPs) (to be updated after PB meeting in June)		498d	Tue 01/03/11	Thu 31/01/13	Eurosystem																									

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017	
								1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2
2829	1061000	Contract Signature for dedicated link		0d	Thu 31/01/13	Thu 31/01/13	Eurosystem											31/01/2013															
2837	1064100	Implementation Phase 2 - VAN Network		322d	Wed 01/08/12	Mon 04/11/13																											
2842	1067100	Start of VAN Networks connectivity tests with CSDs/CBs (Finish acceptance VAN Networks by 4CB)		0d	Mon 04/11/13	Mon 04/11/13	Eurosystem																04/11/2013										
2843	1077300	Implementation - Phase 2 - Dedicated Links		196d	Fri 01/02/13	Mon 04/11/13	Eurosystem																										
2847	1077700	Start of DL connectivity tests with DiCoAs		0d	Mon 04/11/13	Mon 04/11/13	Eurosystem																	04/11/2013									
2849	1037100	Implementation - Phase 3 - Network - Connectivity Guides		173d	Tue 30/04/13	Thu 02/01/14																											
2850	1038100	Internal Eurosystem Preparation [Connectivity Guide]		173d	Tue 30/04/13	Thu 02/01/14																											
2852	1042200	[Deliverable] - Connectivity Guide for VAN and Direct connectivity (Testing) V1.0		0d	Tue 30/07/13	Tue 30/07/13	Eurosystem																										
2855	1043100	[Deliverable] - Connectivity Guide for VAN and Direct connectivity V2.0		0d	Thu 02/01/14	Thu 02/01/14	Eurosystem																										
2856	1081100	INFORMATION SECURITY		1221d	Wed 01/09/10	Fri 29/05/15																											
2857	1082100	INFORMATION SECURITY		1221d	Wed 01/09/10	Fri 29/05/15																											
2858	1084280	T2S Threat Catalogue		508d	Mon 03/01/11	Thu 13/12/12																											
2859	1084290	Internal Eurosystem Preparation [T2S Threat Catalogue]		505d	Mon 03/01/11	Mon 10/12/12																											
2867	1091500	[Deliverable] - T2S Threat Catalogue		0d	Thu 13/12/12	Thu 13/12/12	Eurosystem																										
2906	1107250	Risk analysis on T2S Compliance with T2S Information Security policy [Risk evaluation table & Risk treatment plan]		197d	Wed 13/08/14	Fri 22/05/15																											
2907	1107260	Internal Eurosystem Preparation [Risk analysis on T2S Compliance with T2S Information Security policy]		197d	Wed 13/08/14	Fri 22/05/15																											
2920	1108100	[Deliverable] - Risk Analysis on T2S Compliance with T2S Information Security policy		0d	Fri 22/05/15	Fri 22/05/15	Eurosystem																										
2932	1109200	OPERATIONS		1275d	Thu 01/12/11	Wed 02/11/16																											
2933	1110100	OPERATIONAL PROCEDURES		1275d	Thu 01/12/11	Wed 02/11/16																											
2934	1111100	Manual of Operational Procedures (MOP)		1275d	Thu 01/12/11	Wed 02/11/16																											
2935	1111150	Production MOP V1.0 (before starting User Test)		616d	Thu 01/12/11	Thu 24/04/14																											
2936	1112050	First set of review cycles		348d	Thu 01/12/11	Mon 08/04/13																											
2942	1113500	First Market consultation on Manual of Operational Procedures (MOP)		198d	Thu 28/06/12	Mon 08/04/13																											
2946	1115100	Review MOP V0.1 by OMG		30d	Fri 13/07/12	Thu 23/08/12	OMG																										
2950	1119100	Review MOP V0.2 by OMG		30d	Tue 23/10/12	Mon 03/12/12	OMG																										
2963	1124000	Second set of review cycles		275d	Tue 12/03/13	Mon 07/04/14																											
2966	1124300	Second Market consultation on Manual of Operational Procedures (MOP)		215d	Tue 04/06/13	Mon 07/04/14																											
2983	1140100	[Deliverable] - Manual of Operational Procedures (MOP) V1.0 for Business Day Test wave 1		0d	Thu 24/04/14	Thu 24/04/14	Eurosystem																										
2984	1140200	Production MOP V1.2 (revised MOP V1.0 before Start Operation in T2S wave 1)		18d	Tue 19/05/15	Thu 11/06/15																											
2988	1121100	[Deliverable] - Manual of Operational Procedures (MOP) V1.2 before Start Operation in T2S Wave 1		0d	Thu 11/06/15	Thu 11/06/15	Eurosystem																										
2989	1121200	Production MOP V1.3 (revised MOP V1.2 after Start Operation in T2S wave 1 and during Business Day Test wave 2)		121d	Tue 21/07/15	Thu 07/01/16																											

T2S Operational Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017	
								1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	
2995	1145200	[Deliverable] - Manual of Operational Procedures (MOP) V1.3 during Business Day Test Wave 2	◆	0d	Thu 07/01/16	Thu 07/01/16	Eurosystem																										
2996	1145300	Production MOP V1.4 (revised MOP V1.3 after Start Operation in T2S wave 2 and during Business Day Test wave 3)		50d	Thu 25/02/16	Mon 02/05/16																											
3002	1145800	[Deliverable] - Manual of Operational Procedures (MOP) V1.4 during Business Day Test Wave 3	◆	0d	Mon 02/05/16	Mon 02/05/16	Eurosystem																										
3003	1145900	Production MOP V2.0 (Operational activities after Start Operation in T2S wave 3)		97d	Thu 23/06/16	Wed 02/11/16																											
3009	1146050	[Deliverable] - Manual of Operational Procedures (MOP) V2.0 after start of operations in T2S of wave 3	◆	0d	Thu 23/06/16	Thu 23/06/16	Eurosystem																										
3017	1110200	SERVICE LEVEL AGREEMENT		0d	Fri 30/12/11	Fri 30/12/11																											
3018	1187100	MIGRATION		1956d	Thu 23/07/09	Mon 30/01/17																											
3019	1187200	MIGRATION PREPARATION		1800d	Thu 23/07/09	Thu 30/06/16																											
3027	1200100	Preparation phase		1337d	Mon 02/05/11	Thu 30/06/16																											
3028	1201100	Processes and tools for Data Migration		244d	Mon 02/05/11	Thu 05/04/12																											
3029	1201200	Internal Eurosystem Preparation [Processes and tools for Data Migration]		67d	Mon 02/05/11	Tue 02/08/11																											
3033	1203400	Market consultation on Processes and tools for Data Migration	◆	122d	Wed 19/10/11	Thu 05/04/12																											
3049	1206100	[Deliverable] - User Requirements for data migration tools V1.0	◆	0d	Thu 05/04/12	Thu 05/04/12	Eurosystem																										
3050	1207100	Composition of Migration Waves & Dates		116d	Fri 29/06/12	Mon 10/12/12																											
3051	1207150	Reception of Proposal of migration waves plus migration dates for each CSD/CB (as part of the feasibility study)	◆	0d	Fri 29/06/12	Fri 29/06/12	CSDs,CBs																										
3052	1207200	Eurosystem consultation: review of CSDs proposal by the Eurosystem	◆	71d	Fri 29/06/12	Mon 08/10/12																											
3053	1209100	Coordination by Eurosystem of proposal for the Composition of migration waves (incl. CSD/CBs views)	◆	26d	Fri 29/06/12	Fri 03/08/12	Eurosystem,CSDs,CBs																										
3054	546350	[Deliverable] - Composition and Timing Migration Waves by CSDs/CBs	◆	0d	Fri 03/08/12	Fri 03/08/12	CSDs,CBs																										
3055	1209130	Evaluation by Eurosystem of proposal for the timing of migration waves (incl. CSD/CBs views)	◆	40d	Mon 06/08/12	Fri 28/09/12	Eurosystem,CSDs,CBs																										
3056	1209150	Confirmation of the Timing and Composition of Migration Waves by Eurosystem	◆	0d	Mon 08/10/12	Mon 08/10/12	Eurosystem																										
3057	1209160	Market Consultation on Composition of Migration Waves & Dates (only whether CSDs proposal conflicts with migration criteria)	◆	96d	Fri 27/07/12	Mon 10/12/12																											
3075	1218000	[Deliverable] - Confirmation of composition and timing of Migration Waves V1.0	◆	0d	Mon 10/12/12	Mon 10/12/12	Eurosystem																										
3076	1218100	Migration profiles & Registration Guide		289d	Mon 03/10/11	Fri 09/11/12																											
3077	1218200	Internal Eurosystem Preparation [Migration profiles & Registration Guide]		95d	Mon 03/10/11	Fri 10/02/12																											
3080	1220400	Market Consultation on Migration profiles & Registration Guide	◆	194d	Mon 13/02/12	Fri 09/11/12																											
3084	1222250	Review Migration profiles & Registration Guide V0.1 by MSG	◆	15d	Tue 27/03/12	Mon 16/04/12	OMG																										
3088	1222650	Review Migration profiles & Registration Guide V0.2 by MSG	◆	15d	Wed 02/05/12	Tue 22/05/12	OMG																										
3092	1222850	Review Migration profiles & Registration Guide V0.2 by MSG	◆	15d	Thu 07/06/12	Wed 27/06/12	OMG																										
3106	1222100	[Deliverable] - Registration Guide for Migration V1.0	◆	0d	Fri 09/11/12	Fri 09/11/12	Eurosystem																										
3107	1228100	Standard Migration plans (including Fallback and Roll-back Procedures)		464d	Mon 16/01/12	Fri 01/11/13																											
3108	1228200	Internal Eurosystem Preparation [Standard Migration plans (including Fallback and Roll-back Procedures)]		230d	Mon 16/01/12	Mon 03/12/12																											

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1
3113	1229500	Market consultation on Standard Migration plan and Tailored	◆	234d	Tue 04/12/12	Fri 01/11/13	Eurosystem																									
3143	1232800	[Deliverable] - Standard Migration Plan V1.0	◆	0d	Fri 01/11/13	Fri 01/11/13																										
3144	1232900	Migration Weekend Script (including Fallback and Roll-back Procedures)		797d	Mon 03/06/13	Thu 30/06/16																										
3145	1233000	Internal Eurosystem Preparation [Migration Weekend Script for wave 1]		150d	Mon 03/06/13	Fri 03/01/14																										
3150	1233340	Market consultation on Migration Weekend Script	◆	230d	Mon 06/01/14	Tue 25/11/14	Eurosystem																									
3176	1235400	[Deliverable] - Detailed Migration Weekend Script V1.0 Wave 1	◆	0d	Fri 28/11/14	Fri 28/11/14																										
3177	1235500	Review Migration Weekend Script for wave 1 before Start Operation in T2S		31d	Fri 24/04/15	Mon 08/06/15																										
3179	1235650	Market consultation Migration Weekend Script for wave 1 before Start Operation in T2S	◆	21d	Fri 08/05/15	Mon 08/06/15																										
3183	1236000	[Deliverable] - Detailed Migration Weekend Script V1.2 Wave 1	◆	0d	Mon 08/06/15	Mon 08/06/15	Eurosystem																									
3184	1236400	Internal Eurosystem Preparation [Migration Weekend Script for wave 2]		90d	Mon 02/03/15	Thu 02/07/15																										
3187	1236640	Market consultation Migration Weekend Script for wave 2	◆	92d	Fri 03/07/15	Mon 09/11/15																										
3196	1237300	[Deliverable] - Detailed Migration Weekend Script V2.2 Wave 2	◆	0d	Mon 09/11/15	Mon 09/11/15																										
3197	1237350	Review Migration Weekend Script for wave 2 before Start Operation in T2S wave 2		26d	Wed 09/12/15	Thu 14/01/16	Eurosystem																									
3199	1237450	Market consultation Migration Weekend Script for wave 2 before Start Operation in T2S	◆	16d	Tue 22/12/15	Thu 14/01/16																										
3203	1236020	[Deliverable] - Detailed Migration Weekend Script V2.4 Wave 2	◆	0d	Thu 14/01/16	Thu 14/01/16																										
3204	1237400	Internal Eurosystem Preparation [Migration Weekend Script for wave 3]		80d	Thu 20/08/15	Wed 09/12/15																										
3207	1237540	Market consultation on Migration Weekend Script for wave 3	◆	149d	Thu 10/12/15	Thu 30/06/16	Eurosystem																									
3216	1238200	[Deliverable] - Detailed Migration Weekend Script V3.2 Wave 3	◆	0d	Tue 12/04/16	Tue 12/04/16																										
3217	1234650	Review Migration Weekend Script for wave 3 before Start Operation in T2S wave 3		26d	Thu 26/05/16	Thu 30/06/16																										
3219	1235710	Market consultation Migration Weekend Script for wave 3 before Start Operation in T2S	◆	16d	Wed 08/06/16	Thu 30/06/16																										
3223	1236040	[Deliverable] - Detailed Migration Weekend Script V3.4 Wave 3	◆	0d	Thu 30/06/16	Thu 30/06/16	Eurosystem																									
3239	1269100	PRE-MIGRATION TASKS (WAVE 1)		255d	Fri 20/06/14	Fri 19/06/15																										
3240	1235410	Implementation Migration phase (wave 1)		80d	Mon 17/11/14	Thu 12/03/15																										
3241	1244100	Preparation of Migration Weekend (wave 1)		80d	Mon 17/11/14	Thu 12/03/15																										
3242	124410	Start preparation of Migration Weekend	◆	0d	Mon 01/12/14	Mon 01/12/14	Eurosystem																									
3244	387100	Network ready for Production		0d	Mon 01/12/14	Mon 01/12/14																										
3247	1247100	Registration Form filled in (wave 1 + CSDs/CBs with Common Static Data)	◆	0d	Fri 12/12/14	Fri 12/12/14		CSDs,CBs																								
3248	1249100	Preparation of production environment		80d	Mon 17/11/14	Thu 12/03/15																										
3250	1250100	Synchronization Point [SP13 - Eurosystem ready for Production]	◆	0d	Mon 01/12/14	Mon 01/12/14	Eurosystem																									
3257	1257100	Synchronization Point [SP14.1 -Ready to connect to Production wave 1]	◆	0d	Thu 05/02/15	Thu 05/02/15		Eurosystem,CSDs																								
3259	1263100	Successful connectivity tests CSD (wave 1)	◆	0d	Thu 12/03/15	Thu 12/03/15	CSDs																									

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1
3260	1255400	Successful connectivity tests CB (wave 1)		0d	Thu 12/03/15	Thu 12/03/15	CBs																12/03/2015									
3266	1272100	Synchronization Point [SP15.1 - Ready to upload Static Data wave 1]		0d	Thu 19/03/15	Thu 19/03/15	Eurosystem,CSDs																19/03/2015									
3268	1268200	Migration Common Static Data		105d	Fri 23/01/15	Fri 19/06/15																										
3275	1269200	Migration Proprietary Static Data (wave 1)		105d	Fri 23/01/15	Fri 19/06/15																										
3282	1275000	MIGRATION WEEKEND (WAVE 1)		48d	Fri 22/05/15	Mon 27/07/15																										
3288	1275100	Synchronization Point [SP16.1 - Ready for T2S Go-Live (Wave 1)]		0d	Fri 19/06/15	Fri 19/06/15	CSDs,CBs,Eurosystem																19/06/2015									
3290	1279100	Wave 1 Start Operations in T2S		0d	Mon 22/06/15	Mon 22/06/15	Eurosystem,CSDs																22/06/2015									
3291	1279200	Migration closing phase Wave 1		15d	Tue 07/07/15	Mon 27/07/15																										
3294	835100	[Deliverable] - End of Migration Report (Wave 1)		0d	Mon 27/07/15	Mon 27/07/15	Eurosystem															550	27/07/2015									
3295	1280200	PRE-MIGRATION TASKS (WAVE 2)		416d	Fri 20/06/14	Fri 29/01/16																										
3296	1281000	Implementation Migration phase (wave 2)		55d	Mon 17/08/15	Fri 30/10/15																										
3297	1281100	Preparation of Migration Weekend (wave 2)		55d	Mon 17/08/15	Fri 30/10/15																										
3298	1281200	Start preparation of Migration Weekend (wave 2)		0d	Mon 17/08/15	Mon 17/08/15	Eurosystem																17/08/2015									
3301	1281500	Registration Form filled in (CSDs/CBs) (wave 2)		0d	Fri 11/09/15	Fri 11/09/15	CSDs,CBs																11/09/2015									
3302	1281600	Preparation of production environment		35d	Mon 14/09/15	Fri 30/10/15																										
3309	1283500	Synchronization Point [SP14.2 - Ready to connect to Production wave 2]		0d	Fri 02/10/15	Fri 02/10/15	Eurosystem,CSDs																02/10/2015									
3311	1283370	Successful connectivity tests CSD (wave 2)		0d	Fri 30/10/15	Fri 30/10/15	CSDs																30/10/2015									
3312	1283390	Successful connectivity tests CB (wave 2)		0d	Fri 30/10/15	Fri 30/10/15	CBs																30/10/2015									
3318	1283100	Migration Proprietary Static Data (wave 2)		158d	Tue 23/06/15	Fri 29/01/16																										
3323	1285200	Synchronization Point [SP15.2 - Ready to upload Static Data wave 2]		0d	Fri 06/11/15	Fri 06/11/15	Eurosystem,CSDs																06/11/2015									
3326	1287000	MIGRATION WEEKEND (WAVE 2)		48d	Fri 01/01/16	Mon 07/03/16																										
3332	1287100	Synchronization Point [SP16.2 - Ready for Migration Wave 2]		0d	Fri 29/01/16	Fri 29/01/16	Eurosystem,CSDs																29/01/2016									
3334	1291100	Wave 2 Start Operations in T2S		0d	Mon 01/02/16	Mon 01/02/16	Eurosystem,CSDs																01/02/2016									
3335	1291200	Migration closing phase Wave 2		15d	Tue 16/02/16	Mon 07/03/16																										
3338	1025100	[Deliverable] - End of Migration Report (Wave 2)		0d	Mon 07/03/16	Mon 07/03/16	Eurosystem															550	07/03/2016									
3339	1293000	PRE-MIGRATION TASKS (WAVE 3)		543d	Fri 20/06/14	Mon 18/07/16																										
3340	1293100	Implementation Migration phase (wave 3)		475d	Fri 20/06/14	Fri 15/04/16																										
3341	1293200	Preparation of Migration Weekend (wave 3)		52d	Mon 08/02/16	Fri 15/04/16																										
3342	1293300	Start preparation of Migration Weekend (wave 3)		0d	Mon 08/02/16	Mon 08/02/16	Eurosystem																08/02/2016									
3345	1293600	Registration Form filled in (CSDs/CBs) (wave 3)		0d	Fri 04/03/16	Fri 04/03/16	CSDs,CBs																04/03/2016									
3346	1293700	Preparation of production environment		32d	Mon 07/03/16	Fri 15/04/16																										

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

	Task		Task		Critical Milestone		Milestone		Critical Task		Project Summary		Group By Summary	

T2S Operational Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017	
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half	
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2
3862	2012300	SP10.3 -Start Community Testing (wave 3)		0d	Mon 09/11/15	Mon 09/11/15																											
3863	2012400	SP11.1 - Start Business Day Testing (wave 1)		0d	Mon 18/05/15	Mon 18/05/15																											
3864	2012500	SP11.2 - Start Business Day Testing (wave 2)		0d	Mon 09/11/15	Mon 09/11/15																											
3865	2012600	SP11.3 - Start Business Day Testing (wave 3)		0d	Wed 27/04/16	Wed 27/04/16																											
3866	2013100	SP12.1 - End of User Testing Execution Phase (wave 1)		0d	Mon 15/06/15	Mon 15/06/15																											
3867	2013200	SP12.2 - End of User Testing Execution Phase (wave 2)		0d	Mon 18/01/16	Mon 18/01/16																											
3868	2013300	SP12.3 - End of User Testing Execution Phase (wave 3)		0d	Wed 29/06/16	Wed 29/06/16																											
3869	2014100	SP13 - Eurosystem ready for Production		0d	Mon 01/12/14	Mon 01/12/14																											
3870	2015100	SP14.1 - Ready to connect to Production (wave 1)		0d	Thu 05/02/15	Thu 05/02/15																											
3871	2015200	SP14.2 - Ready to connect to Production (wave 2)		0d	Fri 02/10/15	Fri 02/10/15																											
3872	2015300	SP14.3 - Ready to connect to Production (wave 3)		0d	Tue 22/03/16	Tue 22/03/16																											
3873	2016100	SP15.1 - Ready to upload Static Data (wave 1)		0d	Thu 19/03/15	Thu 19/03/15																											
3874	2016200	SP15.2 - Ready to upload Static Data (wave 2)		0d	Fri 06/11/15	Fri 06/11/15																											
3875	2016300	SP15.3 - Ready to upload Static Data (wave 3)		0d	Fri 22/04/16	Fri 22/04/16																											
3876	2017100	SP16.1 - Ready for T2S Go-Live (wave 1)		0d	Fri 19/06/15	Fri 19/06/15																											
3877	2017200	SP16.2 - Ready for Migration Wave 2		0d	Fri 29/01/16	Fri 29/01/16																											
3878	2017300	SP16.3 - Ready for Migration Wave 3		0d	Fri 15/07/16	Fri 15/07/16																											
3879	2017400	SP16.5 - Ready for Contingency Migration Weekend		0d	Fri 27/01/17	Fri 27/01/17																											
3880	2018300	SP17 - Closing of migration		0d	Mon 10/10/16	Mon 10/10/16																											

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 2 – ANNEX 3

T2S DETAILED PLAN

Disclaimer:

Planning is an ongoing process and Annexes with planning elements are subject to change during the lifetime of a project. Planning workshops with CSDs and CBs will continue to agree on the planning for Connectivity, User Testing and Migration. Subsequent plan updates follow the process, documented in the Schedule 2, Section 7.

Annexes 2, 3, 4, 7, 8, 9 and 10 document the planning status as at 7 Nov. 2011.

T2S Detailed Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017			
								1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1			
1	100	PRODUCT READINESS		1945d	Tue 01/04/08	Fri 02/10/15																													
2	500	SPECIFICATION AND DOCUMENTATION		1417d	Fri 28/11/08	Mon 19/05/14																													
3	1100	REQUIREMENTS		692d	Thu 26/03/09	Thu 17/11/11																													
27	11400	Submission CR for URD v 5.01 & 4CB cost assessment to AG		0d	Wed 22/06/11	Wed 22/06/11	Eurosystem																												
28	13100	AG Meeting: Approval of CR for URD v 5.01		2d	Thu 30/06/11	Fri 01/07/11	AG																												
35	16100	[Deliverable] - User Requirement Document (URD) 5.01		0d	Thu 17/11/11	Thu 17/11/11	Eurosystem																												
36	18100	SPECIFICATIONS		1401d	Fri 28/11/08	Thu 24/04/14																													
37	18200	General Specification (GS)		1401d	Fri 28/11/08	Thu 24/04/14																													
45	26100	GS v. 2.0		257d	Wed 24/04/13	Thu 24/04/14																													
46	26200	Internal Eurosystem Preparation [General Specifications v. 2.0]		219d	Mon 10/06/13	Thu 17/04/14																													
55	34150	[Deliverable] - General Specification (GS) V. 2.0		0d	Wed 24/04/13	Wed 24/04/13	Eurosystem																												
67	47100	General Functional Specifications (GFS)		1231d	Mon 19/01/09	Mon 14/10/13																													
81	60100	GFS 4.0 - aligned with URD 5.0		347d	Tue 02/02/10	Wed 01/06/11																													
99	74400	Feedback of the ECB T2S project team to the Market on GFS V4.0 13/04		15d	Mon 04/04/11	Fri 22/04/11	Eurosystem																												
101	74500	Delivery GFS Note		0d	Wed 01/06/11	Wed 01/06/11	Eurosystem																												
102	73400	GFS 5.0		139d	Tue 02/04/13	Mon 14/10/13																													
103	73500	Internal Eurosystem Preparation [Production of the GFS V5.0]		134d	Tue 02/04/13	Mon 07/10/13																													
113	88150	[Deliverable] - General Function Specification (GFS) V 5.0		0d	Mon 14/10/13	Mon 14/10/13	Eurosystem																												
132	155150	Internal Detailed Functional Specification (IDFS)		910d	Wed 16/12/09	Tue 18/06/13																													
133	156100	Settlement Algorithm Objectives Document		327d	Fri 15/01/10	Fri 15/04/11																													
148	165100	Production of IDFS		910d	Wed 16/12/09	Tue 18/06/13																													
156	172200	WS - Delivery IDFS V0.85 to the Development Coordination		0d	Tue 15/02/11	Tue 15/02/11	Eurosystem																												
170	97100	User Detailed Functional Specifications (UDFS)		1300d	Thu 01/01/09	Tue 07/01/14																													
182	550200	Work on Messages Pillar I-III		1300d	Thu 01/01/09	Tue 07/01/14																													
183	105100	Message standardisation		1300d	Thu 01/01/09	Tue 07/01/14																													
184	106100	Sub-group for Message Standardisation		1300d	Thu 01/01/09	Tue 07/01/14	SGMS																												
185	107100	Monitoring of message standard development		1300d	Thu 01/01/09	Tue 07/01/14	Eurosystem																												
186	108100	Participation in message standardisation market practice for (ISO's RMG and SC4, SMPG) & contributions to publications		1300d	Thu 01/01/09	Tue 07/01/14	SMPG																												
194	116200	Production of UDFS V1.0, V1.1, V1.2 (in line with GFS V4.0)		560d	Mon 03/08/09	Fri 23/09/11																													
195	116300	Production of UDFS V1.0 [dialogue between T2S and Its users and detailed msg specification]		560d	Mon 03/08/09	Fri 23/09/11																													
231	190500	UDFS v1.0 - Messages		207.75d	Thu 01/04/10	Fri 14/01/11																													

Task Task Critical Milestone Milestone Critical Task Project Summary Group By Summary

T2S Detailed Plan with Critical Path
31/10/2011

2 of 27

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011 1st Half Qtr 1	2011 2nd Half Qtr 2	2011 2nd Half Qtr 3	2011 2nd Half Qtr 4	2012 1st Half Qtr 1	2012 1st Half Qtr 2	2012 2nd Half Qtr 3	2012 2nd Half Qtr 4	2013 1st Half Qtr 1	2013 1st Half Qtr 2	2013 2nd Half Qtr 3	2013 2nd Half Qtr 4	2014 1st Half Qtr 1	2014 1st Half Qtr 2	2014 2nd Half Qtr 3	2014 2nd Half Qtr 4	2015 1st Half Qtr 1	2015 1st Half Qtr 2	2015 2nd Half Qtr 3	2015 2nd Half Qtr 4	2016 1st Half Qtr 1	2016 1st Half Qtr 2	2016 2nd Half Qtr 3	2016 2nd Half Qtr 4	2017 1st Half Qtr 1
232	190550	Pillar III (T2S specific messages)		207.75d	Thu 01/04/10	Fri 14/01/11																										
233	190580	Detailed T2S message specification, development and T2S documentation for UDFS		207.75d	Thu 01/04/10	Fri 14/01/11																										
239	192400	Production of first draft T2S customised schema files/documentation by 4CB		79.75d	Tue 28/09/10	Fri 14/01/11																										
241	134940	Validation of draft T2S customised files/docum. By SGMS (incl. Incorporation of		47d	Thu 11/11/10	Fri 14/01/11	SGMS																									
242	190450	Validations of the version v0.3 to produce the UDFS V1.0		517d	Thu 01/10/09	Fri 23/09/11																										
243	190460	Validation of v0.3 by PMC & ECB T2S Programme Office		51d	Thu 30/12/10	Wed 09/03/11																										
244	190465	UDFS market workshop V0.3		0d	Thu 13/01/11	Thu 13/01/11	Eurosystem,CSDs																									
245	190470	ECB T2S programme Office /Market review of UDFS V0.3 (one month)		21d	Thu 30/12/10	Wed 26/01/11	Eurosystem																									
246	190490	Reception of consolidated ECB/Market feedback on UDFS v0.3 to FC		0d	Wed 26/01/11	Wed 26/01/11	Eurosystem																									
247	190560	Integration of PMC & ECB T2S Programme Office comments in v0.3 to produce the V1.0 of UDFS (1,5 month)		30d	Thu 27/01/11	Wed 09/03/11	Eurosystem																									
250	190700	Delivery of UDFS V1.0 to the Market by the ECB		1d	Fri 25/03/11	Fri 25/03/11	Eurosystem																									
251	190800	Validation of complete UDFS V1.0 by the Market		107d	Thu 10/03/11	Fri 05/08/11																										
252	193400	Fifth workshop with the Market on the UDFS		1d	Wed 30/03/11	Wed 30/03/11	Eurosystem,CSDs																									
253	193500	Sixth workshop with the Market on the UDFS (Cancelled)		1d	Wed 11/05/11	Wed 11/05/11	Eurosystem,CSDs																									
254	195100	Feedback from the Market on the UDFS V1.0		45d	Mon 28/03/11	Fri 27/05/11	CSDs																									
256	196100	Consolidation of Market comments by the ECB		10d	Mon 30/05/11	Fri 10/06/11	Eurosystem																									
257	198100	Integration of Market comments in complete UDFS V1.0 (two months)		40d	Mon 13/06/11	Fri 05/08/11	Eurosystem																									
258	199100	Delivery to ECB T2S Programme Office of UDFS V1.1		0d	Fri 05/08/11	Fri 05/08/11	Eurosystem																									
259	199200	UDFS v1.2 - Messages		486d	Thu 01/10/09	Wed 10/08/11																										
260	134500	Pillar II (new standard)		288d	Thu 28/01/10	Fri 04/03/11																										
262	134570	Detailed T2S message specification and T2S documentation for UDFS		288d	Thu 28/01/10	Fri 04/03/11																										
263	134600	Customisation of draft ISO schema files (incl. definition of fields)/documentation,		288d	Thu 28/01/10	Fri 04/03/11																										
265	134670	Validation of draft T2S customised files/documentation by		288d	Thu 28/01/10	Fri 04/03/11	SGMS																									
266	124150	Final Validation Pillar II by the SGMS		0d	Fri 04/03/11	Fri 04/03/11	SGMS																									
267	134700	Pillar III (T2S specific messages)		486d	Thu 01/10/09	Wed 10/08/11																										
268	134730	Detailed T2S message specification, development and T2S documentation for UDFS		486d	Thu 01/10/09	Wed 10/08/11																										
269	134770	Creation of HLBR by 4CB for delivery to SWIFT; Validation by SGMS (as BVG)		371d	Thu 01/10/09	Wed 02/03/11																										
270	134800	Creation of HLBR for delivery to SGMS (incl. First SWIFT and FC review)		346d	Thu 01/10/09	Wed 26/01/11	Eurosystem																									
271	134830	SGMS Validate the HLBR (incl. Incorporation of comments by 4CB)		330d	Fri 27/11/09	Wed 02/03/11	SGMS																									
272	134870	Production of first draft ISO schema files/document. By SWIFT/RA, iterative process with		79d	Tue 01/02/11	Fri 20/05/11	Eurosystem																									
273	134900	Production of first draft T2S customised schema files/documentation by 4CB		100.75d	Wed 23/03/11	Wed 10/08/11																										

Task Task Critical Milestone Milestone Critical Task Project Summary Group By Summary

Task		Task		Critical Milestone		Milestone		Critical Task		Project Summary		Group By Summary	

T2S Detailed Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1	Qtr 2	2nd Half Qtr 3	Qtr 4	1st Half Qtr 1
363	281600	Market Feedback on T2S GUI		10d	Fri 01/04/11	Thu 14/04/11	CSDs,CBs	4/2011																								
364	281700	Early market validation of GUI screens		1d	Fri 29/04/11	Fri 29/04/11	CSDs,CBs	/04/2011																								
366	281800	GUI Usability Workshops after SIBOS		76d	Mon 07/11/11	Mon 20/02/12	Eurosystem,CSDs,CBs																									
367	281850	Sixth Workshop on T2S GUI		0d	Mon 07/11/11	Mon 07/11/11	Eurosystem,CSDs,CBs																									
368	281900	Market Feedbacks on T2S GUI		44d	Mon 07/11/11	Thu 05/01/12	CSDs,CBs	07/11/2011																								
369	281950	Seventh Workshop on T2S GUI		0d	Mon 06/02/12	Mon 06/02/12	Eurosystem,CSDs,CBs																									
370	282000	Market Feedbacks on T2S GUI		11d	Mon 06/02/12	Mon 20/02/12	CSDs,CBs	06/02/2012																								
373	282200	DOCUMENTATION		1045d	Tue 04/05/10	Mon 19/05/14																										
374	252100	T2S Smooth Cross CSD settlement		305d	Tue 04/05/10	Fri 01/07/11																										
378	253200	1st Mini-consultation		89d	Wed 08/09/10	Fri 07/01/11																										
391	257275	2nd Mini-consultation		55d	Tue 30/11/10	Fri 11/02/11																										
394	257320	Analysis and preparation of consultation results		35d	Tue 28/12/10	Fri 11/02/11	TF																									
395	257325	3nd Task Force meeting		1d	Fri 21/01/11	Fri 21/01/11	TF																									
396	257330	Publication of mini-consultation results		0d	Fri 11/02/11	Fri 11/02/11	Eurosystem																									
398	257400	4rd Task Force meeting		2d	Mon 14/02/11	Tue 15/02/11	TF	11																								
399	257420	Consultation of NUGS		23d	Tue 01/03/11	Thu 31/03/11	NUGs	011																								
400	257440	Report preparation for March 2011 AG		7d	Fri 25/02/11	Mon 07/03/11	TF	011																								
401	257460	Submission of report to AG		0d	Mon 07/03/11	Mon 07/03/11	Eurosystem																									
402	257470	AG Meeting		2d	Tue 08/03/11	Wed 09/03/11	AG	2011																								
403	257480	5rd Task Force meeting		1d	Wed 23/03/11	Wed 23/03/11	TF	/2011																								
404	257490	6rd Task Force meeting		1d	Tue 17/05/11	Tue 17/05/11	TF	7/05/2011																								
405	257500	Preparation of final deliverable of smooth cross-CSD settlement in T2S		89d	Mon 28/02/11	Thu 30/06/11	TF	011																								
406	257520	7th Task Force meeting		1d	Thu 09/06/11	Thu 09/06/11	TF	09/06/2011																								
407	257540	Preparation of Report to the June 2011 AG to present the solutions and recommendations on the issues in the list		9d	Fri 10/06/11	Wed 22/06/11	TF	10/06/2011																								
408	257560	Submission report to the AG		0d	Wed 22/06/11	Wed 22/06/11	Eurosystem																									
409	257570	AG Meeting		2d	Thu 30/06/11	Fri 01/07/11	AG	30/06/2011																								
410	258100	Final Delivery of T2S Smooth Cross CSD settlement		0d	Thu 30/06/11	Thu 30/06/11	Eurosystem																									
411	259100	[Deliverable] - T2S Smooth Cross CSD settlement Report V1.0		0d	Thu 30/06/11	Thu 30/06/11	Eurosystem	107																								
412	259200	Adaptation to Cross CSD settlement		369d	Fri 01/07/11	Thu 29/11/12																										
413	259300	Task Force Activities/ Meetings		369d	Fri 01/07/11	Thu 29/11/12																										
416	259600	1st Task Force meeting		1d	Wed 07/09/11	Wed 07/09/11	TF	07/09/2011																								

Task		Task		Critical Milestone		Milestone		Critical Task		Project Summary		Group By Summary	

T2S Detailed Plan with Critical Path
31/10/2011



T2S Detailed Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
664	388100	EUROSYSTEM ACCEPTANCE TEST		1225d	Mon 03/01/11	Fri 02/10/15																										
665	389200	EAT PREPARATION		1225d	Mon 03/01/11	Fri 02/10/15																										
983	451300	[Deliverable] - CSDs Market specific test cases for EAT V1.0		0d	Thu 17/10/13	Thu 17/10/13	CSDs																									
984	451700	[Deliverable] - CBs Market specific test cases for EAT V1.0		0d	Thu 17/10/13	Thu 17/10/13	CBs																									
1045	451400	[Deliverable] - EAT Documentation V1.0 (EAT Test Sets)		0d	Thu 14/11/13	Thu 14/11/13	Eurosystem																									
1071	482300	EAT EXECUTION		265d	Mon 02/12/13	Mon 15/12/14																										
1074	485100	Execution Phase EAT Critical		236d	Wed 15/01/14	Fri 12/12/14																										
1075	464150	Synchronization Point [SP5: Start of Eurosystem Acceptance Test]		0d	Wed 15/01/14	Wed 15/01/14	Eurosystem																									
1076	486120	Start EAT - Eurosystem Acceptance Test (following the Entry Criteria)		0d	Wed 15/01/14	Wed 15/01/14	Eurosystem																									
1089	493130	[Deliverable] EAT Assessment Report		0d	Mon 01/09/14	Mon 01/09/14	Eurosystem																									
1090	493160	Go-no go decision with CSDs to start the User Testing		0d	Mon 15/09/14	Mon 15/09/14	T2SPB																									
1094	498100	EAT Status update (recurrent task during EAT phase until 1 month prior the start of UT)		23d	Wed 12/02/14	Fri 14/03/14																										
1099	451800	[Deliverable] - EAT Status update (recurrent task)		0d	Fri 14/03/14	Fri 14/03/14	Eurosystem																									
1194	524100	CLIENT READINESS		2134d	Mon 17/11/08	Mon 30/01/17																										
1195	524200	SYNCHRONISATION AND ON-BOARDING		2134d	Mon 17/11/08	Mon 30/01/17																										
1196	534200	CSD READINESS		1950d	Fri 31/07/09	Mon 30/01/17																										
1275	536000	CSDs Feasibility Assessment		280d	Mon 21/11/11	Mon 17/12/12																										
1276	536100	Preparation of impact assessment and adaptation plan by CSDs		160d	Mon 21/11/11	Fri 29/06/12	CSDs																									
1277	213100	[Deliverable] - CSD Feasibility Assessment		0d	Fri 29/06/12	Fri 29/06/12	CSDs																									
1280	538200	Assessment of feasibility confirmation		0d	Fri 10/08/12	Fri 10/08/12	Eurosystem																									
1281	214100	Synchronization Point [SP2 - Feasibility Confirmation by CSD/CB]		0d	Fri 10/08/12	Fri 10/08/12	Eurosystem																									
1283	540800	Confirmation of T2S programme plan status and achieved milestones		0d	Mon 17/12/12	Mon 17/12/12	Eurosystem																									
1284	553000	Update on CSD Feasibility Assessment		0d	Mon 17/12/12	Mon 17/12/12	CSDs																									
1285	553100	Synchronisation Point [SP3 - T2S Programme Plan Comprehensiveness]		0d	Mon 17/12/12	Mon 17/12/12	Eurosystem,CSD																									
1546	625200	Proof of Eligibility to Participate in T2S (Wave 1)		67d	Mon 10/11/14	Mon 16/02/15																										
1551	625460	Send Check List of Implementation Guide for Eligibility Criteria to the CSDs		0d	Tue 16/12/14	Tue 16/12/14	Eurosystem																									
1552	625500	Delivery the Proof of Eligibility to Participate in T2S by CSDs to ECB: CSDs submit their application to access T2S services with a self-assessment report		0d	Mon 19/01/15	Mon 19/01/15	CSDs																									
1553	625600	[Deliverable] - Proof of Eligibility to Participate in T2S (Wave 1)		0d	Mon 19/01/15	Mon 19/01/15	CSDs																									
1555	625800	PB provides confirmation to the CSDs		0d	Mon 16/02/15	Mon 16/02/15	T2SPB																									
1556	625900	Proof of Eligibility to Participate in T2S (Wave 2)		67d	Mon 13/07/15	Tue 13/10/15																										
1561	626500	Send Check List of Implementation Guide for Eligibility Criteria to the CSDs		0d	Tue 18/08/15	Tue 18/08/15	Eurosystem																									

T2S Detailed Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half				
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
1562	626600	Delivery the Proof of Eligibility to Participate in T2S by CSDs to ECB: CSDs submit their application to access T2S services with a self-assessment report		0d	Tue 15/09/15	Tue 15/09/15	CSDs																									
1563	626700	[Deliverable] - Proof of Eligibility to Participate in T2S (Wave 2)		0d	Tue 15/09/15	Tue 15/09/15	CSDs																									
1565	626900	PB provides confirmation to the CSDs		0d	Tue 13/10/15	Tue 13/10/15	T2SPB																									
1566	627000	Proof of Eligibility to Participate in T2S (Wave 3)		67d	Fri 01/01/16	Tue 29/03/16																										
1571	627800	Send Check List of Implementation Guide for Eligibility Criteria to the CSDs		0d	Thu 04/02/16	Thu 04/02/16	Eurosystem																									
1572	627900	Delivery the Proof of Eligibility to Participate in T2S by CSDs to ECB: CSDs submit their application to access T2S services with a self-assessment report		0d	Thu 03/03/16	Thu 03/03/16	CSDs																									
1573	628000	[Deliverable] - Proof of Eligibility to Participate in T2S (Wave 3)		0d	Thu 03/03/16	Thu 03/03/16	CSDs																									
1575	628400	PB provides confirmation to the CSDs		0d	Tue 29/03/16	Tue 29/03/16	T2SPB																									
1576	544100	CB READINESS		882d	Fri 31/07/09	Mon 17/12/12																										
1581	536300	CBs Feasibility Assessment		280d	Mon 21/11/11	Mon 17/12/12																										
1582	536310	Preparation of impact assessment and adaptation plan by CBs		160d	Mon 21/11/11	Fri 29/06/12	CBs																									
1583	546500	[Deliverable] - CB Feasibility Assessment		0d	Fri 29/06/12	Fri 29/06/12	CBs																									
1586	546595	Assessment of feasibility confirmation		0d	Fri 10/08/12	Fri 10/08/12	Eurosystem																									
1587	546600	Synchronization Point [SP2 - Feasibility Confirmation by CSD/CB]		0d	Fri 10/08/12	Fri 10/08/12	Eurosystem																									
1589	540900	Confirmation of T2S programme plan status and achieved milestones		0d	Mon 17/12/12	Mon 17/12/12	Eurosystem																									
1590	553200	Update on CB Feasibility Assessment		0d	Mon 17/12/12	Mon 17/12/12	CBs																									
1591	546800	Synchronisation Point [SP3 - T2S Programme Plan Comprehensiveness]		0d	Mon 17/12/12	Mon 17/12/12	Eurosystem,CB																									
1633	516600	USER TRAINING AND TESTING		1953d	Fri 02/01/09	Wed 13/07/16																										
1634	555100	TRAINING PREPARATION		1119d	Mon 02/08/10	Mon 01/12/14																										
1635	556100	Preparation of the T2S Training Framework		480d	Mon 02/08/10	Thu 31/05/12																										
1645	558100	Training Framework Phase		436d	Thu 30/09/10	Thu 31/05/12																										
1654	559700	Consultation of Public Training Framework V0.1 with CSDs and CBs		35d	Mon 16/01/12	Fri 02/03/12																										
1655	559800	Delivery of Public Training Framework V0.1 to the CSDs and CBs for advice		0d	Mon 16/01/12	Mon 16/01/12	Eurosystem																									
1656	559900	Feedback from CSDs and CBs on Public Training Framework v0.1		20d	Mon 16/01/12	Fri 10/02/12	CSDs,CBs																									
1658	556500	Workshop with CSDs and CBs on Public Training Framework V0.1 (in case of need)		1d	Fri 02/03/12	Fri 02/03/12	ECB,4CB,CSDs,CBs																									
1659	556600	Integration of CSDs and CBs feedback in Public Training Framework v0.2		15d	Mon 05/03/12	Fri 23/03/12	Eurosystem																									
1668	562100	[Deliverable] - T2S Public Training Framework V1.0		0d	Thu 31/05/12	Thu 31/05/12	Eurosystem																									
1678	563100	Training Materials preparation		603d	Mon 23/07/12	Mon 01/12/14																										
1685	566400	Publication of T2S Training Calendar		0d	Mon 17/12/12	Mon 17/12/12	Eurosystem																									
1686	566500	Internal Eurosystem Preparation [Training Materials]		540d	Fri 28/09/12	Mon 10/11/14																										
1700	568100	[Deliverable] - Basic Training Materials		0d	Mon 03/06/13	Mon 03/06/13	Eurosystem																									

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

T2S Detailed Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
1702	568400	[Deliverable] - Technical Training Materials		0d	Tue 03/09/13	Tue 03/09/13	Eurosystem													03/09/2013												
1704	568600	[Deliverable] - Functional Training Materials		0d	Tue 03/12/13	Tue 03/12/13	Eurosystem														03/12/2013											
1706	568800	[Deliverable] - Operational Training Materials		0d	Fri 20/06/14	Fri 20/06/14	Eurosystem															20/06/2014										
1708	569000	[Deliverable] - Testing Training Materials		0d	Tue 03/06/14	Tue 03/06/14	Eurosystem															03/06/2014										
1710	569200	[Deliverable] - Migration Training Materials		0d	Mon 01/12/14	Mon 01/12/14	Eurosystem																01/12/2014									
1711	574200	TRAINING EXECUTION		786d	Mon 01/07/13	Wed 13/07/16																										
1712	575100	Training Session		471d	Mon 01/07/13	Wed 06/05/15																										
1713	575101	Start training session		0d	Mon 01/07/13	Mon 01/07/13	Eurosystem,CSDs,CBs														01/07/2013											
1714	575900	First series of basic training sessions		66d	Mon 01/07/13	Mon 30/09/13	Eurosystem,CSDs,CBs													01/07/2013		30/09/2013										
1715	576100	Training sessions for technical advanced training		62d	Tue 01/10/13	Mon 30/12/13	Eurosystem,CSDs,CBs													01/10/2013		30/12/2013										
1716	578100	Training sessions for functional advanced training		61d	Mon 06/01/14	Mon 31/03/14	Eurosystem,CSDs,CBs													06/01/2014		31/03/2014										
1717	577100	Training session for operational advanced training		66d	Tue 01/07/14	Tue 30/09/14	Eurosystem,CSDs,CBs													01/07/2014		30/09/2014										
1718	580100	Training sessions on testing		66d	Tue 01/07/14	Tue 30/09/14	Eurosystem,CSDs,CBs													01/07/2014		30/09/2014										
1719	580200	Second series of basic training sessions		63d	Wed 01/10/14	Fri 02/01/15	Eurosystem,CSDs,CBs													01/10/2014		02/01/2015										
1720	579100	First series of Migration training sessions		88d	Fri 02/01/15	Wed 06/05/15	Eurosystem,CSDs,CBs													02/01/2015		06/05/2015										
1721	580150	CSDs and CBs training sessions finalised before wave 1		0d	Wed 06/05/15	Wed 06/05/15	Eurosystem,CSDs,CBs															06/05/2015										
1722	581100	Refresh-training before go-live		300d	Thu 28/05/15	Wed 13/07/16																										
1726	583100	USER TESTING PREPARATION		1463d	Fri 02/01/09	Wed 27/08/14																										
1734	592200	T2S User Testing Calendar		224d	Mon 29/04/13	Thu 13/03/14																										
1735	592300	Internal Eurosystem Preparation [T2S User Testing Calendar]		90d	Mon 29/04/13	Fri 30/08/13																										
1739	593400	Market consultation on T2S User Testing calendar		134d	Mon 02/09/13	Thu 13/03/14																										
1756	597300	[Deliverable] - User Testing Calendar		0d	Thu 13/03/14	Thu 13/03/14	Eurosystem														88		13/03/2014									
1757	616200	Certification Test Sets		334d	Fri 01/03/13	Thu 19/06/14																										
1758	616300	Internal Eurosystem Preparation [Certification Test Sets]		334d	Fri 01/03/13	Thu 19/06/14																										
1762	616540	Market Consultation / Information on Certification test sets		164d	Mon 28/10/13	Thu 19/06/14																										
1780	634600	[Deliverable] - CSD Certification Test Cases		0d	Thu 19/06/14	Thu 19/06/14	Eurosystem															88		19/06/2014								
1781	634700	[Deliverable] - CB Certification Test Cases		0d	Thu 19/06/14	Thu 19/06/14	Eurosystem																88		19/06/2014							
1782	634800	[Deliverable] - DCP Certification Test Cases		0d	Thu 19/06/14	Thu 19/06/14	Eurosystem																	88		19/06/2014						
1807	603100	UT Registration Guide		284d	Mon 04/03/13	Fri 11/04/14																										
1808	603200	Internal Eurosystem Preparation [UT Registration Guide]		100d	Mon 04/03/13	Fri 19/07/13																										
1812	606140	Market information on UT Registration Guide		128d	Mon 22/07/13	Wed 22/01/14																										

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
1827	607200	[Deliverable] - Registration Guide for User Testing		0d	Wed 22/01/14	Wed 22/01/14	Eurosystem													42		22/01/2014										
1828	627100	Completed UT Registration Guide for User Testing (network registration)		0d	Fri 11/04/14	Fri 11/04/14	CSDs,CBs															11/04/2014										
1829	611100	User Testing Guide		283d	Mon 04/02/13	Wed 12/03/14																										
1830	611200	Internal Eurosystem Preparation [User Testing Guide]		150d	Mon 04/02/13	Fri 30/08/13																										
1834	612240	Market consultation on User Testing Guide		133d	Mon 02/09/13	Wed 12/03/14																										
1849	616100	[Deliverable] - User Testing Guide		0d	Wed 12/03/14	Wed 12/03/14	Eurosystem													18		12/03/2014										
1857	626100	[Predecessors] UT Environment Preparation		114d	Mon 30/12/13	Wed 11/06/14																										
1858	629100	Completed network connectivity set-up by CSDs,CBs with the Network Service Provider		0d	Fri 11/04/14	Fri 11/04/14	CSDs,CBs															11/04/2014										
1859	626150	Delivery of Connectivity Set-up report by CSDs/CBs		0d	Thu 24/04/14	Thu 24/04/14	CSDs,CBs															24/04/2014										
1860	628150	Send UT Registration Guide to the CSDs/CBs		0d	Wed 14/05/14	Wed 14/05/14	Eurosystem															14/05/2014										
1861	628200	UT Registration Guide filled in by CSDs/CBs		0d	Tue 10/06/14	Tue 10/06/14	CSDs,CBs															10/06/2014										
1864	629200	Readiness of interconnected system (T2,CCBM2)		0d	Mon 30/12/13	Mon 30/12/13	Eurosystem														30/12/2013											
1865	630100	UT Environment Preparation		20d	Wed 11/06/14	Tue 08/07/14																										
1869	634200	UT environment ready		0d	Wed 11/06/14	Wed 11/06/14	Eurosystem															11/06/2014										
1870	634300	Delivery updated version of the EAT Status update		0d	Wed 27/08/14	Wed 27/08/14	Eurosystem																27/08/2014									
1871	497100	Synchronization Point [SP6 - Eurosystem Ready for User Testing]		0d	Tue 02/09/14	Tue 02/09/14	Eurosystem																02/09/2014									
1872	635900	Predecessor of Connectivity before Interoperability Testing		126d	Mon 30/12/13	Mon 30/06/14																										
1873	641100	Delivery MOP		0d	Thu 24/04/14	Thu 24/04/14	Eurosystem															24/04/2014										
1874	641130	Internal system adapted according to UDFS specifications by CBs		0d	Mon 30/06/14	Mon 30/06/14	CBs															30/06/2014										
1875	641150	Internal system adapted according to UDFS specifications by CSDs/CBs		0d	Mon 30/06/14	Mon 30/06/14	CSDs,CBs															30/06/2014										
1876	643100	Completed Registration to the (testing) network (Users, ECB)		0d	Tue 24/06/14	Tue 24/06/14	Eurosystem,CSDs															24/06/2014										
1877	644100	Completed training sessions on Connectivity		0d	Mon 30/12/13	Mon 30/12/13	Eurosystem,CSDs														30/12/2013											
1878	644200	Interim verification of the List of Potential Show stopper from CSDs (dependencies with local regulation)		0d	Mon 09/06/14	Mon 09/06/14	CSDs,CBs															09/06/2014										
1879	636100	USER TESTING EXECUTION		517d	Mon 07/07/14	Wed 29/06/16																										
1880	645100	Synchronization Point [SP7 - Start Connectivity Testing]		0d	Mon 07/07/14	Mon 07/07/14	Eurosystem,CSDs,CBs																07/07/2014									
1881	645150	Connectivity Testing for Interoperability wave 1		82d	Mon 07/07/14	Wed 29/10/14																										
1886	646160	[Deliverable] - User Testing Stage Report (Wave 1) V1.0 [Connectivity phase]		0d	Tue 30/09/14	Tue 30/09/14	Eurosystem															201		30/09/2014								
1890	649200	Synchronization Point [SP8 - Start Bilateral Interoperability Testing]		0d	Wed 01/10/14	Wed 01/10/14	Eurosystem,CSDs,CBs																01/10/2014									
1891	649250	Acceptance Phase		126d	Thu 02/10/14	Thu 02/04/15																										
1892	647200	CSD Acceptance phase wave 1		60d	Thu 02/10/14	Mon 29/12/14																										
1893	647300	CSD Acceptance wave 1		60d	Thu 02/10/14	Mon 29/12/14	CSDs,CBs															02/10/2014										

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

Task		Task		Critical Milestone		Milestone		Critical Task		Project Summary		Group By Summary	

T2S Detailed Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
1928	648250	[Deliverable] - Eurosystem T2S Certification (Wave 2)	◆	0d	Wed 01/04/15	Wed 01/04/15	Eurosystem																									
1929	648290	CB Certification phase wave 2	◆	125d	Thu 02/10/14	Wed 01/04/15																										
1930	648300	CB Certification wave 2	◆	120d	Thu 02/10/14	Wed 25/03/15	CSDs,CBs																									
1932	648360	[Deliverable] - Eurosystem T2S Certification (Wave 2)	◆	0d	Wed 01/04/15	Wed 01/04/15	Eurosystem																									
1933	648390	CSD Certification phase wave 3	◆	184d	Thu 02/10/14	Mon 22/06/15																										
1934	648400	CSD Certification wave 3	◆	179d	Thu 02/10/14	Wed 17/06/15	CSDs,CBs																									
1936	648550	[Deliverable] - Eurosystem T2S Certification (Wave 3)	◆	0d	Mon 22/06/15	Mon 22/06/15	Eurosystem																									
1937	648590	CB Certification phase wave 3	◆	184d	Thu 02/10/14	Mon 22/06/15																										
1938	648600	CB Certification wave 3	◆	179d	Thu 02/10/14	Wed 17/06/15	CSDs,CBs																									
1940	648650	[Deliverable] - Eurosystem T2S Certification (Wave 3)	◆	0d	Mon 22/06/15	Mon 22/06/15	Eurosystem																									
1941	650100	Interoperability - Community - Business Day Testing Wave 1		447d	Mon 01/09/14	Wed 18/05/16																										
1942	652100	Interoperability Bilateral Testing Wave 1		55d	Wed 01/10/14	Thu 18/12/14																										
1944	653110	Start Interoperability Bilateral Testing Wave 1	◆	0d	Wed 01/10/14	Wed 01/10/14	Eurosystem,CSDs																									
1999	714200	Finish Interoperability Bilateral Testing Wave 1	◆	0d	Thu 18/12/14	Thu 18/12/14																										
2001	714280	[Deliverable] - User Testing Stage Report (Wave 1) V1.1 Interoperability Bilateral phase]	◆	0d	Thu 18/12/14	Thu 18/12/14	Eurosystem																									
2002	714300	Synchronization Point [SP9.1 - Start Multilateral Interoperability Testing (wave 1)]	◆	0d	Mon 29/12/14	Mon 29/12/14	Eurosystem,CSDs,CBs																									
2003	722000	Interoperability Multilateral testing Wave 1	◆	45d	Tue 30/12/14	Wed 04/03/15																										
2007	723100	[Deliverable] - User Testing Stage Report (Wave 1) V1.2 [Interoperability Multilateral phase]	◆	0d	Wed 04/03/15	Wed 04/03/15	Eurosystem																									
2040	726400	Connectivity Testing for Migration wave 1		42d	Mon 01/09/14	Wed 29/10/14																										
2044	726800	Migration Wave 1	◆	100d	Wed 03/09/14	Tue 27/01/15																										
2053	730100	Synchronization Point [SP10.1 - Start Community Testing Wave 1]	◆	0d	Wed 04/03/15	Wed 04/03/15	Eurosystem,CSDs,CBs																									
2054	730200	Connectivity Testing for Community wave 1		20d	Thu 05/02/15	Wed 04/03/15																										
2057	731100	Community testing Wave 1		50d	Wed 04/03/15	Thu 14/05/15																										
2058	732100	Community Testing Wave 1 - [First Window]		25d	Wed 04/03/15	Wed 08/04/15																										
2059	732101	Start Community Test Wave 1	◆	0d	Wed 04/03/15	Wed 04/03/15	Eurosystem,CSDs,CBs																									
2090	762100	Community Testing Wave 1 - [Second Window]		20d	Thu 09/04/15	Thu 07/05/15																										
2118	789200	Finish Community Test Wave 1	◆	0d	Thu 07/05/15	Thu 07/05/15	Eurosystem,CSDs																									
2120	789400	[Deliverable] - User Testing Stage Report (Wave 1) V1.3 [Community phase]	◆	0d	Thu 14/05/15	Thu 14/05/15	Eurosystem																									
2121	789500	DCP-DCAH Certification phase wave 1	◆	30d	Thu 05/03/15	Wed 15/04/15																										
2124	789800	[Deliverable] - Certification report for DCPs (Wave 1)	◆	0d	Wed 15/04/15	Wed 15/04/15	Eurosystem																									
2127	792000	[Deliverable] - Certification report for DCAH (Wave 1)	◆	0d	Wed 15/04/15	Wed 15/04/15	Eurosystem																									

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
2128	796000	Synchronization Point [SP11.1 - Start Business Day Testing Wave 1]		0d	Mon 18/05/15	Mon 18/05/15	Eurosystem,CSDs,CBs																									
2129	796100	Business day test Wave 1		19d	Mon 18/05/15	Fri 12/06/15																										
2130	796200	Start Business day test Wave 1		0d	Mon 18/05/15	Mon 18/05/15																										
2151	831200	Finish Business day test Wave 1		0d	Mon 08/06/15	Mon 08/06/15	Eurosystem,CSDs																									
2153	832300	[Deliverable] - User Testing Stage Report (Wave 1) V1.4 [Business day phase]		0d	Fri 12/06/15	Fri 12/06/15	Eurosystem																									
2154	832400	Progress Report Wave 1(recurrent task during UT phase until End of User Testing Wave 1)		10d	Fri 28/11/14	Thu 11/12/14																										
2155	832500	Preparation Progress Report Wave 1 (recurrent task)		10d	Fri 28/11/14	Thu 11/12/14	CSDs,CBs																									
2156	832600	[Deliverable] - Progress Report Wave 1		0d	Thu 11/12/14	Thu 11/12/14	CSDs,CBs																									
2157	836100	Support Testing for other waves		258d	Mon 01/06/15	Wed 18/05/16																										
2158	836200	Support Community Test of wave 2		100d	Mon 01/06/15	Wed 14/10/15	CSDs																									
2159	836300	Support Community Test of wave 3		140d	Tue 10/11/15	Wed 18/05/16	CSDs																									
2160	833100	Synchronization Point [SP12.1 - End of User Testing Execution Phase Wave 1]		0d	Mon 15/06/15	Mon 15/06/15	Eurosystem,CSDs,CBs																									
2161	840100	Interoperability - Community - Business Day Testing Wave 2		487d	Mon 07/07/14	Wed 18/05/16																										
2162	840200	Connectivity Testing for Interoperability wave 2		82d	Mon 07/07/14	Wed 29/10/14																										
2167	840560	[Deliverable] - User Testing Stage Report (Wave 2) V2.0 [Connectivity phase]		0d	Fri 26/09/14	Fri 26/09/14	Eurosystem																									
2168	842100	Interoperability Bilateral testing Waves 2		115d	Wed 01/10/14	Wed 18/03/15																										
2169	843100	Interoperability Bilateral Testing Waves 2 [First Window]		55d	Wed 01/10/14	Thu 18/12/14																										
2170	843101	Start Interoperability Bilateral Testing Waves 2		0d	Wed 01/10/14	Wed 01/10/14	Eurosystem,CSDs,CBs																									
2199	879100	Interoperability Bilateral Testing Wave 2 [Second Window]		50d	Thu 08/01/15	Wed 18/03/15																										
2225	912150	Finish Interoperability Bilateral Testing Wave 2		0d	Wed 18/03/15	Wed 18/03/15	Eurosystem,CSDs																									
2227	914180	[Deliverable] - User Testing Stage Report (Wave 2) V2.1 [Interoperability Bilateral phase]		0d	Wed 18/03/15	Wed 18/03/15	Eurosystem																									
2228	913000	Synchronization Point [SP9.2 - Start Multilateral Interoperability Testing (wave 2)]		0d	Thu 02/04/15	Thu 02/04/15	Eurosystem,CSDs,CBs																									
2229	911000	Interoperability Multilateral testing Wave 2		40d	Fri 03/04/15	Fri 29/05/15																										
2233	913100	[Deliverable] - User Testing Stage Report (Wave 2) V2.2 [Interoperability Multilateral phase]		0d	Fri 29/05/15	Fri 29/05/15	Eurosystem																									
2266	917300	Connectivity Testing for Migration wave 2		42d	Wed 01/10/14	Fri 28/11/14																										
2270	917700	Migration Wave 2		150d	Mon 06/10/14	Fri 08/05/15																										
2280	920100	Synchronization Point [SP10.2 - Start Community Testing Wave 2]		0d	Fri 29/05/15	Fri 29/05/15	Eurosystem,CSDs,CBs																									
2281	920200	Connectivity Testing for Community wave 2		40d	Fri 03/04/15	Fri 29/05/15																										
2284	922100	Community Testing Wave 2		115d	Fri 29/05/15	Wed 04/11/15																										
2285	922200	Community Testing Wave 2 - [First Window]		65d	Fri 29/05/15	Wed 26/08/15																										
2286	922101	Start Community Test Wave 2		0d	Fri 29/05/15	Fri 29/05/15	Eurosystem,CSDs																									

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
2345	954000	Finish Community Test Wave 2		0d	Wed 28/10/15	Wed 28/10/15	Eurosystem,CSDs																									
2347	979300	[Deliverable] - User Testing Stage Report (Wave 2) V2.3 [Community phase]		0d	Wed 04/11/15	Wed 04/11/15	Eurosystem																									
2348	979400	DCP-DCAH Certification phase wave 2		65d	Thu 09/07/15	Wed 07/10/15																										
2351	979700	[Deliverable] - Certification report for DCPs (Wave 2)		0d	Wed 07/10/15	Wed 07/10/15	Eurosystem																									
2354	981000	[Deliverable] - Certification report for DCAH (Wave 2)		0d	Wed 07/10/15	Wed 07/10/15	Eurosystem																									
2355	1024400	Synchronization Point [SP11.2 - Start Business Day Testing Wave 2]		0d	Mon 09/11/15	Mon 09/11/15	Eurosystem,CSDs,CBs																									
2356	986100	Business day test Wave 2		44d	Mon 09/11/15	Mon 11/01/16																										
2357	986200	Start Business day test Wave 2		0d	Mon 09/11/15	Mon 09/11/15	Eurosystem,CSDs																									
2378	1021200	Finish Business day test Wave 2		0d	Mon 28/12/15	Mon 28/12/15	Eurosystem,CSDs																									
2380	1022300	[Deliverable] - User Testing Stage Report (Wave 2) V2.4 [Business day phase]		0d	Mon 11/01/16	Mon 11/01/16	Eurosystem																									
2381	1022500	Progress Report Wave 2 (recurrent task during UT phase End of User Testing Wave 2)		10d	Fri 28/11/14	Thu 11/12/14																										
2382	1022600	Preparation Progress Report Wave 2 (recurrent task)		10d	Fri 28/11/14	Thu 11/12/14	CSDs,CBs																									
2383	1022700	[Deliverable] - Progress Report Wave 2 (recurrent task)		0d	Thu 11/12/14	Thu 11/12/14	CSDs,CBs																									
2384	1022800	Support Testing for other waves		319d	Thu 05/03/15	Wed 18/05/16																										
2385	1022900	Support Community Test of wave 1		75d	Thu 05/03/15	Thu 18/06/15	CSDs																									
2386	1023000	Support Community Test of wave 3		140d	Tue 10/11/15	Wed 18/05/16	CSDs																									
2387	1023100	Synchronization Point [SP12.2 - End of User Testing Execution Phase Wave 2]		0d	Mon 18/01/16	Mon 18/01/16	Eurosystem,CSDs,CBs																									
2388	2200000	Interoperability - Community - Business Day Testing Wave 3		517d	Mon 07/07/14	Wed 29/06/16																										
2389	2200100	Connectivity Testing for Interoperability wave 3		82d	Mon 07/07/14	Wed 29/10/14																										
2394	2200600	[Deliverable] - User Testing Stage Report (Wave 3) V3.0 [Connectivity phase]		0d	Tue 30/09/14	Tue 30/09/14	Eurosystem																									
2395	2201000	Interoperability Bilateral testing Wave 3		185d	Wed 01/10/14	Tue 23/06/15																										
2396	2202000	Interoperability Bilateral Testing Wave 3 [First Window]		80d	Wed 01/10/14	Wed 28/01/15																										
2397	2203000	Start Interoperability Bilateral Test Wave 3		0d	Wed 01/10/14	Wed 01/10/14	Eurosystem,CSDs																									
2455	2273000	Finish Interoperability Bilateral Testing Wave 3 Second window		0d	Tue 23/06/15	Tue 23/06/15	Eurosystem,CSDs																									
2457	2273080	[Deliverable] - User Testing Stage Report (Wave 3) V3.1 Interoperability Bilateral phase]		0d	Tue 23/06/15	Tue 23/06/15	Eurosystem																									
2458	2273500	Synchronization Point [SP9.3 - Start Multilateral Interoperability Testing (wave 3)]		0d	Tue 23/06/15	Tue 23/06/15	Eurosystem,CSDs,CBs																									
2459	2273100	Interoperability Multilateral testing Wave 3		93d	Wed 24/06/15	Fri 30/10/15																										
2463	2275000	[Deliverable] - User Testing Stage Report(Wave 3) V3.2 [Interoperability Multilateral phase]		0d	Fri 30/10/15	Fri 30/10/15	Eurosystem																									
2496	2282050	Connectivity Testing for Migration wave 3		40d	Fri 10/04/15	Fri 05/06/15																										
2500	2282400	Migration Wave 3		148d	Fri 17/04/15	Mon 09/11/15																										
2504	2276000	[Predecessors] Community test		138d	Thu 02/04/15	Mon 12/10/15																										

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
2505	2276100	Delivery certification Step1 (CSDs able to use T2S functionalities)		0d	Mon 22/06/15	Mon 22/06/15	CSDs																									
2507	2281000	Confirmation that CSDs participants are ready (wave 3)		0d	Mon 12/10/15	Mon 12/10/15	CSDs																									
2508	2282000	Confirmation that CB members are ready (wave 3)		0d	Mon 12/10/15	Mon 12/10/15	CBs																									
2510	2284000	Synchronization Point [SP10.3 - Start Community Testing Wave 3]		0d	Mon 09/11/15	Mon 09/11/15	Eurosystem,CSDs,CBs																									
2511	2284100	Connectivity Testing for Community wave 3		40d	Tue 13/10/15	Mon 07/12/15																										
2514	2285000	Community testing Wave 3		125d	Mon 09/11/15	Wed 27/04/16																										
2515	2286000	Community Testing Wave 3 [First Window]		70d	Mon 09/11/15	Fri 12/02/16																										
2516	2287000	Start Community Test Wave 3		0d	Mon 09/11/15	Mon 09/11/15	Eurosystem,CSDs																									
2575	2319800	Finish Community Test Wave 3		0d	Wed 20/04/16	Wed 20/04/16	Eurosystem,CSDs																									
2577	2345100	[Deliverable] - User Testing Stage Report (Wave 3) V3.3 [Community phase]		0d	Wed 27/04/16	Wed 27/04/16	Eurosystem																									
2578	2346000	DCP-DCAH Certification phase wave 3		135d	Tue 22/12/15	Wed 22/06/16																										
2581	2346300	[Deliverable] - Certification report for DCPs (Wave 3)		0d	Fri 18/03/16	Fri 18/03/16	Eurosystem																									
2584	2346700	[Deliverable] - Certification report for DCAH (Wave 3)		0d	Fri 18/03/16	Fri 18/03/16	Eurosystem																									
2585	2351100	Synchronization Point [SP11.3 - Start Business Day Testing Wave 3]		0d	Wed 27/04/16	Wed 27/04/16	Eurosystem,CSDs,CBs																									
2586	2352000	Business day test Wave 3		40d	Wed 27/04/16	Wed 22/06/16																										
2587	2353000	Start Business day test Wave 3		0d	Wed 27/04/16	Wed 27/04/16	Eurosystem,CSDs																									
2608	2389000	Finish Business day test Wave 3		0d	Wed 15/06/16	Wed 15/06/16	Eurosystem,CSDs																									
2610	2390200	[Deliverable] - User Testing Stage Report (Wave 3) V3.4 [Business day phase]		0d	Wed 22/06/16	Wed 22/06/16	Eurosystem																									
2611	2391000	Progress Report Wave 3 (recurrent task during UT phase End of User Testing Wave 3)		10d	Fri 28/11/14	Thu 11/12/14																										
2612	2391100	Preparation Progress Report Wave 3 (recurrent task)		10d	Fri 28/11/14	Thu 11/12/14	CSDs,CBs																									
2613	2391200	[Deliverable] - Progress Report Wave 3 (recurrent task)		0d	Thu 11/12/14	Thu 11/12/14	CSDs,CBs																									
2614	2394400	Support Testing for other waves		161d	Thu 05/03/15	Wed 14/10/15																										
2615	2394500	Support Community Test of wave 1		75d	Thu 05/03/15	Thu 18/06/15	CSDs																									
2616	2394600	Support Community Test of wave 2		100d	Mon 01/06/15	Wed 14/10/15	CSDs																									
2617	2394200	Synchronization Point [SP12.3 - End of User Testing Execution Phase Wave 3]		0d	Wed 29/06/16	Wed 29/06/16	Eurosystem,CSDs,CBs																									
2618	2394300	Defects and Release Management during UT phases		452d	Mon 07/07/14	Wed 30/03/16	Eurosystem																									
2619	1310100	CONTRACTUAL FRAMEWORK		602d	Tue 01/09/09	Wed 21/12/11																										
2748	1027100	OPERATIONAL READINESS		1984d	Mon 15/06/09	Mon 30/01/17																										
2749	1027200	NETWORK AND CONNECTIVITY		1260d	Mon 15/06/09	Thu 24/04/14																										
2750	1028100	NETWORK AND CONNECTIVITY		1260d	Mon 15/06/09	Thu 24/04/14																										
2809	1063480	Tender process for Value-Added Services (VA-NSPs)		147d	Fri 08/07/11	Tue 31/01/12																										

	Task		Task		Critical Milestone		Milestone		Critical Task		Project Summary		Group By Summary	

	Task		Task		Critical Milestone		Milestone		Critical Task		Project Summary		Group By Summary	

T2S Detailed Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
2988	1121100	[Deliverable] - Manual of Operational Procedures (MOP) V1.2 before Start Operation in T2S Wave 1		0d	Thu 11/06/15	Thu 11/06/15	Eurosystem																									
2989	1121200	Production MOP V1.3 (revised MOP V1.2 after Start Operation in T2S wave 1 and during Business Day Test wave 2)		121d	Tue 21/07/15	Thu 07/01/16																										
2990	1121300	Monthly Telco (Recurring task)		1d	Tue 21/07/15	Tue 21/07/15	Eurosystem																									
2991	1121400	Quarterly meeting (Recurring task)		1d	Wed 16/09/15	Wed 16/09/15	Eurosystem,CSDs,CBs																									
2993	1143160	Submission MOP V1.3 after Start Operation in T2S wave 1 to OMG		0d	Wed 30/09/15	Wed 30/09/15	Eurosystem																									
2994	1143170	Approval MOP V1.3 after Start Operation in T2S wave 1 by OMG		0d	Wed 07/10/15	Wed 07/10/15	OMG																									
2995	1145200	[Deliverable] - Manual of Operational Procedures (MOP) V1.3 during Business Day Test Wave 2		0d	Thu 07/01/16	Thu 07/01/16	Eurosystem																									
2996	1145300	Production MOP V1.4 (revised MOP V1.3 after Start Operation in T2S wave 2 and during Business Day Test wave 3)		50d	Thu 25/02/16	Mon 02/05/16																										
2997	1145400	Monthly Telco (Recurring task)		1d	Thu 25/02/16	Thu 25/02/16	Eurosystem																									
2998	1145450	Quarterly meeting (Recurring task)		1d	Wed 06/04/16	Wed 06/04/16	Eurosystem,CSDs,CBs																									
3000	1145600	Submission MOP V1.4 after Start Operation in T2S wave 2 to OMG		0d	Wed 20/04/16	Wed 20/04/16	Eurosystem																									
3001	1145700	Approval MOP V1.4 after Start Operation in T2S wave 2 by OMG		0d	Wed 27/04/16	Wed 27/04/16	OMG																									
3002	1145800	[Deliverable] - Manual of Operational Procedures (MOP) V1.4 during Business Day Test Wave 3		0d	Mon 02/05/16	Mon 02/05/16	Eurosystem																									
3003	1145900	Production MOP V2.0 (Operational activities after Start Operation in T2S wave 3)		97d	Thu 23/06/16	Wed 02/11/16																										
3004	1145950	Monthly Telco (Recurring task)		1d	Tue 16/08/16	Tue 16/08/16	Eurosystem																									
3005	1145960	Quarterly meeting (Recurring task)		1d	Wed 12/10/16	Wed 12/10/16	Eurosystem,CSDs,CBs																									
3007	1146020	Submission MOP V2.0 after Start Operation in T2S wave 3 to OMG		0d	Wed 26/10/16	Wed 26/10/16	Eurosystem																									
3008	1146040	Approval MOP V2.0 after Start Operation in T2S wave 3 by OMG		0d	Wed 02/11/16	Wed 02/11/16	OMG																									
3009	1146050	[Deliverable] - Manual of Operational Procedures (MOP) V2.0 after start of operations in T2S of wave 3		0d	Thu 23/06/16	Thu 23/06/16	Eurosystem																									
3017	1110200	SERVICE LEVEL AGREEMENT		0d	Fri 30/12/11	Fri 30/12/11																										
3018	1187100	MIGRATION		1956d	Thu 23/07/09	Mon 30/01/17																										
3019	1187200	MIGRATION PREPARATION		1800d	Thu 23/07/09	Thu 30/06/16																										
3027	1200100	Preparation phase		1337d	Mon 02/05/11	Thu 30/06/16																										
3028	1201100	Processes and tools for Data Migration		244d	Mon 02/05/11	Thu 05/04/12																										
3029	1201200	Internal Eurosystem Preparation [Processes and tools for Data Migration]		67d	Mon 02/05/11	Tue 02/08/11																										
3033	1203400	Market consultation on Processes and tools for Data Migration		122d	Wed 19/10/11	Thu 05/04/12																										
3034	1204170	Meeting with CSDs/CBs		1d	Wed 19/10/11	Wed 19/10/11	PMG																									
3035	1204180	Feedbacks from CSDs/CBs		15d	Thu 20/10/11	Wed 09/11/11	CSDs,CBs																									
3037	1204210	Submission User Requirements for data migration tools to CSDs/CBs (1st review cycle)		0d	Wed 23/11/11	Wed 23/11/11	Eurosystem																									
3039	1204350	Feedbacks from CSDs/CBs		20d	Fri 02/12/11	Thu 29/12/11	CSDs,CBs																									
3041	1205200	Submission User Requirements for data migration tools to CSDs/CBs (2nd review cycle)		0d	Thu 12/01/12	Thu 12/01/12	Eurosystem																									

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

T2S Detailed Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017	
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half	
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	
3043	1205350	Feedbacks from CSDs/CBs		10d	Wed 01/02/12	Tue 14/02/12	CSDs,CBs					01/02/2012	14/02/2012																				
3049	1206100	[Deliverable] - User Requirements for data migration tools V1.0		0d	Thu 05/04/12	Thu 05/04/12	Eurosystem					73	05/04/2012																				
3050	1207100	Composition of Migration Waves & Dates		116d	Fri 29/06/12	Mon 10/12/12																											
3051	1207150	Reception of Proposal of migration waves plus migration dates for each CSD/CB (as part of the feasibility study)		0d	Fri 29/06/12	Fri 29/06/12	CSDs,CBs						29/06/2012																				
3052	1207200	Eurosystem consultation: review of CSDs proposal by the Eurosystem		71d	Fri 29/06/12	Mon 08/10/12																											
3053	1209100	Coordination by Eurosystem of proposal for the Composition of migration waves (incl. CSD/CBs views)		26d	Fri 29/06/12	Fri 03/08/12	Eurosystem,CSDs,CBs					29/06/2012	03/08/2012																				
3054	546350	[Deliverable] - Composition and Timing Migration Waves by CSDs/CBs		0d	Fri 03/08/12	Fri 03/08/12	CSDs,CBs					593	03/08/2012																				
3055	1209130	Evaluation by Eurosystem of proposal for the timing of migration waves (incl. CSD/CBs views)		40d	Mon 06/08/12	Fri 28/09/12	Eurosystem,CSDs,CBs					06/08/2012	28/09/2012																				
3056	1209150	Confirmation of the Timing and Composition of Migration Waves by Eurosystem		0d	Mon 08/10/12	Mon 08/10/12	Eurosystem					593	08/10/2012																				
3057	1209160	Market Consultation on Composition of Migration Waves & Dates (only whether CSDs proposal conflicts with migration criteria)		96d	Fri 27/07/12	Mon 10/12/12																											
3059	1209200	Submission revised proposal of Composition of migration waves & dates V 0.1 to MSG (1st review cycle)		0d	Thu 09/08/12	Thu 09/08/12	Eurosystem						09/08/2012																				
3060	1209300	Migration Sub Group (MSG) Meeting		1d	Tue 04/09/12	Tue 04/09/12	PMG					04/09/2012	04/09/2012																				
3062	1209500	Submission Composition of migration waves & dates V0.2 to MSG (2st review cycle)		0d	Tue 11/09/12	Tue 11/09/12	Eurosystem						11/09/2012																				
3063	1209600	Migration Sub Group (MSG) Meeting		1d	Wed 26/09/12	Wed 26/09/12	PMG					26/09/2012	26/09/2012																				
3068	1211000	Submission Composition of migration waves & dates V1.0 to CSG		0d	Mon 22/10/12	Mon 22/10/12	Eurosystem						22/10/2012																				
3069	1212000	CSG Meeting: approval of Composition of migration waves & dates V1.0		1d	Tue 06/11/12	Tue 06/11/12	CCG					06/11/2012	06/11/2012																				
3075	1218000	[Deliverable] - Confirmation of composition and timing of Migration Waves V1.0		0d	Mon 10/12/12	Mon 10/12/12	Eurosystem					71	10/12/2012																				
3076	1218100	Migration profiles & Registration Guide		289d	Mon 03/10/11	Fri 09/11/12																											
3077	1218200	Internal Eurosystem Preparation [Migration profiles & Registration Guide]		95d	Mon 03/10/11	Fri 10/02/12																											
3080	1220400	Market Consultation on Migration profiles & Registration Guide		194d	Mon 13/02/12	Fri 09/11/12																											
3082	1222200	Submission Migration profiles and Registration Guide V0.1 to MSG (1st review cycle)		0d	Fri 23/03/12	Fri 23/03/12	Eurosystem						23/03/2012																				
3083	1222300	Migration Sub Group (MSG) Meeting		1d	Mon 26/03/12	Mon 26/03/12	PMG					26/03/2012	26/03/2012																				
3084	1222250	Review Migration profiles & Registration Guide V0.1 by MSG		15d	Tue 27/03/12	Mon 16/04/12	OMG					27/03/2012	16/04/2012																				
3086	1222500	Submission Migration profiles and Registration Guide V0.2 to MSG (2st review cycle)		0d	Mon 30/04/12	Mon 30/04/12	Eurosystem						30/04/2012																				
3087	1222600	Migration Sub Group (MSG) Meeting		1d	Tue 01/05/12	Tue 01/05/12	PMG					01/05/2012	01/05/2012																				
3088	1222650	Review Migration profiles & Registration Guide V0.2 by MSG		15d	Wed 02/05/12	Tue 22/05/12	OMG					02/05/2012	22/05/2012																				
3090	1222800	Submission Migration profiles and Registration Guide V0.3 to PMG		0d	Tue 05/06/12	Tue 05/06/12	Eurosystem						05/06/2012																				
3091	1222900	Migration Sub Group (PMG) Meeting		1d	Wed 06/06/12	Wed 06/06/12	PMG					06/06/2012	06/06/2012																				
3092	1222850	Review Migration profiles & Registration Guide V0.2 by MSG		15d	Thu 07/06/12	Wed 27/06/12	OMG					07/06/2012	27/06/2012																				
3097	1221300	Submission to PMG Migration profiles and Registration Guide V0.5		0d	Wed 01/08/12	Wed 01/08/12	Eurosystem						01/08/2012																				
3098	1221400	PMG Meeting		1d	Thu 23/08/12	Thu 23/08/12	PMG					23/08/2012	23/08/2012																				

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

Task		Task		Critical Milestone		Milestone		Critical Task		Project Summary		Group By Summary	

T2S Detailed Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
3158	1233850	Review Detailed migration script V0.2 by OMG		15d	Thu 08/05/14	Wed 28/05/14	OMG																									
3160	1234000	Submission Detailed migration script V0.3 for each migration group to PMG (3st review cycle)		0d	Wed 11/06/14	Wed 11/06/14	Eurosystem																									
3161	1234100	Migration Sub Group (PMG) Meeting		1d	Thu 12/06/14	Thu 12/06/14	PMG																									
3162	1234150	Review Detailed migration script V0.3 by OMG		15d	Fri 13/06/14	Thu 03/07/14	OMG																									
3164	1234300	Submission Detailed migration script V0.4 for each migration group to T2S Board		0d	Thu 17/07/14	Thu 17/07/14	Eurosystem																									
3165	1234400	PB Meeting		2d	Fri 01/08/14	Mon 04/08/14	PMG																									
3167	1234600	Submission to PMG of Detailed migration script V0.5for each migration group		0d	Thu 14/08/14	Thu 14/08/14	Eurosystem																									
3168	1234700	PMG Meeting		1d	Fri 05/09/14	Fri 05/09/14	PMG																									
3170	1234900	Submission to CSG of Detailed migration script V1.0 for each migration group		0d	Fri 12/09/14	Fri 12/09/14	Eurosystem																									
3171	1235000	CSG Meeting		1d	Thu 02/10/14	Thu 02/10/14	CSG																									
3176	1235400	[Deliverable] - Detailed Migration Weekend Script V1.0 Wave 1		0d	Fri 28/11/14	Fri 28/11/14	Eurosystem																									
3177	1235500	Review Migration Weekend Script for wave 1 before Start Operation in T2S		31d	Fri 24/04/15	Mon 08/06/15																										
3179	1235650	Market consultation Migration Weekend Script for wave 1 before Start Operation in T2S		21d	Fri 08/05/15	Mon 08/06/15																										
3180	1235700	Submission Detailed migration script V1.1 for migration wave 1		0d	Fri 08/05/15	Fri 08/05/15	Eurosystem																									
3181	1235800	Migration Sub Group (MSG) Meeting		1d	Mon 01/06/15	Mon 01/06/15	PMG																									
3183	1236000	[Deliverable] - Detailed Migration Weekend Script V1.2 Wave 1		0d	Mon 08/06/15	Mon 08/06/15	Eurosystem																									
3184	1236400	Internal Eurosystem Preparation [Migration Weekend Script for wave 2]		90d	Mon 02/03/15	Thu 02/07/15																										
3187	1236640	Market consultation Migration Weekend Script for wave 2		92d	Fri 03/07/15	Mon 09/11/15																										
3189	1236700	Submission Detailed migration script V2.0 for migration wave 2		0d	Thu 30/07/15	Thu 30/07/15	Eurosystem																									
3190	1236800	Migration Sub Group (MSG) Meeting		1d	Fri 21/08/15	Fri 21/08/15	PMG																									
3192	1237000	Submission draft version of Detailed migration script V2.1 for migration wave 2 to MSG		0d	Fri 18/09/15	Fri 18/09/15	Eurosystem																									
3193	1237100	Migration Sub Group (MSG) Meeting		1d	Mon 12/10/15	Mon 12/10/15	PMG																									
3196	1237300	[Deliverable] - Detailed Migration Weekend Script V2.2 Wave 2		0d	Mon 09/11/15	Mon 09/11/15	Eurosystem																									
3197	1237350	Review Migration Weekend Script for wave 2 before Start Operation in T2S wave 2		26d	Wed 09/12/15	Thu 14/01/16																										
3199	1237450	Market consultation Migration Weekend Script for wave 2 before Start Operation in T2S		16d	Tue 22/12/15	Thu 14/01/16																										
3200	1235720	Submission draft version of Detailed migration script V2.3 for migration wave 2		0d	Tue 22/12/15	Tue 22/12/15	Eurosystem																									
3201	1235820	Migration Sub Group (MSG) Meeting		1d	Thu 07/01/16	Thu 07/01/16	PMG																									
3203	1236020	[Deliverable] - Detailed Migration Weekend Script V2.4 Wave 2		0d	Thu 14/01/16	Thu 14/01/16	Eurosystem																									
3204	1237400	Internal Eurosystem Preparation [Migration Weekend Script for wave 3]		80d	Thu 20/08/15	Wed 09/12/15																										
3207	1237540	Market consultation on Migration Weekend Script for wave 3		149d	Thu 10/12/15	Thu 30/06/16																										
3209	1237600	Submission draft version of Detailed migration script V3.0 for migration wave 3		0d	Thu 07/01/16	Thu 07/01/16	Eurosystem																									

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

T2S Detailed Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
3210	1237700	Migration Sub Group (MSG) Meeting		1d	Fri 29/01/16	Fri 29/01/16	PMG																									
3212	1237900	Submission draft version of Detailed migration script V3.1 for migration wave 3 to MSG		0d	Wed 24/02/16	Wed 24/02/16	Eurosystem																									
3213	1238000	Migration Sub Group (MSG) Meeting		1d	Thu 17/03/16	Thu 17/03/16	PMG																									
3216	1238200	[Deliverable] - Detailed Migration Weekend Script V3.2 Wave 3		0d	Tue 12/04/16	Tue 12/04/16	Eurosystem																									
3217	1234650	Review Migration Weekend Script for wave 3 before Start Operation in T2S wave 3		26d	Thu 26/05/16	Thu 30/06/16																										
3219	1235710	Market consultation Migration Weekend Script for wave 3 before Start Operation in T2S		16d	Wed 08/06/16	Thu 30/06/16																										
3220	1235740	Submission draft version of Detailed migration script V3.3 for migration wave 3		0d	Wed 08/06/16	Wed 08/06/16	Eurosystem																									
3221	1235840	Migration Sub Group (MSG) Meeting		1d	Thu 23/06/16	Thu 23/06/16	PMG																									
3223	1236040	[Deliverable] - Detailed Migration Weekend Script V3.4 Wave 3		0d	Thu 30/06/16	Thu 30/06/16	Eurosystem																									
3239	1269100	PRE-MIGRATION TASKS (WAVE 1)		255d	Fri 20/06/14	Fri 19/06/15																										
3240	1235410	Implementation Migration phase (wave 1)		80d	Mon 17/11/14	Thu 12/03/15																										
3241	1244100	Preparation of Migration Weekend (wave 1)		80d	Mon 17/11/14	Thu 12/03/15																										
3242	124410	Start preparation of Migration Weekend		0d	Mon 01/12/14	Mon 01/12/14	Eurosystem																									
3243	1245100	[Predecessors] Preparation of Production Environment		10d	Mon 01/12/14	Fri 12/12/14																										
3244	387100	Network ready for Production		0d	Mon 01/12/14	Mon 01/12/14	Eurosystem																									
3246	1246200	Collection of Registration Forms from CSDs / CBs (wave 1 + CSDs/CBs with Common Static Data)		10d	Mon 01/12/14	Fri 12/12/14	Eurosystem																									
3247	1247100	Registration Form filled in (wave 1 + CSDs/CBs with Common Static Data)		0d	Fri 12/12/14	Fri 12/12/14	CSDs,CBs																									
3248	1249100	Preparation of production environment		80d	Mon 17/11/14	Thu 12/03/15																										
3249	1258200	T2S helpdesk is operational and contact details have been communicated to all relevant T2S parties		0d	Mon 17/11/14	Mon 17/11/14	Eurosystem																									
3250	1250100	Synchronization Point [SP13 - Eurosystem ready for Production]		0d	Mon 01/12/14	Mon 01/12/14	Eurosystem																									
3253	1252150	Input Registration Data completed		0d	Thu 29/01/15	Thu 29/01/15	Eurosystem																									
3254	1256100	PROD environment available for users		0d	Thu 05/02/15	Thu 05/02/15	Eurosystem																									
3255	1255200	Completed network registration by CSDs (wave 1)		0d	Thu 05/02/15	Thu 05/02/15	CSDs																									
3256	1255300	Completed network registration by CBs (wave 1)		0d	Thu 05/02/15	Thu 05/02/15	CBs																									
3257	1257100	Synchronization Point [SP14.1 -Ready to connect to Production wave 1]		0d	Thu 05/02/15	Thu 05/02/15	Eurosystem,CSDs																									
3258	1255100	Prod Connectivity testing (wave 1)		20d	Fri 13/02/15	Thu 12/03/15	CSDs																									
3259	1263100	Successful connectivity tests CSD (wave 1)		0d	Thu 12/03/15	Thu 12/03/15	CSDs																									
3260	1255400	Successful connectivity tests CB (wave 1)		0d	Thu 12/03/15	Thu 12/03/15	CBs																									
3266	1272100	Synchronization Point [SP15.1 - Ready to upload Static Data wave 1]		0d	Thu 19/03/15	Thu 19/03/15	Eurosystem,CSDs																									
3268	1268200	Migration Common Static Data		105d	Fri 23/01/15	Fri 19/06/15																										
3269	1268300	Start Static Data identification and collection (for all CSDs/CBs with Common Static Data)		0d	Fri 23/01/15	Fri 23/01/15	CSDs,CBs																									

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

T2S Detailed Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1				
3270	1268400	Relevant Static Data ready by CSDs (for all CSDs with Common Static Data)		0d	Thu 05/03/15	Thu 05/03/15	CSDs																									
3271	1268500	Relevant Static Data ready by CBs (for all CBs with Common Static Data)		0d	Thu 05/03/15	Thu 05/03/15	CBs																									
3272	1268600	T2S System Configuration parameters finalised		0d	Thu 29/01/15	Thu 29/01/15	ECB,4CB																									
3273	1268700	Common Static Data input by CSDs and CBs and Maintenance Static Data (for all CSDs/CBs with Common Static Data)		65d	Fri 20/03/15	Fri 19/06/15	CBs, CSDs,Eurosystem																									
3275	1269200	Migration Proprietary Static Data (wave 1)		105d	Fri 23/01/15	Fri 19/06/15																										
3276	1270100	Start Static Data identification and collection (wave 1)		0d	Fri 23/01/15	Fri 23/01/15	CSDs,CBs																									
3277	1271200	Relevant Static Data ready by CSDs (wave1)		0d	Thu 05/03/15	Thu 05/03/15	CSDs																									
3278	1271300	Relevant Static Data ready by CBs (wave1)		0d	Thu 05/03/15	Thu 05/03/15	CBs																									
3279	1270400	T2S System Configuration parameters finalised		0d	Thu 29/01/15	Thu 29/01/15	Eurosystem																									
3280	1273100	Proprietary Static Data input by CSDs and CBs and Maintenance Static Data (wave 1)		65d	Fri 20/03/15	Fri 19/06/15	CBs, CSDs,Eurosystem																									
3282	1275000	MIGRATION WEEKEND (WAVE 1)		48d	Fri 22/05/15	Mon 27/07/15																										
3283	1272200	Final verification of the list of showstoppers wave 1 (dependencies with local regulation)		0d	Fri 22/05/15	Fri 22/05/15	CSDs,CBs																									
3284	1277000	Confirmation that migration script has been integrated in internal plans (wave 1)		0d	Fri 12/06/15	Fri 12/06/15	CSDs,CBs																									
3285	1277200	Internal staff trained for change-over Weekend and operations (wave 1)		0d	Thu 18/06/15	Thu 18/06/15	CSDs,CBs																									
3286	1277300	Confirmation that internal control mechanisms are in place (wave 1)		0d	Fri 05/06/15	Fri 05/06/15	CSDs,CBs																									
3287	1277400	External communication has been rolled-out (wave 1)		0d	Fri 05/06/15	Fri 05/06/15	CSDs,CBs																									
3288	1275100	Synchronization Point [SP16.1 - Ready for T2S Go-Live (Wave 1)]		0d	Fri 19/06/15	Fri 19/06/15	CSDs,CBs,Eurosystem																									
3289	1276100	Dynamic data upload by CSDs/CBs		2d	Sat 20/06/15	Sun 21/06/15	Eurosystem,CSDs																									
3290	1279100	Wave 1 Start Operations in T2S		0d	Mon 22/06/15	Mon 22/06/15	Eurosystem,CSDs																									
3291	1279200	Migration closing phase Wave 1		15d	Tue 07/07/15	Mon 27/07/15																										
3294	835100	[Deliverable] - End of Migration Report (Wave 1)		0d	Mon 27/07/15	Mon 27/07/15	Eurosystem																									
3295	1280200	PRE-MIGRATION TASKS (WAVE 2)		416d	Fri 20/06/14	Fri 29/01/16																										
3296	1281000	Implementation Migration phase (wave 2)		55d	Mon 17/08/15	Fri 30/10/15																										
3297	1281100	Preparation of Migration Weekend (wave 2)		55d	Mon 17/08/15	Fri 30/10/15																										
3298	1281200	Start preparation of Migration Weekend (wave 2)		0d	Mon 17/08/15	Mon 17/08/15	Eurosystem																									
3299	1281300	[Predecessors] Preparation of Production Environment		20d	Mon 17/08/15	Fri 11/09/15																										
3300	1281400	Collection of Registration Forms from CSDs/CBs (wave 2)		20d	Mon 17/08/15	Fri 11/09/15	Eurosystem																									
3301	1281500	Registration Form filled in (CSDs/CBs) (wave 2)		0d	Fri 11/09/15	Fri 11/09/15	CSDs,CBs																									
3302	1281600	Preparation of production environment		35d	Mon 14/09/15	Fri 30/10/15																										
3305	1283400	PROD environment available for users		0d	Fri 02/10/15	Fri 02/10/15	Eurosystem																									
3306	1283350	Completed network registration by CSDs (wave 2)		0d	Fri 02/10/15	Fri 02/10/15	CSDs																									

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

T2S Detailed Plan with Critical Path
31/10/2011

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
3307	1283380	Completed network registration by CBs (wave 2)		0d	Fri 02/10/15	Fri 02/10/15	CBs																									
3308	1283700	T2S helpdesk is operational and contact details have been communicated to all relevant T2S parties		0d	Mon 21/09/15	Mon 21/09/15	Eurosystem																									
3309	1283500	Synchronization Point [SP14.2 - Ready to connect to Production wave 2]		0d	Fri 02/10/15	Fri 02/10/15	Eurosystem,CSDs																									
3310	1283300	Prod Connectivity testing (wave 2)		20d	Mon 05/10/15	Fri 30/10/15	CSDs																									
3311	1283370	Successful connectivity tests CSD (wave 2)		0d	Fri 30/10/15	Fri 30/10/15	CSDs																									
3312	1283390	Successful connectivity tests CB (wave 2)		0d	Fri 30/10/15	Fri 30/10/15	CBs																									
3318	1283100	Migration Proprietary Static Data (wave 2)		158d	Tue 23/06/15	Fri 29/01/16																										
3319	1282100	Common Static Data Maintenance (Production System)		140d	Tue 23/06/15	Tue 05/01/16	Eurosystem,CSDs																									
3320	1284150	Start Static Data identification and collection (wave 2)		0d	Mon 14/09/15	Mon 14/09/15	CSDs,CBs																									
3321	1284200	Relevant Static Data ready CSD (wave 2)		0d	Fri 09/10/15	Fri 09/10/15	CSDs																									
3322	1284300	Relevant Static Data ready CB (wave 2)		0d	Fri 09/10/15	Fri 09/10/15	CBs																									
3323	1285200	Synchronization Point [SP15.2 - Ready to upload Static Data wave 2]		0d	Fri 06/11/15	Fri 06/11/15	Eurosystem,CSDs																									
3324	1286100	Proprietary Static Data input by CSDs and CBs and Maintenance Static Data		59d	Mon 09/11/15	Fri 29/01/16	Eurosystem,CSDs																									
3326	1287000	MIGRATION WEEKEND (WAVE 2)		48d	Fri 01/01/16	Mon 07/03/16																										
3327	1287050	Final verification of the list of showstoppers wave 3 (dependencies with local regulation)		0d	Fri 01/01/16	Fri 01/01/16	CSDs																									
3328	1287200	Confirmation that migration script has been integrated in internal plans (Wave 2)		0d	Fri 22/01/16	Fri 22/01/16	CSDs,CBs																									
3329	1287300	Internal staff trained for change-over Weekend and operations (Wave 2)		0d	Thu 28/01/16	Thu 28/01/16	CSDs,CBs																									
3330	1287400	Confirmation that internal control mechanisms are in place (Wave 2)		0d	Fri 15/01/16	Fri 15/01/16	CSDs,CBs																									
3331	1287500	External communication has been rolled-out (Wave 2)		0d	Fri 15/01/16	Fri 15/01/16	CSDs,CBs																									
3332	1287100	Synchronization Point [SP16.2 - Ready for Migration Wave 2]		0d	Fri 29/01/16	Fri 29/01/16	Eurosystem,CSDs																									
3333	1288100	Dynamic data upload		2d	Sat 30/01/16	Sun 31/01/16	Eurosystem,CSDs																									
3334	1291100	Wave 2 Start Operations in T2S		0d	Mon 01/02/16	Mon 01/02/16	Eurosystem,CSDs																									
3335	1291200	Migration closing phase Wave 2		15d	Tue 16/02/16	Mon 07/03/16																										
3338	1025100	[Deliverable] - End of Migration Report (Wave 2)		0d	Mon 07/03/16	Mon 07/03/16	Eurosystem																									
3339	1293000	PRE-MIGRATION TASKS (WAVE 3)		543d	Fri 20/06/14	Mon 18/07/16																										
3340	1293100	Implementation Migration phase (wave 3)		475d	Fri 20/06/14	Fri 15/04/16																										
3341	1293200	Preparation of Migration Weekend (wave 3)		52d	Mon 08/02/16	Fri 15/04/16																										
3342	1293300	Start preparation of Migration Weekend (wave 3)		0d	Mon 08/02/16	Mon 08/02/16	Eurosystem																									
3343	1293400	[Predecessors] Preparation of Production Environment		20d	Mon 08/02/16	Fri 04/03/16																										
3344	1293500	Collection of Registration Forms from CSDs/CBs (wave 3)		20d	Mon 08/02/16	Fri 04/03/16	Eurosystem																									
3345	1293600	Registration Form filled in (CSDs/CBs) (wave 3)		0d	Fri 04/03/16	Fri 04/03/16	CSDs,CBs																									

Task

Task

Critical Milestone

Milestone

Critical Task

Project Summary

Group By Summary

Task		Task		Critical Milestone		Milestone		Critical Task		Project Summary		Group By Summary	

	Task		Task		Critical Milestone		Milestone		Critical Task		Project Summary		Group By Summary	

ID	ID Number (Number 1)	Task Name	CSD/CB relevant activities	Duration	Start	Finish	Resource Group for PMG	2011				2012				2013				2014				2015				2016				2017
								1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half		2nd Half		1st Half
								Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
3872	2015300	SP14.3 - Ready to connect to Production (wave 3)	◆	0d	Tue 22/03/16	Tue 22/03/16																										
3873	2016100	SP15.1 - Ready to upload Static Data (wave 1)	◆	0d	Thu 19/03/15	Thu 19/03/15																										
3874	2016200	SP15.2 - Ready to upload Static Data (wave 2)	◆	0d	Fri 06/11/15	Fri 06/11/15																										
3875	2016300	SP15.3 - Ready to upload Static Data (wave 3)	◆	0d	Fri 22/04/16	Fri 22/04/16																										
3876	2017100	SP16.1 - Ready for T2S Go-Live (wave 1)	◆	0d	Fri 19/06/15	Fri 19/06/15																										
3877	2017200	SP16.2 - Ready for Migration Wave 2	◆	0d	Fri 29/01/16	Fri 29/01/16																										
3878	2017300	SP16.3 - Ready for Migration Wave 3	◆	0d	Fri 15/07/16	Fri 15/07/16																										
3879	2017400	SP16.5 - Ready for Contingency Migration Weekend	◆	0d	Fri 27/01/17	Fri 27/01/17																										
3880	2018300	SP17 - Closing of migration	◆	0d	Mon 10/10/16	Mon 10/10/16																										

Task



Task



Critical Milestone



Milestone



Critical Task



Project Summary



Group By Summary



CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 2 – ANNEX 4

T2S PROGRAMME PLAN ASSUMPTIONS

Disclaimer:

Planning is an ongoing process and Annexes with planning elements are subject to change during the lifetime of a project. Planning workshops with CSDs and CBs will continue to agree on the planning for Connectivity, User Testing and Migration. Subsequent plan updates follow the process, documented in the Schedule 2, Section 7.

Annexes 2, 3, 4, 7, 8, 9 and 10 document the planning status as at 8 Nov. 2011.

Currency Participation Agreement

Schedule 2 – Annex 4 – T2S Programme Plan Assumptions

1. Generic assumptions

For consultation, depending on the complexity and scope of changes, the review period should vary between *1 week and 2 months*.

2. From Specification Phase to Start of User Testing (UT)

The preparation of the UDFS V1.2 and the BPD (Business Process Description) are vital for the end of the specification phase (SP1: synchronisation point) and for the start of the CSDs'/CBs' internal assessment.

- Prior to the publication of UDFS V1.2 a review of UDFS V1.0 by the Market and 2 months of market consultation are planned.
- CSDs/CBs will have 8 months after the delivery of UDFS 1.2 to confirm their feasibility assessment.
- Between the completion of SP1 and the completion of SP2, 8 months are necessary.
- *After the delivery of UDFS V1.2* CSDs/CBs will have 24 months for adapting their internal systems.

Registration for CSDs/CBs :

- 1 month is required to fill in the Registration Guide

Training Sessions:

- the training sessions required for UT will start at least 12 months before UT
- the training sessions required for Migration rehearsal will start at least 6 months before each Migration rehearsal.

The Eurosystem will confirm the acceptance test for the VAN at the latest 9 months prior to the start of UT.

The CB/CSDs should finalise the negotiations with the NSP at least 3 months prior the start of the connectivity tests.

The *Dedicated lines Connectivity specifications* are delivered at least 1 year before starting the UT.

Currency Participation Agreement

Schedule 2 – Annex 4 – T2S Programme Plan Assumptions

The first delivery of the Manual of Operational Procedure (MOP) will be ready 6 months before the start of UT. A revised version of the MOP will be delivered 1 month before each go-live.

Pilot testing:

- A pilot testing might be offered only to the CSDs participating to the UT Wave 1.
- Takes place in parallel of the EAT and before the UT starts.
- This pilot testing is lasting 3 months

3. UT

The UT is split into the following stages:

- Bilateral stages:
 - o Connectivity
 - o Interoperability (IO) Bilateral
 - o CSD/CB Acceptance
 - o CSD/CB Certification
- Multilateral stages:
 - o IO Multilateral
 - o Community
 - o Business Day

The Eurosystem Acceptance Test Assessment Report is an *entry criteria for the UT*.

Before starting the UT, the Eurosystem will provide enough assurance as regard the capacity of the T2S application/infrastructure to meet the non-functional requirements.

3.1 UT Waves

The T2S Programme Plan is based on the assumption that the UT and migration will be done by migration waves. There is a *maximum of four migration waves* (and contingency wave) spread over a maximum of 18 months (from go-live wave 1 to go-live contingency).

The assumptions for UT duration are as follow:

- Wave 1: 12 months (including pilot testing).
- Wave 2: 18 months
- Wave 3 and subsequent waves: at least 18 months.

All CSDs and CBs having links with the CSDs and CBs migrating must participate in IO Multilateral, Community and Business Day.

CSD/CB can start UT when they want, planning enough time to complete all their testing within the defined time line.

Currency Participation Agreement

Schedule 2 – Annex 4 – T2S Programme Plan Assumptions

3.2 Connectivity

Connectivity Testing VAN: the T2S Programme Plan assumes 1 month for connectivity and is a predecessor of the UT (IO Phase).

Connectivity Testing for Dedicated lines: further information will be provided in the future.

3.3 IO

IO testing is divided in two: IO Bilateral and IO Multilateral.

IO environment remains available for IO Bilateral and Multilateral during the Community and Business Day testing.

3.4 Migration Test

Migration Test runs in parallel with IO, Community Testing and Business Day.

3.5 CSD/CB Certification

CSD/CB Certification runs in parallel of the IO Bilateral.

A CSD/CB has to be certified to participate to the IO Multilateral.

3.6 CSD Acceptance

CSD Acceptance starts together with the bilateral IO for all waves (SP8 – Start bilateral IO).

CSD Acceptance lasts up to 6 months.

3.7 Community

3.7.1 DCP/DCAH Certification

DCP/DCAH Certification runs in parallel of the Community Testing.

3.8 Business Day

Business Day Test: the following assumptions are taken for the duration:

- Wave 1: 3 weeks
- Wave 2 and subsequent waves: at least 1 months

3.9 Transition phase between stages:

From bilateral to multilateral stages, two weeks are planned in parallel of the bilateral stage.

From multilateral to community stages, 4 weeks are planned. 3 weeks run in parallel of the multilateral stage and 1 week between multilateral and community stages.

The *IO exit criteria and Community entry criteria* have to be met within:

- Wave 1: 3 months

Currency Participation Agreement

Schedule 2 – Annex 4 – T2S Programme Plan Assumptions

- Wave 2 and subsequent waves: at least 6 months

From community to business day stages, 4 weeks are planned. 3 weeks run in parallel of the community stage and 1 week between community and business day stages.

The *Community exit criteria and BD entry criteria* have to be met within:

- Wave 1: 4.5 months

- Wave 2 and subsequent waves: at least 5 months

At the end of business day stage, 3 weeks are planned. 2 weeks run in parallel of the business day stage and 1 week during the freeze period.

3.10 Other Assumptions for UT

There is a freeze period of two weeks between the end of the UT and the Migration WE of each wave.

4. Pre-Migration and Migration

All CSDs and CBs belonging to the *same wave migrate at the same time.*

Connectivity to production environment: T2S Programme Plan foresees 2 weeks of production connectivity testing.

Production Environment: will be available for Users 3 months before the go-live of wave 1.

CSD/CB Static Data Cleansing according to the T2S migration rules: 1 month planned before Load Static Data.

Load Static Data: 3 months planned before the go-live in parallel to UT.

There is a minimum of *3 months between two migration waves* (Schedule 4).

Migration cannot happen during critical times (e.g. end of the year)

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 2 - ANNEX 5

T2S PROGRAMME PROGRESS REPORTING TEMPLATES

Currency Participation Agreement

Schedule 2 - Annex 5 – T2S Programme Progress Reporting Templates

1 1 Template for reporting at T2S programme Work Stream and Sub-Stream Level:

2

Reports change in status compared to previous reporting period for status

Summarises the overall assessment of the quality, time and scope dimensions for the work sub-stream.

Expected trend for next reporting period

Highlights whether critical risks exist

Reports change in risk situation compared to previous reporting period

PROGRAMME WORKSTREAM		STATUS	CHANGE	TREND	RISK	CHANGE
Programme WBS item 1	Sub Stream monitoring element 1	R	↓	↗	R	→
	Financial Framework	Y	↓	↗	Y	→
	Sub Stream monitoring element 3	G	→	→	G	→
Programme WBS item 2	Sub Stream monitoring element n	R	→	→	R	→
PRODUCT READINESS	Specification and Documentation	R	↓	→	R	↓
	Sub Stream monitoring element n	N/A	→	→	N/A	→
	Eurosystem Acceptance Test	G	→	→	R	→
...	User Test Start	G	→	→	G	→
	Sub Stream monitoring element n	G	→	→	G	→
	Sub Stream monitoring element n	Y	→	→	G	→
Programme WBS item x	Sub Stream monitoring element n	G	→	→	G	→
	Migration	G	→	→	G	→
	Sub Stream monitoring element n	Y	→	↗	Y	→

T2S Programme Work

T2S Work Sub-Stream

Currency Participation Agreement

Schedule 2 - Annex 5 – T2S Programme Progress Reporting Templates

2 Template for reporting the T2S Detailed Status:

T2S Detailed Status for reporting:

5

DELIVERABLE / MILESTONE	DATE	STATUS	CHANGE	TREND	RISKS	CHANGE
[Placeholder for name of deliverable/milestone] [Placeholder for relevant milestone of a deliverable, if applicable]	[Date]	R	→	→	G	→
Status Update ▪ [Lists milestones achieved for reporting period] ▪ [Lists missed milestones or deadlines for previous reporting period] ▪ [if applicable] List of mitigating actions – [Placeholder for explanation]						

Currency Participation Agreement

Schedule 2 - Annex 5 – T2S Programme Progress Reporting Templates

3 Status Assessment at T2S Programme Work Stream and Sub-Stream Level:

The responsible for each ECB workstream makes his/her assessment according to the conventions defined above.

At aggregated level (Dashboard) the business rule is: if the progress assessment is not uniformly Green for all deliverables/activities belonging to a specific stream or sub-stream, at least a Yellow status is reported at aggregated level.

The detailed information by deliverable or activity is then provided at the Detailed status report level.

4 Status Assessment at CSD/CB level:

Each CSD/CB makes its assessment. This is discussed with the Relationship Manager during the MCR sessions (see T2S Monitoring of Client Readiness Framework, Annex 5).

The various assessments are collected and discussed internally within the Client Readiness Workstream.

Based on the discussion outcomes, the Relationship Manager assesses the overall CSD/CB readiness for the respective activity or milestone, following these business rules:

- In case the assessment is not Green for all CSDs or CBs, the “Green” status is not allocated, i.e. at least Yellow.
- Confidentiality rules applies (see Monitoring of Client Readiness Framework, Annex 5) to explain the overall status if different from Green.

Once discussed, the assessment is reflected in the global progress status dashboard and a detailed status is prepared for all deliverables having a status “Yellow” or “Red”.

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 2 - ANNEX 6

T2S RISK AND ISSUE REPORTING TEMPLATE

Currency Participation Agreement

Schedule 2 - Annex 6 – T2S Risk and Issue Reporting Template

1 Risk and Issue Reporting

Parties to this agreement who have identified and assessed a programme risk or an issue originating/occurring in their own institution provide the T2S Programme Office with a filled-in risk/issue identification form. The form shall provide at least the following information:

Risk identification form:

- Work stream / Sub-Work stream / Deliverable / Milestone / Synchronisation Point
- Risk name
- Risk description (background)
- Reported by
- Status (raised / mitigation in process / mitigated / accepted)
- Probability (level 1-5)
- Impact (level 1–5)
- Criticality (colour)
- Risk Response
- Root cause category (product & services/external/internal)

Issue identification form:

- Work stream / Sub-Work stream / Deliverable / Milestone / Synchronisation Point
- Issue name
- Issue description (background)
- Reported by
- Resolution strategy
- Target Date for resolution

The T2S Programme Office includes the information received from risk/issue owners in the forthcoming risk report to be submitted to the T2S Board. For a detailed process description for the reporting and sharing of identified risks/issues, see Annex 2.

Currency Participation Agreement

Schedule 2 - Annex 6 – T2S Risk and Issue Reporting Template

27 Based on the information received from contractual parties, the T2S Programme Office will
28 prepare its regular assessment reports. To that end, it may use the following (sample) templates
29 for the reporting of risks and issues:

30 Risk Reporting:



T2S Programme Risk Reporting



	Reporting risk owner		OWNER	
	Probability of Risk		PROBABILITY	
	Impact of Risk		IMPACT	
	Criticality of Risk		CRITICALITY	Y
DELIVERABLE/ MILESTONE				
ID	Unique Risk ID			
RISK	Summary of risk description			
RISK STATUS	e.g. Raised / Mitigation in Progress / Mitigated			
BACKGROUND	Background to provide context of the risk			
RISK RESPONSE	Proposed mitigation measures			

31

32 Issue Reporting:



T2S Programme Issue Reporting



	Reporting issue owner		OWNER	
			ID	Unique Issue ID
DELIVERABLE/ MILESTONE				
ISSUE	Summary Description for Issue			
TARGET DATE	Target resolution date for issue			
ISSUE BACKGROUND & RESPONSE	Details regarding issue and proposed response			

33

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 2 – ANNEX 7

T2S PROGRAMME WORK BREAKDOWN STRUCTURE

Disclaimer:

Planning is an ongoing process and Annexes with planning elements are subject to change during the lifetime of a project. Planning workshops with CSDs and CBs will continue to agree on the planning for Connectivity, User Testing and Migration. Subsequent plan updates follow the process, documented in the Schedule 2, Section 7.

Annexes 2, 3, 4, 7, 8, 9 and 10 document the planning status as at 7 Nov. 2011.

Currency Participation Agreement

Schedule 2 – Annex 7 – T2S Programme Work Breakdown Structure

Programme Workstream	Deliverable Stream	Deliverable Substream
Client Readiness	Contractual Framework	Framework Agreement Currency Participation Agreement
	User Training and Testing	Training Preparation Training Execution User Testing Preparation User Testing Execution
	Synchronization and on-boarding	CSD Readiness CB Readiness Eurosystem Readiness*
	Relationship Management*	CSDs* CBs* DCPs* Market Report*
	Other Documentation*	
Product Readiness	Specification and Documentation	Requirements Specifications Documentation
	Development	Software & 4CB Testing Infrastructure
	Eurosystem Acceptance Test	EAT Preparation EAT Execution
Operational Readiness	Operations	Operational Procedures Service Level Agreement
	Migration	Migration Preparation Pre-Migration Tasks (per waves) Migration WE (per waves)
	Network and connectivity Information Security	
Policy and Marketing	Policy Framework and Governance	Harmonisation Other policy frameworks* Governance*
	Marketing and Communication*	
	Financials*	Liability* Financials planning and procedures*
	Relationship Management*	Regulators* Public authorities* Other External stakeholders*
Legal*	Legal Framework*	L2/L3 Agreement* Other Legal Acts*
Programme Planning and Monitoring		

* Elements provided only for information, as they cover Eurosystem internal work.

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 2 – ANNEX 8

T2S DELIVERABLES LIST AND MANAGEMENT PROCESS

Disclaimer:

Planning is an ongoing process and Annexes with planning elements are subject to change during the lifetime of a project. Planning workshops with CSDs and CBs will continue to agree on the planning for Connectivity, User Testing and Migration. Subsequent plan updates follow the process, documented in the Schedule 2, Section 7.

Annexes 2, 3, 4, 7, 8, 9 and 10 document the planning status as at 7 Nov. 2011.

Currency Participation Agreement

Schedule 2 – Annex 8 – T2S Deliverables list and management process

1. Document Scope and Objective

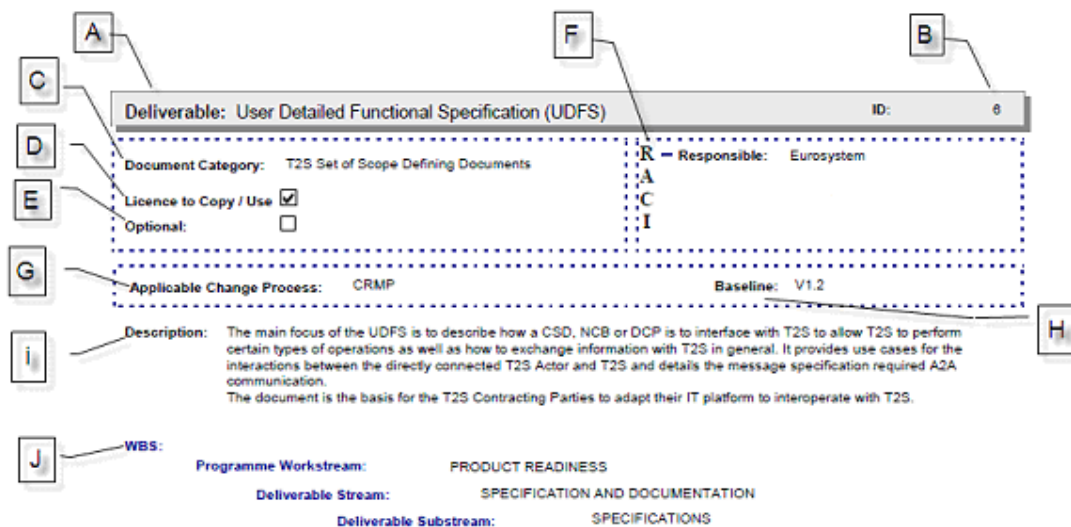
The objective of this document is to provide a baseline catalogue of T2S deliverables that are of interest for CSDs and CBs and that describes the scope of and the respective responsibilities for each deliverable. This catalogue defines a deliverable only once, even though the programme requires several versions of a deliverable, such as regular updates or a dedicated version of a deliverable specific to a migration wave.

The deliverable monitoring is part of the Monitoring Framework process as defined in the main document of the Schedule 2.

2. T2S Deliverables

2.1 Deliverable Specification

This annex provides a standardised definition of each T2S deliverable. The standardised definition documents not only a deliverable's purpose and scope, but also additional characteristics relating to responsibilities and Change Management.



Currency Participation Agreement

Schedule 2 – Annex 8 – T2S Deliverables list and management process

Label	Attribute Name	Description
A	Deliverable	This attribute documents the name of the deliverable.
B	ID	This attribute specifies the unique identifier of the deliverable. The Operational Plan and the Synchronisation Point (if relevant) use the identifier to reference the underlying deliverable.
C	Document Category	This attribute specifies the category of document to which the deliverable belongs (see below table in this annex).
D	License to Copy/Use	Each deliverable has an attribute that states who owns the Intellectual Property Rights and whether a licence to copy or use exists for the other parties as set out in the FA (article 28) and CPA (article 31).
E	Optional	This attribute specifies whether this deliverable is optional or mandatory. <u>Value</u> <u>Description</u> Ticked Optional Empty Mandatory
F	RACI	The attribute defines the responsibilities and accountabilities for a deliverable.
G	Applicable Change Management Process	This attribute specifies which Change Management process applies to the deliverable, e.g. <u>Value</u> <u>Description</u> CRMP Change and Release Management Process according to Schedule 9 of this agreement. ...
H	Baseline	The attribute specifies the version of the deliverable from which the Change Management process specified by the attribute “Applicable Change Management Process” applies.
i	Description	The attribute provides a short description of the scope and content of the deliverable.
J	Work Breakdown Structure (WBS)	This attribute specifies the classification in the WBS of the T2S Programme Plan under which the deliverable is managed and reported.

2.2 Responsible, Accountable, Consulted, Informed (RACI)

2.2.1 Responsible

This classifier assigns to a deliverable *those who do the actual work* by specifying the Party, i.e. Eurosystem, CSD or CB, responsible for creating and maintaining the deliverable throughout its life cycle.

2.2.2 Accountable

This classifier assigns to a deliverable *those who are ultimately accountable for the completion of the work*. The body that is accountable is the approving body. The FA-CPA Agreement defines the body

Currency Participation Agreement

Schedule 2 – Annex 8 – T2S Deliverables list and management process

that is accountable for the legal documents and the T2S Scope Defining Set of Documents. Schedule 8 of this Agreement defines in its section “Decision-making on relevant matters other than Change Requests” the body that is accountable for all other deliverables.

For the purpose of the Annex 8, Deliverable List, the body mentioned will be the sub-structure that writes a recommendation to approve to the Steering Level.

2.2.3 Consulted

This classifier assigns to a deliverable *those who provide input* as needed by specifying whether or not the Party to the Agreement is consulted regarding the T2S deliverable. The T2S Programme Plan specifies the frequency and the duration of the consultation for the deliverable. Consulted can mean written procedures or workshops. In case Change Request affects a deliverable, then the consultation also applies for subsequent updated versions.

Consulted refers to a formal process where the Responsible expects comments from other Parties to the Agreement (in particular CSDs and CBs). This means that the Responsible submits a DRAFT version and collects the comments. The Responsible analyses all comments and must:

- (a) consider the comments and/or produce a new version; or
- (b) explain why a comment has not been taken on board.

2.2.4 Informed

This classifier assigns to a deliverable *those who need to be kept up to date* on progress of the particular phase. The Responsible submits a proposal as regard the distribution list (bodies to be informed) to the Accountable body together with the draft document. Being informed might take the form of an early involvement.

2.3 Baseline

The Responsible produces the draft version that upon approval as described in the Section 3 becomes a ‘Baseline’ (with or without consultation of the other Party). A ‘Baseline’ serves as basis/reference for the Party to undertake a series of actions required for the T2S Programme completion. Each deliverable has an attribute that specifies the version number that will be considered as ‘Baseline’. This version number also appears in the Plan. Any change to the baseline follows a formal change process, as defined thereafter. The latest baseline version available for this release of T2S must be easily identifiable.

Currency Participation Agreement

Schedule 2 – Annex 8 – T2S Deliverables list and management process

Outside of the Legal Acts, the initial baseline number is indicated in the T2S List of deliverables.

2.4 Applicable Process per Document Type

Each deliverable has an attribute that specifies the applicable process for approving the baseline or the changes to it – which is summarised in the table below. Some deliverables are not subject to any formal Change Management process. The deliverables subject to a Change Management process are communicated either in a complete version (with revision marks if technically possible or with indication of a list of changes) or in an intermediate document (e.g. Document Change Notice) to avoid waiting for the next release of the deliverable. The modalities for communication are defined, on a case-by-case basis, in the course of the Change Management process.

Currency Participation Agreement

Schedule 2 – Annex 8 – T2S Deliverables list and management process

Document Category		Description ¹	Initial Baseline number is indicated in	Substructure involved	Change Management Process
Legal Acts		Means the FA / CPA and their respective schedules.	N/A	N/A	Specific FA / CPA Process
T2S Scope Defining Set of Documents		Means the set of documents defining the scope of T2S composed of the URD, the UDFS, the GUI Business Functionality, GFS Functional Chapter and the Dedicated Link Connectivity Specifications.	The deliverables list	CRG	Change Request (Schedule 9)
T2S Documentation	T2S Specification	Means the set of documents, when added to the T2S Scope Defining Set of Documents, provide a full description of T2S. This includes the GFS non-Functional Chapter.	The deliverables list	CRG	Deliverable Change Process (Schedule 2) Unless otherwise specified in the list of deliverables
	T2S Operational Phase Documents	Means the set of documents that describes how T2S provides its services when it is in production. It encompasses the documentation for T2S as a software application and the manuals describing the rules and procedures for operating T2S.	The deliverables list	OMG	Deliverable Change Process (Schedule 2) Unless otherwise specified in the list of deliverables
	T2S Project Documents	Means the set of documents required for planning, monitoring and successfully completing the scheduled activities (e.g. User Testing, Migration, client readiness tracking) in the T2S project lifecycle but not during the operational part, i.e. from the start of the T2S Programme until T2S is live, or during any subsequent preparation for releases.	The deliverables list	PMG	Deliverable Change Process (Schedule 2) Unless otherwise specified in the list of deliverables

¹ As included in Schedule 1.

Currency Participation Agreement

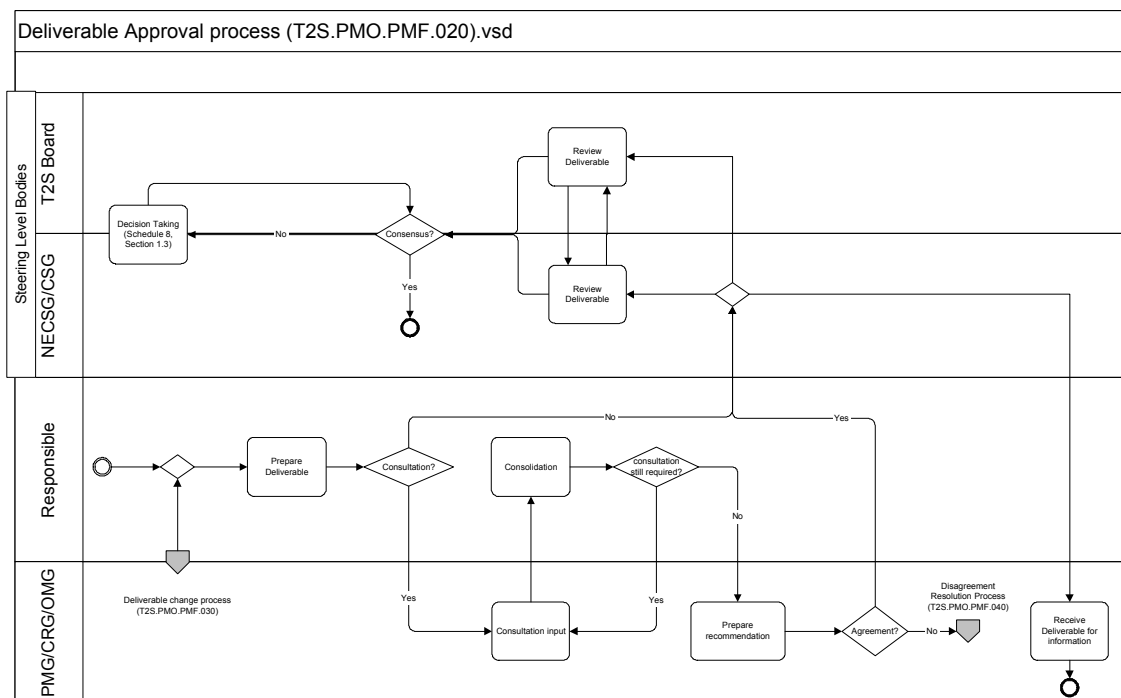
Schedule 2 – Annex 8 – T2S Deliverables list and management process

3. Deliverable Approval and Change Process

This section describes the approval and change process for deliverables which are neither subject to the FA/CPA Change Management process nor to the CRMP (Schedule 9).

3.1 High-Level Deliverable Approval Process – Creation of a Baseline

The following process applies for the approval of the first Baseline for each Deliverable:



3.1.1 Process Actors and their Roles

Process Actor	Process Role
Responsible	As above defined.
PMG/CRG/OMG <i>(one body only, depending on the deliverable category)</i>	In this process, the Responsible consults the PMG/ORG/OMG. It is the responsibility of the consulted body to provide comments during the approval process and to proactively and in good faith try achieving agreement among its members.
CSG/NECSG	The CSG/NECSG is responsible for reviewing the Deliverable, taking into account the recommendations supplied by the PMG and taking all necessary steps to reach a consensus at Steering Level.

Currency Participation Agreement

Schedule 2 – Annex 8 – T2S Deliverables list and management process

T2S Board	The T2S Board is responsible for endorsing the Deliverable, taking into account the recommendations supplied by the PMG and taking all necessary steps to reach a consensus at Steering Level. The T2S Board also coordinates the work at Steering Level to reach a consensus following the process described in Schedule 8, Section 1.3.

3.1.2 High-Level Process Description

This section provides an overview of the process for Baseline creation for deliverables.

The Responsible after drafting the deliverable and if applicable, sends the deliverable for consultation of other parties.

During consultation, in case of diverging views the PMG/CRG/OMG members have the opportunity to inform the NECSG/CSG about their diverging views (in line with the section 7.4 Disagreement Resolution process in Schedule 2).

After consultation and in line with RACI information, the Responsible presents the deliverable for approval to the Steering Level. If consulted, the PMG/CRG/OMG writes a recommendation to approve. This recommendation is attached to the Deliverable submission to the Steering Level.

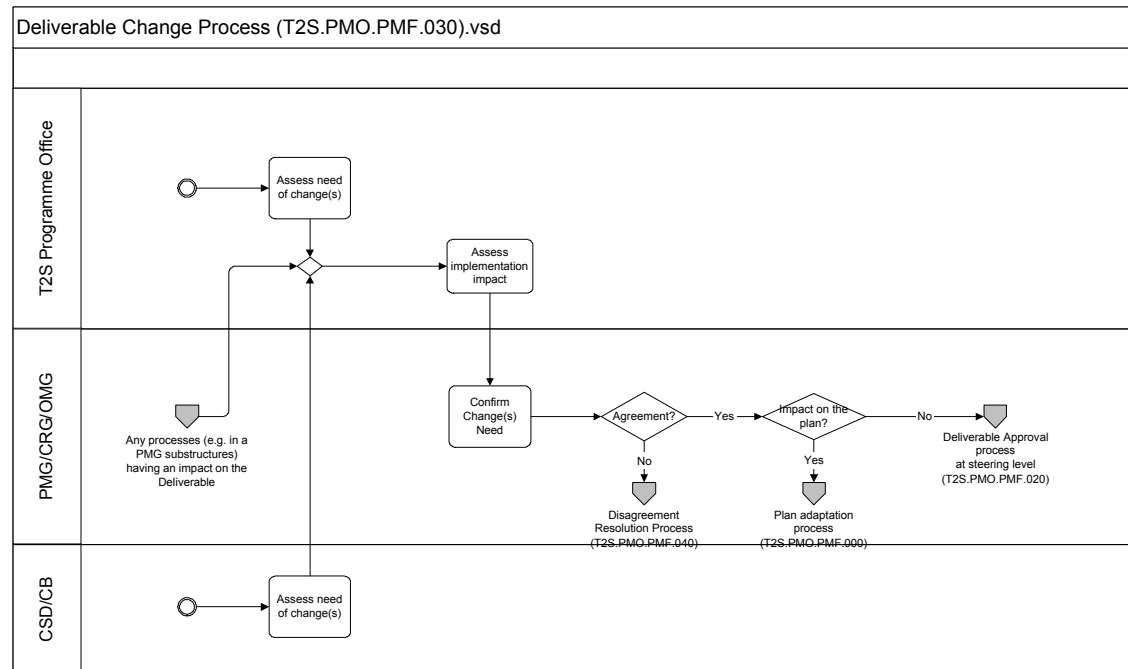
The Steering Level endorses the deliverable by consensus. The T2S Board coordinates the work at Steering Level to reach a consensus following the process described in Schedule 8, Section 1.3.

Currency Participation Agreement

Schedule 2 – Annex 8 – T2S Deliverables list and management process

3.2 Deliverable Change Process – Updating a Baseline

Each deliverable has a specific Change Management process. This process is described either in the Schedule 9 – Change Request– or in this section. The below process applies to all deliverables for which the ‘Applicable Process’ clearly foresees ‘*Deliverable Change Process*’ as opposed to other value (e.g. Change Request).



3.2.1 Process Actors and their Roles

Process Actor	Process Role
T2S Programme Office	The T2S Programme Office is in charge of: - identifying, collecting and raising Change Requests (e.g. need to update due to another deliverable); - undertaking the assessment of changes request; - communicating the results of the assessment to the PMG/CRG/OMG; and - implementing the change when the Eurosystem is the Responsible.
CSD, CBs	The CSDs and/or CBs are in charge of: - implementing the change when CSDs and/or CBs are the Responsible; and - identifying and raising Change Requests, if relevant.
PMG/CRG/OMG (one body only, depending on the Deliverable)	In this process, the PMG/CRG/OMG is in charge of: - reviewing and discussing the Change Requests; - confirming the need of the change or rejecting the request; and - in case of disagreement, escalation to the NECSG/CSG or T2S Board (in line with the section 7.4 Disagreement Resolution process in Schedule 2).

Currency Participation Agreement

Schedule 2 – Annex 8 – T2S Deliverables list and management process

3.2.2 High Level Process Description

This section provides an overview of the process for Baseline update for deliverables.

The T2S Programme Office and/or CSDs and/or CBs may wish to change a deliverable.

T2S Programme Office collects the change(s) request. Thereafter, the T2S Programme Office assesses the change(s) request (including Plan impact assessment). The PMG/CRG/OMG reviews the change(s) request together with the T2S Programme Office assessment.

After agreement on the change(s) at PMG/CRG/OMG level, the approval process at Steering Level should follow the initial approval process used to create the baseline (see section 3.1).

In case of disagreement, the PMG/CRG/OMG may initiate the disagreement resolution process to get agreement on the proposed change(s) (in line with the section 7.4 Disagreement Resolution process in Schedule 2).

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: Graphical User Interface (GUI) Business Functionalities

ID: 3

Document Category: T2S Scope Defining Set of Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: CRG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: CRMP

Baseline: V1.0

Description: The scope of this document is to provide a list of business functions- expected for the T2S Graphical User Interface and to provide a brief description covering the purpose and key features of the business functions. It also depicts the framework for logical association of business functions applicable for a business object. (The framework diagrams in this document do not depict certain access features that are purely of technical nature like returning to the previous or exit from a function).

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: SPECIFICATION AND DOCUMENTATION

Deliverable Substream: SPECIFICATIONS

Deliverable: User Detailed Functional Specification (UDFS)

ID: 6

Document Category: T2S Scope Defining Set of Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: CRG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: CRMP

Baseline: V1.2

Description: This deliverable is the manual that describes how a T2S Actor can interface ist software applications with T2S to enable T2S to execute certain types of operations and to exchange information with T2S. It provides use cases for the interactions between the Directly Connected T2S Actor and T2S and details the message specification required A2A communication. The UDFS also contains the specifications required in order to set-up and manage the direct connectivity with T2S. The document is the basis for the T2S Contracting Parties to adapt their IT platform to interoperate with T2S.

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: SPECIFICATION AND DOCUMENTATION

Deliverable Substream: SPECIFICATIONS

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: T2S Dedicated Link Connectivity Specifications

ID: 7

Document Category: T2S Specifications

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: CRMP

Baseline: V1.0

Description: This documents provides the CSD, DCP, CB and DCAHs with the detailed specifications to be respected in order to set-up a direct connectivity line between CSDs, CBs, DCPS and T2S.

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: NETWORK AND CONNECTIVITY

Deliverable Substream: NETWORK AND CONNECTIVITY

Deliverable: T2S Connectivity Guide

ID: 8

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: The connectivity guide documents the steps required for T2S Actors to connect to T2S test and production environments. The document will present the technical landscape (tools and network provider selection) used to facilitate the understanding, and will also present the protocols supported. A checklist will summarize the requirements to connect.
The document will cover both A2A and U2A aspects it also covers both VANs and Direct Connectivity. The information provided may vary depending on the provider.

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: NETWORK AND CONNECTIVITY

Deliverable Substream: NETWORK AND CONNECTIVITY

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: User Hand Book (UHB)

ID: 9

Document Category: T2S Specifications

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: CRG

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: Deliverable Change Process (CRG)

Baseline: V2.0

Description: The UHB describes the Graphical User Interface (GUI) of T2S, i.e. U2A communication. It is intended for the business user, who will interact with T2S for updating and querying data. It presents information on the application behaviour, window navigation, windows, fields and validation rules in order to explain how a user can perform specific operations in T2S through the GUI.

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: SPECIFICATION AND DOCUMENTATION

Deliverable Substream: DOCUMENTATION

Deliverable: Manual of Operational Procedures (MOP)

ID: 10

Document Category: T2S Operational Phase Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: OMG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Deliverable Change Process (OMG)

Baseline: V1.0

Description: This manual provides the detailed procedures to be followed by the T2S Actors and the Eurosystem to ensure the smooth functioning of T2S for normal operations as well as in contingency and exceptional situations (e.g. Disaster Recovery and Business Continuity).

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: OPERATIONS

Deliverable Substream: OPERATIONAL PROCEDURES

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: Information Security Policy

ID: 12

Document Category: Legal Acts

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: N/A

Baseline: FA/CPA

Description: The Information Security Policy for T2S is a high-level document that defines the principle and scope of, allocation of responsibilities for and other relevant aspects of information security for T2S.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: CONTRACTUAL FRAMEWORK

Deliverable Substream: FRAMEWORK AGREEMENT

Deliverable: User Testing Strategy

ID: 17

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Final

Baseline: V1.0

Description: This strategy document presents the high-level planning, stages and roles of the various T2S Actors in the User Testing phase of T2S. It serves as guideline for Schedule 3 of the Framework Agreement and Currency Participation Agreement on User Testing.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING PREPARATION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: User Testing Guide

ID: 18

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: Provides the required information to enable the CSDs/CBs to carry out testing activities.
Provides details on the organisation of testing, processes, roles and responsibilities, monitoring and reporting, test coverage matrixes for each test stage, and the principles of the execution plan for each test stage.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING PREPARATION

Deliverable: Migration Strategy

ID: 25

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Final

Baseline: V1.0

Description: The scope of this document is to present the migration approach that will be used to prepare and conduct the migration in T2S. This document covers the framework applicable for the migration, the roles and responsibilities of the parties involved and the activities to be performed to prepare, execute and monitor the migration process.

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: MIGRATION

Deliverable Substream: MIGRATION PREPARATION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: Standard Migration Plan

ID: 26

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This document presents the detailed standard and tailored plans for all T2S Contracting Parties. The tailored migration plan per group of CSDs/CBs or individual CSD/CB depending on its specificities.

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: MIGRATION

Deliverable Substream: MIGRATION PREPARATION

Deliverable: Detailed migration weekend script

ID: 27

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: The scope of this document is to provide the T2S Actors with the required information to execute the tasks requested for the preparation and execution of the T2S migration weekend. Tasks detailing the pre-migration phase (load static data...) and migration phase (detailed migration sequence of activities and organisation) are covered. Rollback and fallback procedures are presented as potential consequences of the decision points to be taken during the migration WE. More precisely, this document covers the schedule, the roles and responsibilities, and the identification of the success factors. The document takes into account the lessons learnt from the previous waves.

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: MIGRATION

Deliverable Substream: MIGRATION PREPARATION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: CSD Certification Test Cases

ID: 30

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation:

I – Information: CSD

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This deliverable specifies the technical requirements that a CSD must fulfil as well as the test cases in a pre-defined, standardised format that a CSD must execute successfully as prerequisite before entering in the Community Testing Stage in User Testing. The successful execution of certification test cases by a CSD ensures that a CSD creates no adverse effects on T2S or T2S Actors.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING PREPARATION

Deliverable: T2S Non-Functional Testing Scenarios

ID: 32

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This deliverable documents the test scenarios and test cases that the Eurosystem will execute to verify that T2S complies with the non-functional user requirements. The non-functional testing comprises performance testing, Disaster Recovery and Business Continuity testing, and compliance with information security requirements.

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: NETWORK AND CONNECTIVITY

Deliverable Substream: NETWORK AND CONNECTIVITY

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: CSD/CB's T2S Non-Compliance Notification

ID: 35

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: CSD/CB

A – Accountable: CSD/CB

C – Consultation: Eurosystem (MCR)

I – Information:

Applicable Change Process: N/A

Baseline: V1.0

Description: This report is a deliverable of the CSD/CB in which the CSD/CB formally documents the specific reason or reasons for its refusal to accept T2S. The report must include the acceptance test scenarios and test cases that the CSD/CB considers to have failed to execute successfully in T2S.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING EXECUTION

Deliverable: CSD/CB's T2S Compliance Confirmation

ID: 36

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: CSD/CB

A – Accountable: CSD/CB

C – Consultation: Eurosystem (MCR)

I – Information:

Applicable Change Process: N/A

Baseline: V1.0

Description: This deliverable is a standardised form that the Eurosystem provides to the CSDs/CBs and that a CSD/CB completes and returns to the Eurosystem to confirm its acceptance of T2S at the end of the CSD/CB Acceptance Testing Phase.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING EXECUTION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: Eurosystem T2S Certification

ID: 37

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: N/A

Baseline: V1.0

Description: This deliverable is the assessment of the Eurosystem whether or not a CSD, a CB or a DCP successfully completed its certification testing for this specific release of T2S. In case the assessment is negative, the Eurosystem formally documents the specific reason or reasons for its refusal to certify a T2S Actor for this specific release of T2S.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING EXECUTION

Deliverable: Testing Progress Report

ID: 39

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: Provides the status, the general progress, the measures to mitigate risks that could endanger the timely execution of test activities, and the progress against the planning (Eurosystem reports on the Test Plan, whilst the CSDs/CBs report on their Test Plan). This report will be delivered for the various testing phases of the T2S Programme (EAT and UT Stages). The progress report also includes the list of pending defects identified for the stage, which will be used to allow proper monitoring of the defects identified.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING EXECUTION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: T2S Training Framework

ID: 40

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: The training framework defines the scope of T2S training programme and its related training objectives. It specifies the required set of training documents and materials, the intended audience definition, the training organisation (train the trainer concept) and the high-level training timeline.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: TRAINING PREPARATION

Deliverable: Registration Guide for User Testing

ID: 42

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: Contains the required details provided by the CSDs/CBs in order to carry out User Testing on the testing environments. Includes the full set of administrative forms required for the participation to the User Tests. It will enable the CSDs/CBs to describe their connectivity data, T2S Services used, initial static data such as accounts, static data for logically segregated testing, etc.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING PREPARATION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: Implementation Guide for CSD Eligibility Criteria

ID: 43

Document Category: Legal Acts

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: N/A

Baseline: V1.0

Description: This deliverable documents and explains the conditions that CSDs must fulfil to participate in T2S. The 5 criteria to be respected are defined under article 4.3 of the Framework Agreement. Also see Del ID 425 on "Proof of eligibility for participation in T2S".

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: SYNCHRONISATION AND ON-BOARDING

Deliverable Substream: CSD READINESS

Deliverable: T2S Release Note

ID: 44

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This deliverable details for T2S Actors Release changes and/or enhancements that the Eurosystem has made in a new version of the T2S software and includes a list of recommended regression tests for T2S Actors. It also documents any known defects in the software release.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING EXECUTION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: CB Certification Test Cases

ID: 45

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation:

I – Information: CB

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This deliverable documents the technical requirements that a CB must fulfil as well as in a pre-defined, standardised format the test scenarios and test case that a CB must execute successfully in T2S to obtain approval to connect directly to the T2S production environment. The document specifies the mandatory test scenarios and test cases by the role that the CB takes in T2S.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING PREPARATION

Deliverable: DCP Certification Test Cases

ID: 46

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation: CSD

I – Information: DCP

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This deliverable documents the technical requirements that a DCP (including directly connected DCAHs) must fulfil as well as in a pre-defined, standardised format the test scenarios and test case that a DCP must execute successfully in T2S to obtain approval to connect directly to the T2S production environment. The document specifies the mandatory test scenarios and test cases by the role that the DCP takes in T2S.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING PREPARATION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: General Functional Specification (GFS)

ID: 49

Document Category: T2S Scope Defining Set of Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: CRG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: CRMP

Baseline: V4.0

Description: The specification documents the functional design of T2S and how the user requirements will be implemented from a functional perspective.

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: SPECIFICATION AND DOCUMENTATION

Deliverable Substream: SPECIFICATIONS

Deliverable: General Technical Design (GTD)

ID: 50

Document Category: T2S Specifications

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: CRG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Deliverable Change Process (CRG)

Baseline: V2.0

Description: The document describes the design of T2S from the technical infrastructure and architecture perspective. CSDs and CBs were consulted on specific chapters related to connectivity issues (Chapters 3.5 and 3.6)

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: SPECIFICATION AND DOCUMENTATION

Deliverable Substream: SPECIFICATIONS

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: General Specification (GS)

ID: 51

Document Category: T2S Specifications

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: N/A

Baseline: V2.0

Description: The document represents the high-level description of T2S as an executive summary. It aims at giving a global and comprehensive picture of the T2S solution and at explaining how the User Requirements which are not covered by the General Functional Specifications (GFS) and General Technical Design (GTD) will be fulfilled.

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: SPECIFICATION AND DOCUMENTATION

Deliverable Substream: SPECIFICATIONS

Deliverable: User Requirement Document (URD)

ID: 64

Document Category: T2S Scope Defining Set of Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: CRG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: CRMP

Baseline: V5.01

Description: In line with the Schedule 1 definition: [means the latest available document setting out the User requirements for T2S Services as published by the ECB as subsequently amended through the Change and Re-lease Management process.] This document defines the requirements for the T2S Services eg: the Cross Border DVP settlement in Central Bank Money.

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: SPECIFICATION AND DOCUMENTATION

Deliverable Substream: REQUIREMENTS

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: Tender for Network Connectivity (VAN)

ID: 69

Document Category: T2S Specifications

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: N/A

Baseline: V1.0

Description: The tender defines the requirements that a potential network provider must fulfil to be considered suitable for offering its network services to the T2S community.

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: NETWORK AND CONNECTIVITY

Deliverable Substream: NETWORK AND CONNECTIVITY

Deliverable: Processes and Tools for Data Migration

ID: 73

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: The document defines the steps with their sequencing that a CSD or CB needs to undertake to successfully migrate to T2S. Furthermore, it explains the various options that T2S provides to migrate specific types of data to T2S and to ensure the integrity of migrated data. It also documents the specific migration obligations of CSDs and CBs resulting from the phased migration in multiple waves.

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: MIGRATION

Deliverable Substream: MIGRATION PREPARATION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: Registration Guide for Migration

ID: 74

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This document gathers the full set of administrative forms required for set-up. This version will rely on the registration guide created for testing and will complement it with what is required for production.

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: MIGRATION

Deliverable Substream: MIGRATION PREPARATION

Deliverable: Business Process Description (BPD)

ID: 75

Document Category: T2S Specifications

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: Deliverable Change Process (CRG)

Baseline: V1.0

Description: This document provides end-to-end business process descriptions for the life cycle of the different business operations (e.g. distribution or transformation). It describes which T2S services a CSD and CB may use to correctly and completely process a specific business operation.

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: SPECIFICATION AND DOCUMENTATION

Deliverable Substream: DOCUMENTATION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: T2S Glossary

ID: 78

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This document presents, encompasses and harmonises all the definitions included in the various T2S deliverables.

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: SPECIFICATION AND DOCUMENTATION

Deliverable Substream: DOCUMENTATION

Deliverable: User Testing Calendar

ID: 88

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This document provides on the availability of the testing environments and the process scheduling for each of the test environments (e.g. slow motion, fast forward or business day mode).

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING PREPARATION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: Eurosystem Acceptance Testing Assessment Report

ID: 101

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: N/A

Baseline: V1.0

Description: The report documents the Eurosystem's assessment whether T2S fulfils the User Requirements. It documents pending defects with a timeline for their resolution. Where necessary, it includes workarounds for remaining errors.

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: EUROSYSYEM ACCEPTANCE TEST

Deliverable Substream: EAT EXECUTION

Deliverable: T2S Smooth Cross-CSD Settlement

ID: 107

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: CRG

C – Consultation: CSD

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: The document presents the CSD specificities that the T2S users must take into account when instructing securities issued in or when settling with the counterparts in CSDs other than the in which they hold their Securities Account. The document defines and describes the additional conditions required to allow the smooth processing of cross-CSD instructions. This document is also discussed at the AG.

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: SPECIFICATION AND DOCUMENTATION

Deliverable Substream: DOCUMENTATION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: Adaptation to Cross-CSD Settlement

ID: 109

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: CRG

C – Consultation: CSD

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V2.0

Description: This document is based on the T2S Smooth Cross-CSD settlement deliverable (ID 107), it presents the conclusions of the subgroup working on this topic (detailed analysis of deliverable 107)..

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: SPECIFICATION AND DOCUMENTATION

Deliverable Substream: DOCUMENTATION

Deliverable: T2S Training Manual

ID: 110

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: The Eurosystem provides the CSDs/CBs with training on a train-the-trainer basis.If requested by a CSD/ CB, the Eurosystem can also provide these trainings (train the trainer concept) to the CSD/CB customers.These training materials are in line with internal documents such as the Training Framework and Training material guidelines. This document is delivered by topic: Basic, Technical, Functional, Operational, Testing and Migration. The plan details the versioning and delivery dates for each topic.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: TRAINING PREPARATION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: Risk Analysis on T2S Compliance with T2S Information Security Policy	ID: 116

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This document presents Eurosystem analysis on the compliance of T2S with the Information Security requirements and policy, as defined in the FA/CPA.

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: INFORMATION SECURITY

Deliverable Substream: INFORMATION SECURITY

Deliverable: Non Functional Test Report	ID: 141

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This report documents the results of the non-functional testing of T2S by the Eurosystem, (e.g. scalability testing, Disaster Recovery testing and Business Continuity testing).

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: NETWORK AND CONNECTIVITY

Deliverable Substream: NETWORK AND CONNECTIVITY

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: User Testing Stage Report

ID: 201

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.1

Description: Includes a check of the exit and entry criteria for a testing stage, an overview of the test results by testing stage, overview of functionalities delivered, resolved defects (defect ID, defect title, severity, T2S Service affected, impacted parties) and remaining known defects for the next testing stage. Used for the go-no-go decision on the next User Testing stage.
It includes the lessons learnt during the test stage.
Provided at the end of: Connectivity set-up, Interoperability, Community, Business Day (By wave).

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: USER TRAINING AND TESTING

Deliverable Substream: USER TESTING EXECUTION

Deliverable: Schedule 5 - Service Description

ID: 376

Document Category: Legal Acts

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: FA/CPA

Baseline: FA/CPA

Description: This deliverable classifies and decomposes the set of services that T2S will deliver. It provides a description from the T2S clients' perspective for each class of service and well as services within each class. It also defines the service boundaries for the services.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: CONTRACTUAL FRAMEWORK

Deliverable Substream: FRAMEWORK AGREEMENT

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: Proof of eligibility for participation in T2S

ID: 425

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: CSD
A – Accountable: CSD
C – Consultation: Eurosystem
I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This document is the standardised form that CSDs must complete for CSDs to document their compliance with the Eligibility Criteria for Participation in T2S. It describes the type and scope of documentation that the CSDs must provide as proof of eligibility. Also see Del ID 43 on "Implementation Guide for CSD Eligibility Criteria".

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: SYNCHRONISATION AND ON-BOARDING

Deliverable Substream: CSD READINESS

Deliverable: CSD Feasibility Assessment

ID: 430

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: CSD
A – Accountable: CSD
C – Consultation:
I – Information: Eurosystem

Applicable Change Process: N/A

Baseline: V1.0

Description: This deliverable presents the results of the CSD feasibility assessment. It contains a view on their internal adaptation approach and planning. It also presents the efforts the CSD is going to undertake to coordinate the readiness of their clients. As part of this feasibility assessment, CSD will also list the potential showstoppers they have identified. CSDs will include in their assessment a date for their migration to T2S that will be the basis for CSDs for CSD to agree and make their proposal for the composition and timing of migration waves to T2S.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: SYNCHRONISATION AND ON-BOARDING

Deliverable Substream: CSD READINESS

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: CB Feasibility Assessment

ID: 440

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: CB

A – Accountable: CB

C – Consultation:

I – Information: Eurosystem

Applicable Change Process: N/A

Baseline: V1.0

Description: This deliverable presents the results of the CB feasibility assessment. It contains a view on their internal adaptation approach and planning. It also presents the efforts the CB is going to undertake to coordinate the readiness of their clients. As part of this feasibility assessment, CB will also list the potential showstoppers they have identified. CBs will include in their assessment a date for their migration to T2S that will be the basis for CBs for CB to agree and make their proposal for the composition and timing of migration waves to T2S.

WBS:

Programme Workstream: CLIENT READINESS

Deliverable Stream: SYNCHRONISATION AND ON-BOARDING

Deliverable Substream: CB READINESS

Deliverable: EAT Documentation

ID: 466

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: Eurosystem

C – Consultation:

I – Information: CSD, CB

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: Provide, for informational purposes only, details of Eurosystem acceptance test documentation (test calendars etc.) to Contracting CSDs pursuant to ECB's obligations under the Framework Agreement Schedule 3 section 3.2.1 paragraph (ii) and section 3.2.2 paragraph (ii)"

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: EUROSISTEM ACCEPTANCE TEST

Deliverable Substream: EAT PREPARATION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: CSD Market Specific Test Cases for Eurosystem Acceptance Test

ID: 467

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☒

R – Responsible: CSD

A – Accountable: CSD

C – Consultation:

I – Information: Eurosystem

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This deliverable documents the market-specific test cases that a CSD would like the Eurosystem to execute as part of its Eurosystem Acceptance Testing in advance of the User Testing Execution Phase.

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: EUROSISTEM ACCEPTANCE TEST

Deliverable Substream: EAT PREPARATION

Deliverable: CB Market Specific Test Cases for Eurosystem Acceptance Test

ID: 470

Document Category: T2S Project Documents

Licence to Copy / Use ☒

Optional: ☒

R – Responsible: CB

A – Accountable: CB

C – Consultation:

I – Information: Eurosystem

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This deliverable documents the market-specific test cases that a CB would like the Eurosystem to execute as part of its Eurosystem Acceptance Testing in advance of the User Testing Execution Phase.

WBS:

Programme Workstream: PRODUCT READINESS

Deliverable Stream: EUROSISTEM ACCEPTANCE TEST

Deliverable Substream: EAT PREPARATION

Currency Participation Agreement

SCHEDULE 2 – ANNEX 8 – T2S list of Deliverables

Deliverable: End of Migration report

ID: 550

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☐

R – Responsible: Eurosystem

A – Accountable: PMG

C – Consultation: CSD, CB

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This deliverable provides after the go-live of each migration wave the lessons-learned from the respective migration wave to identify and provide recommendations on potential improvements in the scope and content of the User Testing Phase; migration activities, procedures and checkpoints; and operational procedures and controls.

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: MIGRATION

Deliverable Substream: MIGRATION WEEKEND (WAVE 1)

Deliverable: Proposal on the Composition and Timing of the Migration Waves

ID: 593

Document Category: T2S Project Documents

Licence to Copy / Use ☐

Optional: ☒

R – Responsible: CSD/CB

A – Accountable: CSD/CB

C – Consultation: Eurosystem

I – Information:

Applicable Change Process: Deliverable Change Process (PMG)

Baseline: V1.0

Description: This deliverable documents the joint proposal of CSDs/CBs on the composition and timing of the migration waves for the go-live of the initial T2S release. It forms the basis for the Eurosystem decision on the composition and timing of the migration waves.

WBS:

Programme Workstream: OPERATIONAL READINESS

Deliverable Stream: MIGRATION

Deliverable Substream: MIGRATION PREPARATION

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 2 – ANNEX 9

T2S LIST OF SYNCHRONISATION POINTS

Disclaimer:

Planning is an ongoing process and Annexes with planning elements are subject to change during the lifetime of a project. Planning workshops with CSDs and CBs will continue to agree on the planning for Connectivity, User Testing and Migration. Subsequent plan updates follow the process, documented in the Schedule 2, Section 7.

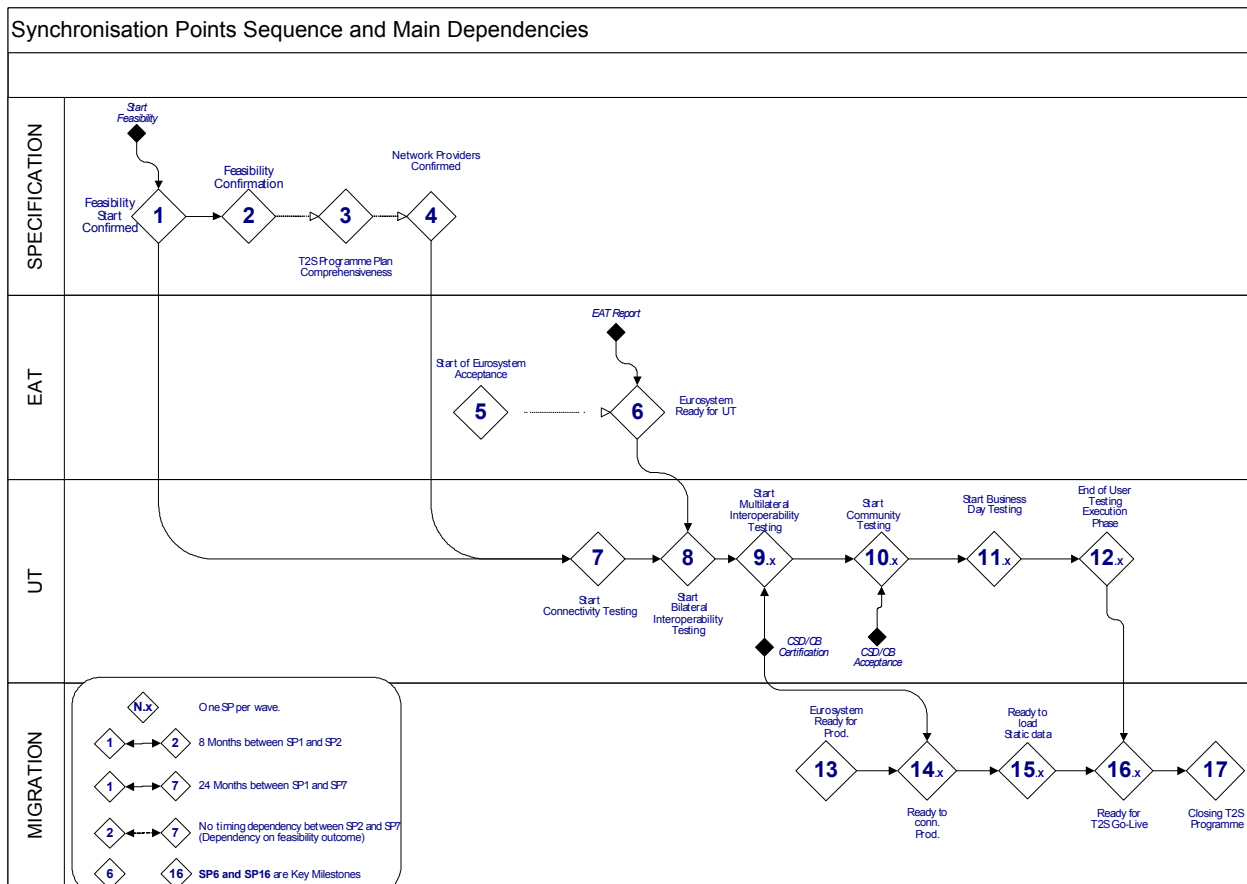
Annexes 2, 3, 4, 7, 8, 9 and 10 document the planning status as at 7 Nov. 2011.

Currency Participation Agreement

Schedule 2 – Annex 9 – T2S list of Synchronisation points

Introduction:

To ease the readability of the Synchronisation Points here is a drawing presenting the sequencing and main dependencies. For the exact timing please refer to the details of each Synchronisation Points.



DARWIN: 42344421

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP1 Start CSD/CB Feasibility Assessment Confirmed

20/12/11

SP1 marks the agreement between the Eurosystem and the respective CSDs and CBs that the Eurosystem has provided the specifications and documents to the CSDs and CBs in order for them to confirm that they have started their detailed feasibility assessment for the adaptation of their IT system and processes to T2S.

[Plan reference ID](#) 2006100

Eurosystem:

The Eurosystem confirms that it has provided the specifications and documents in the required scope and quality.

CSDs and CBs:

Each CSD and CB confirms that the Eurosystem has delivered the complete set of specifications and documents for the feasibility assessment. Each CSD and CB has confirmed that it has initiated its feasibility assessment.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ [Deliverable] - General Function Specification (GFS) V 4.0	49	Eurosystem	74100	31/05/10
☐ [Deliverable] - Graphical User Interface (GUI) Business Functionalities	3	Eurosystem	281100	28/02/11
☐ Delivery GFS Note	49	Eurosystem	74500	01/06/11
☐ [Deliverable] - T2S Smooth Cross CSD settlement Report V1.0	107	Eurosystem	259100	30/06/11
☐ [Deliverable] - Service Description	376	Eurosystem	1310380	21/07/11
☐ [Deliverable] - User Detailed Functional Specification (UDFS) V1.2	6	Eurosystem	211100	31/10/11
☐ Start feasibility study		CSDs,CBs	211200	02/11/11
☐ [Deliverable] - User Requirement Document (URD) 5.01	64	Eurosystem	16100	17/11/11
☐ [Deliverable] - Business Process Description V 1.0 (BPD)	75	Eurosystem	230000	18/11/11
☐ [Deliverable] - Legal Act of Implementation Guide for CSD Eligibility Criteria V2.0	43	Eurosystem	623900	28/11/11
☐ Confirm comprehensiveness to start feasibility assessment		CSDs,CBs	536200	15/12/11

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP2 Feasibility Confirmation by CSD/CB

10/08/12

SP2 marks the confirmation by CSDs and CBs that the adaptation of their IT systems and processes to interoperate with T2S are feasible from a functional and time perspective.

[Plan reference ID](#) 2007100

[Eurosystem:](#)

Based on the documentation from CSDs and CBs, defined as deliverables for this synchronisation point, the Eurosystem confirms that the T2S Programme Plan Assumptions for the overall T2S Programme Plan remain valid. It performs an impact assessment to ensure that any changes in assumptions do not have a material impact on the T2S Programme, and informs the T2S governance bodies if this is the case.

[CSDs and CBs:](#)

CSDs and CBs have reviewed the specifications and documents that the Eurosystem delivered for SP1 and confirm that it is feasible to adapt their IT systems and processes to interoperate with T2S. As part of their feasibility assessment, CSDs and CBs have identified their approach to the adaptation of their IT systems as well as impacts on processes and potential changes to their service offering. They have identified and logged potential showstoppers. CSDs and CBs have completed their high-level planning for going live with T2S and communicated their planning to the Eurosystem. The CSDs and CBs have submitted a proposal for the composition of the migration waves.

[Checklist:](#)

[Description:](#)

	Del ID:	Owner:	Plan ID:	Date:
☐ SP1 - Start Feasibility Confirmed			2006100	20/12/11
☐ [Deliverable] - CSD Feasibility Assessment	430	CSDs	213100	29/06/12
☐ [Deliverable] - CB Feasibility Assessment	440	CBs	546500	29/06/12
☐ [Deliverable] - Composition and Timing Migration Waves by CSDs/CBs	593	CSDs,CBs	546350	03/08/12
☐ Assessment of feasibility confirmation		Eurosystem	538200	10/08/12

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP3 T2S Programme Plan Comprehensiveness

17/12/12

SP 3 marks the mutual assessment and confirmation that the T2S Programme Plan and the CSDs' and the CBs' plans are comprehensive and adequately reflect any agreed additional specifications or deliverables.

[Plan reference ID](#) 2007200

Eurosystem:

The Eurosystem provides a status on the T2S progress so far and confirms that the actual T2S Programme Plan is comprehensive and adequate.

CSDs and CBs:

The objective of this checkpoint is to verify that each CSD and CB has conducted an internal impact assessment for the implementation of the CASG Standards and other harmonisation initiatives on their own project plan to adapt to T2S. It is also an interim verification point to validate the initial assessment made on SP 2.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ SP2 - Feasibility Confirmation by CSD/CB			2007100	10/08/12
☐ Confirmation of the Timing and Composition of Migration Waves by Eurosystem		Eurosystem	1209150	08/10/12
☐ [Deliverable] - Adaptation to Cross CSD settlement Report	109	Eurosystem	262000	20/11/12
☐ Update on CB Feasibility Assessment		CBs	553200	17/12/12
☐ Update on CSD Feasibility Assessment		CSDs	553000	17/12/12
☐ Confirmation of T2S programme plan status and achieved milestones		Eurosystem	540800	17/12/12

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP4 Network Providers Confirmed

24/04/14

SP 4 marks confirmation that the selected network providers fulfil the technical requirements, as required by the tender.

[Plan reference ID](#) 2008100

[Eurosystem:](#)

The Eurosystem and the selected Network Service Providers (NSP) undertake proof of concept and Network Acceptance Tests (using testing environment) to demonstrate that the NSPs fulfil the technical requirements, as required in the tender in order to provide certainty to CSDs and CBs of the NSP's capability to support T2S connectivity. The Eurosystem presents the results of the Network Acceptance Tests confirming the ability of the NSPs to cope with the defined requirements.

[CSDs and CBs:](#)

The CSDs and CBs have finalised their contracts with their selected Network Service Provider.

[Checklist:](#)

[Description:](#)

	Del ID:	Owner:	Plan ID:	Date:
☐ [Deliverable] - Tender for Network Connectivity (VAN)	69	Eurosystem	1059100	08/07/11
☐ Signature of Network Service Provider Agreement		Eurosystem	1061100	31/01/12
☐ CSD: Network Agreement Contract signed		CSDs	1063120	11/04/14
☐ CB: Network Agreement Contract signed		CBs	1063190	11/04/14

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP5 Start of Eurosystem Acceptance Test

15/01/14

SP 5 marks the start of the Eurosystem acceptance testing.

[Plan reference ID](#) 2009200

[Eurosystem:](#)

The Eurosystem has provided to CSDs and CBs the details of EAT documentation (e.g. test cases, test calendars, etc.). The Eurosystem confirms that it is ready to start the acceptance testing.

[CSDs and CBs:](#)

CSDs and CBs have reviewed the EAT documentation and potentially have identified specific additional test cases (optional) to increase the coverage of the EAT to market-specific requirements.

[Checklist:](#)

[Description:](#)

	Del ID:	Owner:	Plan ID:	Date:
☐ [Deliverable] - CSDs Market specific test cases for EAT V1.0	467	CSDs	451300	17/10/13
☐ [Deliverable] - CBs Market specific test cases for EAT V1.0	470	CBs	451700	17/10/13
☐ [Deliverable] - EAT Documentation V1.0 (EAT Test Sets)	466	Eurosystem	451400	14/11/13

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP6 Eurosystem Ready for User Testing

02/09/14

SP 6 marks the start of the User Testing.

[Plan reference ID](#) 2009100

[Eurosystem:](#)

The Eurosystem confirms that the CSDs and CBs can start User Testing. The Eurosystem has set-up the T2S User Testing environment(s), implemented all supporting processes, trained the support teams and provided the required documentation. It has defined and communicated the test cases for certification of CSDs and CBs.

[CSDs and CBs:](#)

The CSDs and CBs have submitted their completed registration guide for User Testing and have finalised their verification test cases.

[Checklist:](#)

[Description:](#)

	Del ID:	Owner:	Plan ID:	Date:
☐ [Deliverable] - Data Migration Tools specifications and related procedures V1.0	73	Eurosystem	1206100	31/10/12
☐ [Deliverable] -User Hand Book (UHB) V1.0	9	Eurosystem	324100	27/12/12
☐ [Deliverable] - User Hand Book V2.0 (UHB)	9	Eurosystem	335200	17/09/13
☐ [Intermediate Deliverable] Draft Non functional Testing Report for information V1.0	141	Eurosystem	384200	17/12/13
☐ [Deliverable] - Registration Guide for User Testing	42	Eurosystem	607200	22/01/14
☐ [Deliverable] - Functional Training Materials	110	Eurosystem	568600	03/03/14
☐ [Deliverable] - User Testing Guide	18	Eurosystem	616100	12/03/14
☐ [Deliverable] - User Testing Calendar	88	Eurosystem	597300	13/03/14
☐ [Deliverable] - Testing Training Materials	110	Eurosystem	569000	03/06/14
☐ [Deliverable] - CB Certification Test Cases	45	Eurosystem	634700	19/06/14
☐ [Deliverable] - CSD Certification Test Cases	30	Eurosystem	634600	19/06/14
☐ Helpdesk set-up and Ready to support CSDs/CBs		Eurosystem	630200	23/06/14
☐ Delivery updated version of the EAT Status update		Eurosystem	634300	27/08/14
☐ [Deliverable] EAT Assessment Report	101	Eurosystem	493130	01/09/14

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP7 Start Connectivity Testing

07/07/14

SP 7 marks the start of the connectivity tests by the CSDs and the CBs to the T2S User Testing environment(s).

[Plan reference ID](#) 2010100

Eurosystem:

The Eurosystem confirms the operational readiness of the networks for CSD and CB connectivity testing. The Eurosystem has issued the connectivity guides to the T2S user test environment(s). The Eurosystem confirms helpdesk is in place and problem management processes are operational.

CSDs and CBs:

CSDs and CBs have configured their network connectivity, according to the connectivity guide for the T2S user test environment(s). CSDs and CBs have completed the adaptation of their IT systems, according to T2S specifications and documentation. The starting date presented is the earliest starting date, since this is a bilateral phase, CSD and CB may decide to start this stage at a later date.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ [Deliverable] - Connectivity Guide for VAN and Direct connectivity (Testing) V1.0	8	Eurosystem	1042200	30/07/13
☐ [Deliverable] - Basic Training Materials	110	Eurosystem	568100	02/09/13
☐ Start of VAN Networks connectivity tests with CSDs/CBs (Finish acceptance VAN		Eurosystem	1067100	04/11/13
☐ [Deliverable] - Technical Training Materials	110	Eurosystem	568400	02/12/13
☐ [Deliverable] - UDFS v.2.0	6	Eurosystem	223150	19/12/13
☐ Completed UT Registration Guide for User Testing (network registration)		CSDs,CBs	627100	11/04/14
☐ SP4 - Network Service Provider Confirmed			2008100	24/04/14
☐ UT environment ready		Eurosystem	634200	11/06/14

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP8 Start Bilateral Interoperability Testing (for all waves)

01/10/14

SP 8 marks the start of the Bilateral Interoperability phase.

[Plan reference ID](#) 2011100

[Eurosystem:](#)

The Eurosystem confirms that Eurosystem Acceptance Test results have provided assurance that the quality required to start the User Testing is met. The Eurosystem confirms helpdesk is in place and problem management processes are operational. Documentation on testing processes has been delivered.

[CSDs and CBs:](#)

CSDs and CBs confirm their readiness for interoperability testing, including compliance of their adapted IT systems with the CASG Standards and other harmonisation initiatives. They have completed the training of staff involved in testing. They have communicated any identified potential showstoppers to the Eurosystem.

Test cases for acceptance have been communicated and agreed. The CSDs and CBs can now start the Bilateral Interoperability phase where they are going to execute the test cases for acceptance and the test cases required to get the certification. The starting date presented is the earliest starting date, since this is a bilateral phase, CSD and CB may decide to start this stage at a later date.

[Checklist:](#)

[Description:](#)

	Del ID:	Owner:	Plan ID:	Date:
☐ Interim verification of the List of Potential Show stopper from CSDs (dependencie		CSDs,CBs	644200	09/06/14
☐ Internal system adapted according to UDFS specifications by CSDs/CBs		CSDs,CBs	641150	30/06/14
☐ SP6 - Eurosystem Ready for User Testing			2009100	02/09/14
☐ [Deliverable] - User Testing Stage Report (Wave 2) V2.0 [Connectivity phase]	201	Eurosystem	840560	26/09/14
☐ [Deliverable] - User Testing Stage Report (Wave 1) V1.0 [Connectivity phase]	201	Eurosystem	646160	30/09/14
☐ [Deliverable] - User Testing Stage Report (Wave 3) V3.0 [Connectivity phase]	201	Eurosystem	2200600	30/09/14

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP9.1 Start Multilateral Interoperability Testing (Wave 1)

29/12/14

SP 9.1 marks the start of the Multilateral Interoperability Phase for the CSDs and CBs of the wave 1.

[Plan reference ID](#) 2011200

Eurosystem:

The Eurosystem has monitored the CSD and CB activity during the Bilateral Interoperability and has confirmed the CSD and CB capability to cope with the required T2S knowledge before starting the Multilateral Interoperability. The Eurosystem has issued the certificates for CSDs having passed the Certification test case execution.

CSDs and CBs:

CSDs and CBs have completed the execution of the certification test cases and have been certified. They are now ready to start the multilateral interoperability test phases where they will continue to test T2S in collaboration with other CSDs and CBs. In this phase, the CSDs and CBs will also complete their acceptance testing.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ Confirmation of the Timing and Composition of Migration Waves by Eurosystem		Eurosystem	1209150	08/10/12
☐ [Deliverable] - Registration Guide for Migration V1.0	74	Eurosystem	1222100	29/08/13
☐ [Deliverable] - Standard Migration Plan V1.0	26	Eurosystem	1232800	01/11/13
☐ Registration Guide for Migration filled in by CSDs/CBs (Wave 1)		CSDs,CBs	727100	03/09/14
☐ [Deliverable] - Migration Training Materials	110	Eurosystem	569200	01/12/14
☐ [Deliverable] - User Testing Stage Report (Wave 1) V1.1 Interoperability Bilateral	201	Eurosystem	714280	18/12/14
☐ [Deliverable] - Eurosystem T2S Certification (Wave 1)	37	Eurosystem	647960	29/12/14
☐ [Deliverable] - Eurosystem T2S Certification (Wave 1)	37	Eurosystem	647850	29/12/14

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP9.2 Start Multilateral Interoperability Testing (Wave 2)

02/04/15

SP 9.2 marks the start of the Multilateral Interoperability Phase for the CSDs and CBs of the wave 2.

[Plan reference ID](#) 2011300

Eurosystem:

The Eurosystem has monitored the CSD and CB activity during the Bilateral Interoperability and has confirmed the CSD and CB capability to cope with the required T2S knowledge before starting the Multilateral Interoperability. The Eurosystem has issued the certificates for CSDs having passed the Certification test case execution.

CSDs and CBs:

CSDs and CBs have completed the execution of the certification test cases and have been certified. They are now ready to start the multilateral interoperability test phases where they will continue to test T2S in collaboration with other CSDs and CBs. In this phase, the CSDs and CBs will also complete their acceptance testing.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ Registration Guide for Migration filled in by CSDs/CBs (Wave 2)		CSDs,CBs	917100	06/10/14
☐ [Deliverable] - User Testing Stage Report (Wave 2) V2.1 [Interoperability Bilateral	201	Eurosystem	914180	18/03/15
☐ [Deliverable] - Eurosystem T2S Certification (Wave 2)	37	Eurosystem	648250	01/04/15
☐ [Deliverable] - Eurosystem T2S Certification (Wave 2)	37	Eurosystem	648360	01/04/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP9.3 Start Multilateral Interoperability Testing (Wave 3)

23/06/15

SP 9.3 marks the start of the Multilateral Interoperability Phase for the CSDs and CBs of the wave 3.

[Plan reference ID](#) 2011400

[Eurosystem:](#)

The Eurosystem has monitored the CSD and CB activity during the Bilateral Interoperability and has confirmed the CSD and CB capability to cope with the required T2S knowledge before starting the Multilateral Interoperability. The Eurosystem has issued the certificates for CSDs having passed the Certification test case execution.

[CSDs and CBs:](#)

CSDs and CBs have completed the execution of the certification test cases and have been certified. They are now ready to start the multilateral interoperability test phases where they will continue to test T2S in collaboration with other CSDs and CBs. In this phase, the CSDs and CBs will also complete their acceptance testing.

[Checklist:](#)

[Description:](#)

	Del ID:	Owner:	Plan ID:	Date:
☐ Registration Guide for Migration filled in by CSDs/CBs (Wave 3)		CSDs,CBs	2282500	17/04/15
☐ [Deliverable] - Eurosystem T2S Certification (Wave 3)	37	Eurosystem	648550	22/06/15
☐ [Deliverable] - Eurosystem T2S Certification (Wave 3)	37	Eurosystem	648650	22/06/15
☐ [Deliverable] - User Testing Stage Report (Wave 3) V3.1 Interoperability Bilateral	201	Eurosystem	2273080	23/06/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP10.1 Start Community Testing (Wave 1)

04/03/15

SP 10.1 marks the start of Community Testing Phase.

[Plan reference ID](#) 2012100

Eurosystem:

Eurosystem confirms the necessary information for DCP/ DCAH certification and migration dress rehearsal has been provided. The Eurosystem is ready to initiate community testing.

CSDs and CBs:

CSD and CB Acceptance process has been finalized. CSDs and CBs have successfully completed interoperability tests and have proved that their adapted IT platforms interoperate correctly with T2S. CSDs and CBs confirm their internal operational readiness to enter this test phase, i.e. internal staff trained, required procedures are operational, and local operations are familiar with the operation of T2S. CSDs and CBs have trained their communities and agreed certification processes/approach with their respective DCPs. CSDs and CBs are ready to execute migration tests and dress rehearsals.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ Confirmation that CB members are ready (Wave 1)		CBs	728300	04/02/15
☐ Confirmation that test cases and supporting data and processes are ready for Co		CSDs,CBs	728400	04/02/15
☐ Confirmation that CSD participants are ready (Wave 1)		CSDs	728200	04/02/15
☐ [Deliverable] - User Testing Stage Report (Wave 1) V1.2 [Interoperability Multilater	201	Eurosystem	723100	04/03/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP10.2 Start Community Testing (Wave 2)

29/05/15

SP 10.2 marks the start of Community Testing Phase.

[Plan reference ID](#) 2012200

Eurosystem:

Eurosystem confirms the necessary information for DCP/ DCAH certification and migration dress rehearsal has been provided. The Eurosystem is ready to initiate community testing.

CSDs and CBs:

CSD and CB Acceptance process has been finalized. CSDs and CBs have successfully completed interoperability tests and have proved that their adapted IT platforms interoperate correctly with T2S. CSDs and CBs confirm their internal operational readiness to enter this test phase, i.e. internal staff trained, required procedures are operational, and local operations are familiar with the operation of T2S. CSDs and CBs have trained their communities and agreed certification processes/approach with their respective DCPs. CSDs and CBs are ready to execute migration tests and dress rehearsals.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ SP10.1 - Start Community Testing (wave 1)			2012100	04/03/15
☐ Confirmation that CB members are ready (Wave 2)		CBs	918300	30/04/15
☐ Confirmation that test cases and supporting data and processes are ready for Co		CSDs,CBs	918400	30/04/15
☐ Confirmation that CSD participants are ready (Wave 2)		CSDs	918200	30/04/15
☐ [Deliverable] - User Testing Stage Report (Wave 2) V2.2 [Interoperability Multilate	201	Eurosystem	913100	29/05/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP10.3 Start Community Testing (Wave 3)

09/11/15

SP 10.3 marks the start of Community Testing Phase.

[Plan reference ID](#) 2012300

Eurosystem:

Eurosystem confirms the necessary information for DCP/ DCAH certification and migration dress rehearsal has been provided. The Eurosystem is ready to initiate community testing.

CSDs and CBs:

CSD and CB Acceptance process has been finalized. CSDs and CBs have successfully completed interoperability tests and have proved that their adapted IT platforms interoperate correctly with T2S. CSDs and CBs confirm their internal operational readiness to enter this test phase, i.e. internal staff trained, required procedures are operational, and local operations are familiar with the operation of T2S. CSDs and CBs have trained their communities and agreed certification processes/approach with their respective DCPs. CSDs and CBs are ready to execute migration tests and dress rehearsals.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ SP10.1 - Start Community Testing (wave 1)			2012100	04/03/15
☐ Confirmation that test cases and supporting data and processes are ready for Co		CSDs	2283000	12/10/15
☐ Confirmation that CB members are ready (wave 3)		CBs	2282000	12/10/15
☐ Confirmation that CSDs participants are ready (wave 3)		CSDs	2281000	12/10/15
☐ [Deliverable] - User Testing Stage Report(Wave 3) V3.2 [Interoperability Multilater	201	Eurosystem	2275000	30/10/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP11.1 Start Business Day Testing (Wave 1)

18/05/15

SP 11.1 marks the start of Business Day Testing Phase

[Plan reference ID](#) 2012400

Eurosystem:

The Eurosystem confirms the team readiness to support the simulation of several consecutive business days of T2S operation. These business operations days will be executed after a migration rehearsal for the respective CSD and CB migration wave. The Eurosystem has provided the detailed migration playbook (Script) for the migration WE execution. DCP/DCAH Certification process has been completed.

CSDs and CBs:

CSDs and CBs learned from the Community testing phase and have adapted their operational processes accordingly.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ [Deliverable] - Manual of Operational Procedures (MOP) V1.0 for Business Day T	10	Eurosystem	1140100	24/04/14
☐ [Deliverable] - Operational Training Materials	110	Eurosystem	568800	03/06/14
☐ [Deliverable] - Certification report for DCPs (Wave 1)	46	Eurosystem	789800	15/04/15
☐ [Deliverable] - Certification report for DCAH (Wave 1)	46	Eurosystem	792000	15/04/15
☐ [Deliverable] - User Testing Stage Report (Wave 1) V1.3 [Community phase]	201	Eurosystem	789400	14/05/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP11.2 Start Business Day Testing (Wave 2)

09/11/15

SP 11.2 marks the start of Business Day Testing Phase

[Plan reference ID](#) 2012500

Eurosystem:

The Eurosystem confirms the team readiness to support the simulation of several consecutive business days of T2S operation. These business operations days will be executed after a migration rehearsal for the respective CSD and CB migration wave. The Eurosystem has provided the detailed migration playbook (Script) for the migration WE execution. DCP/DCAH Certification process has been completed.

CSDs and CBs:

CSDs and CBs learned from the Community testing phase and have adapted their operational processes accordingly.

Checklist:

Description:

Del ID: Owner: Plan ID: Date:

☐ SP10.1 - Start Community Testing (wave 1)			2012100	04/03/15
☐ [Deliverable] - Certification report for DCAH (Wave 2)	46	Eurosystem	981000	07/10/15
☐ [Deliverable] - Certification report for DCPs (Wave 2)	46	Eurosystem	979700	07/10/15
☐ [Deliverable] - User Testing Stage Report (Wave 2) V2.3 [Community phase]	201	Eurosystem	979300	04/11/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP11.3 Start Business Day Testing (Wave 3)

27/04/16

SP 11.3 marks the start of Business Day Testing Phase

[Plan reference ID](#) 2012600

Eurosystem:

The Eurosystem confirms the team readiness to support the simulation of several consecutive business days of T2S operation. These business operations days will be executed after a migration rehearsal for the respective CSD and CB migration wave. The Eurosystem has provided the detailed migration playbook (Script) for the migration WE execution. DCP/DCAH Certification process has been completed.

CSDs and CBs:

CSDs and CBs learned from the Community testing phase and have adapted their operational processes accordingly.

Checklist:

Description:

Del ID: Owner: Plan ID: Date:

☐ SP10.1 - Start Community Testing (wave 1)			2012100	04/03/15
☐ [Deliverable] - Certification report for DCAH (Wave 3)	46	Eurosystem	2346700	18/03/16
☐ [Deliverable] - Certification report for DCPs (Wave 3)	46	Eurosystem	2346300	18/03/16
☐ [Deliverable] - User Testing Stage Report (Wave 3) V3.3 [Community phase]	201	Eurosystem	2345100	27/04/16

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP12.1 End of User Testing Execution Phase (Wave 1)

15/06/15

SP 12.1 marks the end of User Testing by CSDs and CBs.

[Plan reference ID](#) 2013100

[Eurosystem:](#)

The Eurosystem confirms compliance of Eurosystem, CSDs and CBs as well as directly connected parties, with exit criteria for the user test. The Eurosystem provides a test report on the results of the user test that documents remaining defects and a plan for their resolution.

[CSDs and CBs:](#)

The CSDs and CBs confirm the Eurosystem Final User Test Report regarding the remaining defects and the priorities for their resolution. CSDs and CBs assess their operational readiness status and provide a clear status on the readiness to go-live with T2S to their respective community. CSDs have assessed whether their DCPs fulfil any specific requirements for local processing.

[Checklist:](#)

[Description:](#)

[Del ID:](#) [Owner:](#) [Plan ID:](#) [Date:](#)

☐ [Deliverable] - User Testing Stage Report (Wave 1) V1.4 [Business day phase]	201	Eurosystem	832300	12/06/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP12.2 End of User Testing Execution Phase (Wave 2)

18/01/16

SP 12.2 marks the end of User Testing by CSDs and CBs.

[Plan reference ID](#) 2013200

[Eurosystem:](#)

The Eurosystem confirms compliance of Eurosystem, CSDs and CBs as well as directly connected parties, with exit criteria for the user test. The Eurosystem provides a test report on the results of the user test that documents remaining defects and a plan for their resolution.

[CSDs and CBs:](#)

The CSDs and CBs confirm the Eurosystem Final User Test Report regarding the remaining defects and the priorities for their resolution. CSDs and CBs assess their operational readiness status and provide a clear status on the readiness to go-live with T2S to their respective community. CSDs have assessed whether their DCPs fulfil any specific requirements for local processing.

[Checklist:](#)

[Description:](#)

[Del ID:](#) [Owner:](#) [Plan ID:](#) [Date:](#)

☐ [Deliverable] - User Testing Stage Report (Wave 2) V2.4 [Business day phase]	201	Eurosystem	1022300	11/01/16

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP12.3 End of User Testing Execution Phase (Wave 3)

29/06/16

SP 12.3 marks the end of User Testing by CSDs and CBs.

[Plan reference ID](#) 2013300

[Eurosystem:](#)

The Eurosystem confirms compliance of Eurosystem, CSDs and CBs as well as directly connected parties, with exit criteria for the user test. The Eurosystem provides a test report on the results of the user test that documents remaining defects and a plan for their resolution.

[CSDs and CBs:](#)

The CSDs and CBs confirm the Eurosystem Final User Test Report regarding the remaining defects and the priorities for their resolution. CSDs and CBs assess their operational readiness status and provide a clear status on the readiness to go-live with T2S to their respective community. CSDs have assessed whether their DCPs fulfil any specific requirements for local processing.

[Checklist:](#)

[Description:](#)

[Del ID:](#) [Owner:](#) [Plan ID:](#) [Date:](#)

☐ [Deliverable] - User Testing Stage Report (Wave 3) V3.4 [Business day phase]	201	Eurosystem	2390200	22/06/16

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP13 Eurosystem ready for Production

01/12/14

SP13 marks the confirmation of Eurosystem to the CSDs and CBs that the T2S production environment is ready.

[Plan reference ID](#) 2014100

Eurosystem:

The Eurosystem confirms to the CSDs and CBs that the production environment is ready to connect. The environment is ready for the creation of the initial production set-up of system entities, users, access rights and other configuration data, to be performed according to the information received in the registration guides.

CSDs and CBs:

CSDs and CBs have submitted their registration guides for migration and have verified that there are no showstoppers for their connectivity to the T2S production environment.

Checklist:

Description:

Del ID: Owner: Plan ID: Date:

☐ Final Network Acceptance Tests (PROD)		Eurosystem	1066200	11/10/13
☐ [Deliverable] - Non Functional Testing Report	141	Eurosystem	386100	28/02/14
☐ T2S helpdesk is operational and contact details have been communicated to all re		Eurosystem	1258200	17/11/14
☐ Network ready for Production		Eurosystem	387100	01/12/14

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP14.1 Ready to connect to Production (Wave 1)

05/02/15

SP 14.1 marks the confirmation from the CSDs and CBs that they can technically connect to the T2S production environment.

[Plan reference ID](#) 2015100

Eurosystem:

The Eurosystem delivers the connectivity guide for the T2S production environment and the technical helpdesk is ready to support CSDs and CBs connectivity activities to the production environment.

CSDs and CBs:

CSDs and CBs have implemented the required configurations to connect to the production environment and can connect successfully to the T2S production environment.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ [Deliverable] - Data Migration Tools specifications and related procedures V1.0	73	Eurosystem	1206100	31/10/12
☐ [Deliverable] - Registration Guide for Migration V1.0	74	Eurosystem	1222100	29/08/13
☐ [Deliverable] - Connectivity Guide for VAN and Direct connectivity V2.0	8	Eurosystem	1043100	02/01/14
☐ T2S helpdesk is operational and contact details have been communicated to all re		Eurosystem	1258200	17/11/14
☐ SP13 - Eurosystem ready for Production			2014100	01/12/14
☐ Registration Form filled in (wave 1 + CSDs/CBs with Common Static Data)		CSDs,CBs	1247100	12/12/14
☐ [Deliverable] - CSD's T2S Compliance Confirmation (Wave 1)	36	CSDs,CBs	647360	29/12/14
☐ [Deliverable] - Proof of Eligibility to Participate in T2S (Wave 1)	425	CSDs	625600	19/01/15
☐ Input Registration Data completed		Eurosystem	1252150	29/01/15
☐ Completed network registration by CBs (wave 1)		CBs	1255300	05/02/15
☐ Completed network registration by CSDs (wave 1)		CSDs	1255200	05/02/15
☐ PROD environment available for users		Eurosystem	1256100	05/02/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP14.2 Ready to connect to Production (Wave 2)

02/10/15

SP 14.2 marks the confirmation from the CSDs and CBs that they can technically connect to the T2S production environment.

[Plan reference ID](#) 2015200

Eurosystem:

The Eurosystem delivers the connectivity guide for the T2S production environment and the technical helpdesk is ready to support CSDs and CBs connectivity activities to the production environment.

CSDs and CBs:

CSDs and CBs have implemented the required configurations to connect to the production environment and can connect successfully to the T2S production environment.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ SP14.1 - Ready to connect to Production (wave 1)			2015100	05/02/15
☐ [Deliverable] - CSD's T2S Compliance Confirmation (Wave 2)	36	CSDs,CBs	647460	02/04/15
☐ Registration Form filled in (CSDs/CBs) (wave 2)		CSDs,CBs	1281500	11/09/15
☐ [Deliverable] - Proof of Eligibility to Participate in T2S (Wave 2)	425	CSDs	626700	15/09/15
☐ T2S helpdesk is operational and contact details have been communicated to all re		Eurosystem	1283700	21/09/15
☐ Input Registration Data completed (wave 2)		Eurosystem	1262100	02/10/15
☐ Completed network registration by CSDs (wave 2)		CSDs	1283350	02/10/15
☐ Completed network registration by CBs (wave 2)		CBs	1283380	02/10/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP14.3 Ready to connect to Production (Wave 3)

22/03/16

SP 14.3 marks the confirmation from the CSDs and CBs that they can technically connect to the T2S production environment.

[Plan reference ID](#) 2015300

[Eurosystem:](#)

The Eurosystem delivers the connectivity guide for the T2S production environment and the technical helpdesk is ready to support CSDs and CBs connectivity activities to the production environment.

[CSDs and CBs:](#)

CSDs and CBs have implemented the required configurations to connect to the production environment and can connect successfully to the T2S production environment.

[Checklist:](#)

[Description:](#)

	Del ID:	Owner:	Plan ID:	Date:
☐ SP14.1 - Ready to connect to Production (wave 1)			2015100	05/02/15
☐ [Deliverable] - CSD's T2S Compliance Confirmation (Wave 3)	36	CSDs,CBs	647560	02/04/15
☐ [Deliverable] - Proof of Eligibility to Participate in T2S (Wave 3)	425	CSDs	628000	03/03/16
☐ Registration Form filled in (CSDs/CBs) (wave 3)		CSDs,CBs	1293600	04/03/16
☐ T2S helpdesk is operational and contact details have been communicated to all re		Eurosystem	1294800	09/03/16
☐ Completed network registration by CSDs (wave 3)		CSDs	1294200	22/03/16
☐ Input registration data completed (wave 3)		Eurosystem	1261050	22/03/16
☐ Completed network registration by CBs (wave 3)		CBs	1294350	22/03/16

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP15.1 Ready to upload static data (Wave 1)

19/03/15

SP 15.1 marks the start of the upload of the required static and configuration data for the migration to T2S.

[Plan reference ID](#) 2016100

[Eurosystem:](#)

The Eurosystem has tested the migration utilities for static and configuration data successfully with CSDs and CBs during User Testing.

[CSDs and CBs:](#)

CSDs and CBs have established the processes to ensure the update and synchronisation of static and configuration data. They have established the required control mechanisms for reconciliation. They have performed a quality assurance of the static data that needs to be loaded in T2S on their respective operational systems.

[Checklist:](#)

[Description:](#)

	Del ID:	Owner:	Plan ID:	Date:
☐ T2S System Configuration parameters finalised		Eurosystem	1270400	29/01/15
☐ SP14.1 - Ready to connect to Production (wave 1)			2015100	05/02/15
☐ Relevant Static Data ready by CBs (wave1)		CBs	1271300	05/03/15
☐ Relevant Static Data ready by CSDs (wave1)		CSDs	1271200	05/03/15
☐ Successful connectivity tests CSD (wave 1)		CSDs	1263100	12/03/15
☐ Successful connectivity tests CB (wave 1)		CBs	1255400	12/03/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP15.2 Ready to upload static data (Wave 2)

06/11/15

SP 15.2 marks the start of the upload of the required static and configuration data for the migration to T2S.

[Plan reference ID](#) 2016200

[Eurosystem:](#)

The Eurosystem has tested the migration utilities for static and configuration data successfully with CSDs and CBs during User Testing.

[CSDs and CBs:](#)

CSDs and CBs have established the processes to ensure the update and synchronisation of static and configuration data. They have established the required control mechanisms for reconciliation. They have performed a quality assurance of the static data that needs to be loaded in T2S on their respective operational systems.

[Checklist:](#)

[Description:](#)

	Del ID:	Owner:	Plan ID:	Date:
☐ SP15.1 - Ready to upload Static Data (wave 1)			2016100	19/03/15
☐ Relevant Static Data ready CSD (wave 2)		CSDs	1284200	09/10/15
☐ Relevant Static Data ready CB (wave 2)		CBs	1284300	09/10/15
☐ Successful connectivity tests CB (wave 2)		CBs	1283390	30/10/15
☐ Successful connectivity tests CSD (wave 2)		CSDs	1283370	30/10/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP15.3 Ready to upload static data (Wave 3)

22/04/16

SP 15.3 marks the start of the upload of the required static and configuration data for the migration to T2S.

[Plan reference ID](#) 2016300

Eurosystem:

The Eurosystem has tested the migration utilities for static and configuration data successfully with CSDs and CBs during User Testing.

CSDs and CBs:

CSDs and CBs have established the processes to ensure the update and synchronisation of static and configuration data. They have established the required control mechanisms for reconciliation. They have performed a quality assurance of the static data that needs to be loaded in T2S on their respective operational systems.

Checklist:

Description:

Del ID: Owner: Plan ID: Date:

☐ SP15.1 - Ready to upload Static Data (wave 1)			2016100	19/03/15
☐ Relevant Static Data ready CSD (wave 3)		CSDs	1297200	27/03/16
☐ Relevant Static Data ready CB (wave 3)		CBs	1297300	27/03/16
☐ Successful connectivity tests CB (wave 3)		CBs	1294370	15/04/16
☐ Successful connectivity tests CSD (wave 3)		CSDs	1294300	15/04/16

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP16.1 Ready for T2S Go-Live (Wave 1)

19/06/15

SP 16.1 marks the latest checkpoint prior to the migration WE execution.

[Plan reference ID](#) 2017100

Eurosystem:

The Eurosystem confirms that the production environment is ready for the migration of CSDs and CBs to T2S. The Eurosystem has defined and agreed the organisation and timeline of the migration weekend with the relevant stakeholders. The Eurosystem has established the necessary control mechanisms and decision points to ensure a successful execution of the migration procedures or to allow a rollback in contingency situations. The Eurosystem in conjunction with CSDs and CBS has defined the roles and responsibilities of each stakeholder. It has established a formal communication plan and escalation process.

CSDs and CBs:

CSDs and CBs confirm that the final migration dress rehearsal has been successful. They confirm to follow the agreed procedures and processes for the migration weekend. CSDs and CBs have ensured staff availability for the migration weekend. CSDs and CBs have established the necessary internal controls on the migration process to ensure the completeness and the correctness of their migration.

Checklist:

Description:

Del ID: Owner: Plan ID: Date:

☐ [Deliverable] - Detailed Migration Weekend Script V1.0 Wave 1	27	Eurosystem	1235400	28/11/14
☐ SP15.1 - Ready to upload Static Data (wave 1)			2016100	19/03/15
☐ [Deliverable] - Risk Analysis on T2S Compliance with T2S Information Security pol	116	Eurosystem	1108100	22/05/15
☐ Final verification of the list of showstoppers wave 1 (dependencies with local regul		CSDs,CBs	1272200	22/05/15
☐ External communication has been rolled-out (wave 1)		CSDs,CBs	1277400	05/06/15
☐ Confirmation that internal control mechanisms are in place (wave 1)		CSDs,CBs	1277300	05/06/15
☐ Confirmation that migration script has been integrated in internal plans (wave 1)		CSDs,CBs	1277000	12/06/15
☐ Internal staff trained for change-over Weekend and operations (wave 1)		CSDs,CBs	1277200	18/06/15

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP16.2 Ready for T2S Migration Wave 2

29/01/16

SP 16.2 marks the latest checkpoint prior to the migration WE execution.

[Plan reference ID](#) 2017200

Eurosystem:

The Eurosystem confirms that the production environment is ready for the migration of CSDs and CBs to T2S. The Eurosystem has defined and agreed the organisation and timeline of the migration weekend with the relevant stakeholders. The Eurosystem has established the necessary control mechanisms and decision points to ensure a successful execution of the migration procedures or to allow a rollback in contingency situations. The Eurosystem in conjunction with CSDs and CBS has defined the roles and responsibilities of each stakeholder. It has established a formal communication plan and escalation process.

CSDs and CBs:

CSDs and CBs confirm that the final migration dress rehearsal has been successful. They confirm to follow the agreed procedures and processes for the migration weekend. CSDs and CBs have ensured staff availability for the migration weekend. CSDs and CBs have established the necessary internal controls on the migration process to ensure the completeness and the correctness of their migration.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ Final verification of the list of showstoppers wave 1 (dependencies with local regul		CSDs,CBs	1272200	22/05/15
☐ [Deliverable] - Risk Analysis on T2S Compliance with T2S Information Security pol	116	Eurosystem	1108100	22/05/15
☐ SP14.2 - Ready to connect to Production (wave 2)			2015200	02/10/15
☐ SP15.2 - Ready to upload Static Data (wave 2)			2016200	06/11/15
☐ [Deliverable] - Detailed Migration Weekend Script V2.2 Wave 2	27	Eurosystem	1237300	09/11/15
☐ External communication has been rolled-out (Wave 2)		CSDs,CBs	1287500	15/01/16
☐ Confirmation that internal control mechanisms are in place (Wave 2)		CSDs,CBs	1287400	15/01/16
☐ Confirmation that migration script has been integrated in internal plans (Wave 2)		CSDs,CBs	1287200	22/01/16
☐ Internal staff trained for change-over Weekend and operations (Wave 2)		CSDs,CBs	1287300	28/01/16

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP16.3 Ready for T2S Migration Wave 3

15/07/16

SP 16.3 marks the latest checkpoint prior to the migration WE execution.

[Plan reference ID](#) 2017300

Eurosystem:

The Eurosystem confirms that the production environment is ready for the migration of CSDs and CBs to T2S. The Eurosystem has defined and agreed the organisation and timeline of the migration weekend with the relevant stakeholders. The Eurosystem has established the necessary control mechanisms and decision points to ensure a successful execution of the migration procedures or to allow a rollback in contingency situations. The Eurosystem in conjunction with CSDs and CBs has defined the roles and responsibilities of each stakeholder. It has established a formal communication plan and escalation process.

CSDs and CBs:

CSDs and CBs confirm that the final migration dress rehearsal has been successful. They confirm to follow the agreed procedures and processes for the migration weekend. CSDs and CBs have ensured staff availability for the migration weekend. CSDs and CBs have established the necessary internal controls on the migration process to ensure the completeness and the correctness of their migration.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ Final verification of the list of showstoppers wave 1 (dependencies with local regul		CSDs,CBs	1272200	22/05/15
☐ [Deliverable] - Risk Analysis on T2S Compliance with T2S Information Security pol	116	Eurosystem	1108100	22/05/15
☐ [Deliverable] - Detailed Migration Weekend Script V3.2 Wave 3	27	Eurosystem	1238200	12/04/16
☐ SP15.3 - Ready to upload Static Data (wave 3)			2016300	22/04/16
☐ External communication has been rolled-out (Wave 3)		CSDs,CBs	1299600	01/07/16
☐ Confirmation that internal control mechanisms are in place (Wave 3)		CSDs,CBs	1299500	01/07/16
☐ Confirmation that migration script has been integrated in internal plans (Wave 3)		CSDs,CBs	1299300	08/07/16
☐ Internal staff trained for change-over Weekend and operations (Wave 3)		CSDs,CBs	1299400	14/07/16

Currency Participation Agreement

SCHEDULE 2 – ANNEX 9 – T2S list of Synchronisation points

SP17 Closing T2S Programme

10/10/16

SP 17 marks the end of the T2S Programme.

[Plan reference ID](#) 2018300

Eurosystem:

The Eurosystem confirms that the production environment is ready for the migration of CSDs and CBs to T2S. The Eurosystem has defined and agreed the organisation and timeline of the migration weekend with the relevant stakeholders. The Eurosystem has established the necessary control mechanisms and decision points to ensure a successful execution of the migration procedures or to allow a rollback in contingency situations. The Eurosystem in conjunction with CSDs and CBs has defined the roles and responsibilities of each stakeholder. It has established a formal communication plan and escalation process.

CSDs and CBs:

All contracting CSDs and CBs are operational on T2S. They have identified any major pending issues and have communicated them to the Eurosystem for investigation and resolution.

Checklist:

Description:

	<u>Del ID:</u>	<u>Owner:</u>	<u>Plan ID:</u>	<u>Date:</u>
☐ [Deliverable] - End of Migration Report (Wave 1)	550	Eurosystem	835100	27/07/15
☐ [Deliverable] - End of Migration Report (Wave 2)	550	Eurosystem	1025100	07/03/16
☐ [Deliverable] - End of Migration Report (Wave 3)	550	Eurosystem	2394000	22/08/16

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 2 – ANNEX 10

T2S LIST OF MILESTONES ON THE CRITICAL PATH

Disclaimer:

Planning is an ongoing process and Annexes with planning elements are subject to change during the lifetime of a project. Planning workshops with CSDs and CBs will continue to agree on the planning for Connectivity, User Testing and Migration. Subsequent plan updates follow the process, documented in the Schedule 2, Section 7.

Annexes 2, 3, 4, 7, 8, 9 and 10 document the planning status as at 7 Nov. 2011.

Currency Participation Agreement

Schedule 2 – Annex 10 – T2S list of Milestones on the critical path

ID Number*	Milestone Description	Date**	Responsible for delivery
172200	WS - Delivery IDFS V0.85 to the Development Coordination	15/02/2011***	Eurosystem
124150	Final Validation Pillar II by the SGMS	04/03/2011***	SGMS
134150	Final Validation Pillar III by the SGMS	01/07/2011***	SGMS
211100	[Deliverable] - UDFS v1.2	31/10/2011***	Eurosystem
345101	Development Process - M1 - Technical Readiness for integration	30/09/2010***	Eurosystem
351130	Development Process - M2 - UDFS/IDFS stabilised and integrated in the development process iterations	01/04/2011***	Eurosystem
353130	Development process - M3 – Interfaces specifications frozen (UDFS/GUI): iteration 5 technically integrated and tested	31/10/2011***	Eurosystem
354130	Development Process - M4 - Start of 4CB IAC	02/04/2012	Eurosystem
355140	Development process – M5 – Technical stability	28/09/2012	Eurosystem
361101	Development process – M6 – Functional stability	29/03/2013	Eurosystem
339200	Development process – M7 – 4CB Internal Acceptance check point – Progress status	30/09/2013	Eurosystem
378101	Start Execution Infrastructure test	30/04/2013	Eurosystem
386100	[Deliverable] - Outcome of the Non Functional Testing	28/02/2014	Eurosystem
493160	Go-no go decision for the start of the User Testing	15/09/2014	Eurosystem

Currency Participation Agreement

Schedule 2 – Annex 10 – T2S list of Milestones on the critical path

ID Number*	Milestone Description	Date**	Responsible for delivery
580150	CSDs and CBs training session finalised	06/05/2015	Eurosystem, CSDs, CBs
634200	UT environment ready	18/06/2014	Eurosystem
124410	Start preparation of Migration Weekend (wave 1)	01/12/2014	Eurosystem
387100	Network ready for Production	01/12/2014	Eurosystem
1246100	Prod environment availability for 4CB teams	01/12/2014	Eurosystem
1247100	Registration Form filled in (wave 1 + CSDs/CBs with common static data)	12/12/2014	CSDs
1263100	Successful connectivity tests CSD (wave 1 + CSDs with common static data)	12/03/2015	CSDs
1255400	Successful connectivity tests CB (wave 1 + CBs with common static data)	12/03/2015	CBs
1279100	Wave 1 Start Operations in T2S	22/06/2015	Eurosystem, CSDs, CBs
1281200	Start preparation of Migration Weekend (wave 2)	17/08/2015	Eurosystem
1281500	Registration Form filled in (CSDs/CBs) (wave 2)	11/09/2015	CSDs
1283370	Successful connectivity tests CSD (wave 2 + CSDs with common static data)	30/10/2015	CSDs
1283390	Successful connectivity tests CB (wave 2 + CBs with common static data)	30/10/2015	CBs
1291100	Wave 2 Start Operations in T2S	01/02/2016	Eurosystem, CSDs, CBs
1293300	Start preparation of Migration Weekend (wave 3)	08/02/2016	Eurosystem

Currency Participation Agreement

Schedule 2 – Annex 10 – T2S list of Milestones on the critical path

ID Number*	Milestone Description	Date**	Responsible for delivery
1293600	Registration Form filled in (CSDs/CBs) (wave 3)	04/03/2016	CSDs
1294300	Successful connectivity tests CSD (wave 3 + CSDs with common static data)	15/04/2016	CSDs
1294370	Successful connectivity tests CB (wave 3 + CBs with common static data)	15/04/2016	CBs
1304100	Wave 3 Start Operations in T2S	18/07/2016	Eurosystem, CSDs, CBs
2006100	SP1 - Start Feasibility	20/12/2011	Eurosystem
2007100	SP2 - Feasibility Confirmation by CSd/CB	10/08/2012	CSDs, CBs
2009200	SP5 - Eurosystem ready for EAT	30/12/2013	Eurosystem
2009100	SP6 - Eurosystem Ready for User Testing	02/09/2014	Eurosystem
2010100	SP7 - Start Connectivity Test	07/07/2014	Eurosystem, CSDs, CBs
2011100	SP8 - Start Interoperability Bilateral Test	01/10/2014	Eurosystem, CSDs, CBs
2013100	SP12.1 - End of Testing (wave 1)	15/06/2015	Eurosystem, CSDs, CBs
2013200	SP12.2 - End of Testing (wave 2)	18/01/2016	Eurosystem, CSDs, CBs
2013300	SP12.3 - End of Testing (wave 3)	29/06/2016	Eurosystem, CSDs, CBs
2014100	SP13.1 - Eurosystem ready for Production (wave 1)	01/12/2014	CSDs, CBs
2014200	SP13.2 - Eurosystem ready for Production (wave 2)	11/09/2015	CSDs, CBs

Currency Participation Agreement

Schedule 2 – Annex 10 – T2S list of Milestones on the critical path

ID Number*	Milestone Description	Date**	Responsible for delivery
2014300	SP13.3 - Eurosystem ready for Production (wave 3)	04/03/2016	CSDs, CBs
2015100	SP14.1 - Ready to connect to Production Environment (wave 1)	05/02/2015	Eurosystem
2015200	SP14.2 - Ready to connect to Production Environment (wave 2)	02/10/2015	Eurosystem
2015300	SP14.3 - Ready to connect to Production Environment (wave 3)	22/03/2016	Eurosystem
2016100	SP15.1 - Ready to upload Static Data (wave 1)	19/03/2015	Eurosystem, CSDs, CBs
2016200	SP15.2 - Ready to upload Static Data (wave 2)	06/11/2015	Eurosystem, CSDs, CBs
2016300	SP15.3 - Ready to upload Static Data (wave 3)	22/04/2016	Eurosystem, CSDs, CBs
2017100	SP16.1 - Ready for Migration Weekend and Start Operations (wave 1)	19/06/2015	Eurosystem, CSDs, CBs
2017200	SP16.2 - Ready for Migration Weekend and Start Operations (wave 2)	29/01/2016	Eurosystem, CSDs, CBs
2017300	SP16.3 - Ready for Migration Weekend and Start Operations (wave 3)	15/07/2016	Eurosystem, CSDs, CBs
2017400	SP16.5 - Ready for Contingency Migration Weekend	27/01/2017	Eurosystem, CSDs, CBs

*Link with MS Project Plan

** The reference for the dates is the T2S Programme Plan

*** Milestones before the signature of FA, only for information

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 3 USER TESTING

Currency Participation Agreement

Schedule 3 – User Testing

Table of contents

1	Introduction	1
1.1	Context.....	1
1.2	Structure of Schedule.....	1
2	Scope and Objectives	2
2.1	Scope	2
2.2	Objectives	2
3	General Responsibilities of the Contracting Parties	3
3.1	General responsibilities of the Eurosystem.....	3
3.2	General responsibilities of the Connected NCB.....	4
3.3	General responsibilities of the PMG Substructure	5
3.4	General responsibility related to Monitoring Client Readiness.....	6
4	User Testing Preparation Phase	7
5	User Testing Execution Phase.....	9
5.1	Testing Stage Organisation	9
5.2	Connectivity Testing Stage	10
5.2.1	Description	10
5.2.2	Responsibilities.....	10
5.2.3	Entry Criteria.....	11
5.2.4	Exit Criteria	11
5.3	NCBs' Acceptance Testing Stage.....	11
5.3.1	Description	11
5.3.2	Responsibilities.....	12
5.3.3	Entry Criteria.....	13
5.3.4	Exit Criteria	13
5.4	Bilateral Interoperability Testing Stage	13
5.4.1	Description	13
5.4.2	Responsibilities.....	14
5.4.3	Entry Criteria.....	14
5.4.4	Exit Criteria	15
5.4.5	NCB Certification.....	16
5.4.5.1	Description.....	16

Currency Participation Agreement

Schedule 3 – User Testing

5.4.5.2 Responsibilities	17
5.4.5.3 Entry Criteria.....	18
5.4.5.4 Exit Criteria.....	18
5.5 Multilateral Interoperability Testing Stage	18
5.5.1 Description	18
5.5.2 Responsibilities.....	18
5.5.3 Entry Criteria	19
5.5.4 Exit Criteria	19
5.6 Community Testing Stage.....	20
5.6.1 Description	20
5.6.2 Responsibilities.....	20
5.6.3 Entry Criteria	20
5.6.4 Exit Criteria	21
5.6.5 DCA Holder Certification	22
5.6.5.1 Description.....	22
5.6.5.2 Responsibilities	23
5.6.5.3 Entry Criteria.....	23
5.6.5.4 Exit Criteria.....	24
5.7 Business Day Testing Stage	24
5.7.1 Description	24
5.7.2 Responsibilities.....	24
5.7.3 Entry criteria.....	25
5.7.4 Exit criteria	25
6 Non-functional tests	27
6.1 Description	27
6.2 Objectives and responsibilities of performance and stress tests.....	27
6.3 Objectives and responsibilities of Business Continuity tests	28
6.4 Objectives and responsibilities of Security Tests	28
6.5 Performance Tests by NCBs	29
7 User Testing Business processes	30
7.1 User Testing Stage Transition Monitoring Process	31
7.1.1 Process Actors and their Roles	32
7.1.2 Process Description.....	33
7.2 User Testing Stage Transition Assessment Process	34
7.2.1 Process Actors and their Roles	35
7.2.2 Process Description.....	36

Currency Participation Agreement

Schedule 3 – User Testing

7.3	User Testing Stage Transition Bilateral Escalation Process	37
7.3.1	Process Actors and their Roles	38
7.3.2	Process Description.....	38
7.4	User Testing Suspension Process	39
7.4.1	Process Actors and their Roles	40
7.4.2	Process Description.....	40
7.5	Release management during the User Testing	41
7.6	Supporting processes	42
7.6.1	IT Service Management processes	42
8	Post-migration testing.....	43
Annex 1 – Mapping of testing activities on the test environments		1

Currency Participation Agreement

Schedule 3 – User Testing

1 Introduction

1.1 Context

A prerequisite for a secure and smooth transfer of settlement activities from the CSDs' proprietary IT environments to T2S is the thorough testing of T2S in combination with the IT systems of the T2S Actors. According to the T2S Principle 10, "T2S shall be technically capable of settling currencies other than the euro", so non-euro area NCBs may wish to participate in T2S by making their domestic currency available in T2S for central bank money settlement of securities transactions. In which case, the non-euro area NCBs will need to test T2S with their domestic currency to ensure that the liquidity management functions correspond to the requirements of the non-euro area NCBs.

In this context, the Connected National Central Bank (NCB) and the Eurosystem shall cooperate in good faith for the preparation and execution of all relevant User Testing activities according to the T2S Programme Plan and its milestones.

1.2 Structure of Schedule

The Schedule 3 consists of the following sections and Annexes.

Section 1 is the introduction.

Section 2 defines the scope and the objective of User Testing.

Section 3 presents the general responsibilities of the Eurosystem, the NCBs and the PMG substructure for User Testing.

Section 4 describes the objectives of the User Testing preparation phase and the responsibilities of the Eurosystem and the NCBs during this phase.

Section 5 describes the structure of the testing stages for the User Testing Execution Phase with the respective entry and exit criteria for each testing stage as well as the conditions for transitioning between testing stages.

Section 6 presents the description, objectives and responsibilities for the non-functional testing.

Section 7 presents the business processes required to support the successful completion of User Testing including the stage transition process.

Section 8 presents the post-migration testing.

Annex 1 describes the mapping of the testing activities on the test environments.

Currency Participation Agreement

Schedule 3 – User Testing

2 Scope and Objectives

2.1 Scope

The scope of User Testing comprises functional testing and non-functional testing that the Connected NCB and its Dedicated Cash Account (DCA) Holders perform in view of assessing:

- the ability to connect to T2S (connectivity testing);
- the compliance of T2S with the relevant T2S Services as defined in Schedule 5 (Service Description) and the T2S Scope Defining Set of Documents (NCB Acceptance Tests of the T2S Services);
- the ability to interact properly with T2S (bilateral and multilateral interoperability testing as well as community and business day testing) without negative impact on the T2S Platform or other connected parties (NCB certification and DCA Holder certification);
- the ability to migrate static and, to the extent required, transactional data from its legacy systems onto T2S (Migration testing, mainly assessed during bilateral interoperability testing and community testing);
- the ability to extract Static Data and Transactional Data from T2S for reverse migration; and
- the readiness of operational procedures for live operations.

Although the functional and non-functional tests that the Eurosystem performs do not fall into the scope of User Testing, evidence provided through these tests may be used on a discretionary basis by NCBs as a means to limit their efforts during User Testing.

2.2 Objectives

The objectives of the User Testing are:

- to provide evidence that the T2S Platform meets the user requirements, as defined by the most recently approved version of the most detailed document of the T2S Scope Defining Set of Documents and Schedule 5 (T2S Service Description);
- to ensure readiness of the Connected NCB and its DCA Holders as well as its CSD for the migration to and operation on the T2S Platform;
- to allow the Connected NCB to verify and ensure its compliance with Legal and

Currency Participation Agreement

Schedule 3 – User Testing

59 Regulatory Requirements during the Operational Phase of T2S.

60 **3 General Responsibilities of the Contracting Parties**

61 This section defines the respective responsibilities of the Eurosystem, the Connected NCB,
62 whose currency is available for settlement in T2S, and the PMG substructure for the preparation
63 and execution of all User Testing activities. This Schedule does not define the roles and
64 responsibilities of the CSDs, nor of the DCA Holders, but defines the responsibility both of the
65 Eurosystem to ensure that these T2S Stakeholders fulfil their obligations and of the Connected
66 NCB towards its DCA Holders.

67 **3.1 General responsibilities of the Eurosystem**

68 The following specifies the general responsibilities of the Eurosystem with regard to the
69 preparation and execution and completion of the User Testing activities:

- 70 i. The Eurosystem is responsible for coordinating the User Testing activities and
71 communication between the Connected NCB, whose currency is available for
72 settlement in T2S, and its domestic CSD as well as between the Connected NCB and
73 other CSDs participating in the User Testing activities;
- 74 ii. The Eurosystem shall ensure that the User Testing of the NCBs does not place
75 restrictions on the CSDs' testing and that the User Testing of the CSDs does not place
76 restrictions on the NCBs' testing;
- 77 iii. The Eurosystem shall actively take all necessary actions required to facilitate, monitor
78 and support the adequate participation of the Participating CSDs in the testing activities
79 of the Connected NCB, whose currency is available for settlement in T2S, as well as for
80 the adequate participation of the Connected NCB in the testing activities of the
81 Participating CSDs;
- 82 iv. The Eurosystem is responsible for preparing and executing the Eurosystem Acceptance
83 Testing (EAT), and for providing regular progress reporting as well as an assessment
84 report confirming the compliance of T2S with the T2S Scope Defining Set of
85 Documents and Schedule 5 (Service DescriptionT2S Service Description); before the
86 start of User Testing.
- 87 v. The Eurosystem shall provide the reasonable support for testing activities of the
88 Connected NCB in the different stages of User Testing;

Currency Participation Agreement

Schedule 3 – User Testing

- 89 vi. The Eurosystem shall inform the Connected NCB, in a timely manner, about any
90 developments, which may prevent that NCB or its DCA Holder(s) from completing
91 its/their testing activities; and shall propose identified mitigation measures;
- 92 vii. The Eurosystem shall ensure that a PMG substructure is in place, in accordance with
93 the T2S governance framework (section 2.4 of Schedule 8 - Governance), for the
94 planning, coordination and monitoring of the User Testing activities;
- 95 viii. The Eurosystem shall reconcile and consolidate the individual status reports of NCBs
96 and CSDs on the progress of their User Testing activities and shall provide a regular
97 status update based on this consolidation to the Connected NCB through the PMG
98 substructure;
- 99 ix. The Eurosystem shall investigate and reconcile different test outcomes by different
100 NCBs or DCA Holders for delivering a consolidated list of defects to the PMG
101 substructure;
- 102 x. The Eurosystem shall undertake the configuration of test environments for the different
103 testing stages as agreed with the PMG substructure. The Eurosystem will provide the
104 necessary data configurations to ensure the logical segregation of data for the test
105 activities of NCBs;
- 106 xi. The Eurosystem is responsible for maintaining configuration parameters and the User
107 Testing Calendar (settlement day calendar, operating hours, cut-off times, etc.) for each
108 test environment as agreed with the PMG substructure for User Testing;
- 109 xii. Based on the principles of ITIL V3 Service Operation, the Eurosystem shall establish
110 and operate the necessary IT service management processes that include a defect
111 resolution process to remedy errors;
- 112 xiii. The Eurosystem shall operate T2S in accordance with the SLAs for User Testing as
113 defined in Schedule 6 (T2S Service Level Agreement).

3.2 General responsibilities of the Connected NCB

The following specifies the general responsibilities of the Connected NCB for the preparation and execution of the User Testing activities:

- i. The Connected NCB is responsible for the communication with its DCA Holders regarding User Testing;

Currency Participation Agreement

Schedule 3 – User Testing

- 119 ii. The Connected NCB is responsible for ensuring the timely completion of all its testing
120 activities and shall report its findings on the execution of its test cases and test scenarios
121 to the Eurosystem on a regular basis;
- 122 iii. The Connected NCB is responsible for supporting and monitoring the timely
123 completion of the testing activities of its DCA Holders;
- 124 iv. The Connected NCB appoints a single point of contact for all topics related to the User
125 Testing representing the Connected NCB in the PMG substructure;
- 126 v. The Connected NCB, independent of its migration wave and even after having
127 completed its own testing, shall support CSDs in their testing of T2S;
- 128 vi. The Connected NCB shall inform the Eurosystem, in a timely manner, about any
129 developments, which may prevent that NCB or its DCA Holder(s) from completing
130 its/their testing activities;
- 131 vii. The Connected NCB shall provide reasonable support to the Eurosystem by providing
132 information on test outcomes;
- 133 viii. The Connected NCB shall participate in the PMG substructure in charge of User
134 Testing as required to ensure the proper functioning of this body and the smooth
135 coordination of the User Testing activities.

136 **3.3 General responsibilities of the PMG Substructure**

137 The PMG substructure shall be composed of the participating CSDs, euro area NCBs,
138 participating non-euro area NCBs, the 4CB and the ECB. The following specifies the general
139 responsibilities of the PMG substructure in the preparation and execution of the User Testing
140 activities for the initial T2S go-live and new software release after T2S go-live of the final
141 migration wave that the substructure shall be responsible for:

- 142 i. Meet (physically or via conference call) on a regular basis and on an ad hoc basis when
143 requested by one of the members to prepare, plan, coordinate, monitor and review User
144 Testing activities. The PMG substructure determines the frequency of its meetings
145 based on its needs;
- 146 ii. Prepare, update and agree the User Testing Calendar in accordance with the TS
147 Programme Plan;
- 148 iii. Decide on changes to the opening / closing times of the testing environments and
149 operational hours in line with the provisions of the SLA;

Currency Participation Agreement

Schedule 3 – User Testing

- iv. Review the consolidated User Testing status reports from the Eurosystem on the overall progress of NCBs, CSDs and their respective communities on User Testing;
- v. Review the list of incidents;
- vi. Review the software defects, classify the software defects and agree on the contents of a package for a T2S release on the User Testing environments.
- vii. In the case that the PMG substructure cannot reach an agreement, it may escalate to the PMG;
- viii. Prepare communication on the progress of User Testing via the PMG to the Steering Level;
- ix. Coordinate and monitor the participation of the various T2S Actors (Eurosystem, NCBs, CSDs, DCPs and DCA Holders) during the different stages of testing. At its own discretion, the NCB may coordinate testing activities directly with other T2S Actors when it does not conflict with the agreed approach of the PMG substructure;
- x. Identify, manage, report and escalate risks and issues related to User Testing according to the ‘Programme Plan Preparation, Adaptation and Assessment Review Process’ in section 7.2 of Schedule 2 (T2S Programme Planning and Monitoring);
- xi. Request plan changes related to User Testing according to the ‘Programme Plan Preparation, Adaptation and Assessment Review Process’ in section 7.2 of Schedule 2 (T2S Programme Planning and Monitoring);
- xii. Request adaptations of User Testing items documented in Annexes 4 to 10 of Schedule 2, according to the ‘Adaptation Process for Updated Annexes without affecting the plan’ in section 7.3 of Schedule 2 (T2S Programme Planning and Monitoring);
- xiii. Take or request decisions on User Testing related topic according to the decision-making process defined section 1.3 of in Schedule 8 (Governance).

3.4 General responsibility related to Monitoring Client Readiness

The monitoring and reporting of the progress of an individual NCB with its client relationship manager during User Testing will follow the framework for Monitoring Client Readiness (MCR) as defined in Schedule 2 (T2S Programme Planning and Monitoring).

Currency Participation Agreement

Schedule 3 – User Testing

4 User Testing Preparation Phase

The objective of the User Testing preparation phase is to:

- organise processes and activities required for the User Testing Execution Phase, as defined in Section 7 of this Schedule;
- undertake an initial risk assessment for the User Testing Execution Phase as specified by the Schedule 2 risk management framework to ensure the subsequent proactive risk management by the PMG substructure;
- prepare and design all necessary test documentation and testing processes, e.g. User Testing Calendar, Test Plan, test cases for certification, test data.

In this preparation phase for User Testing, the Eurosystem with the support of the Connected NCB through its participation in the PMG substructure for User Testing establishes the required process framework and prepares the agreed deliverables for the User Testing Execution Phase.

The responsibilities of **the Eurosystem** in this phase are:

- i. to establish the processes required for the User Testing Execution Phase as defined in Section 7 of this Schedule;
- ii. to develop a training programme for T2S and deliver a reasonable amount of training to the Connected NCB;
- iii. to provide the Connected NCB with a Test Plan and User Testing Calendar for the Connected NCB to plan its own activities for the User Testing and to inform the Connected NCB, in a timely manner, about any changes made to this plan;
- iv. to prepare and provide the prerequisite deliverables for the Connected NCB to prepare its User Testing, e.g. the User Testing Guide, the Registration Guide, the Connectivity Guide, and the Manual of Operational Procedures;
- v. to provide to the Connected NCB the sets of Eurosystem Acceptance Testing (EAT) functional test cases and test scenarios for information purposes, as an input for the Connected NCB's test preparation.

In this preparation phase for User Testing, the responsibilities of **the Connected NCB** are:

- i. to support the Eurosystem in the preparation of the overall Testing Calendar by

Currency Participation Agreement

Schedule 3 – User Testing

207 providing the Eurosystem with its proposed Test Plan and User Testing Calendar of its
208 activities.

209 ii. to comply with the processes for User Testing, as defined in Section 7 of this Schedule.

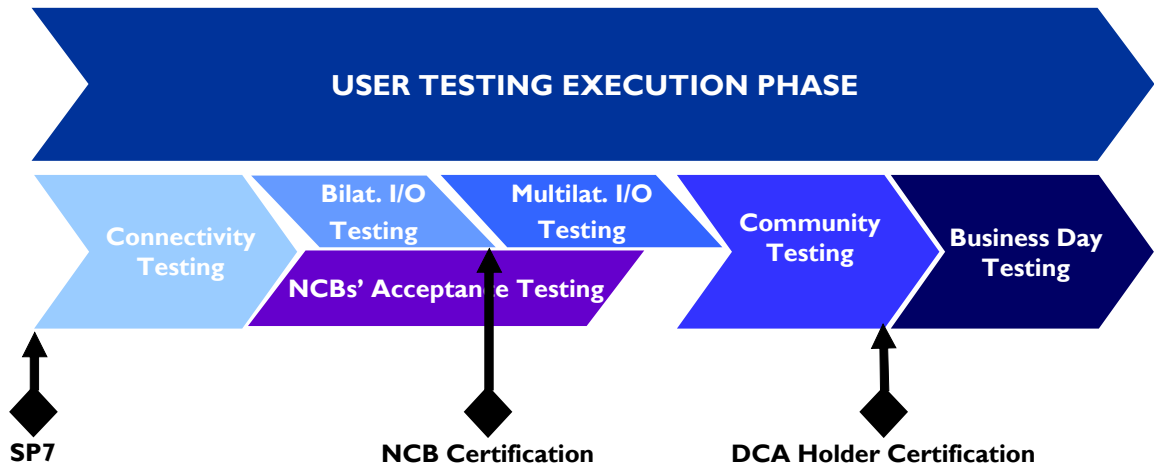
210

5 User Testing Execution Phase

This section describes the structure of the testing stages for User Testing Execution Phase with the respective entry and exit criteria for each testing stage as well as the conditions for transitioning between testing stages.

5.1 Testing Stage Organisation

The User Testing Execution Phase consists of both independent and sequenced testing stages. The purpose of the different testing stages is to increase gradually the number of T2S Actors involved and expand the scope of the testing.



Currency Participation Agreement

Schedule 3 – User Testing

5.2 Connectivity Testing Stage

5.2.1 Description

Establishing the technical connectivity to a test environment is the first stage of User Testing. This is required for each environment that the Connected NCB uses for testing, however the connectivity testing stage is the initial verification that the systems of both the Connected NCB and the Eurosystem can communicate successfully on the technical and application level. The Connected NCB shall repeat these tests for each connectivity channel it intends to use while the connection to further T2S test environments might have a reduced connectivity test scope.

Directly connected DCA Holders will need to perform connectivity testing before they can start DCA Holder Certification Testing. Such connectivity testing has to take place before the start of community testing in compliance with the planning outlined in CPA Schedule 2.

The scope of connectivity testing consists of

- testing the ability to reach the welcome pages of the U2A interface and performing the login to the system;
- exchange of messages on application level (not relevant for directly connected DCA Holders with U2A connection);
- push-and-pull services for reports (not relevant for directly connected DCA Holders with U2A connection).

When the Connected NCB has opted for the Dedicated Link Connection, the testing shall also cover the testing of the technical communication protocol (DEP).

5.2.2 Responsibilities

The following set of responsibilities shall apply for the connectivity testing stage:

- i. The Eurosystem shall support the connectivity testing of the Connected NCB and the DCA Holders.
- ii. The Connected NCB shall acquire T2S specific network connectivity services and ensure the timely readiness of its connection to the relevant T2S environment(s).
- iii. The Connected NCB together with the Eurosystem will evaluate the test results at the end of the connectivity testing stage to assess the fulfilment of the exit criteria for this testing stage.

Currency Participation Agreement

Schedule 3 – User Testing

5.2.3 Entry Criteria

The following conditions shall apply for the start of the connectivity testing stage:

- The Eurosystem has confirmed the successful achievement of synchronisation point 4 – Network Providers Confirmed.
- The Eurosystem has confirmed the successful achievement of synchronisation point 7 – Start Connectivity Testing.
- The Connected NCB has completed the preparation to setup the network connection for the user test environments, according to the T2S Connectivity Guide.
- The Connected NCB has confirmed the adaptation of its IT system according to the T2S specifications and documentation.

5.2.4 Exit Criteria

The following conditions shall apply for the successful conclusion of the connectivity testing stage:

- The Connected NCB confirms to the Eurosystem that its IT platform can successfully exchange message-based communication and receive pushed messages on application level with T2S.

The Connected NCB confirms the correct setup of communication parameters and security features with its Network Service Provider(s) in order to communicate with the T2S test environment(s).

5.3 NCBs' Acceptance Testing Stage

5.3.1 Description

The NCBs' acceptance testing stage is of up to 6 months within the User Testing Execution Phase reserved for NCBs to confirm that based on its testing the relevant T2S Services comply with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents, i.e. services related to cash accounts, liquidity management and auto-collateralisation. Independently from its migration wave, the Connected NCB may start its acceptance testing when the Eurosystem confirms its successful achievement of synchronisation point 8 – Start Bilateral Interoperability Testing.

Currency Participation Agreement

Schedule 3 – User Testing

The NCBs' Acceptance Tests of the T2S Services¹ are bilateral between the Eurosystem and the Connected NCB. The acceptance of one NCB does not prejudice the agreement by other NCBs. Executing this testing stage is optional. The Connected NCB may rely on its test results from its bilateral and multilateral interoperability testing as well as those from its NCB certification testing. Article 13 of the core Agreement defines NCBs' Acceptance Tests further.

In order for the Connected NCB to obtain evidence that T2S fulfils the non-functional user requirements, the Eurosystem will prepare and execute non-functional tests based on test cases that will be shared with the Connected NCB for a consultation, within a specified time frame, before the start of non-functional testing by the Eurosystem. The Eurosystem will deliver a test report with the results of the test execution according to the defined scope of the non-functional tests.

5.3.2 Responsibilities

The following set of responsibilities shall apply for the NCBs' acceptance testing stage:

- i. In the context of the framework set out in Schedule 2 (T2S Programme Planning and Monitoring) on the monitoring of client readiness, the Eurosystem and the Connected NCB shall have regular contact to review the progress of the NCBs' acceptance testing stage;
- ii. The Connected NCB has the obligation to provide regular reporting on the results of its tests in the form of status reports to the Eurosystem. The report shall cover at minimum the number of test cases and test scenarios successfully executed and failed (cases of non-compliance) with the Connected NCB's assessment of the criticality of identified defects and corresponding measures to compensate for potential delays, when required;
- iii. The Connected NCB has the obligation to provide evidence, if it intends not to accept T2S because of failed test cases, that the respective test cases comply with the T2S Scope Defining Set of Documents and Schedule 5 (T2S Service Description).

¹ The term "NCBs' Acceptance Tests of the T2S Services" does not indicate that the T2S Services imply any element of a contract for work under German law. Chapter 2 of this Agreement defines the rights and obligations of the Parties that describe the T2S Services

Currency Participation Agreement

Schedule 3 – User Testing

- iv. Based on the bilateral status reporting from the Connected NCB, the Eurosystem shall monitor the testing. The Eurosystem shall share information about the progress and results of the NCBs' Acceptance Tests of the T2S Services with the NCBs via the PMG substructure on a consolidated basis.
- v. The Connected NCB together with the Eurosystem will evaluate the test results at the end of the NCBs' acceptance testing stage to assess the fulfilment of the exit criteria for this testing stage.

5.3.3 Entry Criteria

The following condition shall apply for the start of the NCBs' acceptance testing stage:

- The Eurosystem has confirmed the successful achievement of synchronisation point 8 – Start Bilateral Interoperability Testing.

5.3.4 Exit Criteria

The following conditions shall apply for the end of the NCBs' acceptance testing stage:

- The criterion for an NCB to exit the NCBs' acceptance testing stage shall be its declaration that evidence from testing (whereby the Connected NCB may rely on its test results from its bilateral and multilateral interoperability testing as well as those from its NCB certification testing) suggests that the relevant T2S services comply with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents.

5.4 Bilateral Interoperability Testing Stage

5.4.1 Description

In the bilateral interoperability testing stage, the Connected NCB tests T2S to ensure the readiness of its adapted IT System to interoperate with T2S and verifies that all relevant T2S Services (e.g. liquidity management, migration procedures) in T2S are working as required. It undertakes its testing without interacting with Participating CSDs. T2S ensures the segregation of the testing activities of the Connected NCB from CSDs' test activities on T2S by creating a set of fictitious CSDs with which the Connected NCB can interoperate. The objective of this testing stage is to ensure that the NCBs' adapted IT System can interoperate with T2S properly before testing with other T2S Actors. An NCB can continue performing bilateral testing even when it undertakes multilateral testing.

Currency Participation Agreement

Schedule 3 – User Testing

5.4.2 Responsibilities

The following set of responsibilities shall apply for the bilateral interoperability testing stage:

- i. The Eurosystem shall establish the operational procedures and service management required to support the bilateral interoperability testing stage;
- ii. The Connected NCB is responsible for organising its bilateral interoperability testing stage in line with the Test Plan and User Testing Calendar;
- iii. The PMG substructure shall be responsible for monitoring the bilateral interoperability testing stage;
- iv. The Connected NCB shall test the migration processes (loading Static Data, loading Transactional Data, migration weekend rehearsals, reverse migration, etc.);
- v. The Connected NCB together with the Eurosystem will evaluate the test results at the end of the bilateral interoperability testing stage to assess the fulfilment of the exit criteria for this testing stage.

5.4.3 Entry Criteria

The following conditions shall apply for the start of the bilateral interoperability testing stage:

- The Connected NCB has completed the connectivity testing stage successfully;
- The Eurosystem has provided the EAT Assessment Report four weeks before synchronisation point 8 – Start Bilateral Interoperability Testing, covering the full scope of Eurosystem Acceptance Testing and confirming that the Eurosystem considers T2S being ready for start of User Testing;
- The Eurosystem has resolved all reported defects classified with critical severity, identified during EAT. Except otherwise agreed between the Parties, the Eurosystem has resolved all recorded defects classified with high severity;
- For the pending errors from the EAT, the Eurosystem has provided a timetable for implementation of software corrections and for regression testing of those corrections for those test cases that failed because of defects in T2S that are not critical;
- The Eurosystem has confirmed the successful achievement of synchronisation point 8 – Start Bilateral Interoperability Testing for the specific migration wave;
- The Eurosystem has delivered to the Connected NCB preliminary evidence that the

Currency Participation Agreement

Schedule 3 – User Testing

364 future T2S production environment will meet the non-functional requirements based on
365 the results of the T2S non-functional tests. The Eurosystem executes these tests in the
366 future T2S production environment;

- 367 ▪ The Eurosystem has confirmed its operational readiness to support the Connected NCB;
- 368 ▪ The Connected NCB has confirmed its readiness to start User Testing;
- 369 ▪ The Eurosystem and the Connected NCB have confirmed completion of the training
370 required to ensure the smooth start of testing activities;
- 371 ▪ The Eurosystem has provided the documentation required for migration testing and
372 migration dress rehearsals.

373 **5.4.4 Exit Criteria**

374 The following condition shall apply for the end of the bilateral interoperability testing stage:

- 375 ▪ The Eurosystem has certified the Connected NCB according to the requirements in
376 Section 5.4.5 of this Schedule.

Currency Participation Agreement

Schedule 3 – User Testing

5.4.5 NCB Certification

5.4.5.1 Description

The NCB certification, conducted during the User Testing Execution Phase, aims at providing evidence by the Connected NCB that its adapted IT platform does not harm T2S as the result of inappropriate technical communication or procedures. It runs in parallel to the bilateral interoperability testing stage. The Connected NCB's participation in the NCB certification testing is mandatory. Certification shall require the Connected NCB to execute a mandatory set of reasonable tests, agreed through the PMG substructure during the User Testing preparation phase². The Eurosystem will exempt the Connected NCB from performing mandatory test cases that are not in the scope of the Connected NCB's intended usage of T2S. The Connected NCB may rely on its test results from its bilateral testing to document its completion of a mandatory certification test case.

NCB certification is bilateral between the Eurosystem and the Connected NCB. The Eurosystem shall provide written confirmation to the Connected NCB after determining whether the Connected NCB has successfully completed its assigned set of mandatory certification test cases, based on a formal report from the Connected NCB in which the Connected NCB shall document its fulfilment of the predefined NCB certification testing exit criteria.

The Eurosystem shall retain as evidence for proper certification the Connected NCB's formal report as well as the Connected NCB's progress reports on its certification testing and reporting on the level of the test cases and test scenarios.

The certification of the Connected NCB shall remain valid until:

- the Eurosystem deploys a major release with a significant scope change in the A2A interface or major structural changes to the processing model and/or data model; or
- the Connected NCB has made major changes to its interface processing for T2S.

² Only for NCB certification there will be mandatory test cases.

Currency Participation Agreement

Schedule 3 – User Testing

In the first case, the Eurosystem shall recommend to the Steering Level whether the new release requires a re-certification of the NCBs and CSDs, based on the scope of the changes that the Change Review Group (CRG) has approved for the new T2S release. In the latter case, the Connected NCB shall assess the scope of the changes and shall decide whether it must undertake a re-certification.

5.4.5.2 Responsibilities

The following set of responsibilities shall apply for the NCB certification testing:

- i. The Eurosystem shall deliver for review to the Connected NCB through the PMG substructure the test scenarios and test cases that the Connected NCB has to execute successfully to achieve its certification;
- ii. The Eurosystem shall consult the PMG substructure on the test cases and test scenarios for NCB certification to ensure and agree the proper scope coverage;
- iii. In the context of the framework set out in Schedule 2 on the monitoring of client readiness, the Eurosystem and the Connected NCB shall have regular contact to review the progress of the NCB's certification testing;
- iv. The Connected NCB shall execute the mandatory test cases and test scenarios for certification within the period foreseen in the T2S Programme Plan for the migration wave in which it is participating;
- v. The Connected NCB has the obligation to provide regular reporting on the results of its certification tests in the form of status reports to the Eurosystem, documenting its progress with, at minimum, the number of test cases and test scenarios successfully executed and failed;
- vi. Based on the bilateral status reporting from the Connected NCB, the Eurosystem shall monitor the certification testing. The Eurosystem shall share information about the progress of and results of the NCB Certification with the NCBs via the PMG substructure on a consolidation basis;
- vii. Based on a formal report from the Connected NCB, the Eurosystem will evaluate the results of the NCB's certification testing to assess whether the Connected NCB executed the certification tests completely and successfully, and such assessment shall not be unreasonably withheld;

Currency Participation Agreement

Schedule 3 – User Testing

- viii. The Eurosystem will issue the NCB Certificate for the Connected NCB when the Eurosystem assesses that the Connected NCB has executed the certification test cases completely and successfully.

5.4.5.3 Entry Criteria

The following conditions shall apply for the start of the NCB certification:

- The Connected NCB has completed the connectivity testing stage successfully;
- As specified in the T2S Programme Plan, the Eurosystem has delivered to the Connected NCB its test scenarios and test cases that the Connected NCB is to execute for its certification;
- The PMG substructure has assessed the test cases and test scenarios for NCB Certification to ensure proper scope coverage.

5.4.5.4 Exit Criteria

The following conditions shall apply for the successful conclusion of the NCB certification:

- The Connected NCB has provided evidence of its successful completion of the mandatory certification test cases and test scenarios;
- The Eurosystem has confirmed in writing to the Connected NCB that the Connected NCB has successfully completed all tests required for certification.

5.5 Multilateral Interoperability Testing Stage

5.5.1 Description

In the multilateral interoperability testing stage, the Connected NCB tests with other Participating CSDs and Central Banks of its migration wave and of previous migration waves. In this stage, the Connected NCB also begins the set-up and testing of configuration data and parameters for the intended production set-up (e.g. message subscriptions, liquidity transfers).

5.5.2 Responsibilities

The following set of responsibilities shall apply for the multilateral interoperability testing stage:

- i. The PMG substructure shall be responsible for the planning and coordination of the multilateral interoperability testing stage;

Currency Participation Agreement

Schedule 3 – User Testing

458 ii. The Connected NCB shall support Participating CSDs of its own migration wave and of
459 subsequent migration waves when it supports cash accounts of customers of those
460 Participating CSDs;

461 iii. The PMG substructure will evaluate the test results at the end of the multilateral
462 interoperability testing stage to assess the fulfilment of the exit criteria for this testing
463 stage.

464 **5.5.3 Entry Criteria**

465 The following conditions shall apply for the start of the multilateral interoperability testing stage:

- 466 ▪ The Connected NCB has obtained its certification in order to start multilateral
467 interoperability testing;
- 468 ▪ The PMG substructure has assessed the User Testing Stage Report detailing the severity
469 of all defects reported during the multilateral interoperability testing stage and not yet
470 resolved.

471 **5.5.4 Exit Criteria**

472 The following conditions shall apply for the end of the multilateral interoperability testing stage:

- 473 ▪ The PMG substructure determines that the Connected NCBs of a migration wave have
474 successfully completed multilateral interoperability testing;
- 475 ▪ No critical software bugs or operational issues remain open. The Eurosystem has
476 resolved all reported defects classified with critical severity. Except the Parties agree
477 otherwise, the Eurosystem has resolved all recorded defects, classified with high severity;
- 478 ▪ The PMG substructure has agreed a timetable for implementation of software corrections
479 and for regression testing of those corrections for those test cases that failed because of
480 non-critical defects in T2S.

Currency Participation Agreement

Schedule 3 – User Testing

5.6 Community Testing Stage

5.6.1 Description

The community testing stage is the stage in which the Connected NCB of a migration wave extends its multilateral testing activities with other relevant T2S Actors to its DCA Holders. The main objective of this stage is to validate that the Connected NCB's DCA Holders can interact correctly end-to-end with T2S, either through the Connected NCB's adapted systems or with T2S directly as a directly connected DCA Holder.

During the testing stage NCBs and their DCA Holders verify the correct functioning of T2S using the target data configuration as configured for the target production environment. The expectation is that processing errors will stem mainly from incorrect data configurations, allowing the Participating NCB to identify and correct such incorrect configurations and from DCA Holders' testing of their interface to T2S. This stage represents the first opportunity of the Connected NCB's DCA Holders to test with T2S, allowing the NCB's DCA Holders to verify that their system interoperate correctly with T2S.

The community testing stage allows the Connected NCB and its DCA Holders to familiarise themselves with operational procedures and service management relevant to this stage to ensure that the operational procedures as described in the Manual of Operational Procedures (MOP).

5.6.2 Responsibilities

The following set of responsibilities shall apply for the community testing stage:

- i. The Connected NCB shall test the migration process (loading Static Data, loading Transactional Data, migration weekend rehearsals, reverse migration, etc.) together with its DCA Holders;
- ii. The Connected NCB shall involve its DCA Holders and other relevant T2S Stakeholders in the testing activities in order to validate the end-to-end business processes supported by T2S;
- iii. The Connected NCB together with the Eurosystem will evaluate the test results at the end of the community testing stage to assess the fulfilment of the exit criteria for this testing stage.

5.6.3 Entry Criteria

The following conditions shall apply for the start of the community testing stage:

Currency Participation Agreement

Schedule 3 – User Testing

- 511 ▪ The Connected NCB has exited the NCBs' acceptance testing and the multilateral
512 interoperability testing stage successfully and declared its operational readiness for
513 community testing;
- 514 ▪ The Eurosystem has confirmed the readiness of its operational teams;
- 515 ▪ The Eurosystem has confirmed the readiness of the Participating CSD(s) of the
516 Connected NCB and of the CSD participants in the tests;
- 517 ▪ The PMG substructure confirms the successful completion of multilateral interoperability
518 testing stage and that the community testing stage can start.

519 **5.6.4 Exit Criteria**

520 The following conditions shall apply for the successful conclusion of the community testing
521 stage:

- 522 ▪ The PMG substructure determines that the Connected NCB, together with its DCA
523 Holders and the relevant CSD(s) have successfully executed the migration rehearsals and
524 business days;
- 525 ▪ No critical software bugs or operational issues remain open that constitute a significant
526 risk to the go-live of the migration wave. The Eurosystem has resolved all reported
527 defects classified with critical severity. Except where otherwise agreed between the
528 Parties, the Eurosystem has resolved all recorded defects classified with high severity
529 except when otherwise agreed between the Parties;
- 530 ▪ The PMG substructure has agreed a timetable for implementation of software corrections
531 and for regression testing of those corrections for those test cases that failed because of
532 defects in T2S that are not critical;
- 533 ▪ The DCA Holder(s) of the Connected NCB has/have successfully completed all tests
534 related to its/their DCA Holder certification which make it/them eligible to participate in
535 the next stage;
- 536 ▪ The relevant operational and the incident management procedures of the Connected NCB
537 and its DCA Holders have been carried out successfully;
- 538 ▪ The NCBs and CSD(s) (of the NCBs) of the respective migration wave confirm their
539 readiness to progress to the business day testing stage.

Currency Participation Agreement

Schedule 3 – User Testing

5.6.5 DCA Holder Certification

5.6.5.1 Description

The DCA Holder Certification aims at providing evidence by those DCA Holders which the Connected NCB has authorised to connected to T2S with an A2A connection and by those DCA Holders which the Connected NCB has authorised to connect to T2S with a U2A connection that its adapted IT platform does not harm T2S as the result of inappropriate technical communication or procedures. DCA Holders could be given both U2A and A2A access. DCA Holder Certification does not verify the compliance with either the Connected NCB's adaptation to T2S nor with the Connected NCB's business processing requirements. Thus, user certification is necessary but not sufficient prerequisite for a DCA Holder to use an NCB's DCA in T2S. When conducted during the User Testing Execution Phase, it runs in parallel to the community testing stage for those participants of the Connected NCB that request to connect directly to T2S. Participants of the Connected NCB also have the option to undertake their DCA Holder Certification at anytime after the Connected NCB is operating on T2S. The DCA Holder certification of an NCB's DCA Holder shall be valid for all Connected NCBs from which it has authorisation to connect directly to T2S. DCA Holder certification requires connectivity testing before the DCA Holder starts its certification testing.

DCA Holder certification is mandatory for any DCA Holder of the Connected NCB that chooses to connect its IT systems directly to T2S. DCA Holder certification shall require the DCA Holder of the Connected NCB to execute a mandatory set of tests, agreed through the PMG substructure during the User Testing Preparation Phase. When the Connected NCB allows its participants to connect directly to T2S and the DCA Holder of the Connected NCB chooses to connect directly to T2S, the Connected NCB shall allow the Eurosystem to undertake the certification process directly with the DCA Holder of the Connected NCB.

A DCA Holder of the Connected NCB has to certify itself once with the Eurosystem to connect directly to T2S. When the Connected NCB allows its participants to connect directly to T2S, the Connected NCB has the obligation to accept the certification of its DCA Holder even when the DCA Holder of the Connected NCB has certified itself with the Eurosystem through another Connected NCB.

The DCA Holder certification of the Connected NCB's DCA Holder shall remain valid until the Eurosystem deploys a major release with a significant scope change in the A2A / U2A interface or major structural changes to the processing model and/or data model. The Eurosystem shall recommend to the Steering Level whether the new release requires a recertification of the DCA Holders, based on the scope of changes that the Change Review Group (CRG) has approved for the new T2S release.

Currency Participation Agreement

Schedule 3 – User Testing

5.6.5.2 Responsibilities

The following set of responsibilities shall apply for the DCA Holder certification testing:

- i. The Eurosystem shall deliver for review to the Connected NCB through the PMG substructure the test scenarios and test cases that a Connected NCB's DCA Holder has to execute successfully to achieve its DCA Holder certification;
- ii. The Eurosystem shall consult the PMG substructure on the test cases and test scenarios for DCA Holder certification to ensure and agree the proper scope coverage;
- iii. The Eurosystem shall undertake the DCA Holder certification process and shall monitor the DCA Holder certification testing. The NCB will during this process act as a connecting link between its DCA Holders and the Eurosystem. The Eurosystem shall share information about the progress and results of the DCA Holder certification with the NCBs via the PMG substructure on a consolidated basis. The Eurosystem shall upon request provide (NCB) with the results of such the DCA holder certification process for (NCB's) DCA Holders;
- iv. The Eurosystem shall provide written confirmation to Connected NCB and to its DCA Holder after determining whether the DCA Holder has successfully completed its assigned set of mandatory certification test cases;
- v. The Eurosystem shall retain as evidence for proper DCA Holder certification the documentation of the DCA Holder's certification testing and reporting on the level of the test cases and test scenarios;
- vi. In good time before the period foreseen in Schedule 2 for the migration wave in which it is participating, the (NCB) shall provide the Eurosystem with the necessary information about those DCA Holders which have been authorised to connect to T2S with an A2A connection and those which have been authorised to connect to T2S via a U2A connection.

5.6.5.3 Entry Criteria

The following conditions shall apply for the start of the DCA Holder certification:

- The Connected NCB has fulfilled the exit criteria for the NCBs' acceptance testing stage.
- The Connected NCB and the Eurosystem have fulfilled the exit criteria for the NCB certification testing;

Currency Participation Agreement

Schedule 3 – User Testing

- The Connected NCB has authorised its respective DCA Holder to connect directly to T2S.

5.6.5.4 Exit Criteria

DCA Holder certification has no exit criteria. However, DCA Holder certification is the prerequisite for the Connected NCB's DCA Holder to take part in community testing of the Connected NCB as a DCA Holder.

5.7 Business Day Testing Stage

5.7.1 Description

The business day testing stage comprises the simulation of several consecutive business days of T2S operation after completing a migration rehearsal for the respective migration wave using the expected production data set-up. It includes all NCBs and their DCA Holders as well as the CSDs of a migration wave and their respective communities. NCBs, CSDs and their communities from previous migration waves participate when deemed necessary, e.g. when links exist.

The objective of the business day testing stage is to verify the correct functioning of T2S under production-like conditions using the target data configuration as expected in the production environment. In this stage of testing, the expectation is that processing errors will stem mainly from incorrectly migrated data (e.g. incorrect positions or missing ISINs) or incorrect configuration (e.g. cross-CSD settlement parameters). This stage enables the T2S Actors, such as the CSDs and their communities, to identify such errors using real business data.

The business day testing stage includes operational procedures and service management to ensure that the operational procedures as described in the Manual of Operational Procedures (MOP) are working as expected.

5.7.2 Responsibilities

The following set of responsibilities shall apply for the business day testing stage:

- i. The Eurosystem shall establish the operational procedures and service management required to support the business day testing stage;
- ii. The Connected NCB shall test the migration process (loading Static Data, loading Transactional Data, migration weekend rehearsals, reverse migration, etc.) together with its DCA Holders;

Currency Participation Agreement

Schedule 3 – User Testing

iii. The Connected NCB shall involve its DCA Holders and other relevant T2S Stakeholders in the testing activities in order to validate the end-to-end business day processes supported by T2S;

iv. The Connected NCB together with the Eurosystem will evaluate the test results at the end of the business day testing stage to assess the fulfilment of the exit criteria for this testing stage.

5.7.3 Entry criteria

The following conditions shall apply for the start of the business day testing stage:

- The Connected NCB has fulfilled the exit criteria for the community testing stage;
- The PMG substructure confirms that the NCBs and their CSD(s) participating in the respective migration wave have fulfilled the exit criteria for community testing.

5.7.4 Exit criteria

The following conditions shall apply for the successful conclusion of the business day testing stage:

- The PMG substructure determines that the NCBs of a migration wave, together with their DCA Holders and the relevant CSDs have successfully executed the migration rehearsals and business days;
- No critical software bugs or operational issues remain open that constitute a significant risk to the go-live of the migration wave. The Eurosystem has resolved all reported defects classified with critical severity. Except otherwise agreed between the Parties, the Eurosystem has resolved all recorded defects classified with high severity;
- The PMG substructure has agreed a timetable for implementation of software corrections and for regression testing of those corrections for those test cases that failed because of non-critical defects in T2S;
- No client systems have become inoperable due to unexpected communication received from the T2S Platform for at least 15 working days prior to the agreed business day testing stage exit date;
- The Eurosystem confirms that testing of operational procedures has been successful;
- The PMG substructure confirms that appropriate fallback arrangements and rollback

Currency Participation Agreement

Schedule 3 – User Testing

- 663 procedures are established and successfully tested for the Migration;
- 664 ▪ The NCBs and CSDs (of the NCBs) of the respective migration wave confirm their
- 665 readiness to go-live on T2S.
- 666

Currency Participation Agreement

Schedule 3 – User Testing

6 Non-functional tests

This section describes the non-functional tests carried out by the Eurosystem in order to confirm non-functional compliance of T2S as well as the non-functional volume tests carried out by the NCBs.

6.1 Description

The non-functional tests aim to check the proper functioning of T2S and are composed of the following tests as defined in the General Technical Design document:

- performance and stress tests;
- business continuity tests;
- security tests.

In principal, the Eurosystem will perform the non-functional tests, involvement of NCBs varies depending on the different types of non-functional test. Prior to the execution, the Eurosystem will provide for a quick consultation these tests to the NCB. After the test execution, the Eurosystem will deliver a test report with results of those tests. Moreover, the Connected NCB will have the opportunity to execute non-functional tests from an end-to-end perspective and respecting the sizing of the related test environments (see also section 6.5 Performance Tests by NCBs).

6.2 Objectives and responsibilities of performance and stress tests

The main objective of the performance and stress tests is to check that the T2S production environment is able to handle the estimated volume of transactions in the peak hour in terms of the number of settlements and a certain number of concurrent interactive users in compliance with a defined response time.

The test plan for the performance and stress tests includes a global system test aimed to measure throughput, response time and resource consumption of the whole system (infrastructure and applications) and volume tests conducted on specific parts of the system in order to optimise the behaviour of these T2S components.

During the performance and stress tests, different test cases shall be performed aiming to simulate the expected daily workload profiles for User-to-Application mode (U2A) and Application-to-Application (A2A) interactions on the available interfaces by using simulators and/or with the collaboration of the Connected NCB.

The test plan for the performance and stress tests shall follow a gradual approach to verify, in

Currency Participation Agreement

Schedule 3 – User Testing

sequence, that all infrastructure components and services are properly sized to handle the defined peak workload of settlements and the T2S application is able to satisfy the defined performance requirements.

The performance and stress tests shall be performed by the Eurosystem. The T2S Actors shall be invited as observers to the performance and stress tests and the results of these tests shall be delivered to the Connected NCB.

6.3 Objectives and responsibilities of Business Continuity tests

The main objective of the business continuity tests is to verify the ability of T2S to guarantee the continuity of business services in case of local component failure or regional disaster event. The business continuity tests shall demonstrate that T2S is sufficiently resilient to meet the agreed service levels, even in case of severe incidents. The tests include intra-region and inter-region failover tests to guarantee that the production environment(s) can be switched to another side or region in a failover situation.

The business continuity tests shall be performed before the go-live and on a regular basis after the go-live.

The test plan for the business continuity tests shall include a comprehensive list of test cases including:

- fault tolerance (i.e. resiliency of single component);
- intra-region recovery;
- inter-region recovery (only regions 1 and 2).

In addition, tests shall be performed to validate the rotation between region 1 and region 2 that is closely linked to the disaster recovery test in terms of organisation and operational procedures.

The business continuity tests shall be performed by the Eurosystem. The T2S actors shall be invited as observers to the business continuity tests and the results of these tests shall be delivered to the Connected NCB.

6.4 Objectives and responsibilities of Security Tests

The main objectives of the security tests are to verify the compliance of the T2S platform with the T2S security requirements. Security tests include:

- Vulnerability assessment;
- Configuration analysis;
- Penetration tests.

Currency Participation Agreement

Schedule 3 – User Testing

729 The Eurosystem shall perform these security tests, which it shall provide to the Connected NCB.

730 **6.5 Performance Tests by NCBs**

731 Performance tests are typical non-functional tests that an NCB or DCA Holder may want to
732 perform. Depending on the intended volumes, such tests shall require central coordination and
733 prior approval.

734 In case the Connected NCB or its DCA Holder(s) intends to exceed the pre-defined hourly
735 volume limits, the Connected NCB shall send a request for additional processing capacity for
736 specific performance tests to the Eurosystem at least 5 working days in advance. The request
737 should contain the expected volumes to be tested and the duration of the test. The Eurosystem
738 will verify whether it can fulfil the request and shall inform the Connected NCB or its DCA
739 Holder accordingly. If the Eurosystem cannot fulfil the request as specified, the Eurosystem shall
740 propose alternative options in terms of dates, times and/or volumes. In case of conflicting
741 requests, the Eurosystem shall consult the PMG substructure.

Currency Participation Agreement

Schedule 3 – User Testing

742 **7 User Testing Business processes**

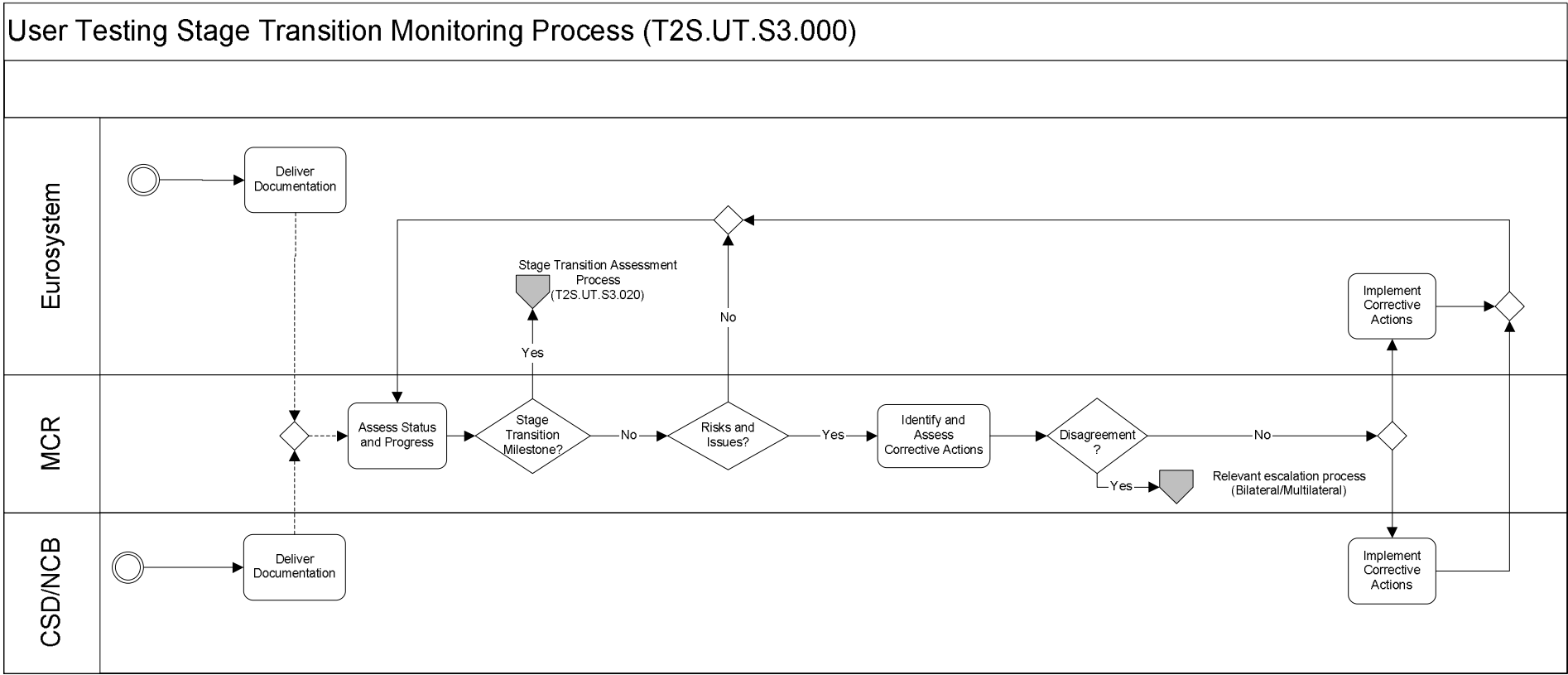
743 This section presents the core business processes that the Eurosystem and Connected NCBs shall comply with for User Testing. The business process description
744 uses a simplified version of the Business Process Modelling Notation (BPMN) 2.0, as specified in Section 7.1 of Schedule 2 (T2S Programme Planning and
745 Monitoring).

Currency Participation Agreement

Schedule 3 – User Testing

746

7.1 User Testing Stage Transition Monitoring Process



Currency Participation Agreement

Schedule 3 – User Testing

7.1.1 Process Actors and their Roles

Process Actor	Process Role
CSD / NCB	In this process, the CSD / NCB is responsible for : ▪ Providing a sufficient level of documentation to the Eurosystem to allow the Eurosystem to assess the Connected NCB's progress for a testing stage; ▪ Assessing its fulfilment of the entry and exit criteria for a testing stage; ▪ Identifying assessing the feasibility of proposed correction actions, when required; and ▪ Discussing the feasibility of the proposed corrective actions with the Eurosystem.
Eurosystem	In this process, the Eurosystem is responsible for: ▪ Providing a sufficient level of documentation to the Connected NCB to allow the Connected NCB to assess the Eurosystem's fulfilment of the entry / exit criteria for a testing stage; ▪ Assessing its fulfilment of the entry and exit criteria for a testing stage; ▪ Identifying assessing the feasibility of proposed correction actions, when required; and ▪ Discussing the feasibility of the proposed corrective actions with the Connected NCB.
Monitoring of Client Readiness (MCR)	In this process, the MCR: ▪ Monitors the Connected NCB's progress in order to determine whether it has fulfilled the entry or exit criteria for a testing stage; and ▪ Discusses and decides on the feasibility of proposed corrective actions; and ▪ Provide guidance to the PMG substructure when required in the case of multilateral escalation.

Currency Participation Agreement

Schedule 3 – User Testing

7.1.2 Process Description

The objective of the User Testing stage transition monitoring process is to ensure bilateral communication between the Eurosystem and the Connected NCB on the progress of the Connected NCB's User Testing

- to ensure adequate coordination of the User Testing activities;
- to enable proactive monitoring of the NCB's fulfilment of the exit and/or entry criteria for User Testing stages; and
- to allow for an early identification of issues and corrective measures for their resolution.

Both the Connected NCB and the Eurosystem provide progress updates for assessing the progress for the current stage of User Testing. The Eurosystem progress update includes any general testing risks and issues encountered that may affect the NCB's timely completion of User Testing stage. The Connected NCB reports on its progress against its test plan and reports any risks and issues that may affect its timely completion of the testing stage. When the progress update is shortly before the stage transition, then the Eurosystem uses the progress update as input for User Testing stage transition assessment.

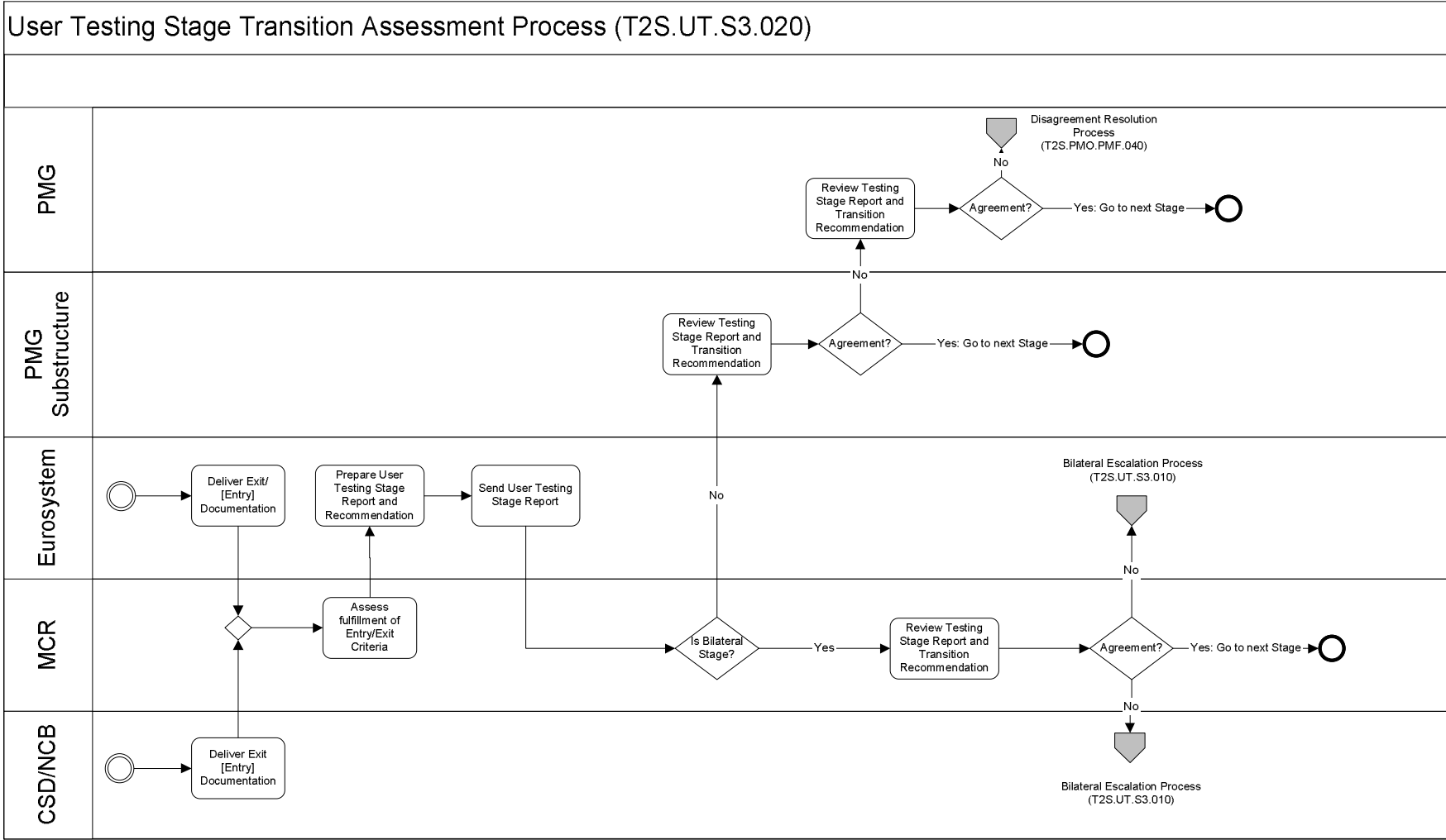
When there is sufficient time remaining before the User Testing stage transition assessment, the Connected NCB and the Eurosystem assess the need for corrective actions to resolve any identified issues and mitigate any identified risks. Both the Connected NCB and the Eurosystem determine whether the implementation of the corrective measures is feasible and undertake their respective actions. If there is disagreement of the corrective actions, then the Connected NCB, the Eurosystem or both can initiate the escalation process.

Currency Participation Agreement

Schedule 3 – User Testing

772

7.2 User Testing Stage Transition Assessment Process



Currency Participation Agreement

Schedule 3 – User Testing

774 7.2.1 Process Actors and their Roles

Process Actor	Process Role
CSD / NCB	In this process, the Connected NCB is responsible for: ▪ Providing a sufficient level of documentation to the Eurosystem to allow the Eurosystem to assess the Connected NCB's fulfilment of the entry and exit criteria for a testing stage; ▪ Carrying out an assessment of its own fulfilment of the entry and exit criteria for a testing stage; ▪ Assessing the proposed correction actions from the bilateral escalation process.
Eurosystem	In this process, the Eurosystem is responsible for: ▪ Delivering the documentation to the Connected NCB to allow the Connected NCB to assess the Eurosystem's fulfilment of the entry / exit criteria for a testing stage; ▪ Carrying out an assessment of the its own fulfilment of the entry or exit criteria for a testing stage; ▪ Assessing the proposed corrective actions; and ▪ Drafting, agreeing and finalising the User Testing stage transition assessment report.
Monitoring of Client Readiness (MCR)	In this process, the MCR has the obligation to: ▪ Monitor the Connected NCB's progress in order to determine whether it has fulfilled the entry or exit criteria for a testing stage; ▪ Propose and discuss corrective actions in case of non fulfilment of either the exit or entry criteria for a User Testing Stage; and ▪ Provide guidance to the PMG substructure when required in the case of multilateral escalation.
PMG Substructure	In this process, the PMG substructure is responsible for: ▪ Discussing the stage transition assessment report and any recommendations; ▪ Providing the final decision during PMG substructure sessions to go forward to the next stage or into multilateral escalation in case of disagreement.
Project Managers Group (PMG)	In this process, the PMG is responsible for resolving any potential disagreement on the decision to go forward to the next stage or to initiate the disagreement resolution process.

775

776

Currency Participation Agreement

Schedule 3 – User Testing

7.2.2 Process Description

The assessment process for User Testing stage transition defines the steps in assessing and reporting on whether the Eurosystem, CSDs and NCBs are prepared to transition jointly from one stage of User Testing to the next based on the exit criteria of the current stage and/or the entry criteria of the next stage.

The Eurosystem provides to the Connected NCB the templates based on which the Connected NCB assesses its fulfilment of the exit criteria of the current stage of User Testing or/and the entry criteria for the next stage of User Testing. The Connected NCB assesses its fulfilment of the exit and/or entry criteria for User Testing stages. The Connected NCB and the Eurosystem jointly review this assessment as part of the monitoring of client readiness to determine whether the Connected NCB has fulfilled the applicable exit and/or entry criteria. Should an exit or entry criteria remain unmet, then the Connected NCB and the Eurosystem identify and assess corrective actions on the part of the Connected NCB, the Eurosystem or both parties, depending on the source and required resolution of the issue.

The Eurosystem prepares the User Testing stage transition assessment report that documents whether the Connected NCBs of a migration wave have fulfilled the exit criteria of the current stage of User Testing or/and the entry criteria for the next stage of User Testing. It documents recommendations for corrective actions should exit or entry criteria remain unfulfilled.

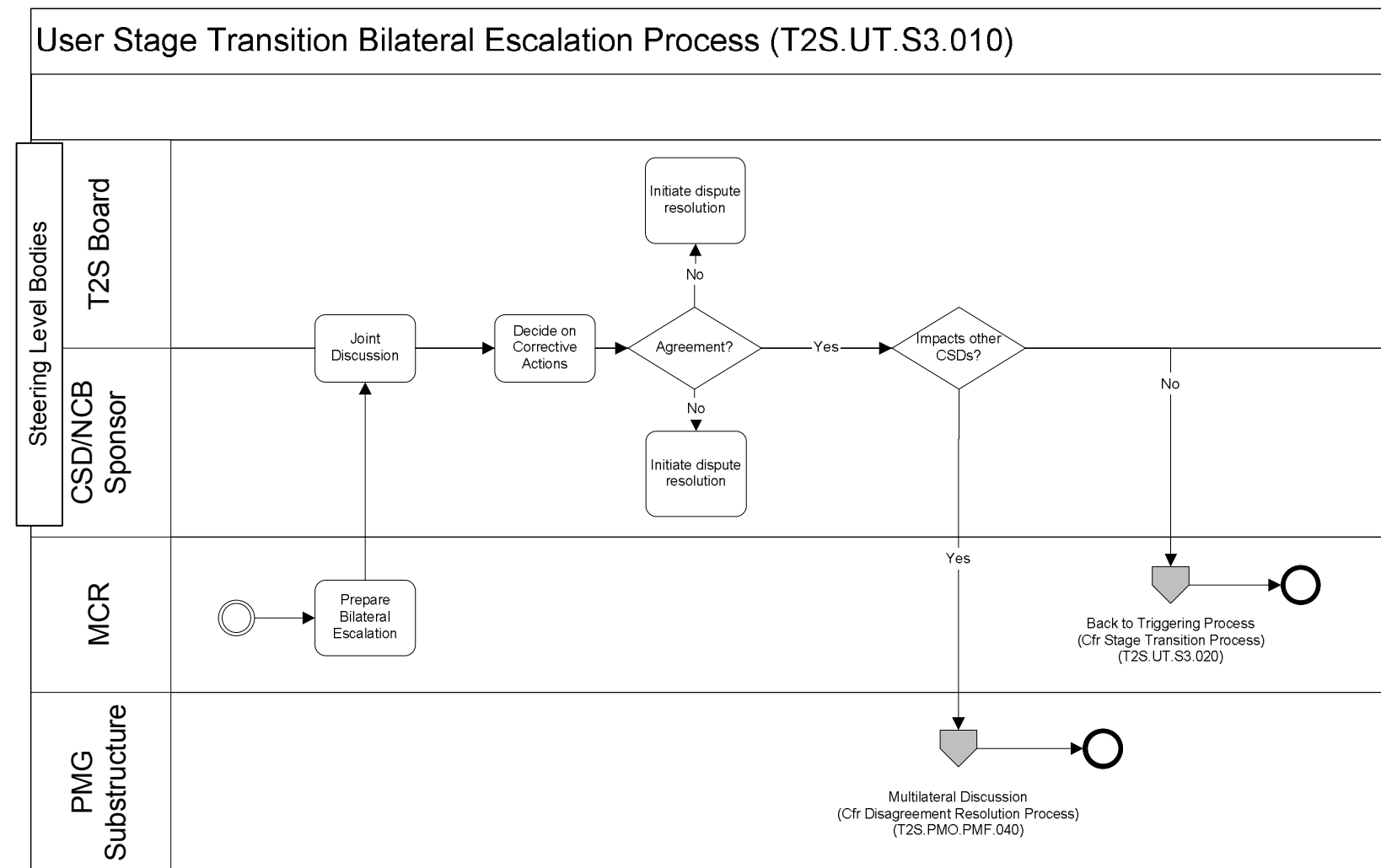
If the User Testing stage transition is bilateral, then the Eurosystem provides the report to the Connected NCB for assessment and both parties agree in the MCR whether there is a need to report risks and issues multilaterally. If the Connected NCB and the Eurosystem agree on the report's conclusions for a stage transition, then the Connected NCB formally enters the next testing stage. If no stage transition is possible or disagreements remain, then the MCR escalates the disagreement as defined in Section 7.3 on bilateral escalation process.

If the User Testing stage transition is multilateral, then the Eurosystem provides the report to the PMG substructure. If the PMG substructure agrees on the report's conclusions for a stage transition, then the Connected NCBs of a migration wave formally enter the next testing stage as a whole. If no stage transition is possible or disagreements remain, then the PMG substructure escalates the disagreement to the PMG. The PMG is responsible for resolving the potential disagreement on the decision to go forward to the next stage of User Testing. If it cannot reach an agreement, then it initiates the disagreement resolution process of Schedule 2 (T2S Programme Planning and Monitoring).

Currency Participation Agreement

Schedule 3 – User Testing

7.3 User Testing Stage Transition Bilateral Escalation Process



Currency Participation Agreement

Schedule 3 – User Testing

811 7.3.1 Process Actors and their Roles

Process Actor	Process Role
T2S Board	In this process, the T2S Board has the responsibility to discuss the escalated issue and attempt to find a resolution with the CSD / NCB Sponsor.
CSD/NCB Sponsor	In this process, the CSD/NCB Sponsor has the responsibility to discuss the escalated issue and attempt to find a resolution with the T2S Board.
Monitoring of Client Readiness (MCR)	In this process, the MCR prepares the bilateral escalation for the T2S Board and the CSD/NCB Sponsor.
PMG substructure	The PMG substructure is responsible for discussing and proposing solutions for a bilateral issue that affects multiple stakeholders and the successful delivery of T2S.

812 7.3.2 Process Description

813 The objective of this process is to resolve bilateral disagreements between the Eurosystem and
814 the Connected NCB in the User Testing Phase. An example of such a disagreement would be
815 differing assessments on whether the Connected NCB has fulfilled the entry or exit criteria for a
816 specific stage of User Testing. The monitoring of client readiness identifies and raises any issues
817 on User Testing that it cannot resolve to the Connected NCB's Sponsor and the T2S Board. At
818 Steering Level, the Connected NCB's Sponsor and the T2S Board will attempt to resolve these
819 disagreements with the objective to avoid entering the disagreement resolution process of
820 Schedule 2.

821 The Steering Level will attempt to resolve the disagreement in a timely manner, taking into
822 account the urgency and the severity of the matter. If the Steering Level has achieved agreement
823 on the disputed issues and the proposed resolution does not affect other T2S Stakeholders, then it
824 submits its resolution to the Connected NCB and the Eurosystem representatives in MCR for
825 implementation. If the Steering Level has achieved agreement on the disputed issues and the
826 proposed resolution affects other T2S Stakeholders, then it submits its resolution to the PMG
827 substructure for review and a recommendation on its implementation. If ultimately the Steering
828 Level cannot reach an agreement on the resolution of an issue, then it can escalate the issue
829 according to disagreement resolution process of Schedule 2 (T2S Programme Planning and
830 Monitoring).

Schedule 3 – User Testing

831



Currency Participation Agreement

Schedule 3 – User Testing

833 7.4.1 Process Actors and their Roles

Process Actor	Process Role
CSD / NCB	The CSD or NCB is responsible for identifying the need to and issuing the request to suspend User Testing.
Eurosystem	The Eurosystem has the responsibility for: ▪ Analysing the CSD or NCB request to suspend User Testing; ▪ Proposing corrective measures to avoid a suspension of User Testing; and ▪ Preparing the assessment of and a recommendation on the suspension request.
Monitoring of Client Readiness (MCR)	In this process, the MCR depicts the bilateral steps of this process for: ▪ Reviewing and discussing the status of User Testing; and ▪ Assessing the status of User Testing and providing guidance to the PMG substructure when required in the case of multilateral escalation.
PMG substructure	In this process, the PMG substructure is responsible for: ▪ Discussing the stage transition assessment report and any recommendations; and ▪ Providing the final decision during PMG substructure sessions to go forward to the next stage or into multilateral escalation in case of disagreement.
Project Managers Group (PMG)	The PMG provides guidance to the PMG substructure in order to resolve disagreements on the potential suspension of User Testing. If the PMG substructure cannot reach an agreement, then the PMG is responsible for resolving any potential disagreement on the decision to suspend or for initiating the disagreement resolution process.

834 7.4.2 Process Description

835 This process describes the steps in taking a decision on a request from a Participating CSD or
836 Participating NCB to suspend the current stage of User Testing. Participating CSDs/NCBs
837 individually or the PMG substructure may identify the need to suspend User Testing, e.g. too
838 many unresolved defects of various severities to allow the continuation of proper testing. The
839 individual Participating CSD/NCB or the PMG substructure submits the request with its business
840 justification to suspend User Testing to the Eurosystem.

841 The Eurosystem analyses the suspension request and, when possible to avoid the suspension to
842 User Testing, proposes corrective action

- 843 ▪ To the individual Participating CSD/NCB that initiated the request when the request is
844 bilateral; and

Currency Participation Agreement

Schedule 3 – User Testing

- To the PMG substructure when it initiated the request as a multilateral request.

When the suspension request is bilateral, then

- the Participating CSD/NCB jointly reviews the Eurosystem assessment of the suspension request in MCR; and
- the Participating CSD/NCB and/or Eurosystem implement(s) any identified corrective actions to limit and/or avoid a suspension of User Testing.

If the suspension of User Testing is unavoidable and has no planning impact, then the MCR may initiate the suspension. If the suspension of User Testing is unavoidable and has a planning impact, then the MCR initiates an assessment of the planning impact that follows the programme plan preparation and assessment process in Schedule 2 (T2S Programme Planning and Monitoring).

When the suspension request is multilateral or the bilateral request has a multilateral impact, then Eurosystem prepares the assessment and recommendation for the assessment in the PMG substructure. The PMG substructure may request guidance from the PMG to facilitate a decision on the potential suspension of User Testing. In the case that the PMG substructure cannot reach an agreement, it may revert to the PMG to reach an agreement. If the PMG substructure cannot reach an agreement on the decision to suspend, then it initiates the disagreement resolution process as defined in Schedule 2 (T2S Programme Planning and Monitoring).

If the PMG substructure reaches an agreement on the request and the request has no planning impact, then the PMG substructure may initiate the suspension. If the suspension of User Testing is unavoidable and has a planning impact, then the PMG substructure initiates an assessment of the planning impact that follows the programme plan preparation and assessment process in Schedule 2 (T2S Programme Planning and Monitoring).

7.5 Release management during the User Testing

The Release Management Process (RMP) during the User Testing execution phase ensures that all aspects, technical and non-technical, originating from defects resolution are considered together, following the principles laid down in Chapter 5 of Schedule 9 (Change and Release Management). The PMG substructure makes a recommendation to the PMG on packaging the bug fixes in a bug fix release.

Currency Participation Agreement

Schedule 3 – User Testing

7.6 Supporting processes

7.6.1 IT Service Management processes

As described in chapter 3.1 it is the Eurosystem's responsibility to establish and operate the necessary IT service management processes that includes a defect resolution to remedy errors based on the principles of ITIL V3 Service Operation.

The details of these IT service management processes such as the defect resolution and incident handling will be described in the Manual of Operational Procedures (MOP). The MOP will describe these processes for T2S Operations and the Operations Managers Group (OMG) will be the main stakeholder in this processes. During User Testing the same processes will apply with one major distinction namely that the PMG substructure will be the main stakeholder instead of the OMG. Furthermore, the definitions of the severity of defect and the incident resolution times applicable during User testing are defined in Schedule 6 (T2S Service Level Agreement).

Currency Participation Agreement

Schedule 3 – User Testing

8 Post-migration testing

Post-migration testing shall refer to all testing activities of CSDs, NCBs, DCA Holders and Directly Connected Parties (DCPs) after go-live of the final migration wave for the initial release of T2S. Events, such as the migration of a new CSD / NCB to T2S or the implementation of a new release, will require post-migration testing.

The following principles shall apply for Post-Migration Testing:

- The Project Managers Group (PMG) shall perform an impact assessment for a new T2S release or a new NCB joining on the T2S Actors in order to determine whether all T2S Actors will need to carry out User Testing for the T2S release or whether only affected T2S Actors need to test.
- Based on the impact assessment, the Project Managers Group (PMG) with the support of the PMG substructure on User Testing shall propose a post-migration test plan to the Steering Level for approval.
- The post-migration test plan must ensure that CSDs, NCBs, DCPs, DCA Holders will have sufficient time to verify that the delivered T2S functionality according to the agreed requirements and specifications.
- Post-migration testing shall use the framework as defined in this Schedule.

The PMG in their impact assessment will make a recommendation to the Steering Level on whether the introduction of the new T2S release will require the recertification of CSDs and/or NCBs. The T2S Board shall take the final decision on whether CSDs and/or NCBs must recertify themselves for a new release of T2S.

Currency Participation Agreement

Schedule 3 – Annex 1 – Mapping of testing activities on the test environments

909 **Annex 1 – Mapping of testing activities on the test environments**

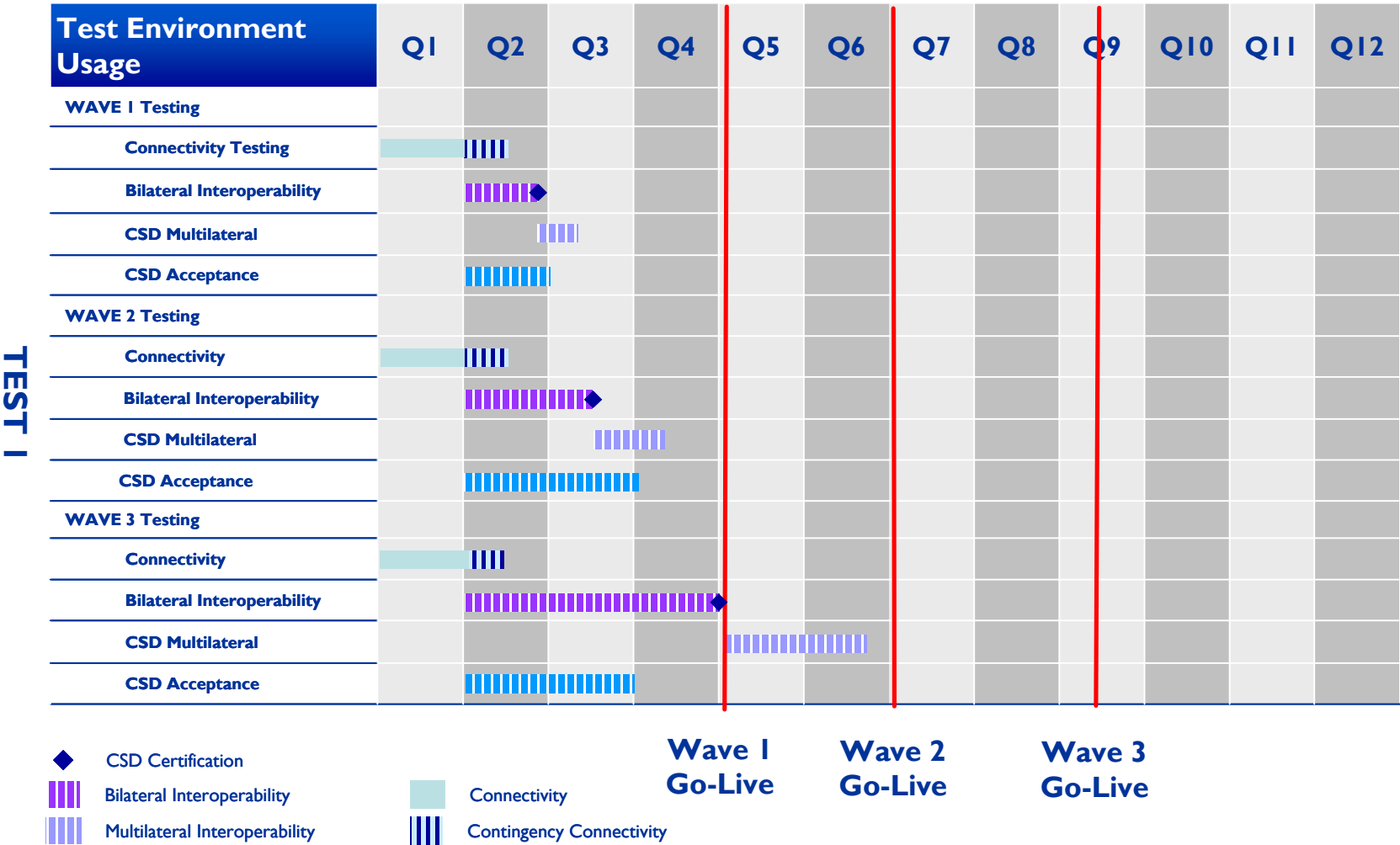
910 In accordance with the principles for sharing testing facilities, the Eurosystem will not plan any
911 Eurosystem Acceptance Testing activity on the testing environments used for User Testing.

912 The following diagram presents the mapping of the testing activities for each migration wave on
913 the test environments.

914

Currency Participation Agreement

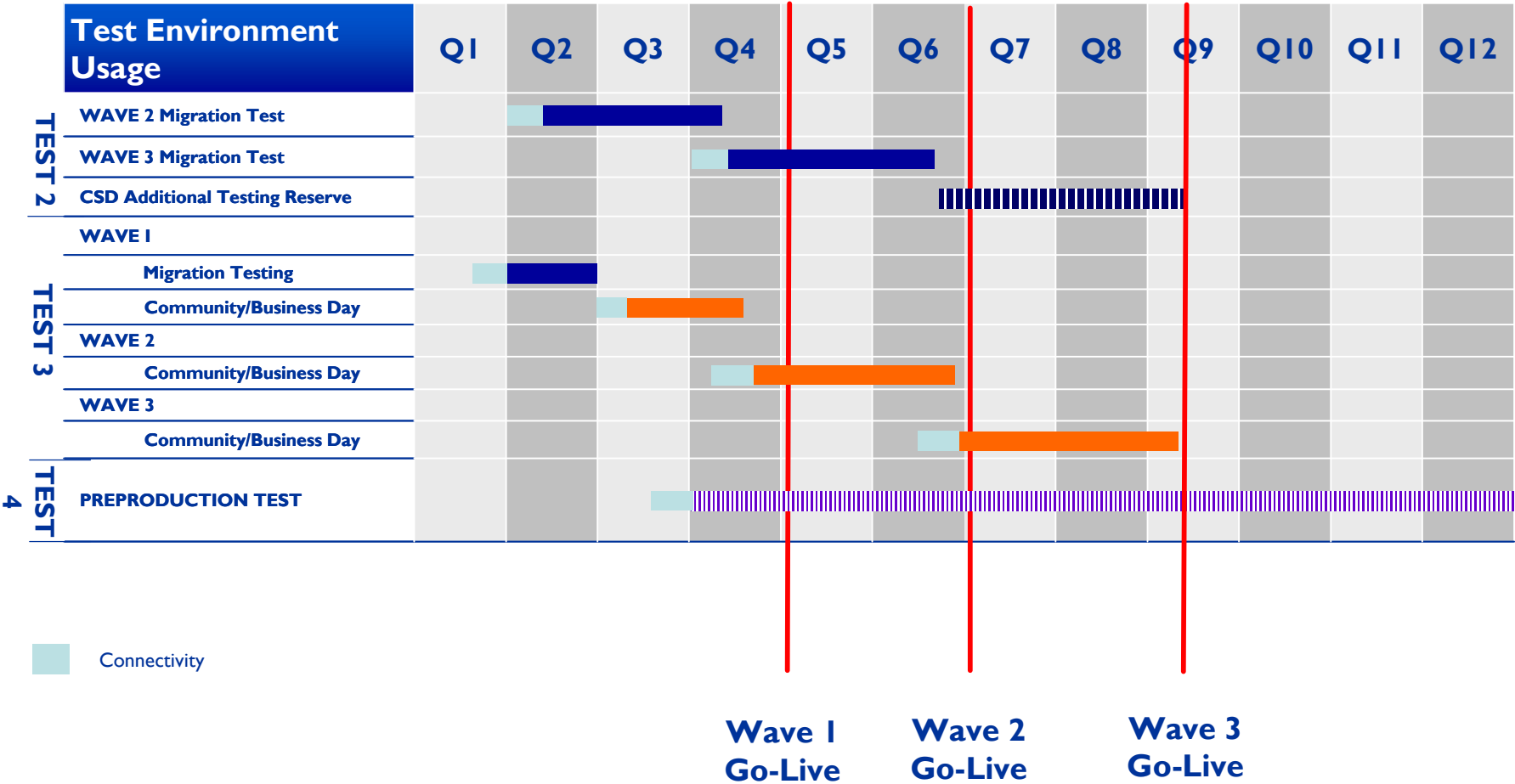
Schedule 3 – Annex 1 – Mapping of testing activities on the test environments



Disclaimer: the timeline is only used to illustrate the usage of the test environments.

Currency Participation Agreement

Schedule 3 – Annex 1 – Mapping of testing activities on the test environments



CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 4

MIGRATION

Currency Participation Agreement

Schedule 4 –Migration

Table of contents

1 Introduction	1
2 Objective, scope and approach of the migration schedule.....	2
2.1 Objective.....	2
2.2 Scope	2
2.3 General migration approach.....	2
3 General responsibilities of the Contracting Parties.....	4
3.1 General responsibilities of the Eurosystem	4
3.2 General responsibilities of the Connected NCB	5
3.3 Cooperation and escalation procedures	7
4 Preparation of the migration	9
4.1 Responsibilities of the Eurosystem.....	9
4.2 Responsibilities of the Connected NCB	11
5 Implementation of the migration	12
5.1 Responsibilities of the Eurosystem.....	12
5.2 Responsibilities of the Connected NCB	13
6 Closing phase.....	15
6.1 Responsibilities of the Eurosystem.....	15
6.2 Responsibilities of the Connected NCB	15
ANNEX 1: Migration milestones.....	1

Currency Participation Agreement

Schedule 4 –Migration

1 1 Introduction

2 This document aims at presenting the provisions related to the framework that will be used to prepare
3 and conduct the migration to T2S of the Connected NCBs and their Dedicated Cash Accounts
4 holders, as well as the roles and responsibilities of the contracting parties along the migration process
5 from the preparation phase until the end of the Migration Period.

6 The document is divided into five chapters, corresponding to the major aspects identified as relevant
7 for the migration framework: i) objective, scope and approach of the migration schedule; ii) general
8 responsibilities of the contracting parties; iii) preparation of the migration, iv) implementation of the
9 migration and v) closing phase.

Currency Participation Agreement

Schedule 4 – Migration

2 Objective, scope and approach of the migration schedule

2.1 Objective

The objective of the T2S migration is to enable a smooth and successful transition to the usage of the T2S Services for all Connected NCBs and their Dedicated Cash Account holders once the pre-requisites for their migration are fulfilled. As stated in the User Requirements Document, *“Migration in the context of T2S means the relocation of data from a CSD to the T2S infrastructure and the associated changes in the processes and technical environment of a CSD on a mutually agreed date”*. Obviously, the same applies to the Connected NCBs to ensure a successful migration to T2S on the agreed date.

2.2 Scope

In terms of activities, the scope of this Migration Schedule covers all activities that are related to the preparation of the T2S production environment for the successful migration of a Connected NCB and its Dedicated Cash Account holders. Chapter 4, 5 and 6 provide the relevant information concerning the migration related activities. Although the migration process is interrelated with others processes, in particular the User Testing until the end of the Migration Period, the T2S Programme Plan and the Release Management during the Migration Period (if releases/ software updates are envisaged during this period), such other activities will be described separately in the relevant Schedules.

With regards to the users, in the context of the Currency Participation Agreement the T2S migration perimeter consists of all non-euro area NCBs that have entered into a contractual relationship with the Eurosystem for the use of T2S in view of their connection to T2S during the Migration Period. Whenever relevant, references will be made to co-ordination of migration activities with other T2S Actors, but the actual provisions applicable to those T2S Actors will be covered as part of the legal relationship with these T2S Actors.

2.3 General migration approach

The migration to T2S will follow a phased approach and will be organised to reach the following objectives:

- give the necessary flexibility for the planning and coordination of the migration activities;

Currency Participation Agreement

Schedule 4 – Migration

- allow for a gradual build-up of volumes;
- mitigate the risk that any Connected NCB fails to successfully migrate to T2S on the agreed date, thereby avoiding interruptions in the Connected NCB's business;
- ensure system stability from a functional and technical perspective throughout the migration process.

This phased approach will be implemented via a migration “by CSD” approach, which allows the CSDs and their Users to migrate to T2S in different waves and on different pre-defined dates.

The migration will be organised targeting a maximum number of 4 migration waves¹, with a minimum period of 3 months between each wave. In addition, one contingency migration date is available (not later than 6 months after the date of the last migration wave), to be used in case the CSD and/or Connected NCB cannot migrate as originally committed. The contingency migration wave can be used by a Connected NCB provided that an agreement has been reached with its national CSD(s)² with respect to the fact that the migration can not take place as originally scheduled and therefore the migration of the Connected NCB and of its national CSD(s) has to be deferred to the contingency wave.

The duration of the migration shall be limited to 18 months, from the T2S Go-Live Date (i.e. date of the first migration wave) until the contingency migration date.

The Connected NCB shall migrate at the latest in the migration wave in which at least one national CSD migrates to T2S. The migration will take place during a weekend and will be driven by settlement date. The migration to T2S will not take place on a “sensitive” weekend during critical periods for CSDs and Connected non-euro CBs such as corporate action season, freeze periods or periods of significant market stress etc.

¹ The fourth migration wave is optional pending the proposal of the CSDs by synchronisation point 2 as defined in Schedule 2 (i.e. Q2 2011)

² A CSD located in the country of the Connected NCB

Currency Participation Agreement

Schedule 4 – Migration

3 General responsibilities of the Contracting Parties

As an overarching principle, the Eurosystem and the Connected NCB shall cooperate in good faith for the preparation and execution of all T2S migration activities.

3.1 General responsibilities of the Eurosystem

In view of preparing and ensuring a successful migration to T2S of all Connected NCBs and their Dedicated Cash Account holders, the Eurosystem shall:

- a) cooperate in good faith with the Connected NCBs and the other T2S Actors and provide them with all relevant information to prepare the necessary procedures and processes for all migration activities and related deliverables, as described in Schedule 2 (T2S Programme Planning and Monitoring);
- b) coordinate, steer and monitor the T2S migration process. In co-operation with the Connected NCBs, it establishes the migration plan, the tasks and the milestones for the migration process and monitors compliance with the agreed procedures and milestones;
- c) prepare the life-cycle of the migration process which consists of three phases: (i) the planning phase, which consists of activities related to the preparation of the migration activities that need to be planned in advance in order to mitigate the migration risks; (ii) the implementation phase, which consists of the actual preparations for live operations and (iii) the closing phase, which consists of preparing closing reports aiming at improving the next migration based on lessons learned from the initial migration. The diagram outlining the sequence and interrelations of the migration activities, as well as the milestones of the T2S migration phases are presented in Annex 1 (Migration milestones) to this Schedule;
- d) set up a PMG substructure, which will be in charge of coordinating, supporting and monitoring the work related to the migration activities, in accordance with the T2S Governance and the provisions set out in section 3.3 of this Schedule;
- e) nominate one person for each Connected NCB as migration correspondent for that non-euro area NCB, as well as a T2S migration coordinator in charge of monitoring and coordinating all activities to be carried out during the migration process;
- f) ensure the readiness of the production environment according to the provisions of Schedule 2 (T2S Programme Planning and Monitoring) in order to enable the Connected NCBs to plan and carry out all activities on the production environment required for its migration to T2S;

Currency Participation Agreement

Schedule 4 – Migration

- g) ensure the readiness of T2S for all migration waves, meaning that the enhancements to the system are reduced to the resolution of blocking and severe defects discovered during the Migration Period;
- h) provide all reasonable support to Connected NCBs in ensuring the readiness of the Dedicated Cash Accounts in their currency, prior to the first settlement of securities transactions by their national CSDs. The opening of these Dedicated Cash Accounts will be driven by the request of the Dedicated Cash Account holders in accordance with the rules and conditions set up by the Connected NCB;
- i) upload and maintain the necessary Central Bank Static Data and system configuration parameters sufficiently in advance of the migration of the Connected NCBs; The Central Bank Static Data will be created upfront with a future “valid from” date;
- j) provide support to the Connected NCB – in particular in accordance with section 21.8 of the URD – for the transfer of its Central Bank Static Data and the Dynamic Data prior to its migration to T2S;
- k) report progress on the overall migration process on a regular basis and share relevant information with the Connected NCBs on their level of readiness (based on information provided by those Connected NCBs);
- l) apply an escalation and decision-making process for any migration related issues in accordance with the general T2S governance arrangements, as specified in Schedule 8 (Governance) and in the provisions set out in section 3.3 of this Schedule;
- m) provide support to the Connected NCBs with regard to their migration activities, including during the process of “de-migration” of the Connected NCB in case the Connected NCB faces severe problems due to significantly degraded Service Level during the week after its migration to T2S;
- n) provide training sessions for the migration to the Connected NCBs and all necessary support to facilitate the training sessions provided by the Connected NCBs to its Dedicated Cash Account holders.

3.2 General responsibilities of the Connected NCB

In view of preparing and ensuring a successful migration to T2S, the Connected NCBs shall:

- a) cooperate in good faith with the Eurosystem and with other relevant T2S Actors and provide all relevant information to prepare the necessary procedures and processes for all migration activities and related deliverables, identified in Schedule 2 (T2S Programme Planning and

Currency Participation Agreement

Schedule 4 – Migration

- 121 Monitoring);
- 122 b) determine, in agreement with its national CSD(s) , the migration wave in which it shall
- 123 migrate to T2S and the respective migration date by synchronisation point 2 as defined in
- 124 Schedule 2 (i.e. Q2 2012);
- 125 c) migrate to T2S at the latest in the migration wave in which at least one national CSD
- 126 migrates to T2S;
- 127 d) ensure its own readiness for the migration to T2S by the agreed date according to the
- 128 procedures and processes agreed with the Eurosystem and other T2S Actors;
- 129 e) take all measures that are reasonably required to facilitate the readiness of its Dedicated Cash
- 130 Account holders for the migration to T2S by the agreed date according to the procedures and
- 131 processes agreed with the Eurosystem and other T2S Actors;
- 132 f) set up its own migration project, define its migration plan, allocate appropriate resources to
- 133 the implementation of such a plan, as well as assess and adjust such migration plan and the
- 134 allocated resources, where necessary, with a view to ensuring a smooth migration to T2S
- 135 according to the agreed plan; the adjustments to migration plans must be discussed and
- 136 agreed with the Eurosystem and other T2S Actors as changes may have an impact on all the
- 137 involved parties;
- 138 g) be involved in the decision to go-live of T2S as a member of the coordination body in charge
- 139 of coordinating, supporting and monitoring the work related to user testing activities,
- 140 independently of its migration wave; in particular, the Connected NCB will be able to
- 141 contribute to this coordination body³ opinion whether or not the exit criteria for the business
- 142 day testing are fulfilled and on the level of comfort that all remaining blocking and severe
- 143 defects will be solved in time in order to avoid any impediments for the later migrating non-
- 144 euro area NCBs;
- 145 h) ensure the readiness of the Dedicated Cash Accounts in its currency prior to the go-live of
- 146 T2S (i.e. if the Connected NCB and at least one national CSD join T2S in the first migration
- 147 wave) or prior to the first settlement of securities transactions by a national CSD (i.e. if the
- 148 Connected NCB and its national CSD join T2S in a later migration wave). The Dedicated
- 149 Cash Accounts in its currency shall be opened in T2S by the Connected NCB upon the
- 150 request of the Dedicated Cash Account holders in accordance with the rules and conditions
- 151 set up by the Connected NCB;

³ If an agreement for a dispute cannot be reached at the level of this coordination body, the dispute resolution and escalation procedure described in art. Article 35 of the CPA applies and follows a decision-making process in accordance with the T2S Governance, as specified in Schedule 8.

Currency Participation Agreement

Schedule 4 – Migration

- i) upload and maintain its Central Bank Static Data sufficiently in advance, typically with maximum three months before the migration of its national CSD (i.e. before the migration wave where the holders of the Dedicated Cash Accounts envisage to settle securities transactions in its currency); the Central Bank Static Data will be created upfront with a future “valid from” date;
- j) ensure the availability of the necessary functions to provide T2S with the required collateral information as of the date of its migration if the Connected NCB decides to use auto-collateralisation functionality to offer intraday credit in T2S;
- k) provide training sessions to its Dedicated Cash Account holders sufficiently in advance of community testing;
- l) report progress on its readiness for migration according to the agreed procedures, frequency and level of detail, with a particular view to identifying developments that might jeopardise the migration of the other T2S Actors according to the agreed plan;
- m) nominate one person for coordinating all migration activities within its own organisation and ensure that such person or an alternate shall duly and regularly participate in the meetings organised by the Eurosystem until the Connected NCB has migrated to T2S, and, in particular where this is not practicable, in the written procedures;

3.3 Cooperation and escalation procedures

The Eurosystem shall apply an escalation and decision-making process for communication in accordance with the general T2S governance arrangements, as specified in Schedule 8 (Governance).

The Eurosystem shall set up a PMG substructure, in accordance with the T2S governance, for the coordination and monitoring of the migration activities. This substructure shall meet on a regular basis and shall at least be composed of the ECB Migration coordinator, the 4CB Migration coordinator, and a Migration coordinator from each Connected NCB (as meant in section 3.2.m of this Schedule).

The role of the substructure in charge of Migration shall be to:

- Coordinate and review Migration activities;
- Monitor the implementation of the Migration plans;
- Review the Connected NCB’s tailored Migration plan;
- Discuss issues raised by the members of the substructure and try to resolve disagreements;

Currency Participation Agreement

Schedule 4 – Migration

182 ▪ Communicate with the T2S Programme management office on the planning of Migration
183 activities;

184 ▪ Prepare communications related to migration to the various T2S Stakeholders and the public
185 at large.

186 In case of an urgent issue requiring immediate action,, the following process shall be followed:

187 ▪ The Connected NCB shall request a conference call with the Eurosystem during the next
188 business day or at its earliest convenience;

189 ▪ The issue shall be discussed during the conference call;

190 ▪ The Eurosystem shall summarize the outcome of the conference call and distribute it to the
191 members of the substructure in charge of Migration.

192 The substructure in charge of Migration shall convene at its earliest convenience to:

193 ▪ Assess the nature of the issue;

194 ▪ Assess the impact of the issue on the various T2S Actors;

195 ▪ Assess any potential impact on the organisation and the timing of the migration activities for
196 the various T2S Actors;

197 ▪ Prepare an action plan, and the necessary communication, if any, to address the issue;

198 In case no agreement can be reached in the substructure, each party shall be entitled to escalate the
199 problem to the Project Managers Group (PMG), where the situation shall be discussed and rapidly
200 assessed.

201 If a mutually agreeable solution cannot be found in the PMG, then the general T2S escalation process
202 shall apply whereby the issue is escalated to the relevant T2S steering bodies in order to receive
203 guidance to resolve the issue. The escalation process shall be in accordance with the general T2S
204 governance arrangements, as specified in the Schedule 8 (Governance).

205 Ultimately there shall be recourse to the dispute resolution process as described in the provisions of
206 the relevant Articles in the core Currency Participation Agreement.

Currency Participation Agreement

Schedule 4 – Migration

4 Preparation of the migration

The activities to be carried out for the preparation of the T2S Go-Live Date and the migration of a Connected NCB and its Dedicated Cash Account holders need to be well planned in advance in order to mitigate the risks related to the migration process.

4.1 Responsibilities of the Eurosystem

In order to prepare and organise the migration related activities, the Eurosystem – in cooperation with the Connected NCB - shall:

- a) set up a coordination body according to the T2S Governance and ensure that all Connected NCB and other T2S Actors are informed via this forum as to the progress of the migration activities;
- b) set up a bilateral coordination structure between the Eurosystem and each Connected NCB in addition to the multilateral structure specified above;
- c) establish the standard migration plan for all Connected NCBs that will join T2S, including aspects related to the set-up of Dedicated Cash Accounts, major project milestones, the necessary Dynamic Data to be input into the system, , as well as checkpoints to be met before the start of the migration weekend;
- d) support the Connected NCB in establishing the tailored migration plan per Connected NCB or group of Connected NCBs depending on its specificities;
- e) establish the detailed migration weekend script for each migration wave which provides the Connected NCB with the required information to execute the tasks and/or to carry out the actions required during the migration weekend;
- f) establish the fall-back arrangements and roll-back procedures specific for each migration wave, in order to manage the necessary processes if the migration needs to be deferred to a later stage due to predictable or unforeseen circumstances, and/or if the activities already performed during the migration weekend need to be unwound if the migration has to be stopped;
- g) provide support to the Connected NCB – in particular in accordance with section 21.8 of the URD – if it has been demonstrated, following the applicable crisis management arrangements, that there is a need to “de-migrate” to its legacy system immediately after its

Currency Participation Agreement

Schedule 4 – Migration

- 236 migration in case the Connected NCB faces severe problems at that time, either due to
237 significantly degraded Service Levels, or because of severe problems at the Connected NCB
238 itself;
- 239 h) define the registration guide/procedures in order to enable the Connected NCB to describe in
240 detail their participation data, services used, account usage details;
- 241 i) establish the structure and elements of the migration profile for each Connected NCB which
242 gives a structured overview of the set-up of Connected NCB on their first day of operation in
243 T2S;
- 244 j) define the necessary Central Bank Static Data and Dynamic Data to be uploaded in the
245 system, as well as the relevant message formats;
- 246 k) re-plan and reschedule certain migration activities as required, based on a strong coordination
247 and decision-making process between the Eurosystem and the Connected NCB, in the
248 eventuality that an unexpected event (within and out of the control of the Connected NCB)
249 will impede the migration of one or more Connected NCBs on the scheduled date;
- 250 l) actively monitor throughout the migration process the level of the Connected NCB's
251 preparedness;
- 252 m) prepare progress reports to the appropriate bodies on the status of each Connected NCB
253 based on the information provided by the Connected NCBs according to pre-agreed
254 dashboard indicators;
- 255 n) establish the communication framework for the migration process which covers the
256 information exchanged with the Connected NCBs and the market about the migration
257 process and about individual migrations. Communications will be prepared jointly by the
258 Eurosystem and the Connected NCBs, in accordance with the provisions set out in the
259 Currency Participation Agreement and in section 3.3 of this Schedule;
- 260 o) report progress on the activities carried out during the planning phase by the Eurosystem and
261 the Connected NCBs according to the agreed procedures, frequency and level of detail, with
262 a particular view to identifying aspects that might jeopardise the migration according to the
263 agreed plan;
- 264 p) establish specific operational procedures and rules, if needed, to be followed by the
265 Connected NCB during the Migration Period where some Contracting CSDs will operate
266 under the new operational regime of T2S.
- 267

Currency Participation Agreement

Schedule 4 – Migration

4.2 Responsibilities of the Connected NCB

In order to prepare and organise the migration related activities, the Connected NCB – in cooperation with the Eurosystem - shall:

- a) organize, prepare and monitor its own migration process and take appropriate measures in order to ensure its own readiness and that of its Dedicated Cash Account holders for joining T2S;
- b) monitor and take all measures that are reasonably required to facilitate the readiness of its Dedicated Cash Account holders for the migration to T2S;
- c) cooperate with the Eurosystem in preparation of the standard migration plan and the detailed migration weekend script;
- d) develop its tailored migration plan (including a fallback plan) based on the standard migration plan;
- e) coordinate the readiness of its Dedicated Cash Account holders for migration to T2S. The Connected NCB shall take all measures that are reasonably required to facilitate the readiness of the Dedicated Cash Accounts of its participants in T2S i.e. the creation and availability of Dedicated Cash Accounts in T2S prior to the first settlement of the securities transactions by its national CSD;
- f) identify any “critical participants” from a cash perspective that might jeopardize the migration of the relevant Connected NCB and its Dedicated Cash Account holders and involve them actively in the migration project, monitoring their preparations more closely and possibly envisaging fallback arrangements to settle their transactions;
- g) communicate the readiness of the Dedicated Cash Accounts, as well as the decision on the readiness of the Dedicated Cash Account holders to operate their Dedicated Cash Accounts in T2S to its Dedicated Cash Account holders well in advance in order to allow them to organise their migration;
- h) report progress to the Eurosystem on the activities carried out during the planning phase according to the agreed procedures, frequency and level of detail, with a particular view to identifying developments that might jeopardise the migration of the other T2S Actors according to the agreed plan;.

Currency Participation Agreement

Schedule 4 – Migration

5 Implementation of the migration

The implementation phase consists of the actual preparations for live operations and the execution of the tasks on the T2S production environment, in particular all activities that need to be carried out from the moment when the Eurosystem has made the T2S production environment available to the Connected NCBs until the successful migration of the last Connected NCB.

5.1 Responsibilities of the Eurosystem

Prior to the start of the implementation phase, the Eurosystem shall:

- a) confirm the readiness of the T2S production environment, including the system's compliance with specific non-functional requirements, in particular related to technical performance, business continuity and information;
- b) make available to the Connected NCBs the versions of all the functional and operational documentation (e.g. GFS, UDFS, User Handbooks, Manual of Operational Procedures), which are compliant with the T2S production environment and/or will be used for live operations according to Schedule 2 (T2S Programme Planning and Monitoring);
- c) set up coordination bodies, in accordance with the T2S governance, for the coordination and monitoring of the activities to be carried out from the moment when the Eurosystem has made the T2S production environment available to the Connected NCB until the successful migration of the last Connected NCB and the other T2S Actors, as well as for the decision-making in case an incident occurs which might jeopardise the migration to T2S.

During the implementation phase, the Eurosystem shall:

- a) carry out all the pre-migration activities and the activities required during the migration weekend, according to the agreed plan;
- b) ensure prior to the T2S Go-Live Date that the complete T2S functionality is available in the T2S production environment and all critical bugs encountered during the User Testing have been corrected, so as to avoid the implementation of functional releases during the Migration Period;
- c) confirm – prior to the start of first migration wave and the subsequent migration waves - the correct functioning of the T2S production environment according to the T2S Scope Defining Set of Documents and other relevant documents, including the successful execution of an

Currency Participation Agreement

Schedule 4 – Migration

- 326 inter-region rotation before the first and second migration wave and that the conditions
327 agreed during the previous Go/ No go decision are met;
- 328 d) upload and maintain the necessary Central Bank Static Data and configuration parameters
329 sufficiently in advance of the migration of the Connected NCB; these data will be created
330 upfront with a future “valid from” date;
- 331 e) confirm the start of the activities during the migration weekend and subsequently the
332 successful completion of each migration on the basis of a report prepared in collaboration
333 with the Connected NCBs; The former confirmation will only be given, in particular, if the
334 exit criteria of the User Testing have been successfully completed and a timetable for
335 implementation of the corrections for the remaining severe defects has been mutually agreed
336 with the Connected NCBs;
- 337 f) provide support to the Connected NCB for the transfer of its Central Bank Static and
338 Dynamic Data prior to migration of the Connected NCB to T2S;
- 339 g) report progress on the activities carried out during the implementation phase by the
340 Eurosystem and the Connected NCBs according to the agreed procedures, frequency and
341 level of detail, with a particular view to identifying aspects that might jeopardise the
342 migration according to the agreed plan;
- 343 h) provide support to the Connected NCBs to perform the required actions for their successful
344 migration according to agreed plan.

345 5.2 Responsibilities of the Connected NCB

346 Prior to the start of the migration weekend i.e. go-live of T2S or any other migration date, the
347 Connected NCB shall:

- 348 a) obtain the certification from the Eurosystem for uploading and maintenance of Central Bank
349 Static Data on the T2S production environment, management of liquidity and collateral as a
350 pre-condition to start any activities on the production environment;
- 351 b) establish and verify its connectivity to the T2S production environment for each of the
352 networks selected by the Connected NCB;
- 353 c) upload and maintain the Central Bank Static Data sufficiently in advance, typically with
354 maximum three months before the migration of its national CSD (i.e. before the migration
355 wave where the holders of the Dedicated Cash Accounts envisage to settle securities
356 transactions in its currency);

Currency Participation Agreement

Schedule 4 – Migration

- d) verify and confirm that its internal systems and processes and those of its Dedicated Cash Account holders are ready to efficiently interact with T2S;
- e) verify and confirm that T2S delivers the expected services as agreed in the T2S Scope Defining Set of Documents, in particular by having obtained the possibility to verify that all critical defects have been solved, including those discovered during the implementation phase;
- f) confirm the availability of the necessary Dedicated Cash Accounts upon the request of the Dedicated Cash Account holders;
- g) confirm the availability of the necessary functions to provide T2S with the required collateral information if the Connected NCB decides to use auto-collateralisation functionality to offer the intraday credit in T2S;
- h) confirm that the T2S Scope Defining Documents and other T2S operational documentation are compliant with the services provided by the T2S and can be used for the live operations;
- i) confirm its readiness for migration and that of its Dedicated Cash Account holders to T2S according to the agreed migration plan;
- j) complete all required forms for the registration on the T2S production environment and provide them to the Eurosystem by the agreed time;
- k) ensure timely access to relevant static data for its Dedicated Cash Account holders;
- l) carry out all the required pre-migration activities according to the agreed migration plan.

During the migration weekend, the Connected NCB shall:

- a) carry out all the activities required during the migration weekend according to the agreed migration plan, including the fall-back arrangements and roll-back procedures as specified in section 4.1 f) of this Schedule;
- b) report on the status of the activities carried out during the migration weekend according to the agreed procedures, frequency and level of detail;
- c) confirm the end of its migration based on the successful completion of the activities to be carried out during the migration weekend according to the agreed plan.

Currency Participation Agreement

Schedule 4 – Migration

6 Closing phase

The closing phase covers the final reporting and the assessment of the lessons learned during the migration process.

6.1 Responsibilities of the Eurosystem

During the closing phase, the Eurosystem shall:

- a) provide reports on lessons learned from a migration wave to be applied to the next migration waves;
- b) ensure the necessary updates and improvements in the migration plans in order to smoothen the next migration waves.

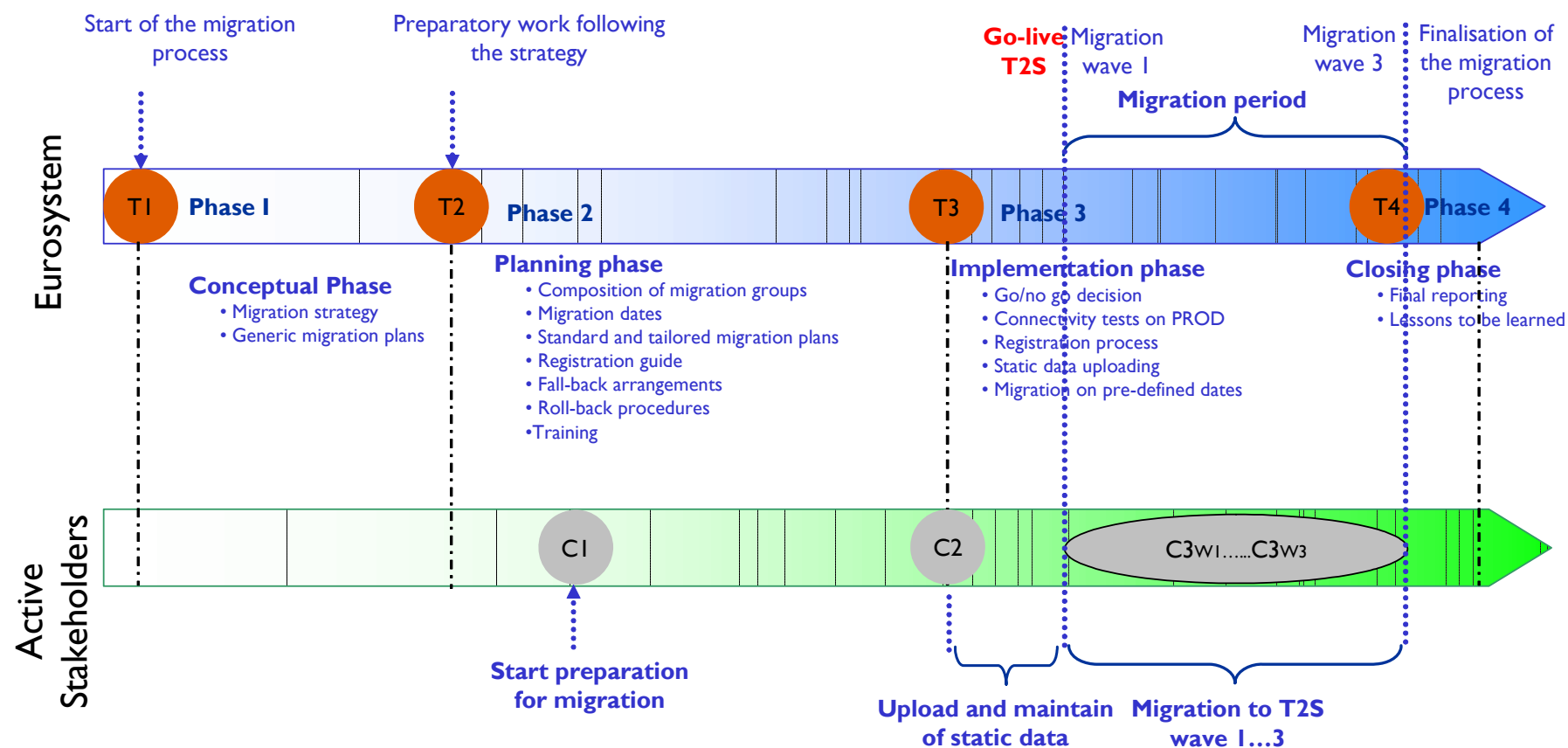
6.2 Responsibilities of the Connected NCB

During the closing phase, the Connected NCB shall provide feedback to the Eurosystem based on its experience gained during its migration in order to improve the migration of the next waves.

Currency Participation Agreement

Schedule 4 – Annex 1 – Migration milestones

ANNEX 1: Migration milestones



CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 5

T2S SERVICE DESCRIPTION

Currency Participation Agreement

Schedule 5 – T2S Service Description

Table of contents

1. T2S Service Description overview	1
1.1. Purpose of this note	1
1.2. Scope of the T2S Service Description	1
1.2.1. Within the scope of the T2S Service Description	1
1.2.2. Outside of the scope of the T2S Service Description	1
1.3. T2S Service Description and its relationship to other documents	2
2. Service delivery framework	3
2.1. Scope of T2S instrument	3
2.2. Scope of T2S instruction and transaction type	3
3. T2S SD: Overview T2S Services	5
4. T2S SD.SETT: Settlement services service class	7
4.1. T2S SD.SETT 010: Business validation service	7
4.2. T2S SD.SETT 020: Matching service	9
4.3. T2S SD.SETT 030: Allegement service	10
4.3.1. T2S DD.SETT 031: Settlement allegement service component	10
4.3.2. T2S SD.SETT 032: Cancellation allegement service component	11
4.4. T2S SD.SETT 040: Settlement sequencing service	11
4.5. T2S SD.SETT 050: Settlement posting service	12
4.5.1. T2S SD.SETT 051: Settlement eligibility check service component	12
4.5.2. T2S SD.SETT 052: Provisioning service component	12
4.5.3. T2S SD.SETT 053: Booking service component	14
4.6. T2S SD.SETT 060: Optimisation service	14
4.6.1. T2S SD.SETT 061: Technical netting and optimisation algorithms service component	15
4.6.2. T2S SD.SETT 062: Prioritisation service component	15
4.6.3. T2S SD.SETT 063: Partial settlement service component	16
4.6.4. T2S SD.SETT 064: Auto-collateralisation service component	17
4.7. T2S SD.SETT 070: Realignment service	20
4.8. T2S SD.SETT 080: Instruction recycling service	21
4.9. T2S SD.SETT 090: Instruction amendment service	21
4.10. T2S SD.SETT 100: Instruction cancellation service	22
4.11. T2S SD.SETT 110: Hold/release service	23

Currency Participation Agreement

Schedule 5 – T2S Service Description

4.12. T2S SD.SETT 120: Earmarking, blocking and reservation service	24
4.12.1. T2S SD.SETT 121: Earmarking service component.....	24
4.12.2. T2S SD.SETT 122: Blocking service component.....	24
4.12.3. T2S SD.SETT 123: Reservation service component	24
4.12.4. T2S SD.SETT 123: Common features of the earmarking, blocking and reservation service component	25
4.13. T2S SD.SETT 140: Conditional Security Delivery (CoSD) service	25
4.14. T2S SD.SETT 150: Linked instructions service	27
4.15. T2S SD.SETT 160: Corporate actions service	28
5. T2S SD.LIM: Liquidity Management Service Class	29
5.1. T2S SD.LIM 010: Liquidity transfer service	29
5.2. T2S SD.LIM 020: Limit management service	31
5.3. T2S SD.LIM 030: End of day (EOD) cash management service.....	33
5.4. T2S SD.LIM 040: Corporate action cash service.....	34
5.5. T2S SD.LIM 050: Cash blocking and reservation service.....	34
5.6. T2S SD.LIM 060: Liquidity monitoring service.....	35
5.7. T2S SD.LIM 070: Multiple liquidity provider service	36
6. T2S SD-STD: Common Static Data Management Service Class	38
6.1. T2S SD.STD 010: Common Static Data management service	38
6.1.1. T2S SD.STD 011: Insert service component.....	39
6.1.2. T2S SD.STD 012: Update service component	39
6.1.3. T2S SD.STD 013: Delete service component	39
6.1.4. T2S SD.STD 014: Reactivate service component	40
6.2. T2S SD.STD 020: Securities Reference Data service	40
6.3. T2S SD.STD 030: T2S Party data service	40
6.4. T2S SD.STD 040: Security Account data service.....	42
6.5. T2S SD.STD 050: Cash account data service	42
6.6. T2S SD.STD 060: T2S User data service	44
6.7. T2S SD.STD 070: Roles and privileges data service	44
6.8. T2S SD.STD 080: Restriction management service.....	45
6.9. T2S SD.STD 090: Attribute domain data service (market-specific attributes).....	47
7. T2S SD. INF: Information Management Service Class.....	48
7.1. T2S SD.INF 010: Status management services.....	48
7.2. T2S SD.INF 020: Report generation service	48
7.3. T2S SD.INF 030: Query service	50
7.3.1. T2S SD.INF 031: Query service for T2S Actor service component.....	50
7.3.2. T2S SD.INF 032: Query service for CSDs service component.....	51

Currency Participation Agreement

Schedule 5 – T2S Service Description

7.3.3. T2S SD.INF 033: Query service for Central Banks service component.....	51
7.3.4. T2S SD.INF 034: Query service for Payment Banks (liquidity providers) service component.....	51
7.3.5. T2S SD.INF 035: Settlement-related queries service component	51
7.3.6. T2S SD.INF 036: Cash balance-related queries service component	52
7.3.7. T2S SD.INF 037: Common Static Data-related queries service component.....	53
8. T2S SD. CON: Connectivity / Communication Service Class	54
8.1. T2S SD.CON 010: Messaging services	54
8.1.1. T2S SD.CON 011: Push messaging service component	55
8.1.2. T2S SD.CON 012: Pull messaging service component	56
8.2. T2S SD.CON 020: Technical validation services	56
8.3. T2S SD.CON 030: Connectivity types services	57
8.3.1. T2S SD.CON 031: Application to Application (A2A) service component	57
8.3.2. T2S SD.CON 032: User to Application (U2A) service component	57
8.4. T2S SD.CON 040: Information security management services	57
8.4.1. T2S SD.CON 041: Authentication service component.....	57
8.4.2. T2S SD.CON 042: Authorisation service component	58
8.4.3. T2S SD.CON 043: 4-eyes principle service component.....	58
8.5. T2S SD.CON 050: Message sequencing services	59
8.6. T2S SD.CON 060: Direct connectivity services	59
8.7. T2S SD.CON 070: Routing services	59
9. T2S SD. SUP: Operations and support service class	61
9.1. T2S SD.SUP 010: Business application configuration services.....	61
9.1.1. T2S SD.SUP 011: T2S Calendar service component	61
9.1.2. T2S SD.SUP 012: T2S Settlement Day service component	62
9.2. T2S SD.SUP 020: Operational monitoring services.....	63
9.3. T2S SD.SUP 030: Business continuity management services	64
9.4. T2S SD.SUP 040: Disaster recovery and crisis management services.....	64
9.5. T2S SD.SUP 050: Archiving services	65
9.6. T2S SD.SUP 060: T2S service desk services	65
9.7. T2S SD.SUP 070: Service Level management services	66
9.8. T2S SD.SUP 080: Invoicing services	66
9.8.1. T2S SD.SUP 081: T2S invoicing to CSDs and Central Banks service component...	67
9.8.2. T2S SD.SUP 082: CSDs / Central Banks invoicing support service component	67
9.9. T2S SD.SUP 090: Change and Release Management services.....	68
9.9.1. T2S SD.SUP 091: Change Management service component.....	68
9.9.2. T2S SD.SUP 092: Release Management service component.....	70

Currency Participation Agreement

Schedule 5 – T2S Service Description

9.10. T2S SD.SUP 100: Test and training services 71

9.10.1. T2S SD.SUP 101: Testing service component 71

9.10.2. T2S SD.SUP 102: Training service component..... 71

Currency Participation Agreement

Schedule 5 – T2S Service Description

1. T2S Service Description overview

1.1. Purpose of this note

This note provides a common base for the description of T2S Services, especially pertaining to the Framework Agreement and to the Currency Participation Agreement.

This T2S Service Description for the Operational Phase of T2S focuses on:

(1) providing a common structure for the services that T2S will deliver, i.e. settlement services, liquidity management, Common Static Data services, information services, connectivity services, operational and support services as well as the individual services;

(2) the content of the service from the T2S Users' perspective, i.e. what services the T2S Users will receive, and the business perspective of the interchanges between T2S and the T2S Users;

(3) the boundaries of the services T2S will deliver to its users, i.e. what is within the scope of T2S Services, and what is outside of the scope of T2S Services.

1.2. Scope of the T2S Service Description

1.2.1. Within the scope of the T2S Service Description

T2S is a technical solution to support Central Securities Depositories (CSDs) by providing core, borderless and neutral settlement services. The objective is to achieve harmonised and commoditised settlement in Central Bank Money (CeBM) in euro and other eligible currencies for substantially all securities in Europe.

The Eurosystem manages and operates the business application and the technical solution providing the T2S Services, this service provision by the Eurosystem is hereafter referred to simply as "T2S". The Contracting CSD will maintain full control over the business and contractual relationship with its customers.

The T2S Service Description describes all services T2S will deliver for the T2S Operational Phase including all services delivered to all Participating CSDs, to all Directly Connected Parties (DCPs), and to all participating Central Banks (CBs, comprised of all euro area NCB and all non-euro area NCB participating in T2S), once T2S is in full operation. The T2S Service Description itself is subject to the rules and procedures established for all Annexes of the Framework Agreement.

1.2.2. Outside of the scope of the T2S Service Description

This Service Description describes only the services T2S will deliver during the Operational Phase. The services delivered by the T2S Programme during the Development Phase and the

Currency Participation Agreement

Schedule 5 – T2S Service Description

- 32 Migration Period are not described in this note¹.
- 33 The Service Description furthermore provides background and relevant information with regard
34 to:
- 35 a. The Service Level Agreement (SLA²), which will contain all Key Performance
36 Indicators (KPIs), the latter will not be defined nor referenced in the Service
37 Description.
 - 38 b. The T2S technical architecture is not described in this Service Description and nor are
39 the technical details required to establish the connectivity to T2S.

40 1.3. T2S Service Description and its relationship to other documents

41 The Service Description is a high level description of the Services T2S delivers during the
42 Operational Phase thereby identifying the scope of the T2S Services and as such complementing
43 the T2S Scope Defining Set of Documents.

44 Since, the Service Description is a high level description, in some parts of the Service
45 Description it has been indicated in which documents, e.g. Business Process Description, User
46 Handbook, Manual of Procedures (MoP), further and more detailed information can be found.

47

¹ Details on the T2S Programme can be found in the Framework Agreement and its relevant Schedules

² The SLA is a separate document linked closely to this Service Description. The Service Description describes the services T2S clients receive, the SLA defines the relevant KPIs, as well as their control and reporting procedures. Therefore, these two documentations are closely linked and harmonised

Currency Participation Agreement

Schedule 5 – T2S Service Description

2. Service delivery framework

2.1. Scope of T2S instrument

In principle, T2S covers all securities that comply with the following eligibility criteria, i.e. that:

1. have an ISIN code, as instrument identifier;
2. can be settled via a CSD in T2S;
3. can be settled in book-entry form; and
4. are fungible (from a settlement processes perspective).

Securities that do not fall within the scope of any connected CSD are not part of T2S either.

T2S can settle only securities that are compliant with the above criteria 1 to 3, certain securities, compliant with the first three criteria, but not compliant with criteria 4 (non-fungible from a settlement perspective), may still be entered in and processed by T2S.

T2S can settle most categories of securities in a standardised settlement process. For example, multilateral instructions can be settled using the standard T2S functionalities, no specific processing is required as T2S allows instruction linkages.

2.2. Scope of T2S instruction and transaction type

The instruction types covered by T2S are the following:

- Settlement Instruction
- Liquidity Transfer
- Settlement Restriction
- Amendment Instruction
- Cancellation Instruction
- Hold / Release Instruction

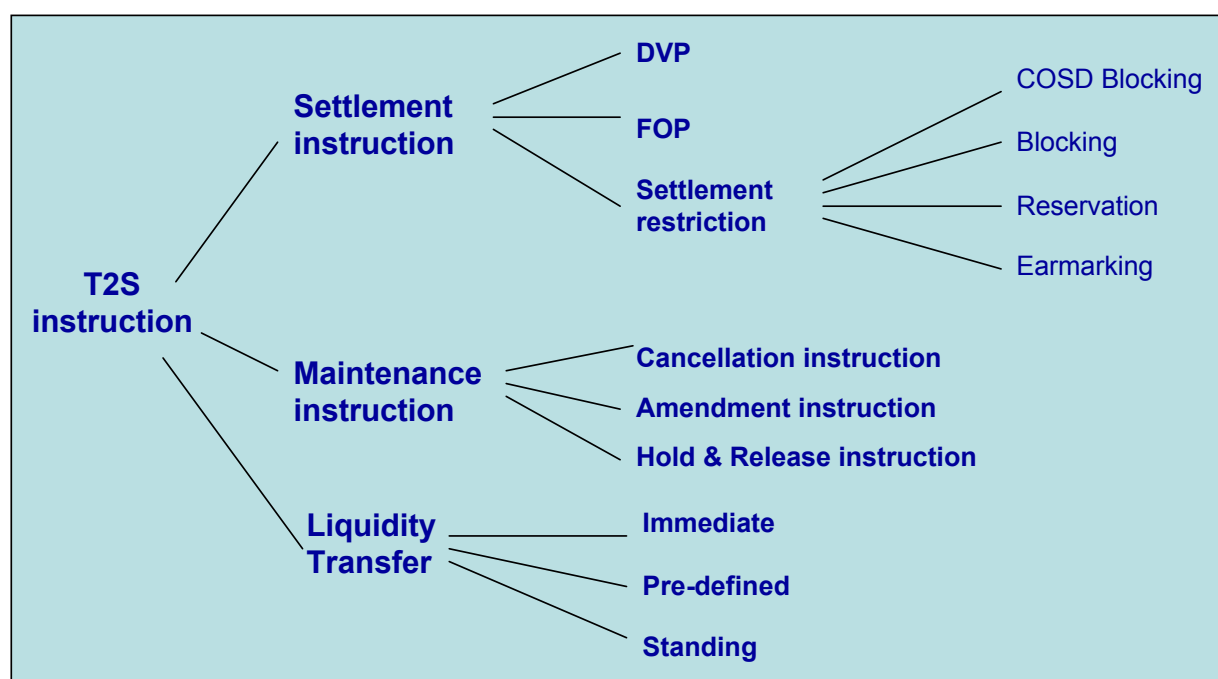
T2S settles only settlement transactions with a CeBM cash leg (or no cash leg), it will not provide settlement in Commercial Bank Money (CoBM). T2S provides services for securities settlement and the related cash settlement using a number of transaction types:

- FOP (Free of Payment) consists of DFP (deliver free of payment) and RFP (receive free of payment). In both cases, securities are delivered / received without payment being made.

Currency Participation Agreement

Schedule 5 – T2S Service Description

- DVP (Delivery versus Payment) and RVP (receive versus payment) define an exchange of securities for cash. DvP and RvP are both securities settlement mechanisms which link a securities transfer and a funds transfer in such a way as to ensure that delivery occurs if - and only if - the corresponding payment occurs.
- DWP (Deliver with Payment) is a type of instruction and settlement mechanism, specifying the delivery of securities together with a cash payment. For example, trade netting by a Central Counterparty (CCP), as an authorised CSD participant, may result in such instructions.
- PFOD (Payment Free of Delivery) defines an exchange of cash without the delivery of securities.



Currency Participation Agreement

Schedule 5 – T2S Service Description

3. T2S SD: Overview T2S Services

T2S deploys a flexible hierarchical party model to allow CSDs and Central Banks to manage their accounts and parties in an efficient way. Roles, including some of the key responsibilities, are allocated in line with the differentiation into

- a securities' perspective (CSDs), and
- a cash accounts' perspective (Central Banks)

The structure of this Service Description document is based on the above mentioned differentiation between the securities perspective (CSDs) and the liquidity management perspective (Central Banks)³:

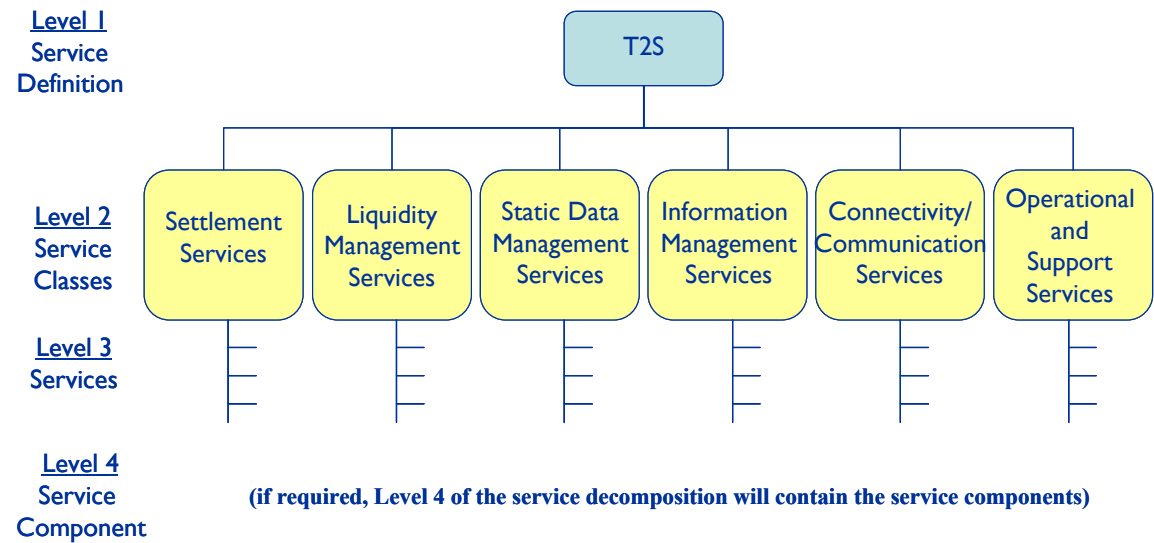
- CSDs are the gateways through which various market parties can access T2S. Depending on their needs, a CSD's parties may continue to contract with one or more CSDs for the settlement of their trades and collateral operations (and those of their customers) in T2S. Each CSD will set up and maintain its own Security Accounts' structure in T2S. Each CSD is responsible for setting up and maintaining all CSD Static Data relating to the settlement activities of its participants. A T2S Actor settling through more than one CSD in T2S will have Security Account(s) with each of the CSDs it uses for settlement.
- All Central Banks whose currencies are available for settlement in T2S have the responsibility to set up and to maintain Dedicated Cash Accounts (DCAs) in T2S if they have concluded a relevant agreement with eligible entities. Furthermore, these Central Banks are also responsible for setting up and maintaining all Central Bank Static Data relating to the DCAs of its members. Cash settlements in T2S take place exclusively on T2S DCAs. Only a CeBM account opened on the books of a Central Bank whose currency is available for settlement in T2S may serve as a T2S DCA.

The totality of the T2S Services (level 1 of the service hierarchy description) are broken down into service classes (level 2 of the service hierarchy) and services (level 3). If the latter (level 3) contain functionally diverse components, level 4 of the service hierarchy describes these service components:

³ A more detailed description of the account structures deployed by T2S can be found in the User Detailed Functional Specifications (UDFS), chapter 1.2.6. Accounts structure and organisation

Currency Participation Agreement

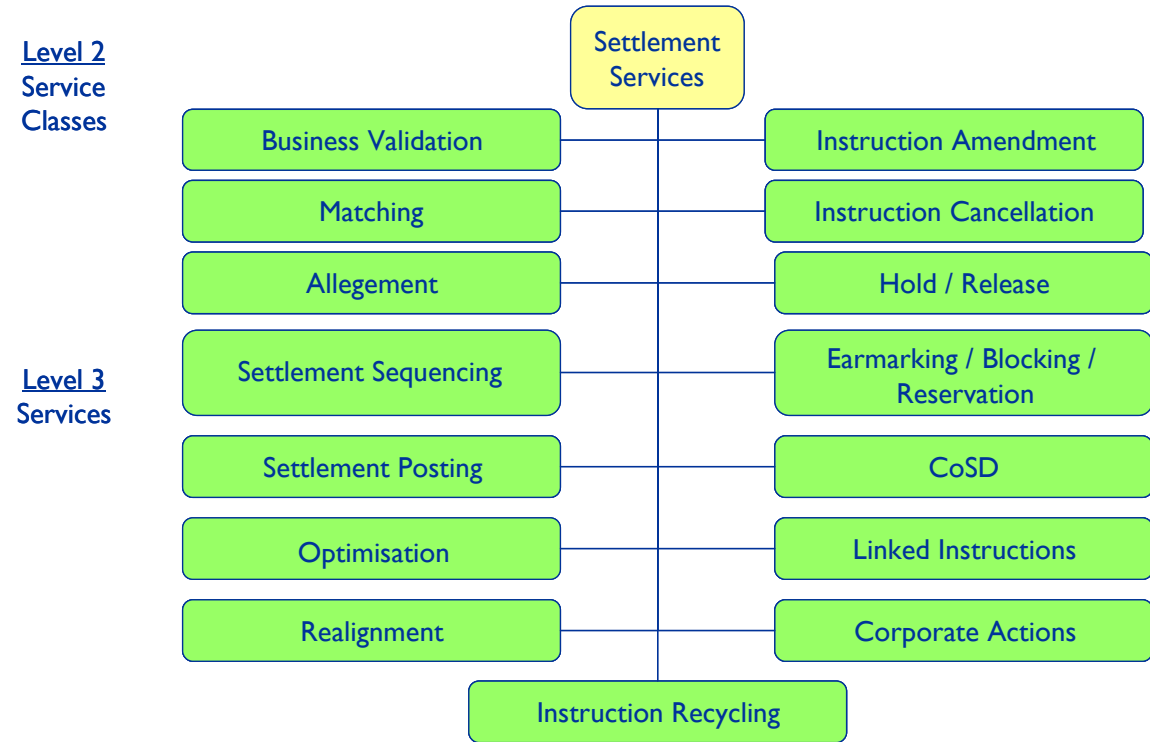
Schedule 5 – T2S Service Description



Currency Participation Agreement

Schedule 5 – T2S Service Description

4. T2S SD.SETT: Settlement services service class



4.1. T2S SD.SETT 010: Business validation service

Communication to and from T2S is message-based. Each message contains only one instruction. For a message containing one instruction with the status “already matched”, T2S generates for further T2S processing two instructions.

With the exception of the additional information fields as described below, the business validation service ensures that the content of the received message is valid, i.e. contains all required fields and complies with the rules defined for the content of these fields. These consistency checks ensure that the message can be processed by T2S as intended and is consistent with the relevant rules for this message stored in Common Static Data.

Business validation in T2S consists of two different types of validations:

1. Contextual checks, that is when the validation of one field is dependent on the content of another field, e.g. reference / Common Static Data or other data provided via the Graphical User Interface (GUI);
2. Event-driven checks, e.g. settlement date change, cancellation instruction arriving.

All incoming messages are validated when they enter T2S and re-validated (as are all pending instructions) at the start of a new T2S Settlement Day. Updates of the Common Static Data used for business validation purposes result in revalidation of all relevant instructions. T2S assigns a

Currency Participation Agreement

Schedule 5 – T2S Service Description

status of matched/unmatched at the same time that the instruction is validated.

Messages sent by a T2S Actor to T2S may contain Additional Information Fields which T2S Actors may use for their own purposes. This additional information is neither required for nor related to any T2S process and is therefore neither validated nor further processed within T2S. T2S stores this additional information together with the information it has processed.

Once T2S has successfully validated the compliance of the data - contained in the instruction with the data stored in Common Static Data relevant for the business validation process - the instruction is routed to the relevant processing module of T2S. If settlement-related process indicators are specified by the instructing T2S Actor, T2S checks that they are valid for the type of instruction and the instructing T2S Actor in question. The settlement-related process indicators are used to perform certain actions in the settlement process relating to an instruction. T2S Actors may use the non-settlement-related link indicator “INFO” to link instructions for information purposes.

In the event of instructions being held/released, cancelled, amended or that make use of a previous settlement restriction, T2S verifies that the previous or related reference exists. T2S performs the business validation on the maintenance/new instruction to ascertain that it is valid and consistent with the previous or related instruction. After identifying a validation error, T2S continues to validate as far as possible (taking into account potential interdependencies between the validated data). If validation errors are found, T2S reports all of them in a single message to the T2S Actor and rejects the instruction.

After successful validation, T2S stores the instruction, assigns the corresponding statuses and informs the instructing T2S Actor and its CSD of the validation result, depending on their message subscription preferences. Once validated:

- settlement instructions that require matching are forwarded for matching,
- maintenance instructions are forwarded to the maintenance functionality,
- settlement restrictions are forwarded for settlement only on their Intended Settlement Date (ISD),

while all other instructions are forwarded directly to the settlement functionality.

T2S must support the CSDs and Central Banks by offering the capability to provide specific validations and processing of messages to fulfil legal, regulatory and supervisory requirements in the markets that they service. T2S therefore allows the CSDs and Central Banks to define their own restriction types.

T2S triggers a revalidation of all relevant recycled instructions when settlement-related Common Static Data change. T2S cancels instructions that do not pass the revalidation successfully and informs both the CSD and the instructing T2S Actor of the cancellation.

T2S validates all incoming and recycled instructions against rules and parameters defined in the

Currency Participation Agreement

Schedule 5 – T2S Service Description

Common Static Data for the configuration of restriction types. T2S thus checks and validates whether there are any applicable restrictions. If there are, and depending on the type of the restriction, T2S either rejects it or puts the instruction on hold until it is released for further processing.

4.2. T2S SD.SETT 020: Matching service

The settlement instruction Matching service in T2S compares the settlement details provided by the buyer of securities with those provided by the seller of the securities in order to ensure that both parties agree on the settlement-related terms of an instruction.

T2S provides real-time matching, compliant with the rules of the European Securities Services Forum (ESSF)/European Central Depositories Association (ECSDA), throughout the operating day (except during the Maintenance Windows). Matching in T2S is mandatory for cross-CSD settlements. Matching for intra-CSD settlements may take place in T2S or in the legacy systems of the CSD.

T2S only attempts to match validated settlement instructions that entered T2S as “unmatched”. If matching is successful, T2S assigns the Match status “matched” to the settlement instructions and informs the T2S Actor of the matching of their settlement instruction. If T2S finds no corresponding unmatched counterpart instruction for the unmatched settlement instruction, the Match status remains unchanged and T2S sends no information to the instructing T2S Actor.

T2S waits for the missing counterpart instruction for a predetermined period before generating an allegation message for the counterpart in the unmatched instruction. T2S sends the allegation message to the relevant counterparty only if the counterpart has subscribed to receive allegation messages.

T2S attempts to match the instruction for 20 working days (T2S calendar) after the Intended Settlement Date or the date of the last status change, in accordance with the ESSF/ECSDA recommendation. After 20 working days, T2S cancels the underlying instruction and informs the relevant T2S Parties.

T2S matches the settlement cash amount with a certain tolerance level (i.e. in the event that there is no perfect match). The tolerance amount has two different bands per currency, depending on the counter value, in line with ECSDA rules. The general tolerance amount proposed by ECSDA for matching the settlement amount field in euro is currently €25 when the counter value is above €100,000 or €2 when it is €100,000 or less. Once T2S has matched two instructions with a difference in the settlement amount that is less than the tolerance amount, T2S shall settle the instruction with the seller’s settlement amount.

T2S matches different types of fields:

1. Mandatory matching fields

Currency Participation Agreement

Schedule 5 – T2S Service Description

Mandatory matching fields are the instruction fields that must have the same values for T2S to determine that two settlement instructions match and are eligible for settlement

2. Non-mandatory matching fields

T2S supports two types of non-mandatory matching fields:

a. Additional matching fields are fields that are initially not mandatory but become mandatory matching fields when either one of the counterparts to the settlement provides a value for them in its instruction. T2S cannot match a filled-in additional matching field with a field with no value (null / zero value).

b. Optional matching fields are fields that are initially not mandatory:

i. If only one T2S Party provides content in an optional matching field, T2S may match with a field with no value (null / zero value).

ii. If both settlement counterparts provide a value for the same field in their instructions, then the optional matching field becomes mandatory for matching

4.3. T2S SD.SETT 030: Allegement service

T2S uses allegement messages to inform counterparties that relevant information is missing. An allegement message advises an account owner that another T2S Actor has issued instructions against its account for which the account owner has no corresponding instruction in the Securities Settlement System. Allegements will be sent only if the counterparty has subscribed to receive such messages. T2S alleges a T2S Actor when a settlement instruction or a cancellation instruction is missing. Allegement messages may be used for any unmatched instruction that requires matching.

4.3.1. T2S DD.SETT 031: Settlement allegement service component

After the first unsuccessful matching attempt, T2S waits for the missing counterparty instruction for a predetermined period of time before generating an allegement message. If the instruction is still unmatched at the end of this period, an allegement message is generated. T2S sends an allegement message for the unmatched instruction only if the counterparty has subscribed to receive allegement messages.

T2S supports two standard delay periods for sending allegements to the counterparties of the unmatched instruction.

- “Allegement from first unsuccessful matching attempt”, as the standard delay period from the first unsuccessful attempt to match a settlement instruction
- “Allegement before Intended Settlement Date”, as the standard delay period measured backwards from the FOP cut-off time on the ntended Settlement Date.

Currency Participation Agreement

Schedule 5 – T2S Service Description

T2S sends out the allegement at the earliest point in time between the two standard delay periods. T2S calculates the standard delay period in hours and minutes.

If the previous allegement message is no longer valid, T2S sends an allegement removal or an allegement cancellation. An allegement cancellation means the cancellation of an allegement message sent previously, due to a cancellation of the settlement instruction by the sender. An allegement removal acknowledges that an allegement message sent previously is no longer valid, because T2S has in the meantime received the missing instruction from the alleged T2S Party.

4.3.2. T2S SD.SETT 032: Cancellation allegement service component

T2S also provides allegement services in the event of a missing counterpart cancellation instruction, via a status advice message. T2S sends out the cancellation allegement without waiting for any predetermined period to have elapsed. The cancellation instruction remains pending until it matches with a valid counterpart cancellation instruction.

If the cancellation allegement sent via status advice is no longer valid because the revalidation of the settlement instruction has been unsuccessful, the counterparty has responded with a cancellation instruction, or the underlying matched settlement instructions have been settled. T2S sends only the settlement confirmation (in case of settled underlying instructions) and status advices (in case of cancelled underlying instructions) to both parties.

T2S does not send a status advice to the counterparty to communicate cancellation of the previous cancellation allegement.

4.4. T2S SD.SETT 040: Settlement sequencing service

Sequencing is the pre-determined order defined in T2S in which instructions are submitted for settlement.

During the Real Time settlement, instructions are processed in the order in which they arrive for settlement.

For night-time settlement, sequencing refers to the order in which the settlement of certain sets of instructions is attempted in T2S. Settlement instructions are processed in a particular sequence, (i.e. in a fixed order) to avoid the use of security positions and/or cash resources for any transaction other than those submitted in the sequence concerned. T2S runs two settlement cycles with predefined settlement sequences during the night. In each settlement sequence, T2S will perform a settlement attempt for those settlement transactions selected based on the eligibility criteria of the sequence including:

- all new instructions with the current ISD entered into T2S until the launch of the current settlement sequence. These instructions include, for instance, settlement instructions

Currency Participation Agreement

Schedule 5 – T2S Service Description

274 providing liquidity via lending (securities lending) that are intended to settling
275 instructions that could not be settled in an earlier settlement attempt;

276 ▪ all recycled instructions that could not be settled in an earlier settlement attempt. Such
277 recycled instructions include all instructions that could not be settled in the previous
278 settlement attempts, including FOP rebalancing and operations with Central Banks that
279 could not be settled during the first settlement cycle, trading-related instructions, and
280 corporate action instructions.

281 **4.5. T2S SD.SETT 050: Settlement posting service**

282 The transactions are settled in T2S by booking the cash and securities debits and credits in
283 accordance with the relevant instructions on the relevant T2S DCAs and Security Accounts
284 (either accounts identified in the instructions being settled or accounts predetermined by default).

285 The settlement posting service consists of three service components:

- 286 ▪ Settlement eligibility check
- 287 ▪ Provisioning
- 288 ▪ Booking

289 **4.5.1. T2S SD.SETT 051: Settlement eligibility check service component**

290 The settlement eligibility check is the final validation before settlement, as it is necessary to
291 identify the appropriate instructions for the final settlement process. The eligibility check
292 considers

- 293 ▪ the Intended Settlement Date (ISD),
- 294 ▪ the potential blocking of the T2S Actor, Security Account, security or T2S DCA from
295 settlement and
- 296 ▪ whether or not the instruction should be put on hold,
- 297 ▪ whether the instruction is linked to other instructions,

298 before an instruction is submitted to the provisioning and booking process. T2S forwards for
299 settlement only those instructions that meet the validation rules/criteria. Settlement instructions
300 which do not meet the validation rules/criteria remain unsettled and are not moved forward when
301 there is any pending intraday restriction.

302 **4.5.2. T2S SD.SETT 052: Provisioning service component**

303 The provisioning or provision-check ensures that the eligible transaction can be forwarded for
304 booking (and thereby finally settled) if, and only if, the booking does not cause the account

Currency Participation Agreement

Schedule 5 – T2S Service Description

balances of the relevant securities and the T2S DCA to become negative, with the exception of T2S Central Banks own accounts, T2S transit accounts and Issuer CSD balance accounts, which may have negative balances.

The provision-check covers both settlement legs of the relevant transaction (e.g. the cash and securities legs for a DvP transaction). T2S does not consider reserved/blocked securities quantities or cash amounts on the relevant accounts as available for the provision-check, unless the instruction being settled refers to the initial reservation/blocking instruction.

When an individual external guarantee limit, unsecured credit limit or auto-collateralisation limit is defined by the relevant Central Bank (or by the relevant Payment Bank for the settlement of the instructions of the T2S parties for which it provides cash settlement services), T2S ensures that the net cash debit resulting from the booking of any instruction(s) of the relevant T2S parties does not exceed the unused part of this external guarantee limit, unsecured credit limit or auto-collateralisation limit.

T2S performs the provision check in the following sequence:

1. Provision check of available securities position on the Security Account (only for the settlement of securities)
2. Provision check for the T2S DCA and auto-collateralisation (if required)
3. Provision check on the external guarantee limit
4. If auto-collateralised: provision check on the auto-collateralisation limit of the client of the Payment Bank
5. Provision check on the unsecured credit limit

When several instructions are submitted together in a settlement attempt, the provision-check considers the final net balance resulting from the booking of all the relevant instructions (and not from each and every instruction). In other words, in its provision-check T2S takes into account the technical netting effect.

If the provision-check on the net balance is not satisfactory, T2S identifies the instruction(s) responsible for the provision-check's failure.

These instructions are either:

- submitted for an auto-collateralisation process if the fail originates from a lack of cash; or,
- submitted for partial settlement (only as a last resort, i.e. if auto-collateralisation is not possible or not sufficient and only if the instructions are eligible and are within the partial settlement window) if the fail originates from a lack of securities or from a required substitution of collateral.

Currency Participation Agreement

Schedule 5 – T2S Service Description

4.5.3. T2S SD.SETT 053: Booking service component

Final booking is only posted if the provision-check on the accounts (securities and T2S DCAs) referred to in the settlement instructions (or on the accounts predetermined by default) is satisfactory.

Once booked by T2S on the T2S parties' Security Accounts and T2S DCAs, cash and securities debits and credits are final, i.e. irrevocable and unconditional. The booking must not be conditional on any external event (e.g. such as another booking in the payment or settlement system/arrangement of an external Central Bank registrar, commercial bank or CSD), this means that any such condition must have been resolved before the booking in T2S is undertaken.

Because bookings are final, T2S will not automatically unwind credit or debit even if it was done incorrectly.

Each and every transaction is booked on a gross basis. This is without prejudice to the use of the technical netting effects in the provision check when several instructions are submitted together for settlement (either for optimisation purposes or because they are linked by a T2S Actor).

4.6. T2S SD.SETT 060: Optimisation service

T2S optimisation services is intended to determine the optimum balance between maximising the volume and the value of the settlement with the available securities, in order to minimise the number and value of unsettled instructions at the end of the night-time settlement process as well as to minimise the number and value of fails at the end of the Settlement Day.

Optimisation procedures are specific processes aimed at increasing settlement efficiency. Such processes detect and resolve settlement gridlocks, and perform technical netting of obligations in cash and securities, with a view to settle new instructions as well as instructions that could not be settled when previously attempted. Optimisation procedures are available both during the night-time settlement window and during the Real Time Settlement. When several unsettled instructions are optimised together and a chain of instructions is submitted for settlement, T2S includes the securities and cash received during the process of settling the relevant chain of instructions in the optimisation process.

During the night-time settlement window, the T2S optimisation procedure covers all instructions submitted for settlement (either new instructions or recycled instructions that could not be settled when previously attempted).

During the Real Time Settlement, T2S optimisation procedure runs in parallel to real-time settlement processes and covers instructions that could not be settled when previously attempted.

When necessary, T2S combines the four optimisation procedures described below (technical netting/ optimisation algorithms, prioritisation, partial settlement and auto-collateralisation).

Currency Participation Agreement

Schedule 5 – T2S Service Description

4.6.1. T2S SD.SETT 061: Technical netting and optimisation algorithms service component

The technical netting is intended to limit the resources necessary for the settlement of a set of instructions submitted together for settlement. Without prejudice to the fact that booking takes place on a gross basis, T2S reduces, through technical netting, the final net balance to be credited and debited on Security Accounts and/or Dedicated Cash Accounts. When performing its provision-check, T2S considers the final net balance that results from the booking of all the instructions submitted together for settlement (and not that resulting from each and every individual instruction).

During the night-time settlement window, T2S submits all eligible instructions for settlement and optimises all these instructions together. During day-time, real-time settlement optimisation, optimisation algorithms identifying chains of instructions (e.g. such as empty circles, back-to-back instructions) are used to resolve gridlock situations, and so increase the volume and value of settlement and hence, to reduce the value and volume of pending instructions.

4.6.2. T2S SD.SETT 062: Prioritisation service component

Optimisation procedures will take into account the four different priority levels of instructions. T2S automatically assigns predetermined levels of priority for certain specific instructions identified in the Common Static Data. The four different levels of priority identified are:

1. Reserved priority: Only Participating CSDs and Central Banks can assign a “reserved priority” for specific instructions such as intraday corporate actions or certain Central Banks’ specific operations related to the provision/ reimbursement of their credit operations.
2. Top priority: T2S automatically assigns top priority to transactions of trading platforms (MTFs, stock exchanges, etc.) with and without CCP and OTC instructions with CCP. To that end, the parameters for identifying transactions (to which this top priority level must be assigned) are predetermined in Common Static Data and apply by default to all the relevant transactions. T2S does not allow top priority to be assigned to any other category of transactions (either by default or at a transaction level)..
3. High priority: T2S Actors can assign high priority to their settlement instructions; or
4. Normal priority: T2S assigns normal priority to all other instructions, but enables T2S parties to assign them a high priority on an instruction-by-instruction basis.

For levels 3 and 4 only, the instructing T2S Actor may change the priority level of an instruction (only the deliverer may change normal priority to high priority or high priority to normal priority).

T2S optimises and recycles settlement instructions in accordance with their priority levels in such a way that if several instructions compete for use of the same securities and/or cash resources, for

Currency Participation Agreement

Schedule 5 – T2S Service Description

settlement purposes preference is given to the instruction with the highest level of priority. In addition to the priority level, T2S also considers the ISD of the instruction so as to favour the settlement of instructions with the earliest settlement date and thus avoid instructions with low priority not being settled.

For Real Time Settlement, the prioritisation applies only to instructions to be recycled in the settlement queue (i.e. failed instructions). Any increase of a position triggers an optimisation for the International Securities Identification Number (ISIN) concerned. T2S recycles instructions if there is insufficient position.

Furthermore, during the Real Time Settlement, the priority level is taken into account by the settlement procedure only for instructions that failed to settle in a previous settlement attempt. These are subsequently submitted for recycling and optimisation procedures.

4.6.3. T2S SD.SETT 063: Partial settlement service component

T2S uses partial settlement for instructions that could not be settled due to the lack of securities providing the settlement instruction fulfils all criteria for partial settlement. A lack of cash does not trigger partial settlement. Instructions linked by T2S Actors are excluded from partial settlement.

The partial settlement procedure is used for all T2S instructions, unless one of the counterparts indicates at instruction level that partial settlement is not allowed (partial indicator set to no/false), and if the following conditions are met:

- the partial settlement threshold criteria are met, set for both securities and cash, and defined as part of the Common Static Data, and
- the partial settlement window is active.

When submitting an unsettled instruction for partial settlement, T2S attempts to settle the maximum quantity of securities available on the Security Account of the seller, taking into account the threshold chosen by the counterparts.

Once partial settlement has been invoked, T2S allows a duly authorised Actor to modify only the priority of the instruction, or to hold, to release or to cancel the pending part of a partially settled instruction. When an instruction is partially settled, T2S does not automatically cancel the original instruction. T2S keeps the original instruction and updates in accordance with the partial settled volumes in the status management.

Reverse collateral instructions are not subject to partial settlement.

T2S uses its own partial settlement parameter to activate and de-activate partial settlement as part of the continuous optimisation process. T2S allows the definition of several T2S parameters for activating and deactivating the partial settlement procedure during the Night-time and Day-time Settlement Periods. The T2S partial settlement parameter defines at which moment in time or

Currency Participation Agreement

Schedule 5 – T2S Service Description

444 based on which event T2S activates or de-activates a partial settlement procedure.

445 In order to minimise fails due to a lack of securities, T2S allows partial settlement in specific
446 time windows, a predefined period before the end of Real Time Settlement and at the end of the
447 last night time cycle during the night-time settlement. T2S submits to partial settlement all
448 eligible instructions that failed to be settled in a previous attempt during the night and deactivates
449 the partial settlement functionality at the closure of the Night-Time Settlement Period. T2S
450 submits at least once all those instructions for partial settlement that it has identified as eligible
451 for partial settlement before the partial settlement procedure is deactivated.

452 T2S informs the CSD and/ or the DCP when partial settlement occurs, depending on the message
453 subscription preferences.

454 **4.6.4. T2S SD.SETT 064: Auto-collateralisation service component**

455 T2S provides auto-collateralisation functionality during the whole T2S settlement period in order
456 to facilitate the settlement of underlying securities-related instructions that would fail to settle
457 due to a lack of cash on a Dedicated Cash Account (DCA) and/or insufficient external guarantee
458 headroom on a Credit Memorandum Balance (CMB)⁴. T2S provides the auto-collateralisation
459 service on the basis of the list of eligible collateral, relevant prices and limits provided by the
460 Central Banks and Payment Banks.

461 The auto-collateralisation functionality with Central Banks and with Payment Banks is available
462 to eligible T2S parties as defined in Common Static Data, provided that auto-collateralisation
463 headroom is available. T2S triggers auto-collateralisation with Central Banks in case of lack of
464 cash on the T2S DCA of the Payment Bank to which the settlement instruction is referring. T2S
465 triggers auto-collateralisation with a Payment Bank (client-collateralisation) in of the event of
466 insufficient external guarantee headroom on the CMB of a client of the Payment Bank, that owns
467 the Security Account to which the settlement instruction refers.

468 T2S allows collateral provided for intraday credit provision in CeBM through auto-
469 collateralisation to be pledged or transferred to a separate account (in accordance with the legal
470 framework chosen by the relevant Central Bank). Collateral provided for auto-collateralisation
471 with Payment Banks can only be transferred to a separate account of the Payment Bank. Intraday
472 credit granted in CeBM through auto-collateralisation can be used only for the settlement of the
473 underlying instructions. The credit amount provided is equal or less than the collateral value of
474 the securities used as collateral, the collateral value being the price provided for a certain security
475 multiplied by the number or nominal amount of the security concerned.

476 An intraday credit provision through auto-collateralisation is always fully collateralised in T2S

⁴ Further described in the relevant chapter of the Liquidity Management Services below.

Currency Participation Agreement

Schedule 5 – T2S Service Description

- Either with securities already held by the buyer via collateral-on-stock, or
- Through collateral-on-flow via the eligible securities that are being purchased.

These securities must be recognised as eligible collateral by Central Banks or Payment Banks and the relevant Payment Bank or its clients must earmark them for their use as collateral. Duly authorised T2S Actor may also earmark a Security Account from which securities may be used for auto-collateralisation.. The security account holding the earmarked securities must be linked to the DCA opened by the Central Bank.

In order to provide intraday credit through auto-collateralisation in T2S to one or several eligible Payment Banks, each national Central Bank has to open a T2S Central Bank cash account on which all debits corresponding to its intraday credit provisions through auto-collateralisation will be posted. The T2S central bank cash account is allowed to have a negative cash balance.

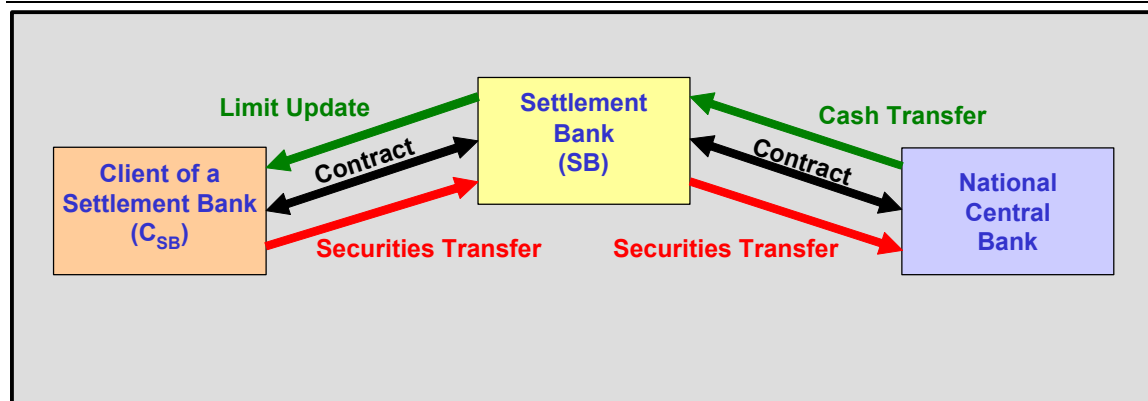
The Payment Banks must open one Security Account (via their CSD) dedicated to auto-collateralisation for each of their clients. T2S uses these accounts when transferring the collateral from the client to the Payment Bank. If allowed by the respective Central Bank, the Payment Banks may use the securities positions received during the client-collateralisation procedure as collateral for auto-collateralisation procedure with the Central Banks. In such cases, the Payment Bank has the option to either earmark the Security Accounts for auto-collateralisation purpose only or earmark specific securities positions in the Security Account for auto-collateralisation. The Payment Bank will be able to use such Security Accounts for both (a) receiving collateral in case of client-collateralisation (b) and providing collateral for auto-collateralisation with Central Banks.

Each national Central Bank is required to determine in Common Static Data the collateralisation procedure for which it opts, i.e. (i) transfer to an account opened in the Central Bank's name, or (ii) transfer to an account pledged in its favour, or (iii) reservation of securities. This must be done for all eligible Payment Banks to which the relevant Central Bank provides intraday credit through auto-collateralisation.

For each of their Security Accounts, T2S parties may indicate via the T2S earmarking service whether T2S may use securities from that account when generating auto-collateralisation operations with Central Banks or Payment Banks on a specific T2S DCA. When such a link exists between a Security Account and a T2S DCA, T2S will use securities from that account in auto-collateralisation operations with either Central Bank or the Payment Bank (acting as credit provider), depending on the earmarking options.

Currency Participation Agreement

Schedule 5 – T2S Service Description



T2S generates auto-collateralisation operations only when they allow the settlement of the underlying settlement transaction(s) and when sufficient headroom exists on the auto-collateralisation limit. When triggering auto-collateralisation, T2S also considers the unsecured credit limit headroom available that could complement the auto-collateralisation operation in the event of auto-collateralisation with Payment Banks (client-collateralisation). Each Central Bank and Payment Bank is able to increase or decrease at any moment of the Settlement Day the auto-collateralisation limit of an eligible Payment Bank or client of the Payment Bank.

T2S submits auto-collateralisation instructions for settlement on an all-or-none basis together with the underlying settlement instructions in order to ensure that the amount of intraday credit provided through auto-collateralisation is automatically and exclusively used to settle the underlying instruction(s).

On the basis of the type of collateral movement chosen by each Central Bank providing credit, T2S will collateralise the intraday credit provided through auto-collateralisation either:

- by transferring the securities from the Security Account of a T2S Actor to the Security Account of the Central Bank providing the credit; or
- by transferring the securities from the account of the bank receiving the credit to another account of this Payment Bank which the NCB has linked to the Payment Bank's DCA for auto-collateralisation in T2S (the second Security Account being pledged to the Central Bank providing the credit where the securities are in the name of the bank receiving the credit); or
- by reserving the securities on the Security Account of the Payment Bank receiving the credit; in such a case, the securities will be reserved in favour of the Central Bank providing the credit and T2S will not allow the Security Account holder to use the relevant securities as long as they are reserved.

When auto-collateralisation on flow and on stock are both possible for the settlement of a transaction or a set of transactions, T2S prefers to resorts to auto-collateralisation on flow before auto-collateralisation on stock. When the collateral value of the securities on flow is not sufficient to cover the amount of credit granted, T2S complements collateral on flow with

Currency Participation Agreement

Schedule 5 – T2S Service Description

collateral on stock. Finally, when securities being purchased in the underlying transaction are not eligible collateral (e.g. equities for Eurosystem intraday credit) and therefore cannot be used as collateral on flow, T2S uses collateral on stock to secure the amount of intraday credit granted through auto-collateralisation.

Whenever T2S generates and settles an auto-collateralisation operation, it creates and sets on hold the reimbursement of that auto-collateralisation operation - an the exact reverse operation (i.e. same amounts, same accounts, etc). The Payment Banks are able to trigger the reimbursement of their auto-collateralisation operations with Central Banks and with their clients at any moment during the daytime real-time settlement by releasing the relevant on hold reimbursement instructions.

Auto-collateralisation provides intraday credit that must be repaid at the end of the day. T2S uses all available liquidity on the cash accounts of the Payment Bank to repay the credit. In normal situations, the Payment Banks have repaid all intraday credit operations with the Central Banks before the auto-collateralization reimbursement is initiated. In this is the case, T2S executes only a cash sweep during which the excess liquidity on the payment's bank's cash accounts is transferred to the relevant Real-Time Gross Settlement (RTGS) systems. If, however, there is not sufficient liquidity on the cash account at the end of the day to fully reimburse the pending intraday credit, special end of day procedures are invoked.

The securities that are held on the accounts of the Central Bank (or pledged) for auto-collateralisation purposes are transferred to the overnight collateral Security Account indicated by the Central Bank. At the same time, the relevant Collateral Management System (CMS) is informed of the move and the credit usage limit for the participant in the RTGS system is increased. This process ensures that the T2S service provides, though a collateralised credit, the same amount of liquidity in the RTGS system as it withdraws⁵.

4.7. T2S SD.SETT 070: Realignment service

When T2S matches a pair of settlement instructions, or receives an already matched pair of instructions, it verifies whether the instructions submitted require realignment instructions on accounts other than those of the T2S Parties submitting the instructions (e.g. on the accounts of the Issuer CSD). If T2S identifies a need to realign, it generates the required realignment instructions, on the basis of the cross-CSD links in the Common Static Data, automatically validates the realignment instruction, and links all settlement instructions to ensure all-or-none settlement.

⁵ Further details especially on the reimbursement procedures and rules can be found in the User detailed Functional Specifications, especially chapter 1.1.2 Liquidity management, and in the General Functional Specifications (GFS), especially chapter 2.3.5 Liquidity Management

Currency Participation Agreement

Schedule 5 – T2S Service Description

If the Issuer CSD is within T2S and the Investor CSDs are not in T2S, the realignment takes place in T2S on the basis of settlement instructions (usually free-of-payment) to be sent by the Issuer CSD.

T2S does not send realignment instructions to the Issuer CSD if the Issuer CSD is outside T2S:

- The realignment process is handled by the Investor CSDs in coordination with the Issuer CSD outside T2S.
- If at least one Investor CSD is within T2S, the Conditional Securities Delivery (CoSD) mechanism can be used by the Investor CSDs, to block the position in T2S and hold the instruction until the settlement is confirmed in the Issuer CSD's books.

4.8. T2S SD.SETT 080: Instruction recycling service

Recycling occurs in anticipation of finding the required securities and/or cash subsequent settlement runs, so that failed transactions can be settled successfully.

Recycling differs slightly depending on whether it occurs during day-time and night-time settlement. In case of night-time settlement, all unsettled settlement instructions are recycled automatically to the next settlement sequence. In day-time settlement, unsettled settlement instructions are recycled when new settlement resources (i.e. securities and/or cash) become available.

Unmatched pending instructions are recycled for 20 days before cancellation by T2S. Matched pending instructions which fail to settle are recycled indefinitely.

The T2S settlement optimisation techniques reduce the number of unsettled settlement instructions at the end of the settlement day (EOD).

4.9. T2S SD.SETT 090: Instruction amendment service

T2S Actors may amend only process indicators, irrespective of the status of the underlying settlement instruction (except for instructions with an end-of-life status). The instructing T2S Party has to cancel and reinstruct the settlement if it wishes to modify any other fields.

T2S allows the amendment of the following process indicators until settlement occurs:

- partial settlement (only for settlement instructions)
- linking instructions
- settlement priority

In case of partially settled instructions, the instructing T2S Party may amend the settlement priority only for the pending part of partially settled instructions.

T2S does not allow any settled or cancelled settlement instruction to be modified.

Currency Participation Agreement

Schedule 5 – T2S Service Description

T2S will reject an amendment sent by a CSD participant other than the T2S Party which submitted the original instruction concerned, or its CSD, if the instruction to be amended was sent as non-modifiable by the CSD or an authorised CSD participant.

T2S informs the instructing T2S Party, as well as any T2S Actor duly authorised to access this information, immediately after the successful amendment of an instruction, in accordance with their message subscription preferences.

If the amendment process fails in T2S, then the amendment instruction is rejected. (e.g. original instruction has settled.)

4.10. T2S SD.SETT 100: Instruction cancellation service

Any instructing T2S Actor or its CSD may cancel its settlement instructions unilaterally prior to matching or its settlement restrictions prior to settlement. In such case, T2S verifies that (a) the instruction that the T2S Actor wishes to cancel exists in T2S and that (b) its cancellation is possible. Whether or not T2S Actors are able to cancel their instructions depends on the status of the instruction.

T2S will reject any cancellation request sent by a CSD participant other than the T2S Party which submitted the original instruction concerned, or its CSD, if the instruction to be cancelled has been sent as non-modifiable by the CSD or an authorised CSD participant

Under the same rules, a CSD may cancel any instruction of any of “its DCP”. Cancellation instructions cannot be cancelled.

Until matching has occurred, T2S allows a T2S Actor to request unilaterally the cancellation of settlement instructions only.

Once matching has occurred, T2S Actors may cancel matched settlement instructions only bilaterally, i.e. both parties must send a cancellation instruction (“binding matching”) for the cancellation to take effect. T2S then matches the cancellation instructions and cancels both settlement instructions.

In the case of bilateral cancellation of settlement instructions, T2S checks whether the cancellation instruction from the counterpart exists and matches the two cancellation instructions.

If the counterpart cancellation instruction does not exist, then the cancellation instruction remains pending until it matches with a valid counterpart cancellation instruction. T2S also accepts cancellation instructions entered as already matched.

In the case of a Conditional Settlement (CoSD), T2S allows only the administering T2S Party identified in the Common Static Data to unilaterally request the cancellation of the instruction that triggered the CoSD process (e.g. when the external condition for settlement is not fulfilled), even after T2S has blocked the relevant securities holding for a CoSD. If a CoSD involves more than one administering T2S Party, the CoSD settlement instruction cannot be cancelled unless

Currency Participation Agreement

Schedule 5 – T2S Service Description

T2S receives cancellation instructions from each administering T2S Party involved in the initial settlement instruction.

T2S notifies the originator of a cancellation instruction when the cancellation instruction has either been executed (i.e. cancellation of the settlement instruction was successful) or denied (i.e. settlement instruction could not be cancelled). In the latter case, the resulting cancellation status value for the cancellation instruction is “denied”.

If the cancellation process in T2S fails, then the cancellation instruction goes through recycling until it is either processed or rejected if the original instruction has already settled.

If the cancellation mechanism is automatically activated by T2S for a given instruction, T2S informs the CSD or the DCP that the instruction was cancelled by T2S. Automatic cancellation rules are applied to invalid or unmatched or failed/outdated instructions, and are compliant with ECSDA recommendations.

Realignment instructions can not be cancelled by any T2S Actor.

4.11. T2S SD.SETT 110: Hold/release service

Hold and release mechanisms allow T2S Actors to hold or release settlement instructions until their actual settlement or cancellation, even beyond their Intended Settlement Date (ISD). These mechanisms give T2S Actors the flexibility to delay the settlement. T2S Actors may send maintenance instructions to hold and release settlement instructions as many times as required.

T2S allows only the T2S Actor that has put an instruction on hold to release it. If there are two executed hold instructions for the same instruction (i.e. one from the CSD participant and one from the CSD), release instructions must also come from both. If T2S receives a hold instruction for a settlement instruction that is already on hold or has been cancelled from the same T2S Actor who has submitted the initial hold or cancellation instruction, T2S denies the hold instruction.

T2S will reject any hold/release instruction sent by a CSD participant other than the T2S Party which submitted the original instruction. or its CSD, if the instruction to be held/released was sent as non-modifiable by the CSD or an authorised CSD participant

All instructions on hold at the end of the ISD remain unsettled and T2S recycles them in accordance with the T2S rules for recycling instructions. Furthermore, T2S allows the remaining part of partially settled instructions to be held and to released.

T2S will reject any hold or release settlement instruction if T2S has already settled or cancelled the underlying settlement instruction. T2S informs the instructing T2S Party accordingly, depending on its message subscription preferences.

Currency Participation Agreement

Schedule 5 – T2S Service Description

4.12. T2S SD.SETT 120: Earmarking, blocking and reservation service

4.12.1. T2S SD.SETT 121: Earmarking service component

In T2S Parties may define that a security position or a security account be earmarked as a settlement restriction. For a position or an account to be earmarked, the securities must be fully available in the relevant account.

Earmarking defines that a security position or security account may be used for one and only one defined purpose. An earmarked position or account can not be used for another purpose unless the earmarking is revoked.

A T2S Actor may earmark a position or an account for a specific purpose such as auto-collateralisation. If there is a conflict regarding use of the earmarked securities for a delivery/receipt owing to contradictory choices between account level and instruction level (that is to say when a settlement instruction refers to a earmarking purpose which is different from that at account level), the choice at account level overrides the choice at position level (T2S will credit or debit the earmarked position according to the purpose at account level and not according to the purpose at the instruction level). If earmarking is done at the Security Account level for a specific purpose, it will not be possible to earmark securities at position level (in the same account), for a different purpose.

Earmarking is not possible for DCAs.

4.12.2. T2S SD.SETT 122: Blocking service component

In addition to earmarking, T2S Parties may define that securities or cash be blocked at the instruction, position or account level as settlement restrictions. A T2S Actor may block securities or cash for a specific purpose. For the securities or cash to be unblocked, the relevant instruction must contain the reference to the specific purpose.

A blocking of cash or securities prevents the transfer of specific securities/cash from a specific Security Account/T2S DCA.

When a blocking restriction is submitted for settlement, and providing sufficient securities and/or cash are available on the relevant accounts, T2S blocks the number of securities and/or the amount of cash specified in the settlement restriction on the relevant securities and/or T2S DCA(s). If insufficient securities and/or cash is available, only those securities and/or cash will be blocked. No further attempt will be made to block the remaining part.

4.12.3. T2S SD.SETT 123: Reservation service component

As a further settlement restriction, T2S Parties may define that a security or a cash instruction or position be reserved. A T2S Actor may create a reservation without having all the securities or

Currency Participation Agreement

Schedule 5 – T2S Service Description

cash specified in the reservation. Any securities or cash arriving will be attributed to the reservation until the reserved volume has been reached.

When a reservation instruction is submitted for settlement, and providing sufficient securities and/or cash are available on the relevant account(s), T2S reserves the number of securities and/or the amount of cash specified in the settlement instruction on the relevant securities and/or T2S DCA(s). If insufficient securities and/or cash are available, T2S:

- reserves the securities and/or the cash already available on the relevant account; and
- supplements it with any incoming securities and/or cash proceeds arriving on this account, provided that the latter are not defined to be used for any other purpose.

A reservation of cash or securities reserves a securities or cash position for the settlement of one or more settlement instructions. A T2S Actor may refer to an existing reservation in another settlement instruction, by means of the reservation's unique reference number. If such references result is made the provisioning process will include the reserved cash or securities in its provisioning check. The reserved securities/cash will be used first (ahead of unreserved securities/cash) for settlement of the instruction.

4.12.4. T2S SD.SETT 123: Common features of the earmarking, blocking and reservation service component

When several reservations/blockings of securities and/or cash have been performed on the same Security Account and/or T2S DCA, and a T2S Actor submits to T2S a settlement instruction referring to one (or some) of those reservation/blocking instructions, the T2S provision-check does not consider the additional securities and/or cash reserved/blocked through reservation instructions other than those referred to in the instruction being settled. However, if the securities/cash reserved/ blocked are not sufficient, T2S also takes into account additional securities and/or cash available on the relevant Security Account and T2S DCAs, provided that the latter have not been reserved/blocked for any other purpose.

If at EOD the reserved and blocked cash has not been used for any purpose, T2S releases the relevant cash. In case of a CoSD blocking, T2S releases the blocked cash at the EOD and creates a new CoSD blocking instruction. As regards securities, if blocked or reserved securities have not been used or released at EOD as a result of an instruction from the relevant T2S Actor, T2S does not release them automatically.

4.13. T2S SD.SETT 140: Conditional Security Delivery (CoSD) service

Conditional Security Delivery (CoSD) is a special functionality which manages instructions that

Currency Participation Agreement

Schedule 5 – T2S Service Description

734 require the fulfilment of a settlement condition outside T2S before securities may be settled in
735 T2S⁶.

736 Through the T2S Change and Release Management, CSDs request the T2S Operator to set up and
737 maintain the rules invoking CoSD, as the CoSD rules of one CSD might have an impact on other
738 T2S Parties. These rules are stored as part of the Common Static Data in T2S. Each rule
739 identifies an administering T2S Party to release the instruction for settlement or to cancel the
740 CoSD flagged settlement instruction and determines events which will result in an instruction
741 automatically being submitted to the CoSD functionality by T2S. One settlement instruction
742 might be subject to more than one CoSD rule and in such cases more than one administering T2S
743 Party is assigned to that instruction.

744 On the ISD, T2S verifies all instructions with that particular ISD in accordance with the CoSD
745 rules. It submits them automatically to the CoSD procedure if one or more CoSD rules are met.
746 In such case, T2S automatically generates a settlement restriction to block the securities position,
747 the cash position, or both.

748 T2S rejects any cancellation request coming from the instructing parties after the activation of the
749 CoSD process, as only administering parties are allowed to cancel settlement instructions
750 submitted to CoSD.

751 T2S blocks the securities in the deliverer's Security Account irrespective of the instruction to
752 which the CoSD rule applies (similar rule applies for cash blocking on the T2S DCA linked to
753 the receiver's Security Account). If two or more CoSD rules apply to the securities delivery
754 instruction or related receiving or realignment instructions and those rules require securities to be
755 blocked, the securities are blocked only once. Likewise, T2S blocks cash only once in the
756 delivering cash account.

757 In a CoSD, securities, cash or both remain blocked and the instruction concerned remains on hold
758 until T2S receives from the administering parties:

- 759 ▪ a release instruction, requesting settlement of the instruction using the previously blocked
760 securities or cash (on the basis of the information contained in the initial instruction); or
- 761 ▪ a cancellation instruction. After receiving cancellation instruction(s) from all
762 administering parties T2S will cancel the CoSD instruction and its underlying
763 instructions. In such case the underlying cash/securities are unblocked and the
764 administering parties and instructing parties receive a confirmation message.

765 A “blocking” status message is sent by T2S to inform the (administering) CSD and/or the DCP

⁶ Further details can be found in the User Detailed Functional Specifications (UDFS), especially chapters 1.1.1. Settlement, 2.4 Send Settlement Restriction on Securities Position, 2.6 Send Release Instruction for CoSD by Administering Party, and 2.7 Send Cancellation Instruction for CoSD by Administering 1 Party

Currency Participation Agreement

Schedule 5 – T2S Service Description

that the securities, cash or both have been blocked for the processing of the original instruction. A “hold” status message is sent by T2S to inform the (administering) CSD and/or the DCP that the instruction related to the original instruction is prepared for settlement and waiting for release.

Only the administering T2S Party can send the release message. If the receiving party is outside T2S, the status information is relayed by the CSD responsible for the account within T2S.

If the CoSD blocking cannot take place, T2S recycles the blocking instruction for the following Settlement Day. Cash blocked under CoSD is released at the EOD and regenerated for the following Settlement Day. Settlement instruction that are on CoSD Hold are recycled for the following Settlement Day (i.e. securities remain blocked and the settlement instruction remains on hold).

If the realignment chain changes or revalidation of the instruction submitted to CoSD and its related instructions is unsuccessful, T2S cancels all the instructions but the blocked securities/cash remain blocked.

4.14. T2S SD.SETT 150: Linked instructions service

T2S Actors may link instructions in order to ensure that a settlement instruction settles at the same time, before or after another settlement instruction. Linked instructions are possible on a

- one-to-one,
- one-to-many, or a
- many-to-many

basis.

When T2S submits several linked instructions for a settlement attempt, it posts the debits and credits for cash and securities from the relevant transactions if the provision check (including account netting effects) is successful. T2S settles sets of linked instructions according to the highest level of priority accorded to any of the instructions within the set (the whole set of linked instructions settles according to this level of priority).

T2S Actors can link instructions by using the ISO settlement link indicators “AFTER”, “BEFORE” and “WITH”. These link indicators will be used in the settlement process.

When T2S receives an instruction which is linked to one or more other instruction(s), it:

1. checks that the linked instruction(s) exist.
2. then validates that the information contained in the new linked instruction is consistent with the instruction which exists and to which it is linked, i.e. the ISD and the Security Account holder used are the same.

Linked instructions are excluded from partial settlement. If at EOD a linked instruction has not been settled it will be recycled.

Currency Participation Agreement

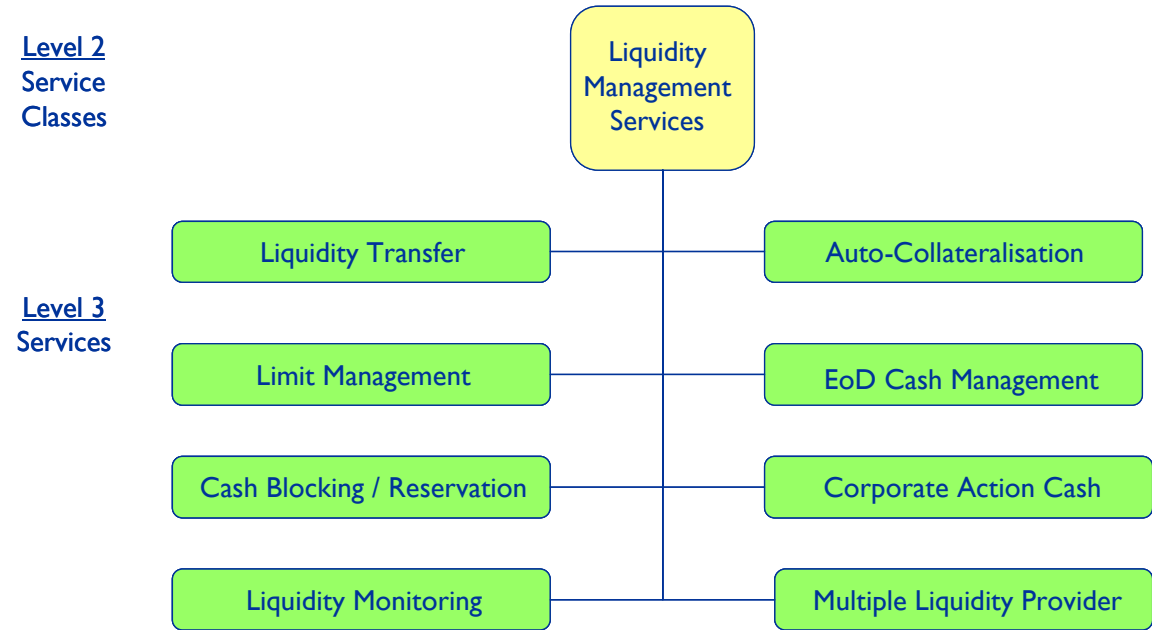
Schedule 5 – T2S Service Description

800 **4.15. T2S SD.SETT 160: Corporate actions service**

801 To support the CSDs in settling corporate action entitlements, T2S uses standard settlement
802 services for security settlement as well as liquidity management/cash settlement.

803

5. T2S SD.LIM: Liquidity Management Service Class



5.1. T2S SD.LIM 010: Liquidity transfer service

A liquidity transfer in T2S is an instruction from a DCA holder to transfer a specified amount of cash balance from its cash account to another cash account. The T2S DCA holders are Payment Banks or Central Banks.

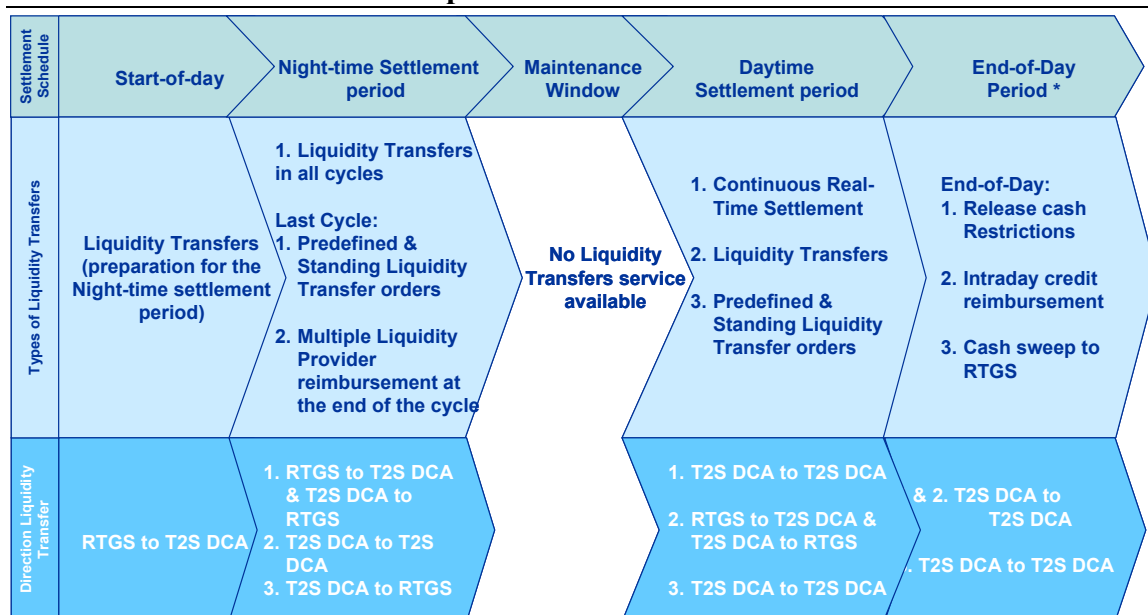
T2S allows a T2S DCA holder to receive liquidity on its T2S DCA(s) from any RTGS account (provided that they are denominated in the same currency and that this is permitted by the relevant Central Bank). In the same way, T2S allows the holder of the T2S DCA to send liquidity from its T2S DCA(s) to any RTGS account (as setup by the relevant Central Bank in T2S) if the currency is the same.

In addition to liquidity transfers between RTGS accounts and T2S as mentioned above, T2S provides T2S DCA holders with a “multiple liquidity providers” functionality, i.e. T2S DCA holders can receive liquidity from and reimburse to several RTGS accounts.

Liquidity transfers are executed in real time upon receipt. During the execution of the liquidity transfer, if the status of the liquidity transfer order changes, T2S informs the T2S Actor about the new status if the latter’s message subscription rules in the Common Static Data so dictate.

Currency Participation Agreement

Schedule 5 – T2S Service Description



T2S supports three types of liquidity transfers between T2S DCAs and RTGS cash accounts and between T2S DCAs.

- Immediate liquidity transfer order:

- Liquidity is transferred in real time on receipt of the instruction from the account holder or a T2S Party with the appropriate rights.
- Used to transfer liquidity between a T2S DCA and the RTGS account or between two T2S DCA (if these DCA belong to the same Payment Bank or are linked to the same RTGS account)
- If an immediate liquidity transfer orders cannot be settled, an alert is sent to the Payment Bank that initiated the transfer in line with the message subscription rules in the Common Static Data.

- Pre-defined liquidity transfer order:

- Liquidity is transferred at a certain time or when a particular business event occurs, as defined by the account holder of the account or a T2S Actor with appropriate rights to debit the account.
- The transfer is executed only once on the basis of a defined time or event
- Liquidity is transferred from a T2S DCA to an RTGS account only (either the specified transfer amount or “all cash” available in the T2S DCA will be transferred)
- Any duly authorised T2S Actor may amend or delete the predefined liquidity transfer order

- Standing liquidity transfer order:

Currency Participation Agreement

Schedule 5 – T2S Service Description

- Liquidity is transferred at a certain time or when a particular business event occurs, as defined by the account holder of the account or a T2S Party with appropriate rights to debit the account.
- The transfer is executed whenever the event in question occurs until the standing order is deleted.
- Liquidity is transferred from a T2S DCA to an RTGS account only (either the specified transfer amount or “all cash” available in the T2S DCA will be transferred)
- Any duly authorised T2S Actor may amend or delete a standing liquidity transfer order.

If insufficient liquidity is available on the accounts to be debited, T2S allows partial execution in the case of pre-defined/ standing liquidity transfers. T2S allows a partial execution of an immediate liquidity transfer only if it is instructed to do so by a Central Bank in its role as RTGS system, or by a CSD acting on behalf of the Payment Bank.

As part of the business validation process, T2S checks that the content of immediate liquidity transfer orders (received from T2S Actors) or liquidity transfers (which have been generated from a standing or predefined liquidity order) is correct, and validates the consistency of the data contained in the immediate liquidity transfer received by T2S with the Common Static Data. A liquidity transfer which has been generated from a standing or predefined liquidity order is not validated by T2S.

After business validation, T2S communicates the acceptance/ rejection of a liquidity transfer order to the Payment Bank and to the Central Bank if the liquidity transfer order was sent from the RTGS system. In the event of failure or rejection, T2S sends a list of error/ reason codes. T2S also communicates all changes in status of a liquidity transfer order.

After successful validation the liquidity transfer order is sent to the settlement functionality for processing. The booking function updates the balances on the DCAs involved on a gross basis. In the case of partial execution or of no execution, no further settlement is attempted. T2S communicates all changes in status of a liquidity transfer order in the course of its execution in accordance with the message subscription rules in the Common Static Data, and confirms all executed transfers between T2S and RTGS.

5.2. T2S SD.LIM 020: Limit management service

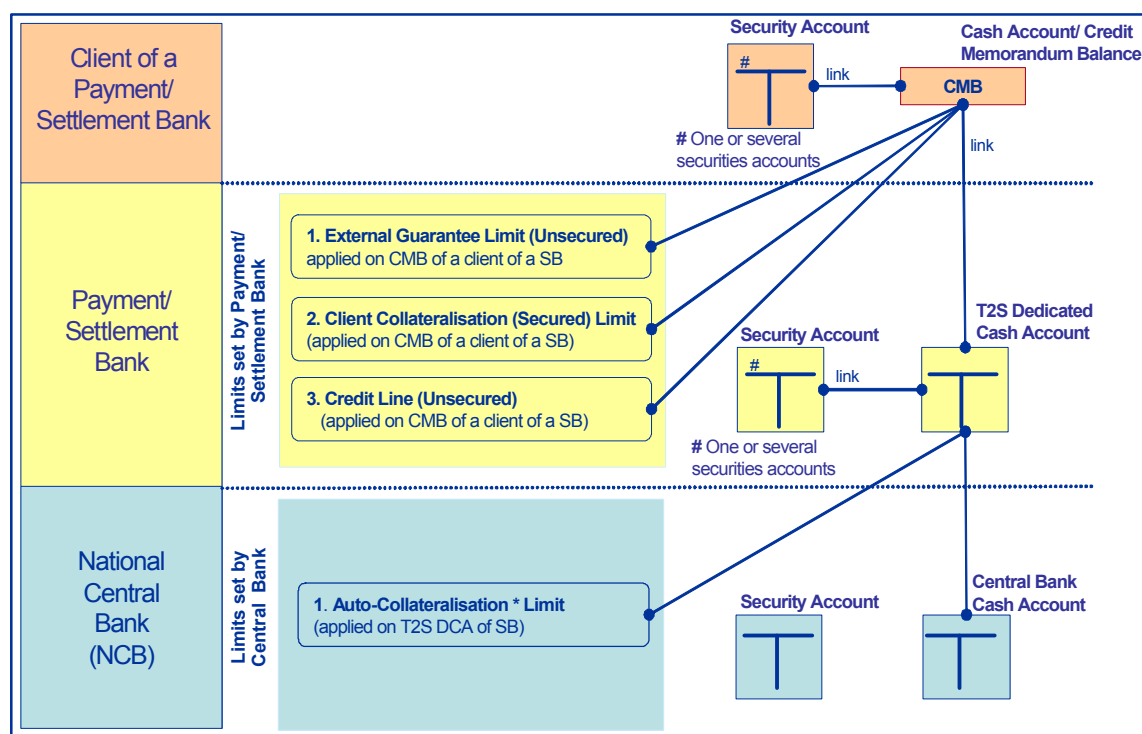
T2S provides the T2S Actor with different liquidity control mechanisms. A Central Bank can control its parties' T2S DCA by setting an auto-collateralisation limit for the T2S DCA. Payment Banks can also set different limits at the client level and monitor their utilisation.

A Payment Bank can set up different limits for the liquidity provided to each of its clients, either

Currency Participation Agreement

Schedule 5 – T2S Service Description

against collateral or without collateralisation. Using T2S queries, the Payment Bank has a consolidated view of its client's collateral holdings at any given point in time across multiple Security Accounts in either the same or different CSDs. The respective limits are automatically updated when used as a part of the settlement process. T2S performs validations to ensure that these limits are not breached. T2S does not allow cash movements between the Cash Payment Bank and its clients in T2S. The only cash in T2S is the cash on the DCA, which is in CeBM.



Central Banks and Payment Banks can set and monitor the limits they provide to their clients.

- **External guarantee limit:** Cap on credit secured outside T2S that the Payment Bank sets for its client. The external guarantee limit and the unsecured credit limit are identical from the T2S viewpoint, except for the sequence in which they are triggered. Usage of the external guarantee limit is triggered before auto-collateralisation..
- **Client-collateralisation limit:** Cap on the amount of credit extended against securities by a Payment Bank in T2S
- **Unsecured credit limit:** Cap on the amount of credit granted by a Payment Bank (generally unsecured outside T2S)
- **Auto-collateralisation limit:** Cap on the amount of credit extended against securities by a Central Bank to the Payment Bank.

T2S ensures that all the required provision checks for the Payment Banks and their clients are performed simultaneously and that collateralisation operations are initiated on the basis of the results of the provision check. A Cash Payment Bank client's credit exposure as well as the

Currency Participation Agreement

Schedule 5 – T2S Service Description

availability of sufficient headroom on different types of credit limits is determined solely on the basis of information available to T2S.

To prepare for client collateralisation, the T2S actor has to provide and to set up the information required for the link between its Security Account and its DCA, and to provide the necessary information for the Credit Memorandum Balance (CMB) Security Account Link Set and CMB Security Account Link⁷.

Furthermore, a T2S Actor can control the use of liquidity by reserving/ blocking cash for specific instructions. The amount of cash reserved/ blocked may not be used to settle instructions, unless the instruction being settled refers to the initial reservation/ blocking instruction.

5.3. T2S SD.LIM 030: End of day (EOD) cash management service

After the cut-off of settlement processing, the EOD processing is conducted in three steps. Information messages are sent to the initiating T2S Actor and other duly authorised T2S Actors in accordance with their message subscription preferences:

1. EOD release of unused cash restrictions:

- All restrictions on cash (blocked cash, reserved cash) are released for the current T2S Settlement Day
- New cash settlement restrictions regarding CoSD blocking are created for the next T2S Settlement Day

2. EOD release of auto-collateralised positions and transfer of cash balance:

- The amount of outstanding auto-collateralisation is validated
- If there is no pending auto-collateralisation: No action is taken
- If there are pending auto-collateralisation(s):
 - and the cash on the T2S DCA is sufficient to reimburse fully the pending auto-collateralisation, including possible cash rebalancing: T2S reimburses
 - and there is insufficient or no cash on the T2S DCA to reimburse the pending auto-collateralisation, T2S:
 - checks for available cash via cash rebalancing from another DCA of the same T2S Actor
 - releases the associated reverse (unwind) settlement instructions previously

⁷ Further details can be found in the User Detailed Functional Specifications (UDFS), especially chapter 1.1.2 Liquidity management

Currency Participation Agreement

Schedule 5 – T2S Service Description

- 929 created
- 930 ▪ creates instructions for positions that will not be released (equivalent to the
- 931 pending amount of auto-collateralisation that cannot be reimbursed out of
- 932 T2S), to transfer the collateral to the Central Bank overnight collateral
- 933 Security Accounts, and
- 934 ▪ Rebalances the account to zero.

935 3. EOD liquidity transfer (cash sweep)

- 936 ▪ Liquidity transfers are created for all T2S DCAs and the Central Bank Account used for
- 937 EOD reimbursement with non-zero cash balances.
- 938 ▪ These liquidity transfers are settled in T2S and sent to the RTGS system.

939 **5.4. T2S SD.LIM 040: Corporate action cash service**

940 T2S enables a T2S Actor, receiving cash proceeds from corporate actions on its T2S DCA, to

941 specify whether T2S should keep the cash proceeds on the T2S DCA or to retransfer them from

942 the T2S DCA to the RTGS account (outside T2S) with which the T2S DCA is linked.

943 In such case, the T2S Actor must define a standing liquidity transfer order for the T2S DCA as

944 part of the Common Static Data to be able to opt for an automated retransfer of cash proceeds to

945 an RTGS account.

946 T2S allows the T2S DCA holders to use different T2S DCAs for the settlement of the cash leg of

947 trading-related instructions and for the settlement of the cash leg of corporate action instructions.

948 During the daytime real-time settlement T2S executes the standing liquidity transfer order as an

949 immediate liquidity transfer to transfer the corporate action proceeds to the RTGS account of the

950 T2S Actor.

951 For the Batch Settlement, as soon as the relevant RTGS becomes available, T2S transfers the

952 liquidity. Without a standing order, the corporate action proceeds are routed to the T2S Actor's

953 DCA.

954 T2S also provides this setup and service for retransferring 'monetary policy Repo' related cash

955 proceeds from a T2S DCA to an RTGS account.

956 **5.5. T2S SD.LIM 050: Cash blocking and reservation service**

957 T2S allows a T2S Party to use restrictions to block or to reserve a cash balance in a T2S DCA.

958 For that purpose the CSD or the Central Bank has to define the relevant restriction types as part

959 of the Common Static Data.

960 Blocking a cash balance involves preventing the transfer of a specified amount of funds in a

961 specific currency in one cash account to any other cash account by linking it to a specific

Currency Participation Agreement

Schedule 5 – T2S Service Description

purpose. Blocking in T2S never results in a negative cash balance, i.e. it is not possible to block an amount of funds greater than the available cash balance on a cash account.

Reserving a cash balance prevents the transfer of a specified amount of funds in a specific currency in one cash account to any other cash account except for the purpose for which the funds were reserved. The settlement of the underlying settlement instruction (for which the funds were reserved) results in the actual transfer of the reserved funds to another cash account and the subsequent removal of the reservation.

A T2S Actor may reserve a cash position without yet disposing of the required full amount of cash in that position. Any cash arriving in the reserved position will be attributed to the reservation until the required amount has been reached.

A T2S Actor may refer to an existing reservation/blocking in another settlement instruction, by referring to the unique reference number of the reservation's/blocking. Such reference will be interpreted in such a way that the provisioning process includes the reserved/blocked amount of cash in its provisioning check. The reserved/blocked cash will be used first (ahead of unreserved/unblocked cash) for settlement of the instruction.

During business validation, T2S checks automatically whether one of these restriction types applies to the submitted settlement instruction or to an instruction for an intra-position movement to determine the further processing required. If the validation process finds a match for a restriction type, then the relevant restriction type is applied to the instruction.

5.6. T2S SD.LIM 060: Liquidity monitoring service

T2S provides different functions for monitoring the actual cash balances of the DCAs as well as the CMB limits to monitor the liquidity of the clients of the Payment Bank. T2S calculates the amount of cash required for the settlement and informs the T2S Actor if more liquidity is needed.

Cash related queries allow duly authorised T2S Actors to obtain information about their account balance on the T2S DCA(s), outstanding intraday credit from auto-collateralisation, and potential liquidity based on securities on stock that can be used for auto collateralisation purposes. In addition, T2S provides information showing the overall liquidity.

A T2S Actor may request information on cash needs for instructions pending for settlement during the current Settlement Day, as well as cash forecasts for the following Settlement Day. Information on cash needs and cash forecasts covers T2S DCA liquidity needs.

Information for the on-going Settlement Day is intended to provide a snapshot of the cash required to settle instructions remaining unsettled at the moment of the snapshot. This information includes (as part of the cash required for the current day settlement) the value of potentially available auto-collateralisation.

Information on cash forecasts for the following Settlement Day and in particular for the following

Currency Participation Agreement

Schedule 5 – T2S Service Description

night-time settlement window is intended to allow T2S Actors to prepare and dedicate in advance sufficient cash for the settlement of their instructions during the following night-time settlement window. The cash forecasts are based on

- cash needs resulting from the net balance between
 - cash proceeds and
 - cash needs
 - expected for settlements with the following day as the ISD, and
- the amount of intraday credit that can be obtained through auto-collateralisation.
- the amount of liquidity credit that can be obtained through external guaranteed limits and unsecured credit lines from Payment Banks or Central Banks

Depending on the chosen report configuration, cash forecasts can be received as reports sent out automatically by T2S at certain points/when certain events occur during the T2S Settlement Day. Preliminary information on cash can also be obtained via the query functionality.

However, it should be noted, that these cash forecasts (received through the above-mentioned reports and via queries) are only indicative of the final cash needs, as the forecasts are based only on the information available in T2S: T2S does not take corporate action proceeds into account, if the relevant instructions are not submitted to T2S.

The T2S Actor has to be aware that these cash forecasts will change in the course of the Settlement Day depending on new settlement instructions/ liquidity transfers submitted to T2S. It is to be expected that the quality of the cash forecast will increase continuously during the day as additional settlement instructions and information become available in T2S.

A T2S Actor is able to define the floor and ceiling amounts per DCA in the Common Static Data. This functionality allows the T2S Actor to receive alerts if the amount of liquidity in the DCA reaches the minimum/maximum the DCA account holder has defined.

5.7. T2S SD.LIM 070: Multiple liquidity provider service

T2S DCA holders may receive liquidity from several RTGS accounts (i.e. from different liquidity providers) and use the proceeds in T2S. This cash can be transferred from the RTGS accounts prior to the start of Batch Settlement in T2S. Subsequently, a T2S DCA holder can use this cash for its own settlement purposes or to provide cash settlement services to its clients, during Batch Settlement in T2S.

At the end of the Batch Settlement, a T2S DCA holder may opt to establish liquidity transfers which will reimburse its different liquidity providers in the relevant RTGS systems with the remaining cash in the T2S DCA. This reimbursement facility is the “multiple liquidity provider” service.

Currency Participation Agreement

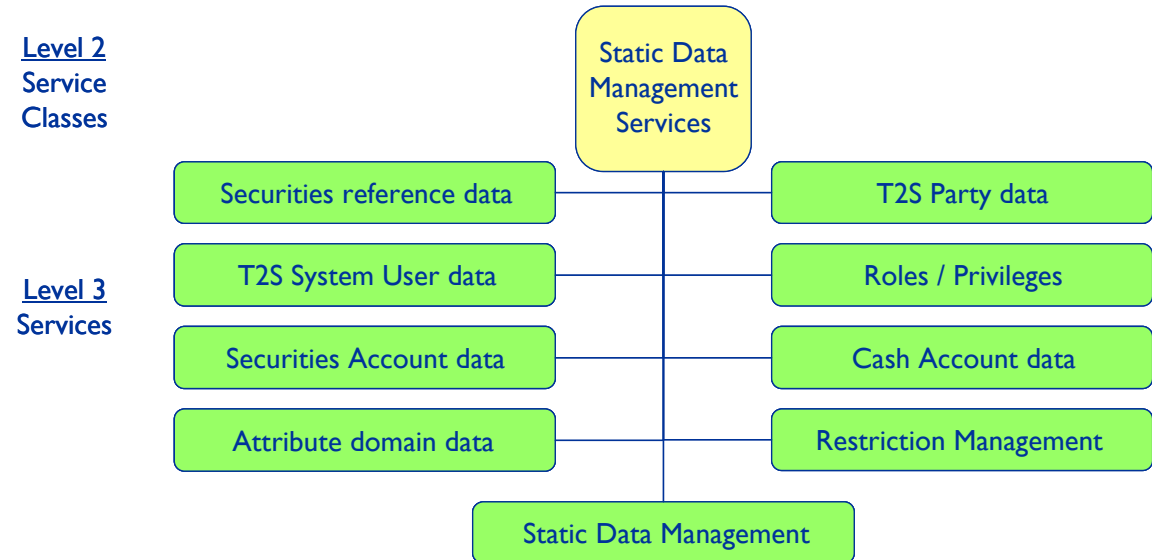
Schedule 5 – T2S Service Description

1031 The reimbursement of cash is executed via outbound liquidity transfers generated by T2S on the
1032 basis of the multiple “standing liquidity transfer order”. The priority of execution is defined by
1033 the T2S Actor in the “order link set” setup in the Common Static Data.

1034 T2S validates whether a T2S DCA holder (liquidity receiver) has opted for a “multiple liquidity
1035 provider” service for reimbursement. In this is the case, T2S reimburses the liquidity providers in
1036 the sequential order of liquidity providers as set up in the order link setup (in the Common Static
1037 Data). T2S aims to reimburse each liquidity provider up to the maximum amount of the cash the
1038 liquidity provider transferred before starting to reimburse the next liquidity provider in the
1039 sequential order concerned. In the order link set, the main liquidity provider is setup as the last
1040 liquidity provider and therefore is the last liquidity provider to be reimbursed (assuming there is
1041 sufficient cash to reimburse all liquidity providers).

1042

6. T2S SD-STD: Common Static Data Management Service Class



6.1. T2S SD.STD 010: Common Static Data management service

Common Static Data management is the service that T2S provides for setting up/inserting, changing/maintaining and inactivating/deleting Common Static Data in T2S regardless of the type of conceptual entity. T2S applies the same functional principles for inserting, maintaining and deleting all entities.

T2S processes all Common Static Data updates in real-time in both User-to-Application (U2A) and Application-to-Application (A2A) mode, except in the case of some preliminary functions which are only available in U2A mode⁸. All Common Static Data entities are stored in the T2S data base with a full audit trail and it is possible to query the actual occurrence of an entity as well as the historical data. Whenever a record in Common Static Data is changed, a new version of this record is stored including the timestamp and the identification of the T2S Actor performing the change, thereby maintaining a full audit trail.

T2S allows T2S Actors to parameterise the entities and the types of updates made by a T2S User or by a T2S process. T2S will process these in real-time except during the maintenance window.

T2S checks for every change in a Common Static Data entity and for the change approval configuration for this entity and processes the update in accordance with to the configured parameters. The privileges of the different T2S Users depend on the Common Static Data entity. Static security data changes made by an automated interface do not require an independent

⁸ The detailed list of available functions for the different modes are part of the UDFS and of the GUI description.

Currency Participation Agreement

Schedule 5 – T2S Service Description

change approval by a second user, but a manual update by a person is subject to such approval (4-eyes principle).

T2S provides duly authorised T2S User with the functionalities to

- identify all static and dynamic data changes awaiting approvals;
- search for specific static and dynamic data changes;
- search and display historic change information, including both approved and rejected changes;
- and approve and reject static and dynamic data changes.

6.1.1. T2S SD.STD 011: Insert service component

T2S allows the duly authorised T2S User to insert a new occurrence of an entity into Common Static Data. A T2S User is an individual or application that is allowed to communicate with T2S when duly authorised and authenticated.

6.1.2. T2S SD.STD 012: Update service component

T2S allows duly authorised T2S User to update an existing occurrence of a Common Static Data entity. T2S allow T2S Users to update occurrences of a Common Static Data entity if the previous update of the same occurrence remains in the change approval queue. T2S prohibits the concurrent update of occurrences of a Common Static Data entity. When a T2S User selects an occurrence for editing, T2S locks the occurrence so that a second T2S User or T2S process cannot access it for updating.

6.1.3. T2S SD.STD 013: Delete service component

When a duly authorised T2S User initiates the deletion of an occurrence in a Common Static Data entity, T2S checks that there are no unsettled instructions and only zero positions pertaining to that data. Only if that is the case will the deletion status of the occurrence be changed from “active” to “deleted”. The deletion of an occurrence of a Common Static Data entity occurs only logically.

The T2S archiving functionality is the only function which will physically delete an occurrence of a Common Static Data entity from the active T2S database. The physical deletion of a Common Static Data occurrence is only possible for logically deleted occurrences. To ensure the referential integrity of data, Common Static Data occurrences are physically deleted from the active database only after archiving processes have removed and archived the related transactional and position data as of a cut-off date that is determined by the retention plan. Data history and data revisions that took place before the archive date will be included in any physical

Currency Participation Agreement

Schedule 5 – T2S Service Description

1095 deletion process even if the current record is still active - since the transactional data for which
1096 they are relevant would be removed by the archiving.

1097 **6.1.4. T2S SD.STD 014: Reactivate service component**

1098 In some instances, it is necessary to reactivate a logically deleted occurrence of Common Static
1099 Data. T2S allows duly authorised T2S Users to specify the Common Static Data entity and the
1100 identifier of an occurrence in that Common Static Data entity, and to reset the deletion status of
1101 an occurrence in that Common Static Data entity from “deleted” back to “active”.

1102 **6.2. T2S SD.STD 020: Securities Reference Data service**

1103 Securities Reference Data in T2S defines the set of entities and attributes that T2S requires for
1104 settlement and auto-collateralisation in CeBM.

1105 The Securities Entity holds all attributes that exist only once for a security. Securities Reference
1106 Data require every security to have an ISIN code, compliant with ISO 3166. The creation of a
1107 new security will be effective immediately unless it requires dual entry approval. This also
1108 applies to updates of all attributes for the Securities Entity. Certain “non-standardised securities”
1109 that comply with all required criteria apart from not being fungible from a settlement perspective
1110 may still be entered in and processed by T2S.

1111 The Securities Reference Data Service allows the CSD to create and maintain the Common Static
1112 Data of those securities for which it is the Issuer CSD or the Securities-Maintaining Entity. The
1113 service allows the Issuer CSD to block or unblock ISINs both for itself and its Investor CSDs.
1114 T2S allows an Investor CSD to block or unblock ISINs only for itself..

1115 **6.3. T2S SD.STD 030: T2S Party data service**

1116 T2S deploys a flexible hierarchical party model to allow CSDs and Central Banks to manage
1117 their accounts and parties in an efficient way. The T2S Operator maintains the first and second
1118 level of the hierarchy. All other levels must be managed by the CSDs and the Central Banks
1119 respectively.

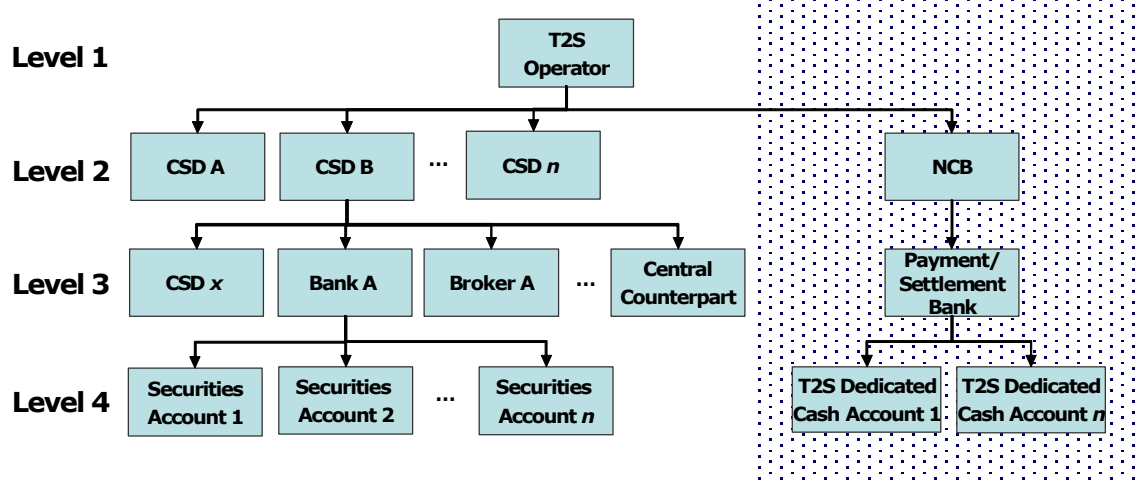
1120 A T2S Party denotes any legal or organisational entity required in T2S as single legal entity to
1121 guarantee data segregation. The same legal entity, or organisational unit of a legal entity, may be
1122 set-up under several CSDs or Central Banks as a result of this principle. This entity includes the
1123 parties from the first three levels of the hierarchy model, the T2S Operator, the CSDs, the
1124 participants of the CSD, the Central Bank and Payment Banks. It also establishes the links
1125 between the different parties on the different hierarchical levels. A CSD can also be a T2S Actor
1126 for its own purposes defined in level 3 of the hierarchy (see graph below).

1127 T2S assigns each party a technical identifier, which the user can also use as the unique T2S Party

Currency Participation Agreement

Schedule 5 – T2S Service Description

code (participant code). T2S will use the BIC of a T2S Party to identify the T2S Party uniquely across in the Central Bank - and CSD-specific reference data.



The CSD-part of this hierarchical structure contains all T2S Party data pertaining to securities settlement. The Security Account (on the lowest level of this part of the hierarchy) is assigned to the CSD participant and to the CSD. Each CSD is responsible for maintaining the hierarchy including the Security Accounts of the different parties which are linked to it. CSDs assign and manage the access rights of their participants, including those of all their DCPs.

Security Accounts linked to the CSD participant and T2S DCAs linked to a Payment Bank form the lowest level of the hierarchy. The Security Accounts can be either omnibus accounts or end-investor accounts for markets with direct holdings systems.

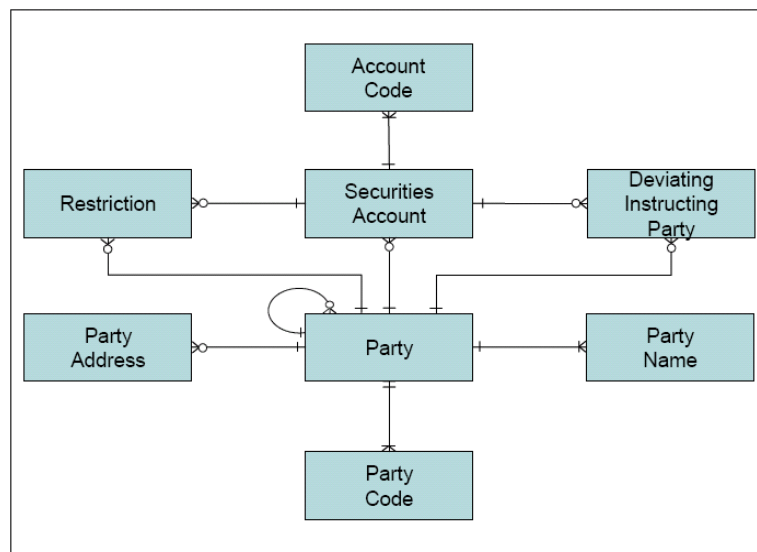
CSDs have access to Central Bank party and account Common Static Data to link Security Accounts to T2S DCAs for the settlement of the cash leg of a settlement instruction. T2S will make available to the CSDs the relevant data for the linking of accounts without publishing all T2S DCAs. Access rights control which CSD is able to see the T2S DCAs needed for linking purpose. When a CSD sets up a Security Account, it can only see those T2S DCAs to which it can link a Security Account for settlement.

The Central Bank part of the hierarchical structure includes all data relating to the Central Bank and the T2S DCAs held with the Central Bank by Payment Banks. In the third tier of this part of the hierarchy includes the Payment Banks which operate T2S DCAs to provide liquidity. The T2S DCAs are the lowest level of the hierarchy. The hierarchy links the T2S DCA to the relevant Central Bank.

Central Banks authorise the access to T2S DCAs by assigning the BIC of those parties, eligible for access to the cash account for settlement, to the T2S DCA. When entering a Security Account, the CSD only sees those T2S DCAs which have the same BIC assigned to them as the T2S Party that owns the Security Account.

Currency Participation Agreement

Schedule 5 – T2S Service Description



6.4. T2S SD.STD 040: Security Account data service

Security Account reference data specify all information required for defining and processing a Security Account in T2S.

Security Accounts in T2S must be opened and closed by the CSD to ensure the consistency and integrity of Security Account reference data between the CSD and T2S. When the CSD opens an account, it must immediately trigger the opening of the relevant account in T2S. The same applies for the closing of an account.

T2S supports a T2S Actor - Security Account Relationship entity to specify a time-dependent relationship between a T2S Actor and a Security Account. The purpose of the entity is to allow a CSD in T2S to transfer a Security Account relationship from one account operator/sub-custodian to another account operator/sub-custodian within the CSD. The functionality enables a CSD to transfer an end-investor Security Account relationship from one account operator to another.

CSDs are also responsible for closing a T2S Security Account by setting the business status to “closed” and confirming the change. T2S only closes an account if:

- there is no un-settled instruction specifying the T2S Security Account for the settlement;
- the T2S Security Account is not part of an active T2S link set;
- there is no securities balance remaining on the T2S Security Account.

In case an unmatched instruction exists concerning an account that is closed, during the business revalidation the unmatched instruction is identified and will be cancelled.

6.5. T2S SD.STD 050: Cash account data service

The T2S DCA model specifies the requirements for assigning T2S DCA to Security Accounts for the settlement of the cash leg of settlement instructions. The T2S DCA entity specifies the T2S

Currency Participation Agreement

Schedule 5 – T2S Service Description

DCAs of Payment Banks in T2S. It also links the T2S DCA to the associated RTGS account concerned as well as establishing the reference link to the Payment Bank that owns the account and to the Central Bank that operates the account.

The key responsibilities of each Central Bank whose currency (euro and non-euro) is available for settlement in T2S are:

- set-up and maintain the DCAs of their RTGS participants for all securities-related payment transactions in their currency in T2S;
- identify securities accounts for use as the pledged accounts to which securities are moved in autocollateralisation
- set up and manage Common Static Data, access rights and configuration data pertaining to its members and its own participation in T2S;
- if required, provide for the interoperability of their own RTGS systems and collateral management (CMS) systems with T2S;
- if the Central Bank chooses to participate in auto-collateralisation:
 - to provide auto-collateralisation in its currency to its members in accordance with its self-defined eligibility criteria;
 - if required, to provide to T2S, for the specific purpose of auto-collateralisation, a list of eligible securities and prices as well as any other data necessary for T2S to judge the eligibility of a specific security for a specific participant;
- be responsible for the choice of its network provider(s) and to make every effort to maintain properly functioning connectivity to T2S functions properly.

Central Banks are also responsible for closing a T2S DCA by setting the business status to “closed” and confirming the change. Unless the Central Bank deems that immediate closure is necessary, T2S only closes an account if:

- there is no unsettled instruction specifying the T2S DCA for the settlement of the cash leg;
- the T2S DCA is not part of an active T2S DCA link set;
- there is no cash balance remaining on the T2S DCA.

The external RTGS Account Entity specifies all the external RTGS payment accounts to which an authorised T2S User can link a T2S DCA. This entity also provides the reference link to the Payment Bank that owns the account and the Central Bank that operates the account.

The Central Banks have to add new external RTGS account for a Payment Bank or another Central Bank in T2S. T2S assigns new external RTGS accounts an opened business status and the

Currency Participation Agreement

Schedule 5 – T2S Service Description

1210 current Settlement Day as the opening date.

1211 An external RTGS account can be closed by setting the business status to “closed” and
1212 confirming the change. T2S will not close an account if:

- 1213 ▪ there is an unsettled payment instruction specifying the external RTGS account;
- 1214 ▪ the external RTGS account has an active link to a T2S DCA;
- 1215 ▪ or if the external RTGS account is defined in a current (not closed, not expired) standing
1216 liquidity transfer order.

1217 T2S allows the blocking/unblocking of an RTGS account using T2S Actor and account
1218 settlement restrictions. The blocking of an RTGS account results in all T2S DCA linked to the
1219 RTGS account being blocking from settlement.

1220 **6.6. T2S SD.STD 060: T2S User data service**

1221 A T2S User is an individual or application that is allowed to communicate with T2S using a login
1222 name and certificate/smartcard and for U2A in addition an optional password and/or certificate
1223 for authentication. The assignment of the T2S User to a T2S Actor establishes the relationship
1224 between the T2S User and the system entity. T2S provides specific roles and privileges to restrict
1225 the access of this T2S User to business data of the CSDs and of the Central Banks.

1226 T2S User maintenance defines the process of adding, changing and deleting users in T2S. Access
1227 to this functionality is restricted to system administrators only.

1228 A system administrator is able to lock and unlock a T2S User without deleting the user by setting
1229 the attribute "lockout status" to "yes" or "no". If the system administrator assigns existing roles to
1230 or deactivates roles for a T2S User, T2S automatically assigns to the T2S User the privileges
1231 associated with that role.

1232 **6.7. T2S SD.STD 070: Roles and privileges data service**

1233 In order to comply with the principle concerning the separation of functions and roles, T2S
1234 implements roles and privileges as business concepts which refer to the right of T2S Actors to
1235 interact with T2S. Duly authorised system administrators configure roles and privileges to
1236 authorise other T2S Users to execute specific functions or view specific data.

1237 A privilege is a right, either granted or denied, to execute certain functions within T2S, or to
1238 access and/or update certain data in T2S. It is through the privileges that access to functionality
1239 and data for specific roles, T2S Parties and T2S Users are granted and restricted. A privilege is
1240 uniquely identifiable, both internally in the application and to the T2S system administrator.
1241 Privileges are classified either as System privileges or Object privileges.

1242 System privileges grant certain rights for a single or a homogeneous group of data objects (e.g.

Currency Participation Agreement

Schedule 5 – T2S Service Description

1243 T2S Calendar). Object privileges grant rights in relation to a single or a group of Common Static
1244 Data objects.

1245 The administrator grants a privilege by specifying whether (1) the associated functionality is
1246 allowed or explicitly denied; (2) the grantee of the privilege is allowed to grant the same privilege
1247 to another user or role; (3) the grantee of the privilege is allowed to use the function associated to
1248 the privilege in accordance with two eyes or four eyes principles.

1249 Account owners (i.e. a CSD or a Central Bank) may grant privileges to their clients, with
1250 different roles and privileges for each one. These roles and privileges can be differentiated by
1251 client and even among different accounts of the same client.

1252 T2S privileges may for example grant:

- 1253 ▪ no access at all;
- 1254 ▪ read only access;
- 1255 ▪ the right to instruct with possible limitations concerning the type of instructions or the
1256 accounts to instruct on.

1257 A role consists of one or more privileges. A CSD or a Central Bank may configure valid roles for
1258 its T2S parties as follows:

- 1259 ▪ If set up by the CSD, DCPs manage their T2S User administration,
- 1260 ▪ If set up by the Central Bank, Payment Banks manage their T2S User administration.

1261 Each CSD or a Central Bank needs to create and authorise a system administrator for each of its
1262 client T2S Actor of that CSD or of that Central Bank. The system administrator is responsible for
1263 maintaining users and roles for this particular client. The CSD or Central Bank administrator has
1264 to ensure, that the system administrator of the T2S Party has access only to those roles that the
1265 CSD or Central Bank permits. Accordingly, T2S enables each CSD or the Central Bank to grant
1266 its clients access to a different set of roles, depending on the services provided by the CSD or the
1267 Central Bank to each T2S Party.

1268 CSDs or Central Banks participating in T2S must continue to comply with legal and regulatory
1269 requirements. T2S therefore allows the configuration of CSD- or Central Bank - specific roles.
1270 The CSDs or Central Bank may differentiate the access they grant to T2S services and functions
1271 on the basis of the regulatory and legal requirements to which they are subject.

1272 **6.8. T2S SD.STD 080: Restriction management service**

1273 T2S must support the T2S Operator, CSDs and Central Banks by enabling them to provide
1274 specific validations and processing of settlement instructions to fulfil legal, regulatory and
1275 supervisory requirements in the markets that they service. T2S therefore allows the T2S
1276 Operator, CSDs and Central Banks to define their own restriction types.

Currency Participation Agreement

Schedule 5 – T2S Service Description

1277 After approval through the T2S Change Management process, only the T2S Operator is allowed
1278 to setup the definition of and to maintain harmonised restrictions, which may be used by all
1279 CSDs and Central Banks.

1280 Restriction types are attributes that define the specific processing characteristics for a securities
1281 position, cash balance, Security Account, T2S DCA, T2S Party or settlement instruction to
1282 ensure configurability of specific requirements, as prescribed by national legal and regulatory
1283 requirements and practices, and to avoid hard-coding in the application software.

1284 T2S provides the following restriction processing types:

- 1285 ▪ Blocking – blocks an instruction from settlement;
- 1286 ▪ Rejection – rejects an instruction at validation;
- 1287 ▪ CSD Validation Hold – accepts a settlement instruction at validation (not applicable to
1288 settlement restrictions) but holds it for a subsequent release by the CSD⁹;
- 1289 ▪ Reservation – reserve a cash balance or securities position;
- 1290 ▪ Balance Type / Earmarking – define and manage position types for securities and balance
1291 types for cash balances;

1292 Restrictions can also be defined as either a positive or negative parameter set and in time (from
1293 and to).

1294 During the validation process, T2S automatically verifies whether one of the defined restrictions
1295 applies to the instruction submitted.

1296 A T2S User may define specific rules for restriction types. These define the sequence in which
1297 T2S applies a logical set of parameters to determine whether a specific restriction applies to the
1298 instruction. The restriction matrix defines the specific parameter values within a rule. T2S stores
1299 matrix entries for a rule in a rule set. A matrix entry defines an occurrence of a valid set of
1300 values, specifying the actual criteria against which T2S must validate a settlement instruction to
1301 determine whether a restriction type applies.

1302 T2S allows duly authorised users to

- 1303 ▪ add new rules for a restriction type;
- 1304 ▪ (re-) define the sequence of rules for a restriction type;
- 1305 ▪ delete rules for a restriction type if the user has deleted all occurrences under that rule;
- 1306 ▪ add and delete matrices in a rule.

⁹ Further details for the CSD validation hold are provided in the User Detailed Functional Specifications (UDFS)
chapter 1.1.1 Settlement

Currency Participation Agreement

Schedule 5 – T2S Service Description

1307 This functionality is also used by CSDs to define which settlement instructions will be put on
1308 CSD Validation Hold. It allows CSDs to execute certain tasks / validations locally prior to the
1309 settlement of the underlying instruction.

1310 **6.9. T2S SD.STD 090: Attribute domain data service (market-specific attributes)**

1311 Attribute domains in T2S provide the valid list of values allowed for an attribute (table column or
1312 a data field in physical terms). They include a list of all the valid values that a user can enter for
1313 an attribute of a static or transactional data entity. T2S uses attribute domains for field validations
1314 and for documenting the business definition of a value in an attribute.

1315 T2S provides a general Common Static Data component that allows the duly authorised T2S User
1316 to logically create, modify and deactivate market-specific attribute domains, on the basis of the
1317 existing data definitions (attributes). These market-specific attribute domains allow the T2S
1318 Operator, CSDs and Central Banks to define their own restriction types as described above. T2S
1319 allows the definition of additional values, mapped to an attribute,

1320 T2S limits the actions that a user can trigger in the database using attribute domain management.
1321 T2S allows the registration and deactivation of attribute domains using pre-defined database
1322 tables.

1323

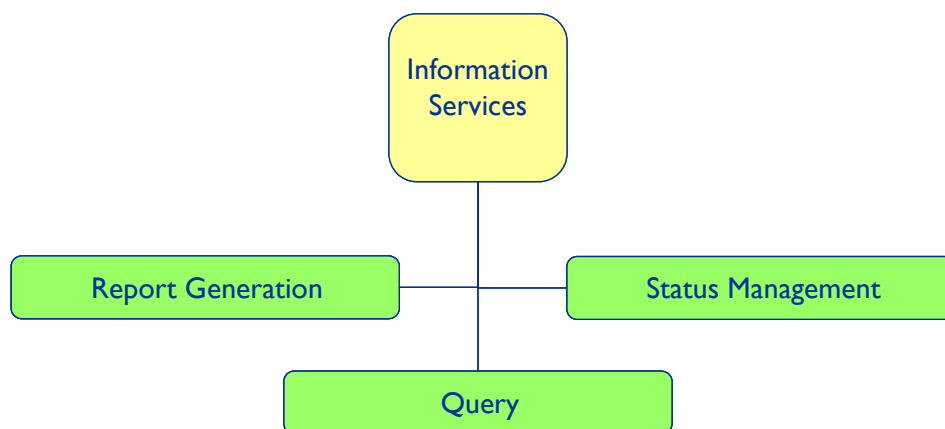
Currency Participation Agreement

Schedule 5 – T2S Service Description

7. T2S SD. INF: Information Management Service Class

Level 2
Service
Classes

Level 3
Services



7.1. T2S SD.INF 010: Status management services

As part of its settlement services, T2S maintains the settlement statuses of any instruction it processes. T2S informs duly authorised T2S Actors of the result of all settlement services and of all changes to the statuses of instructions, depending on the message subscription chosen by the T2S Actor.

T2S provides multiple-statuses reporting that gives more flexibility and brings more efficiency than single-status reporting. In this context, T2S provides the values of the different statuses for each instruction in a status message.

If instructions are rejected, settlement attempts unsuccessful or instructions cancelled, T2S also informs the relevant T2S Actor why this has happened.

7.2. T2S SD.INF 020: Report generation service

T2S provides a defined set of reports. Reports are triggered automatically by T2S. All reports are available in both User-to-Application (U2A) and in Application-to-Application (A2A) mode as in the T2S Connectivity Services description. These reports are not, and should not, be considered as Regulatory Reports. T2S Actors may use the query services described hereafter to receive the necessary information from T2S to provide their regulators with the required information.

T2S reports are either event-triggered or sent at a fixed time. When a CSD, T2S Actor or Central Bank require information at a time not so triggered, the information can also be retrieved using the query service.

Reports containing information either on individual accounts or on a set of accounts can be sent to the relevant CSDs and DCPs, or to the relevant Central Bank. T2S reports are based on the latest available data and contain a date and time stamp. In addition, T2S sends successive versions of defined reports with the information that changed from the previous version to the

Currency Participation Agreement

Schedule 5 – T2S Service Description

1349 next version of that report (delta reporting). The additional information includes the attributes of
1350 the reported items as provided in the previous version of the report.

1351 A DCP may receive reports only on:

- 1352 ▪ its own securities and cash balances, those of its clients and those of any other T2S Actor
1353 for which the appropriate authorisation was granted,
- 1354 ▪ instructions that were submitted by the T2S Actor (or a Third Party with access rights -
1355 supported by power of attorney to do so on behalf of the T2S Actor) and instructions that
1356 refer to the securities or cash account of the T2S Actor (or any sub-account thereof),
- 1357 ▪ its own Common Static Data, as well as some generic Common Static Data on
1358 instruments and the daily schedule.

1359 A CSD may receive reports only on:

- 1360 ▪ instructions that were submitted by the CSD in T2S itself, its DCPs, or by its participants,
- 1361 ▪ securities transactions and balances of the CSDs own accounts in T2S, those of its DCPs
1362 and those of its participants and
- 1363 ▪ Common Static Data of the CSD in T2S itself, its DCPs, and of its participants, where
1364 privileges permit. These Common Static Data include those ISINs for which the CSD
1365 acts as Security Maintaining Entity (SME)¹⁰. Additionally, a CSD may query all
1366 Common Static Data that relate to its admission rule, for securities as well as for parties.

1367 A Central Bank may receive reports only on:

- 1368 ▪ Instructions that were submitted by the Central Bank in T2S itself, or by its Payment
1369 Banks.
- 1370 ▪ cash balances of its own DCAs in T2S and those of its Payment Banks as well as cash
1371 movements on its own DCAs and those of its payment banks, and
- 1372 ▪ Common Static Data of the Central Bank in T2S itself, and of its Payment Banks.
1373 Additionally, a Central Bank may query all Common Static Data that relate to its national
1374 currency.

1375 A Payment Bank may receive reports only on:

- 1376 ▪ Instructions that were submitted by itself.
- 1377 ▪ cash balances of its own DCAs in T2S, and
- 1378 ▪ its own Common Static Data, and that pertaining to its DCAs.

¹⁰ Further details can be found in the Manual of Operational Procedures (MOP)

Currency Participation Agreement

Schedule 5 – T2S Service Description

T2S provides the following report types:

- Statements of holdings
- Transaction reports:
 - Statement of transactions
 - Statement of pending instructions
 - Statement of settlement allegements
 - Statement of Security Accounts at EOD
 - Statement of changes to Common Static Data
 - Billing data report
- Cash forecast reports
 - Current Settlement Day cash information
 - Following Settlement Day cash forecast

7.3. T2S SD.INF 030: Query service

T2S allows information to be queried in T2S. Queries are triggered by the duly authorised T2S Actor. All queries are available in User-to-Application (U2A) and in Application-to-Application (A2A) mode. All securities instructions, and balances and Common Static Data queries are available for all CSDs in T2S, DCPs as well as Central Banks and Payment Banks, in accordance with to the access rights.

T2S accepts all queries at any point in time during T2S opening days. T2S processes all queries in real time, on the basis of the latest available data. During the night-time settlement cycles, T2S stores balance queries sent in Application-to-Application mode. T2S responds to the queries at the end of each sequence inside a cycle with the latest position.

T2S provides standard queries which can be taken as the basis (blueprint) for individual, non-standard queries. For individual, non-standard queries, T2S provides the option of specifying parameters in the query to fulfil the needs of the querying T2S Actor. When processing queries, T2S takes into account all access rights as defined in the Common Static Data. T2S will only return results where the T2S Actor that has submitted the query has the right to access the underlying data. CSD/ Central Bank and T2S Parties may act as service providers for indirect Parties or e.g. remote brokers.

7.3.1. T2S SD.INF 031: Query service for T2S Actor service component

A T2S Actor may query the following – subject to access rights:

Currency Participation Agreement

Schedule 5 – T2S Service Description

- 1410 ▪ its own securities positions;
- 1411 ▪ instructions submitted by the T2S Actor itself (in case of direct connectivity), or by a
- 1412 Third Party that has access rights in T2S supported by a power of attorney;
- 1413 ▪ its own Common Static Data, as well as some generic Common Static Data relating to
- 1414 e.g. instruments and the daily schedule.

1415 **7.3.2. T2S SD.INF 032: Query service for CSDs service component**

1416 A CSD in T2S may query the following:

- 1417 ▪ instructions that were submitted by the CSD itself, or by its DCPs;
- 1418 ▪ securities and cash balances of DCA(s) of the CSD itself and of its T2S parties in T2S;
- 1419 ▪ Common Static Data of the CSD itself, and of its T2S Actors;
- 1420 ▪ Common Static Data pertaining to securities.

1421 **7.3.3. T2S SD.INF 033: Query service for Central Banks service component**

1422 A Central Bank in T2S (acting in its role as Central Bank) may query:

- 1423 ▪ cash balances of the DCAs kept at the Central Bank in question;
- 1424 ▪ movements on the DCAs kept at this Central Bank;
- 1425 ▪ and Common Static Data pertaining to the DCAs for which it is responsible.

1426 Additionally, a Central Bank may act as a T2S Actor of a CSD. In this case, the Central Bank has

1427 the same access rights as any other T2S Actor. Finally, if a Central Bank plays the role of a CSD,

1428 that Central Bank, when doing so it has the same access rights of a CSD.

1429 **7.3.4. T2S SD.INF 034: Query service for Payment Banks (liquidity providers)**

1430 **service component**

1431 A Payment Bank in T2S (acting in its role as liquidity provider) may query:

- 1432 ▪ cash balances of its DCAs;
- 1433 ▪ Common Static Data pertaining to the DCAs for which it is responsible.

1434 **7.3.5. T2S SD.INF 035: Settlement-related queries service component**

1435 During the night-time settlement cycles, T2S stores balance queries sent in Application-to-

1436 Application (A2A) mode, then replies with a message that T2S is currently running a cycle and

1437 that T2S will respond to the query at the end of the cycle with the latest position.

1438 T2S provides different standard queries related to settlement:

Currency Participation Agreement

Schedule 5 – T2S Service Description

- 1439 ▪ Securities balance query:
- 1440 ○ The Securities Balance Query returns an account view on the position at a
- 1441 particular point in time, the latest securities position or at the close of settlement
- 1442 if requested after close of settlement, all positions are summarised in the account
- 1443 structure that is compatible with the query parameters.
- 1444 ○ The Securities Balance History Query returns all positions that occurred during a
- 1445 particular time period, all positions are summarised in the account structure that
- 1446 is compatible with the query parameters.
- 1447 ▪ Settlement instruction query
- 1448 ○ T2S allows T2S Actors to query settlement instructions in accordance with the
- 1449 Actor's roles and privileges.
- 1450 ○ T2S provides a settlement instruction status audit trail query which allows a T2S
- 1451 Actor to query settlement instructions on the basis of the business processing
- 1452 status or a combination of business processing statuses on a specific date or in a
- 1453 specific period in the past

1454 **7.3.6. T2S SD.INF 036: Cash balance-related queries service component**

1455 In accordance with their access rights, Central Banks and settlement/ Payment Banks may query:

- 1456 ▪ the current balance of one or more T2S DCAs.
- 1457 ▪ the total current collateral value of securities earmarked and available (on stock) for auto-
- 1458 collateralisation for a T2S DCA via the Securities Balance query and the Securities
- 1459 Balance History query. The collateral value of securities, calculated by the query, does
- 1460 not include securities on flow, as the settlement process will use these automatically.
- 1461 ▪ for a specific T2S DCA, the current total collateral value of every security, earmarked
- 1462 and available (on stock) for auto-collateralisation via the Securities Balance query and
- 1463 the Securities Balance History query, in all Security Accounts, linked to the T2S DCA
- 1464 for settlement of the cash leg. The collateral value of securities, calculated by the query,
- 1465 does not include securities on flow, as the settlement process will use these
- 1466 automatically.
- 1467 ▪ the amount of outstanding intraday credit stemming from auto-collateralisation, defined
- 1468 as the difference between the credit utilised and the credit reimbursed.
- 1469 ▪ for a specific T2S DCA, the collateral (amounts and securities) utilised for outstanding
- 1470 intraday credit stemming from auto-collateralisation.

Currency Participation Agreement

Schedule 5 – T2S Service Description

- 1471 ▪ the total collateral (amounts and securities) utilised for outstanding intraday credit
1472 stemming from auto-collateralisation.
- 1473 ▪ In addition to the queries described above, T2S provides some screens in the T2S
1474 Interface (U2A mode) which give a consolidated view of the balances available on the
1475 different DCAs of each Payment Bank to facilitate the liquidity management of the
1476 treasurer(s) at the Payment Bank itself. These screens are available to directly connected
1477 Payment Banks and their Central Bank (further detailed in the User Handbook and the
1478 documentation on the GUI interface).
- 1479 ▪ In order to manage the liquidity of their DCAs, Central Banks and their
1480 Settlement/Payment Banks may also query:
- 1481 ○ Limits and their utilisation
- 1482 ○ Liquidity transfer orders
- 1483 ○ Liquidity transfer orders for multiple liquidity providers
- 1484 A CSD in T2S may query the cash balances of its own DCA(s) and those of its T2S parties in
1485 T2S.

1486 **7.3.7. T2S SD.INF 037: Common Static Data-related queries service component**

- 1487 Common Static Data queries are related to all main entities in Common Static Data. CSDs and
1488 CSDs' participants may query Common Static Data in accordance with their access rights
- 1489 T2S also provides a Common Static Data audit trail query which allows a T2S Actor (in
1490 accordance with its access rights) to query all revisions to an occurrence of Common Static Data.
- 1491 Standard Common Static Data queries allow the T2S Actor to query, in accordance with its
1492 access rights:
- 1493 ▪ Security reference data
- 1494 ▪ T2S Actor reference data
- 1495 ▪ Security Account reference data
- 1496 ▪ T2S DCA reference data
- 1497 ▪ T2S calendar and diary/daily schedule
- 1498 ▪ T2S entities
- 1499 ▪ Attribute domains
- 1500 ▪ T2S Actors, roles and privileges
- 1501 ▪ Restrictions
- 1502 ▪ Currency reference data

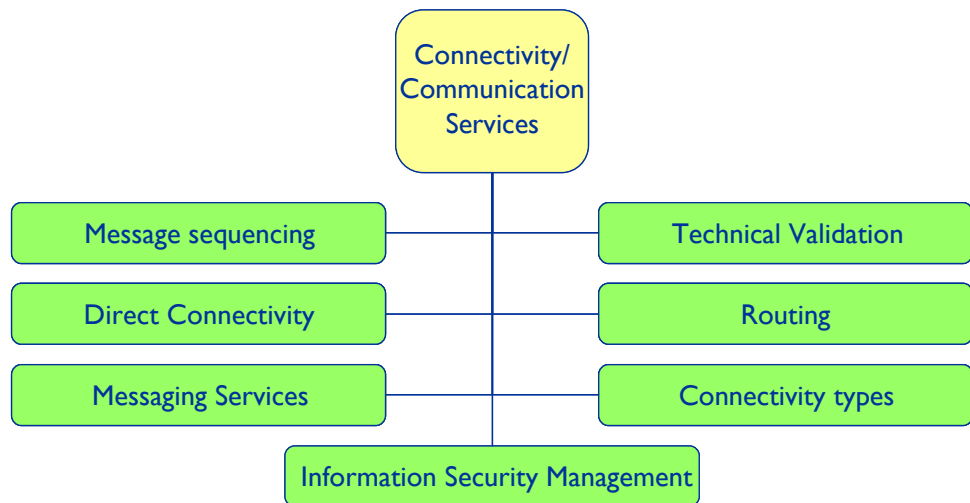
Currency Participation Agreement

Schedule 5 – T2S Service Description

1504 8. T2S SD. CON: Connectivity / Communication Service Class

Level 2
Service
Classes

Level 3
Services



1505

1506 T2S does not provide technical connectivity/network services between the T2S Actors and T2S
1507 among its services. Network services have to be procured by the T2S Actors directly from one or
1508 more of the accredited Network Service Providers (NSP). T2S defines the technical and
1509 operational requirements for the NSPs¹¹.

1510 NSPs offer a catalogue of services with appropriate solutions for high settlement volume and
1511 small settlement volume T2S Actors. The connectivity service catalogue contains the
1512 connectivity to T2S Service NSPs provide and the additional services offered by these NSPs,
1513 including;

- 1514 ▪ detailed services,
- 1515 ▪ service levels, detailing performances, availability and support commitments,
- 1516 ▪ volume related services,
- 1517 ▪ dedicated connectivity solutions,
- 1518 ▪ backup/ alternative network access solutions.

1519 8.1. T2S SD.CON 010: Messaging services

1520 T2S provides standard, time-event-driven and business-event driven messages based on and
1521 compliant to the largest extent possible with the ISO 20022 / UNIFI (Unified Financial Industry
1522 Message Scheme) standard. Communication between T2S Actors and T2S has to comply with

¹¹ The T2S Connectivity Guide provides further details on the different roles and responsibilities regarding the connectivity services

Currency Participation Agreement

Schedule 5 – T2S Service Description

the formats and specifications defined in T2S. T2S supports push and pull mode for files and single messages in Application-to Application mode (A2A), as well as a Graphical User Interface (GUI) in User-to-Application mode (U2A).

In T2S “business terms” a message is a single instruction (e.g. a settlement instruction, matched or unmatched, a Common Static Data maintenance instruction, etc) and in “technical terms” an XML string that refers to one or more “business messages”.

In T2S “business terms” a file is a set of instructions (more than one) and in “technical terms” a XML string that refers to one or more “business messages”, possibly of different types. It’s size should be within a defined range (minimum and maximum considering performance aspects).

For each message or file received by T2S an acknowledgement is sent to the sending T2S Actor. An acknowledgement from the receiving T2S Actor is also expected for each message or file T2S sends out. Security-settlement-related and cash-management-related messages follow the same logic.

Inbound and outbound traffic is stored in T2S in original format messages (before any transformation) and the messages are kept with time-stamping information and signature.

8.1.1. T2S SD.CON 011: Push messaging service component

During the Real Time Settlement T2S sends real-time standard messages to the T2S Actors which are triggered by the relevant business events. These events for the generation and subsequent sending of the different messages are described in the corresponding chapters of this Service Description.

After each cycle of the Batch Settlement T2S sends settlement related messages to the T2S Actors. For a given instruction only the most recent valid statuses will be sent. T2S Actors may choose to receive single messages or one file containing the complete set of such messages.

Depending on their access rights and privileges, T2S Actors can receive any message or any copy of any message. A copy of a message is any message sent to a T2S Actor (who is neither the instructing T2S Actor, nor the counterparty to the instruction), communicating the exact same information as sent to the instructing T2S Actor/counterparty to the instruction.

T2S message subscription is a service that allows a CSD or another duly authorised T2S Actor with direct connectivity to T2S to subscribe to copies of messages sent between a Directly Connected Party (DCP) and T2S in real-time using push mode messaging.

The T2S Actor must define in Common Static Data message subscriptions for all messages they want to receive. T2S only sends those messages the T2S Actor has subscribed to, there are no mandatory messages apart from the technical acknowledgements, which are always delivered to the sender of the message. All messages, which are used by T2S, are available for message subscription. T2S will not send any message not subscribed to beforehand, although T2S

Currency Participation Agreement

Schedule 5 – T2S Service Description

1558 generates all messages in accordance with the business context.

1559 Subscriptions are based on one or more of the following parameters:

- 1560 ▪ Message type;
- 1561 ▪ Instruction type;
- 1562 ▪ Instruction status;
- 1563 ▪ Participant;
- 1564 ▪ Account;
- 1565 ▪ ISIN.

1566 For Central Banks, the messaging service includes i.a.

- 1567 ▪ messages for each utilisation of intra-day credit stemming from auto-collateralisation.
- 1568 ▪ messages for each repayment of intra-day credit stemming from auto-collateralisation.

1569 The message subscription rules are defined and maintained in the Common Static Data by the
1570 T2S Actor.

1571 **8.1.2. T2S SD.CON 012: Pull messaging service component**

1572 T2S Actors may request to receive specific messages from T2S. T2S uses this mode mainly for
1573 query services and reports. Additionally, through the Graphical User Interface (GUI) the T2S
1574 Actor may pull queries and reports..

1575 **8.2. T2S SD.CON 020: Technical validation services**

1576 T2S verifies that all inbound communication (messages and files) is compliant with T2S required
1577 syntax, format and structure. The message and file integrity check is part of the validation and
1578 ensures that only messages and files from T2S Parties enter the T2S applications. T2S validates
1579 files using the same standard as for the messages and ensures that inbound files are not lost, that
1580 outbound files are neither lost nor duplicated and that the recommendations of the Giovannini file
1581 transfer rulebook are applied (generic rules for file construction and best practices for file transfer
1582 operations for any and all file transfers, on any network).

1583 If there are structure problems in a received message, T2S rejects the message. If there are file
1584 transfer or structure problems inside the file, T2S rejects the file in its entirety. If there are
1585 validation problems at the level of individual instructions within the file, the file is normally
1586 processed and a rejection message is sent for each individual invalid instruction the file contains.

1587 T2S verifies whether the communication was received from a secured and recognised technical
1588 address configured in the Common Static Data.

Currency Participation Agreement

Schedule 5 – T2S Service Description

8.3. T2S SD.CON 030: Connectivity types services

8.3.1. T2S SD.CON 031: Application to Application (A2A) service component

Application to Application (A2A) mode in T2S is a connectivity mode to exchange information between the T2S software application and application at the T2S Actor. In T2S, A2A can be based on either XML messages or file transfer. The ISO 20022 standard is applied as far as possible, for both inbound and outbound communication.

8.3.2. T2S SD.CON 032: User to Application (U2A) service component

The duly authorised T2S User can communicate with T2S via a web based Graphical User Interface (GUI), a connectivity mode to exchange information between software application of T2S and a T2S Actor and which is the User-to-Application interface (U2A) for interaction with T2S. The roles and privileges assigned to a T2S User determine which functions this user may execute and which data this user is allowed to see and to maintain.

8.4. T2S SD.CON 040: Information security management services

Information Security management services are a crucial part of the total package of T2S services, in terms of confidentiality, integrity and availability as well as authentication, accountability, non-repudiation and reliability of the T2S information.

Confidentiality or non-disclosure agreements between T2S and the T2S Actors address the requirement to protect Confidential Information using legally enforceable terms. Any access to the service's information by external parties must be controlled. Where there is a business need for working with external parties that may require access to the service's information, or when a product or service is obtained from or supplied to an external party, a risk assessment is carried out to determine Information Security implications and control requirements. Access by external parties to the service's information is not provided until the controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement.

8.4.1. T2S SD.CON 041: Authentication service component

Authentication is a security mechanism which verifies the identity of an individual T2S Actor (the T2S User) or application trying to connect to T2S. A T2S User is an individual or application that is allowed to communicate with T2S using a login name and certificate/smartcard and for U2A in addition an optional password and/or certificate for authentication.

T2S supports different types of authentication:

Currency Participation Agreement

Schedule 5 – T2S Service Description

- 1620 ▪ Simple authentication requires to the T2S User to enter the T2S User ID and the
1621 respective password only. This is applicable only for U2A.
- 1622 ▪ Simple Certificate authentication requires the T2S User to use a certificate without
1623 entering a password in T2S. This is applicable only for A2A.
- 1624 ▪ Advanced Certificate authentication requires the T2S User to use a certificate in in
1625 addition to entering the T2S User ID and respective password in T2S. This is applicable
1626 for U2A only.
- 1627 ▪ Smartcard authentication requires the T2S User to identify himself to the system using a
1628 smartcard in addition to entering the T2S User ID and respective password.
- 1629 T2S stores and manages certificates as part of the Common Static Data. For every inbound
1630 communication T2S verifies
- 1631 ▪ the identification of the sender
- 1632 ▪ whether the digital signature of the inbound communication corresponds to the certificate
1633 of the sender
- 1634 ▪ the T2S Actor technical address
- 1635 ▪ the network service used for the communication
- 1636 ▪ if the sender information of the inbound communication is defined in the Common Static
1637 Data

1638 **8.4.2. T2S SD.CON 042: Authorisation service component**

- 1639 Authorisation is a security mechanism which verifies that a T2S User or application (trying to
1640 connect to T2S) has the appropriate privilege to access certain functions or data within T2S.
1641 Authorisation is managed via the roles and privileges assigned by the T2S system administrators.
- 1642 Initially the CSDs and the Central Banks (with respect to the Payment Banks) grant and manage
1643 the authorisation. Within a DCP or a Payment Bank, a system administrator may grant additional
1644 authorisations which are limited by the authorisation granted to the T2S Actor by the CSD or
1645 Central Bank.
- 1646 T2S verifies the authorisation for every service and data access requested by a T2S User.

1647 **8.4.3. T2S SD.CON 043: 4-eyes principle service component**

- 1648 T2S ensures that any T2S operation to be executed in 4-eyes-mode is confirmed by a second
1649 authorised T2S User. The 4-eyes principle is only possible for U2A communication.
- 1650 When a T2S User changes any occurrence of static or dynamic data, which is subject to
1651 independent approval, T2S creates the changed version of the data as a new occurrence in the

Currency Participation Agreement

Schedule 5 – T2S Service Description

relevant revision entity and accords it a status "awaiting approval". The current version remains unchanged and is used until an independent source approves the update. If the independent approver accepts the change, T2S accepts the update and gives it the status "approved" in the Common Static Data entity. T2S retains the previous version of the data from the current entity as part of the audit trail in the revision history.

If the update is not approved, T2S updates the status of the change to "rejected" and it remains as an unapproved change in the revision history.

8.5. T2S SD.CON 050: Message sequencing services

T2S assigns each outgoing message a business sequence number which allows all T2S Actors to identify the sequence of messages T2S has sent. The receiving T2S Actors can thus identify whether messages are missing or misplaced in the sequence.

This service is used for all business related messages sent out by T2S.

8.6. T2S SD.CON 060: Direct connectivity services

Direct (technical) connectivity is a technical facility which allows T2S Actors to access T2S and use its services without using the relevant CSD/ Central Bank as a relay or proxy. Direct connectivity affects neither the business or legal relationships between CSD and T2S Actor, nor the processing of the instructions of the CSD's or Central Bank's T2S Actor.

Direct connectivity is a technical concept and means the existence of a (direct) A2A network connection between a T2S Actor and T2S. It does not mean that the T2S Actors concerned has any particular roles or privileges.

DCPs have to be certified to participate directly in T2S. The relevant CSD or Central Bank (i.e. the one the DCP is a participant or member of) has to ensure that the DCP fulfils all relevant conditions for participation of the DCP in T2S. T2S ensures that each DCP receives services as authorised by its CSD or Central Bank, and the same Service Levels. Furthermore, T2S ensures that no connected system can harm T2S or any other connected system. Before being able to access the T2S production environment, both the CSD / Central Bank and its DCP(s) therefore have to successfully pass a series of mandatory tests.

An individual T2S Actor may wish to participate as a DCP in more than one CSD or Central Bank. In such case, the T2S Actor is deemed to be a separate DCP within each CSD or Central Bank, and thus has a DCP account and related contractual arrangements with each of the CSDs or Central Banks concerned.

8.7. T2S SD.CON 070: Routing services

T2S allows duly authorised T2S Actors to configure routing information which T2S uses to

Currency Participation Agreement

Schedule 5 – T2S Service Description

1685 deliver outgoing messages to them. Each T2S Actor can set up several routing conditions and
1686 each routing condition includes the network service and the technical address. T2S identifies the
1687 T2S Actor entitled to receive the message on the basis of on the configuration in the Common
1688 Static Data, namely:

- 1689 ▪ the message subscription preference of the recipient.
- 1690 ▪ the technical address to which the message should be routed (when there are multiple
1691 technical addresses, the first technical address (according to priority) is chosen).

1692 T2S ensures that outbound messages will be routed to the appropriate technical address of the
1693 receiving T2S Actors.

1694 T2S sends a message as a direct response upon receipt of a message, It sends the message to the
1695 T2S Actor's technical address, which was used to send the underlying message, rather than the
1696 address defined in the Common Static Data.

1697

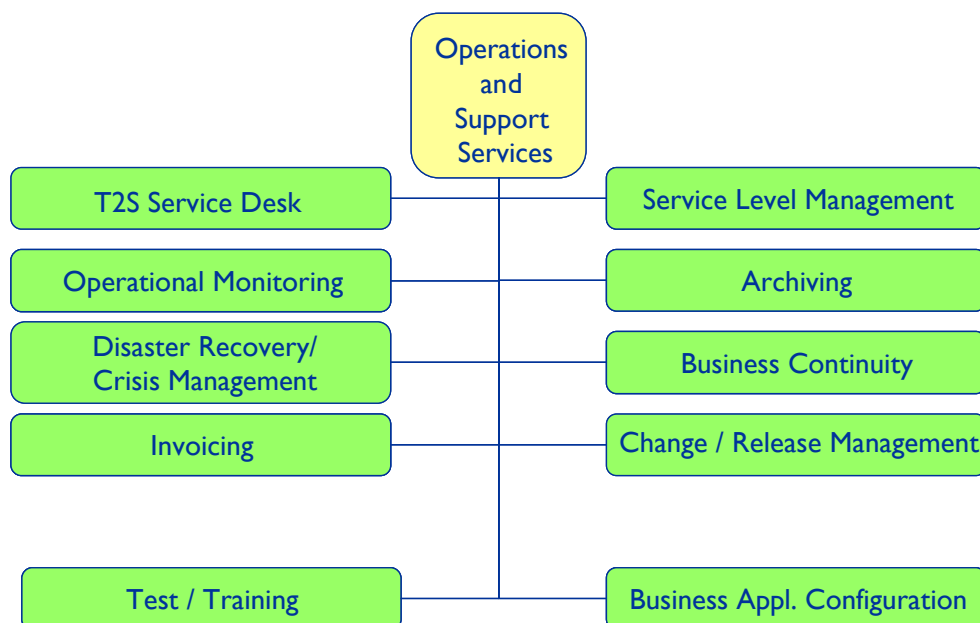
Currency Participation Agreement

Schedule 5 – T2S Service Description

9. T2S SD. SUP: Operations and support service class

Level 2
Service
Classes

Level 3
Services



To ensure service support and delivery in accordance with agreed Service Levels, T2S uses predefined processes based on the proven Information Technology Infrastructure Library (ITIL) concept. ITIL provides a set of best practices for managing information technology (IT) infrastructure, development, and operations.

T2S Service delivery is coordinated through the operations and support services and the required activities and processes are delivered and managed in accordance with agreed Service Levels for T2S.

9.1. T2S SD.SUP 010: Business application configuration services

T2S ensures the continuous management of its configuration.

9.1.1. T2S SD.SUP 011: T2S Calendar service component

For settlement of transactions against payment/delivery and/or free-of-payment/delivery in euro or non-euro CeBM, a common calendar is defined in the Service Level Agreements, as followed by all euro area markets.

During weekends, after the end of the Friday Settlement Day, T2S moves to the Settlement Day of the following Monday and performs the related activities until the end of the Night-Time Settlement Period. On the Monday, T2S starts with the preparation of Day-Time Settlement as

Currency Participation Agreement

Schedule 5 – T2S Service Description

1716 the continuation of the same Settlement Day¹².

1717 **9.1.2. T2S SD.SUP 012: T2S Settlement Day service component**

1718 T2S operates on a single harmonised timeframe for centralised settlement procedures in euro and
1719 non-euro CeBM. This timeframe represents a balance between the user requirements for a pan-
1720 European timetable and the constraints and business needs of existing local schedules, and is in
1721 accordance with the market's request for harmonised post-trading practices in the EU.

1722 T2S settlement services are available continuously during the Night-Time and the Day-Time
1723 settlement periods except for a short period during the Maintenance Window. T2S does not
1724 perform any settlement services outside the Night-Time and Day-Time settlement periods.

1725 The change of the T2S settlement date defines the start of a new Settlement Day. Following the
1726 change of the Settlement Date:

- 1727 ▪ T2S validates settlement instructions against Common Static Data valid as of the new
1728 settlement date and resulting from validated changes to the Common Static Data ; and
- 1729 ▪ T2S settles instructions on the new settlement date.

1730 The following is an overview of the T2S Settlement Day. A detailed description including time
1731 lines can be found in the T2S Manual of Operational Procedures (MOP):

- 1732 ▪ The T2S Settlement Day begins with a start-of-day (“SOD”) period, starting after the
1733 change of the settlement date and ending prior to the start of night-time settlement. It
1734 includes processes that are critical for the smooth preparation of the night-time settlement
1735 procedures, such as the identification and revalidation of eligible instructions and
1736 changes to the Common Static Data valid as from or as for this settlement date. During
1737 this period liquidity transfers from RTGS systems will be accepted.
- 1738 ▪ The following Night-Time Settlement Period starts after the end of the “SOD” period and
1739 ends prior to the Maintenance Window. During the Night-Time Settlement Period mainly
1740 settlement instructions that were input on previous Settlement Days with an Intended
1741 Settlement Date that corresponds to the current settlement date are processed. The Night-
1742 Time Settlement Period consists of two settlement cycles..
- 1743 ▪ After the Night-Time Settlement Period the T2S Schedule includes a technical window
1744 for system maintenance.

¹² Additional detail and further rules regarding the T2S calendar can be found in the Manual of Operating Procedures (MOP)

Currency Participation Agreement

Schedule 5 – T2S Service Description

- 1745 ▪ After the end of the Maintenance Window T2S starts the Day-Time Settlement Period,
1746 which is used mainly for T+0 (same-day or intraday) settlement. In addition, it is during
1747 this period that failures from night-time settlement can be resolved.

- 1748 ▪ Before the End-of-Day (EOD) period starts, T2S operates different cut-off times for DvP,
1749 FoP, Central Bank operations¹³.

1750 The EOD period of T2S starts after the end of the Day-Time processing and finishes prior to the
1751 change of the settlement date, permitting CSDs and their participants to perform critical end-of-
1752 day activities, such as fulfilling reporting requirements. From the start of the end-of-day
1753 procedure, securities and cash positions are stationary (with the exception of EOD procedures
1754 related to the auto-collateralisation as described above) since no settlement can occur until the
1755 start of the next Settlement Day's Night-Time Settlement period.

1756 **9.2. T2S SD.SUP 020: Operational monitoring services**

1757 The T2S Operator monitors the T2S infrastructure and the T2S business application
1758 continuously:

- 1759 ▪ The T2S Operator observes the behaviour of the T2S production environment. If
1760 deviations from the normal Settlement Day are detected (the normal Settlement Day
1761 being defined as the behaviour of T2S over a defined time period):
- 1762 ○ within defined boundaries, the T2S Operator can trigger the appropriate
1763 corrective actions, when required, and
 - 1764 ○ if necessary, the T2S Operator raises the alarms and indicates the appropriate
1765 level of priority as quickly as possible;
- 1766 ▪ In the event of operational issues the T2S Operator cannot resolve, the T2S Operator
1767 reports aggregated, up-to-date monitoring information.
- 1768 ○ In crisis and contingency situations, the T2S Operator provides up-to-date and
1769 comprehensive information to the crisis manager.
 - 1770 ○ In the event of an incident or problem, the T2S Operator provides and tracks
1771 information about the status and logs its history, as well as documenting the
1772 analysis and solution.

¹³ See further details in the SLA and in the MOP

Currency Participation Agreement

Schedule 5 – T2S Service Description

- 1773 ▪ The T2S Operator reports his activities to assist in the Service Performance Indicators
1774 reporting required for Service Information and monthly Service Level Agreement
1775 reporting.

1776 **9.3. T2S SD.SUP 030: Business continuity management services**

1777 Business continuity in T2S is understood to mean managing single component failures as well as
1778 failures of a single site without losing data. The Business Continuity Management service
1779 ensures that the required IT technical and services facilities (including computer systems,
1780 networks, applications, telecommunications, technical support and Service Desk) can be
1781 recovered within required, and agreed, business time-scales.

1782 The technical environment for the T2S data centre and application follows the “two regions / four
1783 sites” architecture. Inside a region, the distance between the two sites is more than 10 kilometres.
1784 System and application software are kept updated in parallel at the four sites and each of the four
1785 T2S sites satisfies the agreed Service Levels.

1786 Different mechanism and procedures are implemented to guarantee business continuity:

- 1787 ▪ Single component failure
- 1788 ○ Hardware/Software and telecommunication components redundancy
- 1789 ○ software quality control and test execution
- 1790 ○ operational procedures (e.g. Change and Release Management)
- 1791 ▪ Site failure
- 1792 ○ Data in the two local sites are mirrored synchronous
- 1793 ○ Local recovery procedure to restart on alternate site

1794 **9.4. T2S SD.SUP 040: Disaster recovery and crisis management services**

1795 Disaster recovery services in T2S are understood to mean ensuring the resumption of T2S
1796 Services which were discontinued due to a high-impact disruption of normal business operations
1797 affecting a large metropolitan or geographic area and the adjacent communities that are
1798 economically integrated with it. In addition to impeding the normal operation of financial
1799 industry participants and other commercial organisations, major operational disruptions typically
1800 affect the physical infrastructure.

1801 Disasters are events which are unforeseeable, unavoidable and beyond the reasonable control of
1802 the T2S Actor affected by the event and which has not been foreseen (“Force Majeure”).

1803 Disaster recovery services ensure that the T2S Services can be recovered in an alternate region
1804 within the times defined in the Service Level Agreement. The T2S Business Application is

Currency Participation Agreement

Schedule 5 – T2S Service Description

installed in two separate regions and the data in the two regions are mirrored in asynchronous mode. Regional disaster recovery procedures are defined to restart the solution and the applications in the alternate region. Additionally, T2S uses a “periodical rotation” procedure to ensure that all staff are properly trained and both regions are capable of hosting the T2S Services. T2S has defined a crisis management process to coordinate all activities in crisis situations. The crisis management process guarantees effective coordination of activities within all the involved organisations and appropriate communication, i.e. early warning and clear instructions to all concerned, if a crisis occurs.

9.5. T2S SD.SUP 050: Archiving services

T2S provides a central archive for its own purposes covering a 10-year period. The T2S central archive includes T2S static and transactional data.

T2S archives immediately all incoming and outgoing messages and files in their original format. After three months, T2S archives all instructions (settlement instruction, cash movements) as well as Common Static Data, billing and audit data.

In order to ensure the integrity of static and transactional data, Common Static Data revisions and Common Static Data history remain in the operational databases until the archiving procedures moves the transactional data that reference it into the archiving database.

CSDs, Central Banks and T2S Operators have direct access to archived data via A2A or U2A interfaces. Provided it is duly authorised by its Central Bank, a DCA holder has direct access to archived data of relevance to it. Other T2S parties have to request their Central Banks to retrieve and provide archived data to them.

9.6. T2S SD.SUP 060: T2S service desk services

T2S service desk provides a single, central point of contact for the CSDs, Central Banks, DCPs (if so authorised by their CSD), or DCA holders (if so authorised by their NCB) for handling all incidents, queries and requests related to business, functional or technical issues related to T2S. The T2S service desk is accessible 24 hours a day on T2S operating days. The Service Levels differ depending on the time of day.

On the basis of the complexity level of the service request/ enquiry, the T2S service desk guarantees different response times, in accordance with the response time matrix as published in the Service Level Agreement. Service Levels are measured against this matrix. All enquiries are recorded, and confirmations are provided to CSDs, Central Banks or DCPs (if duly authorised by their CSDs) when service requests are received.

T2S has ITIL-based problem and incident management processes in place:

Currency Participation Agreement

Schedule 5 – T2S Service Description

- Incident Management - Incident Management captures the details of all incidents reported, implements temporary work-arounds and manages the resolution of incidents. Its goal is to restore normal service operation with minimum disruption to the business.
- Problem Management - The goal of Problem Management is to minimize the adverse impact of incidents and “known errors” on the business. The main focus of Problem Management is to identify the root cause(s) of incidents and to eliminate these if this is possible. While problems are being resolved Problem Management may produce temporary ‘work-arounds.’

An incident is defined as an event which is not part of the standard operation of the T2S Service and which cause, or may cause, an interruption or a reduction of the quality of that service. Incidents must be resolved immediately and are not part of the Change and Release Management.

A problem is defined as an abnormal state or condition at the component, equipment, or sub-system level, which may lead to a failure in T2S that produces incorrect or unexpected results, showing a discrepancy between the relevant specifications and the actual results. Based on reported and acknowledged problems, and their criticality, T2S and the CSDs agree how to resolve them. A problem can result in a Change Request.

9.7. T2S SD.SUP 070: Service Level management services

T2S uses a Service Level Management process to maintain and improve service quality through a constant cycle of agreeing, monitoring and reporting of service achievements and instigating actions to correct non-adequate service delivery.

T2S provides reports on actual Service Levels achieved on a monthly basis. For each service indicator as defined in the Service Level Agreement, the performance achieved is compared with the target values. These reports are provided in accordance with the rules laid down in the Service Level Agreement.

9.8. T2S SD.SUP 080: Invoicing services

Invoicing services in T2S consist of:

- Automatically calculated invoices that are set up on a regular basis
- On demand: Ad hoc invoicing in special cases (for CSDs / Central Banks and / or customers of CSDs / Central Banks)

For both types of invoices, i.e. T2S invoice to CSDs and CSD invoicing support, the Invoice cannot be amended or adapted. Only

- approval
- cancellation and

Currency Participation Agreement

Schedule 5 – T2S Service Description

1871 ▪ (re-) generation

1872 are defined actions.

1873 If a T2S Actor needs to receive a prior invoice (again), it can do so via a query in both A2A and
1874 in U2A mode.

1875 **9.8.1. T2S SD.SUP 081: T2S invoicing to CSDs and Central Banks service**
1876 **component**

1877 T2S automatically calculates invoices based on fees in accordance with the current T2S Tariff
1878 Structure and Price List. T2S invoicing reflects changes in the T2S Tariff Structure and Price
1879 List, which may be implemented at any time, but become effective only at the beginning of a
1880 billing period.

1881 The invoice is calculated at the beginning of each calendar month for the past calendar month.
1882 All prices are calculated in Euro and VAT regimes in the different countries are taken into
1883 account, in case VAT needs to be included. Invoices and the underlying information are archived.
1884 CSDs and Central Banks receive a summary invoice, showing aggregate data for each billing
1885 item.

1886 The prices for instructions are always charged to the CSDs of the two counterparties involved in
1887 a settlement instruction. Each Security Account and DCA needs to be assigned unambiguously to
1888 one CSD or Central Bank for the billing of the fixed fees.

1889 Invoices are sent out once via push mechanism to the technical address which is defined in the
1890 Common Static Data. The invoice can also be queried using the GUI. As an additional service, ad
1891 hoc billing is possible in special cases.

1892 Changes in the Pricing scheme may be implemented at any time, but become effective only at the
1893 beginning of the next billing period.

1894 **9.8.2. T2S SD.SUP 082: CSDs / Central Banks invoicing support service**
1895 **component**

1896 T2S supports the CSDs/ Central Banks by enabling them to invoice their clients in accordance
1897 with their individual tariff structures. To that end, as part of the T2S information services, a CSD/
1898 Central Bank may query any of its assigned accounts, but no others.

1899 T2S provides counters for all settlement process steps and instances as enumerated and described
1900 in the T2S data model. As part of the CSD/ Central Bank invoicing support service, each CSD/
1901 Central Bank is able to query this level of data for each of its customer accounts.

1902 T2S transmits details to the CSD/ Central Bank via a report based on an event at the end of the
1903 invoicing period. The CSD/ Central Bank invoicing support report provides additional
1904 information on billable items at the level of each customer account as an itemised list. This is

Currency Participation Agreement

Schedule 5 – T2S Service Description

1905 either sent in push mode or made available for pull mode.

1906 Furthermore, on a monthly basis T2S provides a standard report containing all detailed
1907 transactional data and counters for each CSD/ Central Bank which is available only to the
1908 respective CSD/ Central Bank in pull mode. Each CSD / Central Bank receives only the data
1909 related to its and its DCPs interactions with T2S, i.e. the invoicing support report is CSD-/
1910 Central Bank - specific and does not contain any data or information concerning any other CSD/
1911 Central Bank.

1912 **9.9. T2S SD.SUP 090: Change and Release Management services**

1913 T2S is an evolving application, increasing and improving services by following a defined Change
1914 and Release Management process. Any T2S Actor who identifies a need to change T2S, may
1915 request new or amended features and/or functionalities following the agreed Change and Release
1916 Management, specified in Schedule 9 to the Framework Agreement and the Currency
1917 Participation Agreement. If there are inconsistencies between the description in this section and
1918 the provisions of the Schedule, the latter shall prevail.

1919 CSDs may change parameters/configuration (i.e. rules for CSD validation hold/reject and the
1920 CoSD functionality) or reference data (i.e. ISIN, Security Account) without launching the
1921 Change and Release Management, although these actions may be subject to operational
1922 procedures, in particular if there is an impact on any other T2S Actors.

1923 T2S uses ITIL based processes for Change and Release Management: These services encompass
1924 all stages of the Change Lifecycle from initiation and recording, through filtering, assessment,
1925 categorization, authorization, scheduling, building, testing, implementation and ultimately their
1926 review and closure.

1927 The Eurosystem has established a Change Review Group (CRG) to evaluate the information
1928 provided in the Change Request and in the preliminary assessment (especially checking its
1929 consistency and completeness across all Change Requests) and to prepare for the change
1930 authorisation or rejection decision. The CRG is responsible for building and maintaining the
1931 scoring mechanism as a tool for facilitating the definition of the content of each T2S release and
1932 making proposals for, reviewing and monitoring the content of T2S releases as well as any
1933 changes to any agreed release.

1934 **9.9.1. T2S SD.SUP 091: Change Management service component**

1935 Changes in T2S, which are subject to the Change and Release Management, are defined as
1936 changes on T2S functionality and/or to the Scope Defining Set of Documents. Changes may arise
1937 for a number of reasons:

- 1938 ▪ Innovation and improvement – the introduction of new services/ technical capability

Currency Participation Agreement

Schedule 5 – T2S Service Description

- 1939 ▪ New functionality to meet business needs of T2S Parties
- 1940 ▪ Changes in law or in regulatory (including fiscal) requirements
- 1941 ▪ Clarifications/corrections to functional and/or technical documentation/gaps in line with
- 1942 the user requirements
- 1943 T2S distinguishes between the following types of changes:
- 1944 - according to beneficiary:
- 1945 ▪ Common Changes include new features, functionalities or services which are
- 1946 implemented for the benefit of – and available without restrictions to – all T2S Actors.
- 1947 They have an impact on all T2S Actors and the costs are shared by all T2S Actors.
- 1948 ▪ Specific Changes are any new feature, functionality or services which is not implemented
- 1949 as a Common Change, but which some CSDs/CBs wish to implement, and to which the
- 1950 other CSDs/CBs do not object. The costs of these changes are shared only by the entities
- 1951 using the feature, functionality or service, which is changed. The functionality is used
- 1952 only by the supporting parties but is made available to all T2S Actors.
- 1953 - according to urgency:
- 1954 ▪ Normal changes are changes that can be planned and go through the whole Change and
- 1955 Release Management before being implemented into the live environment.
- 1956 ▪ Fast-track Changes are changes that are imposed by Legal and Regulatory Requirements,
- 1957 or by CSG resolutions related to risk management requirements, or changes that are
- 1958 critical for the stability of the T2S Platform or by Central Bank decisions related to
- 1959 safeguarding the currency/-ies or related to crisis management measures to ensure
- 1960 financial stability and that, owing to the time constraints, have to be implemented in a
- 1961 shorter timeframe than normal, which will be decided on an ad-hoc basis, as specified in
- 1962 Schedule 9. These changes will also go through the normal CRM process, however, the
- 1963 length of the different process steps will be shortened on an ad-hoc basis, in particular for
- 1964 preliminary and detailed assessment.
- 1965 Each change will be categorised based on the following parameters:
- 1966 ▪ Legal/Business importance
- 1967 ▪ Market implementation efforts
- 1968 ▪ Operational/technical impact
- 1969 ▪ Financial impact for T2S
- 1970 Every initiated Change Request is identified via a Change Request identifier. All Change
- 1971 Requests are published and made available to all duly authorised T2S Actors in accordance with

Currency Participation Agreement

Schedule 5 – T2S Service Description

the agreed Governance arrangements and the agreed Change and Release Management, specified in Schedule 9 to the Framework Agreement and the Currency Participation Agreement.

In certain cases an incident may result in an urgent intervention on T2S aiming to ensure a quick restoration of T2S Services. On account of its urgency, such a intervention cannot be processed via the normal Change and Release Management. These Fast-track Changes are therefore processed via faster operational procedures as defined and further detailed in the Manual of Operational Procedures (MOP).

9.9.2. T2S SD.SUP 092: Release Management service component

Once the changes have been duly authorised for implementation, they are bundled and assigned to future T2S releases. The term “Release” is used to describe a collection of authorised Change Requests which consist of enhancements to the T2S Service and/or a number of bug fixes which are implemented into the production environment. A scoring mechanism is applied to identify all authorised changes and bug fixes for a specific release. The Release Management services include the planning, design, build, configuration and testing of T2S software and hardware needed for the implementation of the changes to create a set of release components.

The Release Management services ensure that all aspects of a change, technical and non-technical, are considered together. The main objective is to deliver, distribute and track one or more changes intended for simultaneous release into T2S operations while protecting the integrity of the T2S production environment and its services. Release Management services ensure that authorised changes and bug fixes that have been agreed as part of a release are secure and traceable, and that only correct, tested and authorised versions are installed into the production environment. Furthermore, through Release Management any amended legal or contractual obligations T2S has to comply with will be implemented.

Before implementing any release, T2S performs T2S-internal acceptance tests to verify that the system operates as predicted and fulfils the requirement and the functional specification of the Change Request.

Once T2S-internal acceptance test is finalised, T2S provides the CSDs and Central Banks with the test results and confirms the readiness of the T2S testing environments for the T2S User Testing. The test calendar is agreed with the CSDs and Central Banks, and information is provided on the testing activities, and regarding the availability of the testing environments.

The release is verified in accordance with the Governance arrangements, with the involvement of the CSDs and Central Banks once the exit criteria of the verification process have been completed successfully.

The delivery of the application software release into the production environment is the final step in the Release Management.

T2S provides and updates T2S User Documentation as part of the Release Management.

Currency Participation Agreement

Schedule 5 – T2S Service Description

2008 **9.10. T2S SD.SUP 100: Test and training services**

2009 **9.10.1. T2S SD.SUP 101: Testing service component**

2010 The objectives of the T2S User Testing are:

- 2011 ▪ to ensure that T2S fully meets user requirements as expressed in the Change Requests of
- 2012 the relevant release, as well as the functional and non-functional specifications agreed by
- 2013 T2S,
- 2014 ▪ to guarantee the readiness of the CSDs, Central Banks and its DCPs to operate in
- 2015 accordance with the agreed release.

2016 T2S provides diverse testing environments for T2S Actor testing activities:

- 2017 ▪ one for the CSD/ Central Bank wanting to test changes in their own applications against
- 2018 the current T2S operating environment,
- 2019 ▪ other(s) for the CSD/ Central Bank to test future T2S releases.

2020 The T2S testing environments are sized and prepared for interconnection with the testing

2021 environments of the T2S Actors via test networks. T2S reserves the right to block one

2022 environment for its own regression testing of new releases.

2023 The security levels of the testing environments are the same as for the T2S production

2024 environment. The testing environments have a substantially lower technical capacity compared to

2025 the production environment. This capacity can be increased to cover specific testing needs (e.g.

2026 high-volume tests during the Community testing and the Business Day testing stages). During the

2027 T2S User Testing execution phase, the T2S operating procedures reflect as much as possible

2028 those that are agreed for live operations.

2029 T2S testing environments use the same problem and incident processes as the operating

2030 environment.

2031 **9.10.2. T2S SD.SUP 102: Training service component**

2032 T2S delivers training services to the CSDs, Central Banks and DCPs based on the “train the

2033 trainer”-concept. The exhaustive and self-explanatory T2S training documentation shall facilitate

2034 in-house training at CSDs, Central Banks and at their participants. The scope of T2S training

2035 sessions covers aspects of the day-to-day activities of technical, functional and operational nature

2036 as well as one-off activities for the testing of and migration to T2S.

2037 T2S provide the CSDs and the Central Banks with the T2S Training Framework, on the basis of

2038 which T2S defines and elaborates the T2S Training Packages. Depending on the training delivery

2039 strategy and mode selected (inherent in the T2S Training Framework), T2S guides, delivers and

2040 provides support for the T2S training for the CSDs and for the Central Banks.

Currency Participation Agreement

Schedule 5 – T2S Service Description

2041 The T2S Training Framework is elaborated and rolled out so that a timely and efficient
2042 knowledge transfer to the end-users of T2S can be accomplished. The T2S Training Framework
2043 further clarifies and details all organisational and planning aspects related to the training.

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 6

T2S SERVICE LEVEL AGREEMENT

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

Table of contents

1. Introduction	1
2. Parties, commencement date and review	2
2.1 Identification of the parties	2
2.2 Scope	2
2.3 Commencement date	2
3. Service responsibilities	4
3.1 Eurosystem's responsibilities	4
3.2 Responsibilities of the [NCB]	6
3.3 Operational procedures	8
4. Service Level targets in the production environment	10
4.1 Definitions of Service Level indicators	10
4.1.1 Service availability	10
4.1.1.1 Availability Period.....	10
4.1.1.2 Substantial Delay.....	11
4.1.1.3 Availability.....	11
4.1.2 System performance	12
4.1.2.1 Business Validation Time	12
4.1.2.2 Cash Transfer Settlement Time	12
4.1.2.3 Central Bank Static Data Processing Time	13
4.1.3 Response times	13
4.1.3.1 A2A Query Response Time	15
4.1.3.2 A2A Message Response Time.....	15
4.1.3.3 U2A Response Time.....	15
4.1.3.4 File Throughput	16
4.1.3.5 Online Storage Period.....	16
4.1.3.6 Archiving Period.....	16
4.1.3.7 Archive Retrieval Response Time	16
4.1.4 Support hours and incident response times	17
4.1.4.1 T2S Settlement Day	17
4.1.4.2 Support Hours.....	17
4.1.4.3 Incident Response Time.....	18
4.1.4.4 Incident Resolution Time	18
4.1.5 Business Continuity and Disaster Recovery.....	18

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

4.1.5.1 Recovery time.....	19
4.1.5.2 Recovery Point Objective	19
4.2 Committed Service Levels for the production environment	20
4.2.1 Operational and support services	20
4.2.2 Settlement services and liquidity management services	22
4.2.3 Central Bank Static Data services.....	22
4.2.4 Information services	23
4.2.5 Connectivity services.....	23
4.3 Targeted Service Levels for the production environment.....	24
4.3.1 Operational and support services.....	24
4.3.2 Settlement services and liquidity management services	24
4.3.3 Central Bank Static Data services.....	25
4.3.4 Information services	25
5. Service Levels for the test environments	26
5.1 Service Levels for the test environment in “current mode”	26
5.1.1 Operational and support services.....	26
5.1.2 Settlement services and liquidity management services	27
5.1.3 Central Bank Static Data services.....	28
5.1.4 Information services	28
5.1.5 Connectivity services.....	28
5.2 Service Levels for the test environment in “future mode”	29
5.2.1 Operational and support services.....	29
5.2.2 Settlement services and liquidity management services	31
5.2.3 Central Bank Static Data services.....	31
5.2.4 Information services	32
5.2.5 Connectivity services.....	32
5.2.6 Additional provisions.....	32
6. System capacity and platform sizing	34
7. Service Level reporting.....	35
7.1 Content of the Reporting.....	35
7.2 Definition of Additional Indicators for Reporting.....	36
7.2.1 Punctuality.....	36
8. Service review meetings	38
9. SLA reviews.....	39
9.1 Initial review	39
9.2 Subsequent review.....	39

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

Annex 1 - Management of non-functional changes 1

Emergency Changes.....1

Other changes 1

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

1. Introduction

This Service Level Agreement (SLA) documents the commitments of the parties named below to each other, in particular the service levels under which the Eurosystem will provide the relevant T2S services to the Connected Central Banks (and vice versa), which have entered into the Currency Participation Agreement with the Eurosystem.

Annex 1 (Management of non-functional changes) to this document covers the process to manage non-functional changes needed to maintain the agreed service levels, or to increase them as a result of the SLA review process.

This SLA assigns responsibilities to and describes interactions between the parties. This SLA defines the agreed service levels for the provided services. The legal rights and obligations between the parties that apply when the service level is not reached, are specified in the provisions laid down in the Currency Participation Agreement.

This SLA is part of the legal arrangements between the Eurosystem and non-euro area Central Banks, under the Currency Participation Agreement. Unless explicitly mentioned this SLA is the same as the one concluded with all other Connected NCBs. It is the intention of both parties to reach the highest possible level of harmonisation between all SLAs. It is intended that the commitments of the Eurosystem and the Connected NCBs set out in chapters 2, 3, 4, 7 and 8 will not be altered without mutual agreement. The commitments in chapters 5 and 6 will be subject to the amendment process defined in the CPA.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

2. Parties, commencement date and review

2.1 Identification of the parties

The parties to this Service Level Agreement are those indicated in the core Currency Participation Agreement, i.e. the Eurosystem and the [NCB].

As a matter of fact, the Dedicated Cash Account (DCA) Holders do not have a direct legal relationship with the Eurosystem for the use of T2S Services. Nevertheless, they will obtain certain rights and be subject to certain obligations from this SLA through the mandatory inclusion of certain provisions in their legal arrangements with their Connected NCB(s). These provisions are explicitly reflected in section 4.2 of this SLA.

2.2 Scope

This SLA relates to the production phase of T2S, as well as to the User Testing phase prior to the migration of the [NCB] to T2S. Consequently, this SLA refers to the T2S production environment and its accompanying test environments both before and after migration. It covers the full range of services as described in Schedule 5 (T2S Service Description) for each of the service classes, i.e. Settlement Services, Liquidity Management Services, Static Data Management Services, Information Services, Connectivity Services, and Operational and Support Services. In addition, this SLA covers the relevant service commitments from the Eurosystem with respect to the support of the User Testing activities as specified in Schedule 3 (User Testing).

2.3 Commencement date

This SLA shall enter into force as from the day the [NCB] starts its User Testing activities on the T2S Platform. More specifically, as from that day until the end of the Migration Period, the provisions with respect to the test environment in “future mode” will apply, as specified in section 5.2, and will apply to any additional test environment that will be made available to support these User Testing activities in accordance with Schedule 3 (User Testing). After the end of the Migration Period, these provisions shall apply again from the day any new release is made available in this environment until the go-live date of this new release.

In addition, as from the start of the first T2S Settlement Day, the Eurosystem is committed to deliver the T2S Services according to the Key Performance Indicators (KPIs) as specified in section 4.2 and 5.1 of this SLA. The values of some KPIs defined in section 4.1 of this SLA will only be specified in section 4.2 after a bedding-down period¹, during which both parties shall aim

¹ The values for these not yet specified KPIs have been stated as “xx”.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

51 to fulfil their obligations on a best effort basis, using all reasonable means and in a constructive
52 spirit. The purpose of the bedding-down period is to fine-tune the operational procedures and the
53 [NCB]'s usage of T2S in a way that ensures that both parties will be able to fulfil their
54 obligations according to the agreed service levels.

55 The bedding-down period shall start on the first Settlement Day of the migration period and shall
56 last for a period of six months after the end of the migration period. Its duration may be shortened
57 or prolonged upon agreement by the parties according to the usage patterns of the T2S service.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

3. Service responsibilities

3.1 Eurosystem's responsibilities

The Eurosystem must:

- a) establish the T2S service desk as a Single Point Of Contact (SPOC) for the [NCB] (for technical and operational problems) and provide its contact details (e-mail, mobile phone, telephone, fax);
- b) support the [NCB] in the operational management of its technical connection and that of its DCA holders if needed;
- c) ensure the permanent reachability of a T2S Crisis manager, T2S Operator's Crisis manager, Service manager and T2S co-ordinator and provide their contact details (e-mail, telephone, fax);
- d) be able to extend the cut-off time for cash transfers in the currency provided by and at the request of the [NCB], in accordance with the provisions of the MOP;
- e) refrain from scheduling T2S downtimes without pre-advice and green light of the Connected NCBs outside the normal Maintenance Windows;
- f) announce planned non-functional changes according to provisions specified in Annex 1 to this Schedule;
- g) provide on-line access to information to allow the [NCB] to track and follow up all incidents, problems and enquiries related to or impacting the [NCB];
- h) manage the impact on the [NCB] and the T2S Service as a whole caused by any party making unusual demands on capacity by:
 - a. contacting the service user without delay if the latter or one of its clients consumes system resources to an extent that exceeds the forecasted capacity and might prevent the Eurosystem from delivering the agreed service to other service users;
 - b. denying (up to and including temporary disconnection) access to a service user or one of its clients (according to the conditions and procedures defined in the MOP), if he is threatening the stability of the platform impacting other service users and does not respond effectively to the Eurosystem's request to reduce the unusual capacity demands;
- i) deny the service by disconnecting any service users that did not respond effectively to a request from the Eurosystem to reduce the unusual capacity demands and that continues

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

90 to threaten the stability of the platform with impact on other service users (according to
91 the conditions and procedures defined in the MOP), until the service user has
92 demonstrated that the threat no longer exists;

93 j) ensure an adequate long-term planning for capacities corresponding to the requirements
94 laid down in section 7 of this SLA;

95 k) inform the [NCB] if technical problems with one of its T2S Dedicated Cash Account
96 Holders are detected that might have an impact on the [NCB] as well;

97 l) maintain documentation pertaining to Crisis management and provide it to the [NCB] on
98 request or after any change;

99 m) support the [NCB] in business continuity testing if required (subject to prior agreement).

100 During normal operation the T2S co-ordinator (appointed by the Eurosystem), the T2S Service
101 manager (appointed by the T2S Operator) and the CB settlement managers (appointed by each
102 Central Bank), will apply the procedures specified in the Manual of Operational Procedures (see
103 also section 3.3). In addition, the Eurosystem stands ready to provide through the T2S Service
104 Desk

105 ▪ information on technical and operational issues, in particular concerning the T2S
106 application and platform;

107 ▪ information on T2S functionality;

108 ▪ up-to-date information concerning the T2S application and platform, if need be.

109 If a Crisis situation, as described in art. 23.1 of the Currency Participation Agreement, arises
110 within the domain of the Eurosystem, the latter will inform the [NCB] according to the agreed
111 response times (see chapter 4.1.4.3).

112 In addition, the following provisions will apply in such case:

113 ▪ The Eurosystem will take all necessary actions to restore the T2S Service according to
114 the agreed business continuity procedures as defined in the MOP. These procedures are
115 based on the following key principles:

116 ○ Any settlement in T2S before the incident will continue to have the legal effect
117 specified in art. 20.1 of the Currency Participation Agreement.

118 ○ If a data loss materialised, the recovery will be done together with the [NCB] by
119 procedural means.

120 ▪ As soon as the Eurosystem identifies the need to switch to the other site in the same
121 region, or to fail-over to the standby region, the T2S co-ordinator initiates a
122 teleconference to inform the settlement manager of the [NCB] about the nature of the

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

event triggering the failure, the nature of the failure and the envisaged plan to recover from the failure.

- The Eurosystem will keep the settlement manager of the [NCB] informed about the progress of the failover activities, and in particular when T2S is available again for normal operations.

- The Eurosystem may decide to gradually re-open T2S, in which case it will seek the approval of the [NCB].

- In case T2S cannot be restarted without a potential data gap, the Eurosystem will first re-open T2S for the purpose of reconciliation only, and will co-ordinate these reconciliation activities.

- During this reconciliation phase, the [NCB] is responsible to verify the status of its T2S records, and to re-send instructions with the aim to bring the T2S records consistent with its internal records. This includes also changes to the T2S records that happened as a result of an interaction with a DCA holder belonging to the [NCB]. It is up to the [NCB] to agree with its DCA holders how this is organised.

- The Eurosystem and the [NCB] will co-operate in good faith and will - if necessary - agree on additional measures with the aim to close the data gap.

- The Eurosystem will seek the agreement of the [NCB] to re-open T2S for normal operations.

- The Eurosystem will provide any service described for normal operations, but balancing this with the need to restore the service.

- The Eurosystem will provide reports on unresolved incidents.

Detailed procedures for incident priority setting and incident handling will be specified in the Manual of Operational Procedures (MOP).

3.2 Responsibilities of the [NCB]

The following responsibilities are accepted by the [NCB] in order to allow the Eurosystem to meet the agreed Service Levels.

The [NCB] must:

- a) appoint and ensure the permanent reach ability of a settlement manager and a Crisis manager as contacts for the Eurosystem and provide their contact details² (e-mail, telephone, mobile phone, fax);

² At the Connected NCB's discretion, the Settlement Manager and the Crisis Manager can be the same person.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

- b) provide contact details for technical staff that is capable of resolving technical issues with their (directly connected) Dedicated Cash Account Holders (e.g. staff belonging to the DCA Holders' organisation);
- c) inform the relevant DCA Holders
 - a. before requesting the Eurosystem to extend the cut-off time for cash transfer in the currency provided by the [NCB],
 - b. before preventing additional cash to be transferred to the Dedicated Cash Accounts, and
 - c. before draining a significant amount of cash from the Dedicated Cash Accounts back to the RTGS system;
- d) have a local service desk to support all its Dedicated Cash Account Holders during normal business hours;
- e) proactively report within a reasonable time any problem or incident relating to T2S including connectivity problems, provide all information that might be helpful and cooperate where requested by taking all appropriate actions for solving the problem or incident;
- f) provide timely information on any changes that may affect the [NCB]'s ability to interact with T2S as expected;
- g) ensure an appropriate use of T2S, interaction with its systems and that the personnel who works on T2S and its own systems and equipments is accordingly qualified and suitably trained;
- h) ensure availability of skilled staff within a pre-agreed time period in order for the Eurosystem to obtain support in handling incidents and/or reducing their impact on the service;
- i) be able to resend – at the request of the Eurosystem - all messages already sent after a specified recovery point during the same Settlement Day (approx. two minutes - in particular in case of disaster recovery scenarios with possible data loss);
- j) keep all access rights it has registered for access in T2S consistent with all relevant user information;
- k) provide all DCA holders with all relevant information to facilitate their smooth migration to and functioning in T2S;
- l) ensure the operational management of its own organisation and systems and impose similar requirements on its customers including DCA holders, as far as applicable;

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

- m) use reasonable efforts to ensure its connectivity with T2S and require the same of its DCA holders, as far as applicable according to Article 30;
- n) take part in the test process for new releases in the test environment;
- o) co-operate with the Eurosystem by promptly reporting any difficulties however small following each release into the production environment;
- p) support the Eurosystem in business continuity testing if required.

3.3 Operational procedures

The Manual of Operational Procedures (MOP) will provide a reference guide for the operational procedures (in normal and abnormal situations) which the directly connected T2S Actors (including the [NCB]) and the Eurosystem should follow to ensure a smooth functioning of T2S. It will contain all the information required for the addressees to carry out all their tasks in normal and abnormal situations.

The day-to-day operational management of T2S will be handled at two levels. First, the T2S coordinator, the service manager and the CB settlement managers (jointly called settlement managers) will jointly perform the tasks and apply the procedures as specified in the MOP. Second, the T2S Crisis manager, the T2S Operator's Crisis manager and the CB Crisis managers (jointly called "the Crisis managers") will make the decisions allocated to them in the MOP, and will take over the management of T2S in situations that are not covered in the MOP. The Crisis managers will be assisted and advised by the settlement managers in that case.

The MOP will also cover the Business Continuity and Disaster Recovery arrangements, i.e. the set of rules and procedures aimed at resuming the normal T2S Services after the occurrence of an incident, as well as at mitigating the impact of such incident.

The key principles for the incident management can be summarised as follows:

If the [NCB] detects an incident that is related to or might have an impact on the T2S Services, it will inform the Eurosystem without undue delay.

If the Eurosystem detects an incident, it will be communicated to the [NCB], if a direct or indirect impact is possible.

If an incident is reported by a DCA holder of the [NCB], the Eurosystem will inform the latter without undue delay, and keep the [NCB] informed about the resolution path of such incident. Any action to escalate such incident, will be undertaken in close co-operation with the [NCB].

Both sides will co-operate to reduce the impact of an incident.

When the relevant incident management procedures have been defined in the MOP, the T2S coordinator (appointed by the Eurosystem), the T2S service manager (appointed by the T2S

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

220 Operator) and the involved CB settlement managers (appointed by each Central Bank) will co-
221 operate in good faith to follow those procedures and exchange all relevant information.

222 When the incident cannot be handled within the procedures specified in the MOP, the T2S Crisis
223 manager (appointed by the Eurosystem), the T2S Operator's Crisis manager (appointed by the
224 T2S Operator), and the CB Crisis managers (appointed by each Central Bank) will decide – in
225 accordance with the applicable governance arrangements – which measures will be taken to
226 mitigate the impact of the incident and to resume normal operations.

227 Both sides will co-operate in analysing the root-cause for an incident.

228 Both sides will co-operate in analysing the management of the incident and updating the MOP
229 should it be found lacking in any way.

230 The Eurosystem will report on the results of the root-cause analysis. An initial report will be
231 provided within two Settlement Days. An interim report will be provided within one week and a
232 final report within two weeks.

233 In situations of market-wide financial turbulence, the T2S Co-ordination function stands ready to
234 support the [NCB] as described in the CPA (on a best effort basis).

235 Whether or not a request to change a cut-off time, either from the Eurosystem or from the [NCB],
236 is related to an incident, the Eurosystem will involve the CB settlement managers and/or the CSD
237 Crisis managers in making such decision, according to the procedures further specified in the
238 MOP.

4. Service Level targets in the production environment

This section describes the Key Performance Indicators (KPIs) agreed for the delivery of the T2S Services. As a general principle, the Eurosystem has to ensure that sufficient efforts are made to fulfil all KPIs, and must take remedial action as soon as it detects that a KPI may not be, or is not, fulfilled, and he has to ensure that sufficient efforts are made to fulfil the KPI.

The [NCB] is committed to provide all reasonable support to the Eurosystem, in order to allow the latter to take such action.

T2S is a service shared between several service users. All specified service levels are therefore multilateral service levels, i.e. they define the service provided to the community of service users as a whole. Nevertheless, the service level reporting will contain the achieved bilateral service levels for the [NCB] in addition to the achieved multilateral service levels. For this bilateral reporting, the service levels reported for the [NCB] will include the service levels obtained by its DCA holders.

4.1 Definitions of Service Level indicators

This chapter provides a common definition of the service level indicators. Section 4.1.1 covers availability, and 4.1.2 and 4.1.3 list the areas identified as requiring Service Level Indicators covering system performance. 4.1.4 and 4.1.5 cover support and recovery issues. The actual agreed levels are stated for each service individually in section 4.2 below.

4.1.1 Service availability

Objective:

These indicators define the times during which the T2S Services are available in relation to the T2S Settlement Days.

4.1.1.1 Availability Period

The Availability Period is the time period during the T2S Settlement Day when the service is expected to be available to the [NCB]. The start and end time of the availability period is based on business events on the T2S Platform. Any times stated are indicative and could be altered in certain circumstances according to the Procedures specified in the Manual of Operational Procedures (e.g. delay of the end-of-day).

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

4.1.1.2 Substantial Delay

If an event defined in the T2S daily schedule is likely to be implemented later than the scheduled and has a potential impact on the [NCB], the Substantial Delay will define for each event the maximum delay that will be tolerated by the Connected NCBs. Any delay exceeding the Substantial Delay will be communicated to the [NCB]'s service desk immediately.

Any delay not exceeding the Substantial Delay is not actively communicated to the [NCB]'s service desk, but is available for querying on the platform.

4.1.1.3 Availability

Definition:

A service is considered to be available when it responds and operates according to its definition in the Service Description and its functional description in the User Detailed Functional Specification (UDFS chapter 1).

Measurement:

The availability of the services is measured continuously and objectively at pre-defined components of T2S, throughout each Settlement Day with the exclusion of the Maintenance Window.

The measurement of downtime is based on auditable data collected either automatically or manually. Manual measurements will be used in situations where no automatic log entries are available (e.g. power failure).

Downtime is the time between the start of an incident that causes the unavailability of a service and the closing of the incident that caused the downtime, i.e. when the service has been restored. In case of multiple incidents at the same time the downtime begins with the start of the first incident and ends with the closing of the last incident.

Calculation:

$$a = \left(1 - \frac{d}{T_m}\right) \times 100$$

Where:

a = availability as percentage

d = cumulative downtime for the reporting period

T_m = total planned up-time for the reporting period

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

The total availability of a service is expressed as a percentage of the aggregated downtime in relation to the aggregated expected up-time during the reporting period. The calculation is based on minutes.

4.1.2 System performance

Objective:

These indicators define the system performance the [NCB] is expecting from the T2S Platform. T2S will be sized as a single shared environment on the basis of data supplied by service users (see section 6), with a margin for exceptional peaks as reported under section 6. If the volumes processed in production exceed the aggregated forecasts provided by all Connected NCBs and CSDs, service performance commitments are not binding for the Eurosystem who will operate T2S on a best effort basis in that case.

4.1.2.1 Business Validation Time

Definition:

The Business Validation Time is the period between the reception of an instruction by T2S and the end of the business validation process, i.e. the time when T2S triggers the generation of the acceptance or rejection message.

Measurement:

The Business Validation Time is measured based on timestamps created by the T2S network interface and the timestamps stored as part of the audit trail in the T2S database.

4.1.2.2 Cash Transfer Settlement Time

Definition:

The Cash Transfer Settlement Time is the time that elapses between the end of the creation of the business objects (i.e. after successful validation) and the end of the first settlement attempt. The end of the settlement attempt is marked by the time T2S triggers the generation of the settlement status notification message.

This indicator is relevant only for settlement instructions sent on the Intended Settlement Date both during the Batch and the Real-time Settlement phase of T2S.

Measurement:

The Cash Transfer Settlement Time is measured based on timestamps stored as part of the audit trail in the T2S database.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

Additional remarks:

For the T2S settlement process several cut-off times have been defined. The T2S platform will ensure that each cash transfer instruction that has been sent and acknowledged before the relevant cut-off time will get a settlement attempt.

4.1.2.3 Central Bank Static Data Processing Time

Definition:

The Central Bank Static Data Processing Time is the time that elapses between the end of a successful business validation and the end of the processing of this request.

This indicator is relevant only for all types of maintenance instructions for Central Bank Static Data

Measurement:

The Central Bank Static Data Processing Time is measured based on timestamps stored as part of the audit trail in the T2S database.

Additional remarks:

During Batch Settlement certain types of static data maintenance requests might be queued to ensure the consistency of the settlement processing. In these cases the processing is considered complete after the creation of a new revision for the relevant entities even though this revision is only activated at a later point in time.

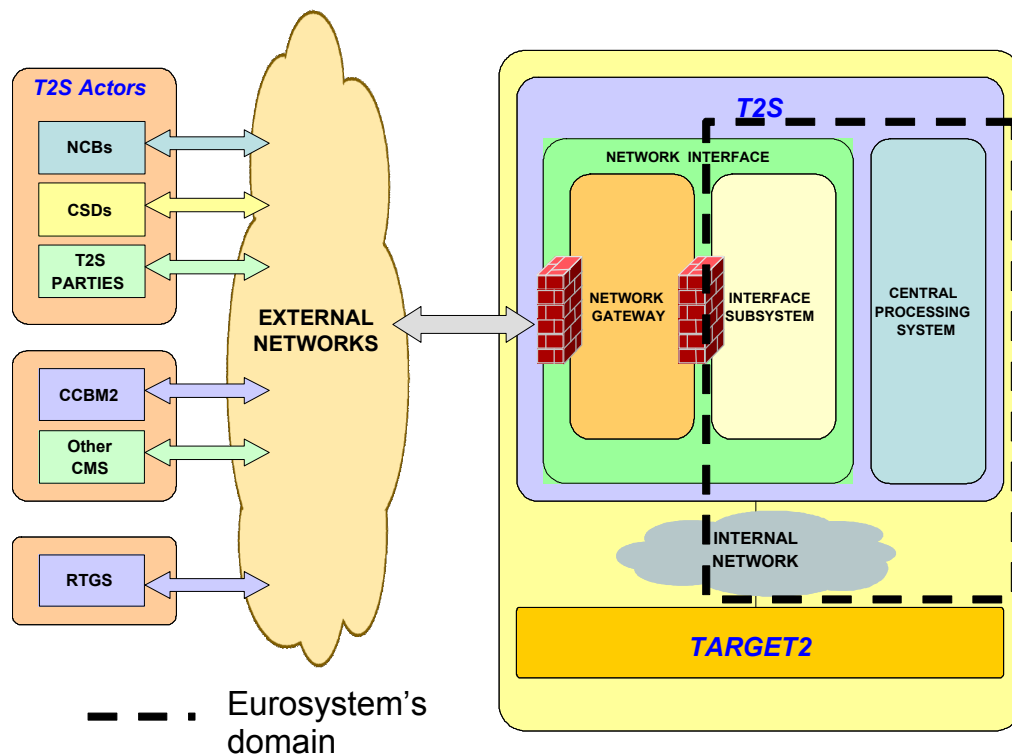
4.1.3 Response times

Objective:

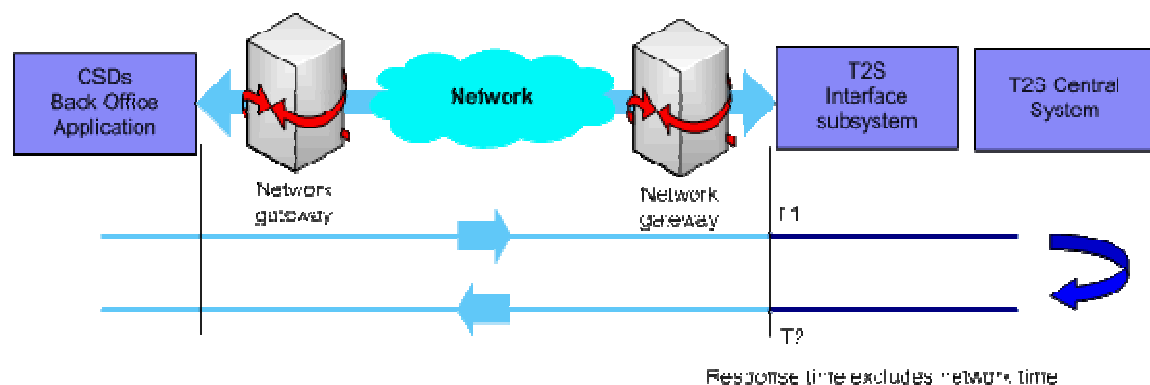
Time indicators provided in the following sections are always measured within the T2S perimeter under the responsibilities of the Eurosystem as shown by the dashed line in the diagram below. The actual transmission time of the data via the network between T2S and the [NCB] is not included in the response time.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement



The response time indicators define the time period between the reception of a request and the corresponding response of the T2S Platform. All performance indicators are measured during each T2S Settlement Day during the time window when the information services are expected to be available.



Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

373 Additional remarks:

374 All messages that have been queued during the Maintenance Window and queries that have been
375 queued during Batch Settlement will not be included in the calculation of the response times.

376 Simple Queries and Complex queries are those referenced as such within the User Detailed
377 Functional Specifications.

378 **4.1.3.1 A2A Query Response Time**

379 Definition:

380 For A2A query requests the response time is defined as the time elapsed between the reception of
381 the query request message and the completion of the sending out of the corresponding result
382 message (see diagram above).

383 Measurement:

384 The response times for A2A queries are measured using the timestamps generated by the T2S
385 network interface.

386 **4.1.3.2 A2A Message Response Time**

387 Definition:

388 For all A2A requests other than A2A Queries the response time is defined as the time elapsed
389 between the reception of the request message by T2S and the sending out of the corresponding
390 acknowledgement message (see diagram above).

391 This KPI does not apply for request messages sent within files.

392 Measurement:

393 The response times for A2A requests are measured using the timestamps generated by the T2S
394 network interface.

395 **4.1.3.3 U2A Response Time**

396 Definition:

397 For all U2A requests the response time is defined as the time between the reception of a user
398 request (HTTP-request) and the completion of the response in form of a web (HTML) page.

399 Measurement:

400 For U2A requests the response time is measured by the T2S Platform within the Eurosystem's
401 domain. These values will be analysed to create metrics for the reports to the Connected NCBs.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

4.1.3.4 File Throughput

Definition:

The File Throughput is defined as the minimum number of megabytes per hour that the interface subsystem has to be able to process in one hour independently for input and output.

Measurement:

The File Throughput is measured by summing up the size of all files received during the reporting period and dividing this value by the actual processing time needed. The processing time is measured using the timestamps generated by the T2S network interface and as part of the T2S audit trail.

4.1.3.5 Online Storage Period

The Online Storage Period defines the minimum time T2S keeps Transactional and Central Bank Static Data available online. The Transactional Data entities this period starts when the entity reaches its final status (i.e. settled, cancelled, etc.). For Static Data entities this period starts when the entity is no longer active and no longer referenced from a Transactional Data entity.

The details concerning the exact condition for the start of the period for each entity will be laid down in a separate document.

4.1.3.6 Archiving Period

The Archiving Period defines the minimum time T2S keeps Transactional and Central Bank Static Data available in an archive for retrieval by the [NCB]. For Transactional Data entities this period starts when the entity reaches its final status (i.e. settled, cancelled, etc.). For Central Bank Static Data entities this period starts when the entity is no longer active and no longer referenced from a Transactional Data entity.

4.1.3.7 Archive Retrieval Response Time

Definition:

The Archive Retrieval Response Time is defined as the time elapsed between the reception of an archive retrieval request and the sending out of the corresponding notification that the data is available for download.

Measurement:

The Archive Retrieval Response Time is measured using the timestamps generated by the T2S network interface.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

4.1.4 Support hours and incident response times

Objective:

These indicators define the response times of the T2S service desk in relation to the type of incident/request and the T2S Settlement Days. An incident is defined as any event which is not part of the standard operation of a service and which causes or may cause an interruption or a reduction in the quality of that service.

Incidents will be categorised in the following priority classes, irrespective of whether they are reported by the [NCB], or by one of its DCA holders:

Incident Priority	Severity	Impact
Priority 1	Critical	Complete unavailability of all T2S Services Complete unavailability of one or more T2S Services for which no workaround is available.
Priority 2	Urgent	Unavailability of a T2S Service, but a workaround is available
Priority 3	Medium priority	All T2S Services are available, but some are experiencing performance problems
Priority 4	Low priority	Query or service request

4.1.4.1 T2S Settlement Day

Definition:

A T2S Settlement Day is a day on which all T2S services are planned to be running.

4.1.4.2 Support Hours

Definition:

The T2S service desk can be contacted via telephone or e-mail by the [NCB]. During Standard Support Hours the T2S service desk can be contacted to communicate technical or business problems on the [NCB]'s side, open tickets for failures of T2S and receive support by the Eurosystem. During Non-standard Support Hours the T2S service desk should be initially contacted via telephone to communicate information that is urgently needed or useful to avoid or limit any negative impact on daily operations, as e-mails will not be monitored during this time. Any e-mail request that is sent during this time will be processed during the next standard support hours only, unless it is pre announced by a telephone call and related to an ongoing incident of priority class 1 or 2, and started outside standard support hours (see above).

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

4.1.4.3 Incident Response Time

Definition:

The Incident Response Time is defined as the time between the incident being detected or information about the incident received by the Eurosystem and the start of action to resolve the incident.

Measurement:

Upon acceptance of an incident or service request the T2S service desk will assign a reference number and a priority level to it. The reference number will allow the [NCB] to monitor the incident's status in the trouble management information tool.

Measurement is done based on the times recorded in the trouble management system.

4.1.4.4 Incident Resolution Time

Definition:

The Incident Resolution Time of an incident is the time between the start of action to resolve the incident and the time it is actually solved or a workaround is available.

Measurement:

Upon acceptance of an incident or service request the T2S service desk will assign a reference number and a priority level to it. The reference number will allow the [NCB] to monitor the incident's status in the online trouble management information tool.

Unless the [NCB] formally objects promptly, both times above are the times recorded by the T2S service desk in the trouble management system.

4.1.5 Business Continuity and Disaster Recovery

Objective:

The Business Continuity and Disaster Recovery mechanisms for T2S are designed to manage failures that require on-site recovery, alternate site recovery and alternate region recovery to ensure a high availability of the T2S Platform.

Business Continuity and Disaster Recovery scenarios will be categorised in the following classes:

Class	Description
Minor failure	a short service interruption (e.g. due to component failures, a system reboot, or a line failure), which can typically be resolved by actions on the primary site

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

Major failure	a serious service interruption (e.g. disruptions caused by fire, flood, terrorist attack or major hardware/ telecommunications faults), which requires the activation of the service in an alternative site.
Regional disaster	a "wide-scale regional disruption" causing severe permanent interruption of transportation, telecommunication, power or other critical infrastructure components across a metropolitan or geographical area and its adjacent communities; or resulting in a wide-scale evacuation or inaccessibility of the population within the normal commuting range of the disruption's origin. These events require the activation of the service in an alternative region.

4.1.5.1 Recovery time

Definition:

The Recovery Time (RTO = recovery time objective) is defined as the maximum acceptable time to restart the T2S Platform after a failure.

Measurement:

The recovery time is measured as the time between detection of an incident that causes the unavailability of the T2S Platform as a whole (or significant parts of it) and the time the incident is resolved or a workaround is in place.

Where the agreed procedures foresee a consultation or decision of service users, the time between informing the service users and the service users' response is excluded from Recovery Time, as is the time needed for reconciliation of lost data (see incident handling in chapter 3.1).

4.1.5.2 Recovery Point Objective

Definition:

The Recovery Point Objective (RPO = recovery point objective) is defined as the maximum acceptable time interval for which data sent to and by T2S is lost when a restart takes place.

Measurement:

The Recovery Point is a point of consistency to which a user wants to recover or restart. The RPO is measured as the amount of time between the moment when the point of consistency was created or captured and that when the failure occurred.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

499 4.2 Committed Service Levels for the production environment

500 4.2.1 Operational and support services

Response times		
	Online Storage Period (4.1.3.5)	90 days
	Archiving Period (4.1.3.6)	10 years
	Archive Retrieval Response Time (4.1.3.7)	72 hours
Availability		
	T2S Settlement Day (4.1.4.1)	all calendar days except: Saturdays, Sundays, 1 January, 25 December and 26 December
Support hours and incident response times		
	Standard Support Hours (4.1.4.2)	from 6:30 am to 7:30 pm CET on all T2S Settlement Days except: Catholic Easter Friday, Catholic Easter Monday, and 1 May
	Non-Standard Support Hours (4.1.4.2)	All times on T2S Settlement Days which fall outside the Standard Support Hours
	Incident Response Time (4.1.4.3)	15 min. during standard support hours 60 min. during non-standard support hours

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

	Incident Resolution Time (4.1.4.4)	Incident Priority	During standard support hours	Outside standard support hours
		1	2 hours	3 hours
		2	Before the start of the next Settlement Day (minimum 2 hours)	
		3	2 Settlement Days or as agreed	
		4	5 Settlement Days or as agreed	
Business Continuity and Disaster Recovery				
	Recovery Time: minor failure (4.1.5.1)	See Incident Response/Resolution Time		
	Recovery Point Objective: minor failure (4.1.5.2)	No data loss		
	Recovery Time: major failure (4.1.5.1)	< 60 minutes (from the decision to failover to the 2 nd site in the same region)		
	Recovery Point Objective: major failure (4.1.5.2)	No data loss		
	Recovery Time: regional disaster (4.1.5.1)	< 120 minutes (from the decision to failover to the other region)		
	Recovery Point Objective: regional disaster (4.1.5.2)	< 2 minutes data loss		
Important events				
	Start of weekly Maintenance Window	Saturday (or the calendar day following the last T2S Settlement Day in a week) 3:00 CET or after sending out the last report after the Batch Settlement (whatever comes later).		
	End of weekly Maintenance Window ³	Monday (or the first T2S Settlement Day in a week) 5:00 CET at the latest		
	Start of daily Maintenance Window	3:00 CET		

³ The weekly Maintenance Window might be shortened based on specific needs of the [NCB] (e.g. migration, issuance in direct holding countries). Such needs have to be pre-announced and the start and end time of the relevant Maintenance Window(s) have to be agreed with the Eurosystem.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

	End of daily Maintenance Window	5:00 CET

501 4.2.2 Settlement services and liquidity management services

Availability		
	Availability (4.1.1.3)	99.7 % / calendar month
	Availability Period (4.1.1.1)	outside the Maintenance Window on all T2S Settlement Days
	Substantial Delay for “Cash Transfer cut-off” (4.1.1.2)	xx minutes
	Substantial Delay for “End of Day Reporting” (4.1.1.2)	xx minutes
	Substantial Delay for “Start of Day” (4.1.1.2)	xx minutes
System capacity		
	Maximum Cash Transfer Settlement Time (4.1.2.2)	xx seconds

502 4.2.3 Central Bank Static Data services

Availability		
	Availability (4.1.1.3)	99.7 % / calendar month
	Availability Period (4.1.1.1)	outside the Maintenance Window on all T2S Opening Days
	Central Bank Static Data Processing Time (4.1.2.3)	5 seconds for 95% of the requests

503

504

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

505 4.2.4 Information services

Availability		
	Availability (4.1.1.3)	99.7 % / calendar month
	Availability Period (4.1.1.1)	outside the Maintenance Window on all T2S Settlement Days
Response times		
	A2A Message Response Time (4.1.3.2)	xx seconds for xx% of the requests
	U2A Response Time (4.1.3.3)	xx seconds
	A2A Query Response Time for Simple Queries ⁴ (4.1.3.1)	3 seconds for 95% of the requests

506 4.2.5 Connectivity services

Availability		
	Availability Period (4.1.1.1)	outside the Maintenance Window on all T2S Settlement Days
System capacity		
	Maximum Business Validation Time (4.1.2.1)	xx seconds (expectation)
	Minimum File Throughput (4.1.3.4)	xx megabytes per hour

⁴ The GFS (Version 4.0, page 582) defines the following queries as simple queries: Settlement Instruction Audit Trail Query, Securities Account Position Query, Securities Account Position History Query, T2S Dedicated Cash Account Balance Query, Outstanding Auto-Collateralisation Credit Query, Limit Utilisation Journal Query, Collateral Value of a Security Query, Securities Deviating Nominal Query, Securities CSD Link Query, Party List Query, Restricted Party Query, Securities Account List Query, T2S Dedicated Cash Account List Query, T2S Calendar Query, T2S Diary Query, System Entity Query, Attribute Domain Query, Attribute Value Query, Privilege Query, Role Query, T2S System User Query, Market-specific Restriction Query, SWIFT BIC Code Query, Report Configuration List Query, Report Configuration Detail Query, Report Query, Cumulative Invoice Query.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

4.3 Targeted Service Levels for the production environment

The more demanding, but non-binding target KPIs defined in this chapter reflect the service level, that is targeted by the Eurosystem. Even if these KPIs are not reached, but the service level is still within the range of the committed service levels (see chapter 4.2), this is no breach of the Service Level Agreement. However, in such a case the Eurosystem stands ready to jointly investigate ways to improve the service.

4.3.1 Operational and support services

Support hours and incident response times				
	Incident Response Time (4.1.4.3)	xx min. during standard support hours (expectation) xx min. during non-standard support hours (expectation)		
	Incident Resolution Time (4.1.4.4)	Incident Priority	During standard support hours	Outside standard support hours
		1	xx hours	xx hours
		2	Before the start of the next Settlement Day (minimum xx hours)	
		3	xx Settlement Days or as agreed	
		4	xx Settlement Days or as agreed	

4.3.2 Settlement services and liquidity management services

Availability		
	Availability (4.1.1.3)	xx % / calendar month
System capacity		
	Maximum Cash Transfer Settlement Time (4.1.2.2)	xx seconds

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

516 4.3.3 Central Bank Static Data services

Availability		
	Availability (4.1.1.3)	xx % / calendar month
	Central bank Static Data Processing Time (4.1.2.3)	xx seconds for xx% of the requests

517 4.3.4 Information services

Availability		
	Availability (4.1.1.3)	xx % / calendar month
Response times		
	A2A Message Response Time (4.1.3.2)	xx seconds for xx% of the requests
	U2A Response Time (4.1.3.3)	xx seconds
	A2A Query Response Time for Simple Queries ⁵ (4.1.3.1)	xx seconds for xx% of the requests

⁵ The GFS (Version 4.0, page 582) defines the following queries as simple queries: Settlement Instruction Audit Trail Query, Securities Account Position Query, Securities Account Position History Query, T2S Dedicated Cash Account Balance Query, Outstanding Auto-Collateralisation Credit Query, Limit Utilisation Journal Query, Collateral Value of a Security Query, Securities Deviating Nominal Query, Securities CSD Link Query, Party List Query, Restricted Party Query, Securities Account List Query, T2S Dedicated Cash Account List Query, T2S Calendar Query, T2S Diary Query, System Entity Query, Attribute Domain Query, Attribute Value Query, Privilege Query, Role Query, T2S System User Query, Market-specific Restriction Query, SWIFT BIC Code Query, Report Configuration List Query, Report Configuration Detail Query, Report Query, Cumulative Invoice Query.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

5. Service Levels for the test environments

5.1 Service Levels for the test environment in “current mode”⁶

5.1.1 Operational and support services

Availability				
	T2S Settlement Day (4.1.4.1)			
Support hours and incident response times				
	Standard Support Hours (4.1.4.2)			
	Non-Standard Support Hours (4.1.4.2)	All times on T2S Settlement Days which fall outside the Standard Support Hours		
	Incident Response Time (4.1.4.3)	xx min. during standard support hours xx min. during non-standard support hours		
	Incident Resolution Time (4.1.4.4)	Incident Priority	During standard support hours	Outside standard support hours
		1	x hours	x hours
		2	xx	
		3	xx	
		4	xx	
	Business Continuity and Disaster Recovery			
	Recovery Time: minor failure (4.1.5.1)	< xx minutes		
	Recovery Point Objective: minor failure (4.1.5.2)	No data loss		
	Recovery Time: major failure (4.1.5.1)	< xx minutes		

⁶ The test environment in “current mode” will be available as from the T2S Go-live Date and will at any time contain the same version of the T2S Business Application as the one installed in the production environment.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

	Recovery Point Objective: major failure (4.1.5.2)	No data loss
	Recovery Time: regional disaster (4.1.5.1)	< xx minutes
	Recovery Point Objective: regional disaster (4.1.5.2)	< xx minutes data loss
Important events		
	Start of weekly Maintenance Window	xx
	End of weekly Maintenance Window	xx
	Start of daily Maintenance Window ⁷	xx
	End of daily Maintenance Window	xx

521 5.1.2 Settlement services and liquidity management services

Availability		
	Availability (4.1.1.3)	xx % / calendar month xx % / calendar year
	Availability Period (4.1.1.1)	outside the Maintenance Window on all T2S Settlement Days
	Substantial Delay for “Cash Transfer cut-off” (4.1.1.2)	xx minutes
	Substantial Delay for “End of Day Reporting” (4.1.1.2)	xx minutes
	Substantial Delay for “Start of Day” (4.1.1.2)	xx minutes
System capacity		
	Maximum Cash Transfer Settlement Time (4.1.2.2)	xx seconds

⁷ The daily ad-hoc Maintenance Window is optional and only scheduled when the T2S Service Operator considers that a change cannot be delayed until the next week-end.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

522 5.1.3 Central Bank Static Data services

Availability		
	Availability (4.1.1.3)	xx % / calendar month xx % / calendar year
	Availability Period (4.1.1.1)	outside the Maintenance Window on all T2S Settlement Days
	Central Bank Static Data Processing Time (4.1.2.3)	xx seconds for 95% of the requests

523 5.1.4 Information services

Availability		
	Availability (4.1.1.3)	xx % / calendar month xx % / calendar year
	Availability Period (4.1.1.1)	outside the Maintenance Window on all T2S Settlement Days
Response times		
	A2A Response Time (4.1.3.2)	xx seconds for xx% of the requests (expectation)
	U2A Response Time (4.1.3.3)	xx seconds
	Response Time for Simple Queries (4.1.3.1)	xx seconds for 95% of the requests

524 5.1.5 Connectivity services

Availability		
	Availability Period (4.1.1.1)	outside the Maintenance Window on all T2S Settlement Days
System capacity		
	Maximum Business Validation Time (4.1.2.1)	xx seconds
	Minimum File Throughput (4.1.3.4)	xx megabytes per hour

525

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

526 5.2 Service Levels for the test environment in “future mode”

527 5.2.1 Operational and support services

Availability				
	T2S Settlement Day (4.1.4.1)	From 7:00 to 19:00 on all calendar days except: Saturdays, Sundays, 1 January, Catholic/Protestant Easter Friday, Catholic/Protestant Easter Monday, 1 May, 25 December and 26 December		
Support hours and incident response times				
	Standard Support Hours (4.1.4.2)			
	Non-Standard Support Hours (4.1.4.2)	All times on T2S Settlement Days which fall outside the Standard Support Hours		
	Incident Response Time (4.1.4.3)	Incident Priority	During standard support hours	Outside standard support hours
		1	15 minutes	1 hour
		2	15 minutes	Next business day
		3	1day	Next business day
4	1 day	Next business day		

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

	Incident Resolution Time (4.1.4.4)	Incident Priority	Incident resolution time	Status call update
		1	1-2 business days	2 hours
		2	2-5 business days	4 hours
		3	According to agreed plan	Upon closure
		4	According to agreed plan	Upon closure
Business Continuity and Disaster Recovery				
	Recovery Time: minor failure (4.1.5.1)	< xx minutes		
	Recovery Point Objective: minor failure (4.1.5.2)	No data loss		
	Recovery Time: major failure (4.1.5.1)	< xx minutes		
	Recovery Point Objective: major failure (4.1.5.2)	No data loss		
	Recovery Time: regional disaster (4.1.5.1)	< xx minutes		
	Recovery Point Objective: regional disaster (4.1.5.2)	< xx minutes data loss		
Important events				
	Start of weekly Maintenance Window	Friday (or the last T2S Settlement Day in a week) 19:00 CET		
	End of weekly Maintenance Window	Monday (or the first T2S Settlement Day in a week) 7:00 CET		
	Start of daily Maintenance Window ⁸	19:00 CET		

⁸ The daily ad-hoc Maintenance Window is optional and only scheduled when the T2S Service Operator considers that a change cannot be delayed until the next week-end.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

	End of daily Maintenance Window	7:00 CET

528 5.2.2 Settlement services and liquidity management services

Availability		
	Availability (4.1.1.3)	85 % / calendar month xx % / calendar year
	Availability Period (4.1.1.1)	outside the Maintenance Window on all T2S Settlement Days
	Substantial Delay for “Cash Transfer cut-off” (4.1.1.2)	xx minutes
	Substantial Delay for “End of Day Reporting” (4.1.1.2)	xx minutes
	Substantial Delay for “Start of Day” (4.1.1.2)	xx minutes
System capacity		
	Maximum Cash Transfer Settlement Time (4.1.2.2)	xx seconds

529 5.2.3 Central Bank Static Data services

Availability		
	Availability (4.1.1.3)	xx % / calendar month xx % / calendar year
	Availability Period (4.1.1.1)	outside the Maintenance Window on all T2S Settlement Days
	Static Data Processing Time (4.1.2.3)	xx seconds for 95% of the requests

530

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

531 5.2.4 Information services

Availability		
	Availability (4.1.1.3)	xx % / calendar month xx % / calendar year
	Availability Period (4.1.1.1)	outside the Maintenance Window on all T2S Settlement Days
Response times		
	A2A Response Time (4.1.3.2)	xx seconds for xx% of the requests (expectation)
	U2A Response Time (4.1.3.3)	xx seconds
	Response Time for Simple Queries (4.1.3.1)	xx seconds for 95% of the requests

532 5.2.5 Connectivity services

Availability		
	Availability Period (4.1.1.1)	outside the Maintenance Window on all T2S Settlement Days
System capacity		
	Maximum Business Validation Time (4.1.2.1)	xx seconds
	Minimum File Throughput (4.1.3.4)	xx megabytes per hour

533 5.2.6 Additional provisions

534 The test environment can be opened with extended hours for a limited period upon request.

535 The Eurosystem will make all reasonable efforts to ensure that the operational hours of the test
536 environments, including on-line availability for end-users and batch processing capabilities for
537 the end of day procedures will be specified in the T2S User Testing Calendar and might be
538 different for each of the testing environments.

539 In certain cases such as the deployment of a new release, the Eurosystem reserves the right to
540 change the T2S User Testing Calendar, which includes changing the opening and closing times
541 of the test environments. All changes to the T2S User Testing Calendar shall be proposed,

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

542 discussed and agreed in the substructure in charge of User Testing, before informing the T2S
543 Users in a timely manner in advance.

544 The Information Security levels of the test environments shall be broadly the same as for the T2S
545 production environment.

546 The test environments will have a substantially lower capacity compared to the production
547 environment (around 10% of production environment). The Eurosystem shall increase the
548 capacity of the test environments to cover specific testing needs (e.g. high-volume tests during
549 the community testing and the business day testing stages) upon a request from – and in
550 agreement with – the [NCB].

551 The T2S service desk shall be the unique point of contact to report incidents and problems, and to
552 ask for guidance on T2S during User Testing. The [NCB] can contact the T2S service desk via
553 phone, fax, and email.

554 The T2S service desk coverage hours shall be aligned to the operation hours of the test
555 environment referred to above.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

6. System capacity and platform sizing

To ensure the proper sizing of the platform that is required to meet the agreed service levels, the CSDs are requested to provide on a quarterly basis updated forecasts for average and expected peak business figures as specified in the URD, to allow the Eurosystem to make an adequate long-term capacity planning. These figures have to include the volumes for the CSDs' DCA Holders as well.

Capacity requirements of Central Banks and Dedicated Cash Account Holders are expected to be negligible compared to capacity requirements of CSDs. Consequently, Central Banks are exempted from specifying any ex-ante capacity requirements. If the expectations change, the [NCB] will inform the Eurosystem in due time (at least 6 months in advance or as soon as the [NCB] receives this information).

In order to process exceptionally high peak volumes, the Eurosystem will ensure that if necessary additional capacity can be added on very short notice, provided no hardware components need to be replaced. However, there will be technical limitations to such a capacity increase.

If exceptional capacity is needed for a one-time event or on shorter notice, the Eurosystem will try to cope with such requests, but on best effort basis only.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

7. Service Level reporting

End-to-end service reports including local service desk operations will be provided on a regular basis in electronic format, focusing on the above defined service metrics.

7.1 Content of the Reporting

In addition, these service reports will contain information on performance against the following indicators:

- resolution times of closed tickets
- escalation status of open tickets
- Punctuality (see 7.2.1)

Performance against Service Level targets will be measured by the Eurosystem in compliance with the procedures agreed between the parties.

Reports on actual service levels achieved will be provided to the [NCB] on a monthly basis. This will cover for each service indicator the performance achieved compared with the target values. For informational purposes the Eurosystem will also report the bilateral service levels achieved for the [NCB]. These reports are to be provided to the [NCB] within ten Settlement Days after the end of each month.

On a daily basis and reflected in the monthly SLA report:

- Unresolved incidents
- Resolved incidents
- Actual service (including security) breaches
- Planned downtime
- Unplanned downtime

On a monthly basis:

- Service availability
- Frequency of incidents
- Cumulative service breaches
- Volumes and peaks
- Overall performance
- Use of T2S service desk (when relevant)

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

- 601 ▪ Application and technology performance specified in this document
 - 602 ▪ Planned changes
 - 603 ▪ Previous month's unresolved incidents
 - 604 ▪ Previous month's resolved incidents
 - 605 ▪ Previous month's unresolved problems
 - 606 ▪ Previous month's resolved problems
 - 607 ▪ Comments and observations from the Eurosystem
 - 608 ▪ Medium term trends of incident and their root cause analysis
 - 609 ▪ Support figures (e.g. number of calls, response time, long abandon rate)
- 610 In addition to the technical indicators the monthly report will also contain other important
611 information like the following:
- 612 ▪ Updates to the T2S release calendar scheduling technical releases with an impact on the
613 [NCB];
 - 614 ▪ Information about upcoming changes without impact on the [NCB];
 - 615 ▪ Information about the planned implementation process (including the test strategy) and
616 timing for upcoming releases.
 - 617 ▪ Information about the operational risk situation in T2S, for those aspects that are not
618 covered in the scope of Schedule 10 (Information Security).

619 **7.2 Definition of Additional Indicators for Reporting**

620 This section defines additional indicators that are used for the reporting, but have no KPI attached
621 to it.

622 **7.2.1 Punctuality**

623 Definition:

624 The Punctuality of T2S is measured by counting the number of occasions when a T2S business
625 event is delayed for a time period exceeding the defined substantial delay for this event.

626 Measurement:

627 The delays will be checked using the planned and the actual timestamps for the relevant events as
628 logged by T2S.

629 The following business events are relevant for this calculation:

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

- 630 ▪ Start of Day
- 631 ▪ Start of the Batch Settlement
- 632 ▪ DvP cut-off
- 633 ▪ FoP cut-off
- 634 ▪ End of the End of Day Reporting

635 Calculation:

636
$$p = \left(1 - \frac{d}{a}\right) \times 100$$

637 Where:

638 p = punctuality as percentage

639 d = number of relevant business events with a substantial delay in the reporting
640 period⁹

641 a = total number of relevant business events in the reporting period

⁹ Events that have been delayed according to the procedures defined in the MOP due to a request from the Connected NCB or another market participant are excluded from this count.

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

8. Service review meetings

The Eurosystem will invite all Connected NCBs on a quarterly basis to a formal Service Review meeting on steering level. In addition the Eurosystem will invite all Connected NCBs on a monthly basis or upon request to meetings on a working level.

This meeting will evaluate the service performance since the last review. In particular the meeting will:

- Review the service achievement (service level target against actual performance)
- Review the Service Level Reports provided in recent periods. However, for the sake of intra-annual comparability, the Service Level Report format might be changed only on a yearly basis.
- Focus particularly on breaches of service levels
- Identify weak areas and potential ways to address problems and initiate service improvement
- Preview issues (anticipated measures) for the coming period

Currency Participation Agreement

Schedule 6 – T2S Service Level Agreement

9. SLA reviews

9.1 Initial review

The parties agree that they shall review the SLA Schedule for the first time on a date no later than the end of the bedding down period.

All resulting changes to this SLA shall be approved by the parties. In case of persistent disagreement between the parties, the dispute resolution procedure laid down in the Currency Participation Agreement shall be activated.

9.2 Subsequent review

The parties agree that the SLA will be reviewed on a yearly basis in order to verify the balance between evolving user requirements and defined T2S Service Levels, as well as to ensure the effectiveness of performance measuring criteria.

If required by the circumstances, the SLA can be reviewed on an ad-hoc basis.

Agreement review meetings provide an opportunity to review the agreement and associated targets. In particular the meeting will:

- Review service achievements with the customer and identifying potential improvement on both sides
- Review the service requirements and identify if any changes have occurred
- Discuss any changes that operations would like to make to the agreement
- Agree on the next step for the SLA: extension, changes or decommissioning.

Changes to chapters 0, 2, 3, 4, 7 and 8 of the SLA will be changed by mutual agreement only, while changes to chapters 5 and 6 will be agreed in accordance with the applicable governance arrangements specified in Schedule 8 (Governance) of the CPA, in particular through the involvement of the Operations Managers Group.

Currency Participation Agreement

Schedule 6 – Annex 1 – Management of non-functional changes

Annex 1 - Management of non-functional changes

Emergency Changes

If an incident occurs, the Eurosystem may have to implement a change that cannot be delayed until the next planned Maintenance Window. The implementation of such a change will cause a system unavailability as described in section 4.2.1.

As a minimum, the Eurosystem will inform the [NCB] ex post about the reason for and the nature of the change. Nevertheless, the Eurosystem will make best efforts to inform the [NCB] ex ante, even at short notice.

Other changes

By default, changes aimed at ensuring that the Eurosystem is capable of delivering the T2S Services according to the KPIs specified in this SLA, or resulting from SLA reviews (see section 9), will be managed by the Eurosystem. If such changes have no impact on the [NCB], the Eurosystem will inform the [NCB] ex ante about the nature and the date of such change.

If such changes have an impact on the [NCB], or if the [NCB] expresses an interest in testing such changes, the Eurosystem and the [NCB] will co-operate in good faith to manage the changes, as much as possible and where relevant, following the provisions of Schedule 9 (Change and Release Management).

The dates reserved by the Eurosystem for implementing changes that have or might have an impact on the [NCB], are documented in a calendar that is shared and agreed in advance with the [NCB]. By default, changes are implemented during a Maintenance Window.

The [NCB] is responsible to involve its DCA Holders in the process if necessary and share the relevant information with them.

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 7

PRICING

Currency Participation Agreement

Schedule 7 – Pricing

Table of contents

1	Introduction	1
2	T2S Pricing policy	2
3	T2S price list.....	3
4	T2S Pricing structure.....	4
4.1	Summary	4
4.2	Settlement services	5
4.3	Information services	13
4.4	Tariff items initially priced at zero	16
4.5	Tariff items priced at zero at least until end of cost-recover period	19
5	Inventory of T2S Service Charges.....	20
5.1	Introduction.....	20
5.2	Changes.....	20
5.2.1	T2S Common Changes	20
5.2.2	T2S Specific Changes	21
5.2.3	Pricing of assessments of Change Requests	21
5.3	RTGS fees for connecting to T2S.....	22
5.4	Training.....	22
5.5	Consultancy.....	22
5.6	Request for an additional test environment.....	22
5.7	Securities Reference Data	23
5.8	Connectivity Services	23
5.9	One-off joining fee	23
5.10	Exit Management.....	23
5.11	External Examiner	23

Currency Participation Agreement

Schedule 7 – Pricing

1 Introduction

2 The Schedule on Pricing consists of four components: (i) the T2S Pricing policy, which describes
3 the Governing Council decision on the Pricing of T2S Services (ii) the T2S price list, which gives
4 the actual T2S prices in eurocent for each of the T2S Services (i.e. settlement, account
5 management and information services); (iii) the T2S pricing structure, which provides a detailed
6 description of the items in the T2S price list, as well as the related fee triggers; and (iv) the
7 Inventory of T2S Service Charges, which provides a description of how T2S will finance changes
8 to T2S, and a number of other services not covered in the T2S price list.

9 It is important to note that the T2S price list displays all T2S prices without VAT. The possible
10 application of VAT is subject to national tax regulation and outside the scope of the T2S Pricing.

11 The Eurosystem will continue to seek broad market advice when discussing possible changes to
12 the Pricing Schedule.

Currency Participation Agreement

Schedule 7 – Pricing

13 **2 T2S Pricing policy**

14 The Governing Council of the European Central Bank (ECB) decided to set the Delivery versus
15 Payment price for TARGET2-Securities (T2S) at 15 eurocent per instruction. This price will be
16 fixed for the period from the T2S Go-Live Date until December 2018. In order to provide
17 assurance to market participants about T2S prices after 2018, the Governing Council has made a
18 commitment not to increase T2S fees by more than 10% per year between 2019 and the end of
19 the cost recovery period.

20 This commitment to set the price at 15 eurocent is subject to the following conditions: (i) non-
21 euro currencies add at least 20% to the euro settlement volume; (ii) the securities settlement
22 volume in the EU is no more than 10% lower than the volumes projected by the T2S Programme
23 Office, which are based on market advice; and (iii) tax authorities confirm that the Eurosystem
24 will not be charged VAT for the T2S Services it provides.

Currency Participation Agreement

Schedule 7 – Pricing

25 3 T2S price list

<i>Tariff items</i>	<i>Price</i>	<i>Explanation</i>
Settlement services		
Delivery versus Payment	15 eurocent	per instruction [†]
Free of Payment	9 eurocent	per instruction [†]
Payment Free of Delivery	9 eurocent	per instruction [†]
Internal T2S liquidity transfer	9 eurocent	per transfer
Account allocation	3 eurocent	per instruction [†]
Matching	3 eurocent	per instruction [†]
Intra-position movement	6 eurocent	per transaction
Intra-balance movement	6 eurocent	per transaction
Auto-collateralisation service with Payment Bank	15 eurocent	for issue and return, charged to collateral provider
Intended Settlement Date failed transaction	15 eurocent	surcharge per Settlement Day failed per instruction [†]
Daytime settlement process	3 eurocent	surcharge per instruction [†]
Daytime congestion charge	0 eurocent [*]	additional surcharge per instruction [†]
Auto-collateralisation service with Central Bank	0 eurocent [*]	for issue and return, charged to the collateral provider
Instruction marked with 'top or high priority'	0 eurocent [*]	surcharge per instruction [†]
Cancellation	0 eurocent [*]	per instruction [†]
Settlement modification	0 eurocent [*]	per instruction [†]
Information services		
A2A reports	0.4 eurocent	Per business item in any A2A report generated
A2A queries	0.7 eurocent	Per queried business item in any A2A query generated
U2A queries	10 eurocent	Per executed search function
Messages bundled into a file	0.4 eurocent	Per message in a file
Transmissions	1.2 eurocent	Per transmission
Account management services		
Securities Account	Free of charge ^{**}	Fee options: a) monthly fee per ISIN in the account <u>or</u> b) monthly fee per account
Fee per T2S Dedicated Cash Account	0 eurocent ^{***}	Monthly

[†] Two instructions per transaction will be charged.

^{*} T2S will be sized in accordance with an expected consumption pattern, i.e. the anticipated distribution of settlement volumes during night-/day-time and peak hours. These items will initially be set at a zero price, presuming that actual usage of T2S will be within this expected consumption pattern. However, should there be a stronger than expected use of T2S resources and the volume distribution pattern be different than expected thus adversely affecting T2S performance, it will be reconsidered to charge for these items. The Eurosystem will regularly review the actual usage of T2S resources against expected consumption patterns.

^{**} Account management services for Securities Accounts will be set at zero and will not be changed until the end of the cost recovery period, at least.

^{***} Account management services for T2S Dedicated Cash Accounts (DCAs) will initially not be charged, presuming that the actual number and usage of DCAs will be within expected consumption patterns. However, should DCAs involve a stronger than expected use of T2S resources thus adversely affecting T2S performance, it will be reconsidered to charge for these items. The Eurosystem will regularly review the matter together with the Central Banks operating DCAs.

Currency Participation Agreement

Schedule 7 – Pricing

4 T2S Pricing structure

4.1 Summary

Tariff items	DvP weight factor	Explanation
Settlement services		
Delivery versus Payment	100%	per instruction [†]
Free of Payment	60%	per instruction [†]
Payment Free of Delivery	60%	per instruction [†]
Internal T2S liquidity transfer	60%	per transfer
Account allocation	20%	per instruction [†]
Matching	20%	per instruction [†]
Intra-position movement	40%	per transaction
Intra-balance movement	40%	per transaction
Auto-collateralisation service with Payment Bank	100%	for issue and return, charged to collateral provider
Intended Settlement Date failed transaction	100%	surcharge per Settlement Day failed per instruction [†]
Daytime settlement process	20%	surcharge per instruction [†]
Daytime congestion charge	0% [*]	additional surcharge per instruction [†]
Auto-collateralisation service with Central Bank	0% [*]	for issue and return, charged to the collateral provider
Instruction marked with ‘top or high priority’	0% [*]	surcharge per instruction [†]
Cancellation	0% [*]	per instruction [†]
Settlement modification	0% [*]	per instruction [†]
Information services		
A2A reports	25% of total T2S revenues	Per business item in any A2A report generated
A2A queries		Per queried business item in any A2A query generated
U2A queries		Per executed search function
Messages bundled into a file		Per message in a file
Transmissions		Per transmission
Account management services		
Securities Account	Free of charge ^{**}	Fee options: a) monthly fee per ISIN in the account <u>or</u> b) monthly fee per account
Fee per T2S Dedicated Cash Account	0% ^{***}	Monthly

[†] Two instructions per transaction will be charged.

* T2S will be sized in accordance with an expected consumption pattern, i.e. the anticipated distribution of settlement volumes during night-/day-time and peak hours. These items will initially be set at a zero price, presuming that actual usage of T2S will be within this expected consumption pattern. However, should there be a stronger than expected use of T2S resources and the volume distribution pattern be different than expected thus adversely affecting T2S performance, it will be reconsidered to charge for these items. The Eurosystem will regularly review the actual usage of T2S resources against expected consumption patterns.

** Account management services for Securities Accounts will be set at zero and will not be changed until the end of the Cost Recovery Period, at least.

*** Account management services for T2S Dedicated Cash Accounts (DCAs) will initially not be charged, presuming that the actual number and usage of DCAs will be within expected consumption patterns. However, should DCAs involve a stronger than expected use of T2S resources thus adversely affecting T2S performance, it will be reconsidered to charge for these items. The Eurosystem will regularly review the matter together with the Central Banks operating DCAs.

Currency Participation Agreement

Schedule 7 – Pricing

4.2 Settlement services

The general principle is that each completed settlement service activity will be counted and reflected in the relevant monthly bill. Unless indicated otherwise, billable events will be charged based on the date that T2S successfully executes the related instructions/the events occur.

Regarding the difference between settlement transaction and settlement instruction, it is noted that the two counterparties to a settlement transaction initiate one instruction each and the two instructions will then be matched and form one transaction.

The T2S Pricing structure aims at charging for resource usage in most instances. The price for settlement services is set relative to a DvP settlement.

Each partial settlement¹ will be charged separately (e.g. a settlement instruction settled in three parts will be charged the DvP or FoP price three times, and any of the parts settled in the period 07:00 – 18:00 will attract the daytime surcharge).

Conditional securities delivery² transactions will get charged according to their individual components, e.g. DvP or FoP, Matching, blocking and unblocking, creation of a condition and release of a condition, i.e. hold and release.

Section 4.4 contains the list of items which will initially be set at a zero price, presuming that actual usage of T2S will be within the expected anticipated distribution of settlement volumes during night-/day-time and peak hours.

Section 4.5 contains the list of items which will be priced at zero and will not be charged until the end of the cost recovery period, at least.

¹ Partial settlement is defined in the URD as “a process that settles only a fraction of settlement instructions original volume and amount when full settlement is not possible due to lack of securities. The residual unsettled volume and amount may settle at a later stage during the Intended Settlement Date. Any residual amount at the end of the intended settlement date results in the reporting of a failed settlement”.

² Conditional securities delivery is defined in the URD as “a procedure in which the final securities and/or cash booking is dependent on the successful completion of an additional action or event (e.g. registration of shares, cash settlement outside T2S)”.

Currency Participation Agreement

Schedule 7 – Pricing

82 Delivery versus Payment

Price	Eurocent 15 per instruction
DvP weight factor	<i>100% (the numeraire)</i>
Background	<i>The DvP requests a simultaneous transfer of securities versus cash. Both instructing parties will get charged. The DvP price constitutes the numeraire for other instruction related charges (i.e. other instruction charges are indicated as a percentage of the DvP price). Realignment instructions resulting from a DvP will not be charged.</i>
Fee trigger	<i>Each successfully completed DvP settlement.</i>

83 Free of Payment

Price	Eurocent 9 per instruction
DvP weight factor	<i>60%</i>
Background	<i>The FoP requests a transfer of securities only. There is no cash processing required. Both parties to the FoP will get charged. Realignment instructions resulting from a FoP will not be charged.</i>
Fee trigger	<i>Each successfully completed FoP settlement.</i>

84 Payment Free of Delivery

Price	Eurocent 9 per instruction
DvP weight factor	<i>60%</i>
Background	<i>The PFOD requests a transfer of cash only. There is no securities processing required. Both parties to the PFOD will get charged. Realignment instructions resulting from a PFOD will not be charged.</i>
Fee trigger	<i>Each successfully completed PFOD settlement.</i>

85

Currency Participation Agreement

Schedule 7 – Pricing

86 Internal T2S liquidity transfer

Price	Eurocent 9 per transfer
DvP weight factor	60%
Background	<i>Internal liquidity transfers between two T2S Dedicated Cash Accounts will be charged with a DvP weight factor of 60%.</i> <i>Liquidity transfer charges will be invoiced to T2S Users via the T2S Users' Central Bank.</i> <i>Payments triggered as part of a DvP are of course included within the DvP instruction charge.</i>
Fee trigger	<i>All successfully executed liquidity transfers between two T2S Dedicated Cash Accounts.</i> <i>The fee will get charged to the instructing party, i.e. the party which will get debited.</i>

87 Account allocation

Price	Eurocent 3 per instruction
DvP weight factor	20%
Background	<i>An account allocation in a “direct holding market” is an instruction involving at least one Securities Account which has been flagged as an “end-investor account”. Two instructions per transaction will be charged. If the account allocation instructions are sent unmatched, the Matching fee will be charged. The definitions of a “direct holding market” and “end-investor account” in the context of the T2S Pricing Schedule are provided below.</i> <i>For the purpose of T2S Pricing, a “direct holding market” is defined as a market:</i> <i>1. in which, at a minimum, for holdings of domestic securities generally held by domestic residents, end-investors (retail investors in particular) would generally have an account directly in the Issuer CSD; and</i> <i>2. which brings all segregated end-investor accounts to T2S that contain securities that are available in T2S.</i> <i>For the purpose of T2S Pricing, the following markets are considered as direct</i>

Currency Participation Agreement

Schedule 7 – Pricing

	<i>holding markets according to paragraph 1: Cyprus, Denmark, Estonia, Finland, Greece, Iceland, Malta, Norway, Romania, Slovakia, Slovenia, Sweden. This list is subject to review by the T2S Governance bodies when needed, following the procedure for ‘Decision-making on relevant matters other than Change Requests’ in Schedule 8 (Governance).</i> <i>Definition of “end-investor accounts” and instructions eligible for the reduced account allocation fee</i> <i>For the purpose of T2S Pricing, there are two options which a CSD serving a direct holding market in T2S can choose with respect to the definition of “end investor accounts and the instructions which are eligible for the account allocation fee:</i> <i>Option A for a direct holding market in T2S:</i> <i>a. All segregated accounts of customers of CSD participants are eligible to be flagged as ‘end-investor account eligible for the account allocation fee’. It is noted that it is the responsibility of the respective CSD in a direct holding market in T2S in cooperation with its participants to ensure a proper flagging of accounts.</i> <i>b. FoP instructions involving at least one account flagged as ‘end-investor account eligible for the account allocation fee’ are charged the account allocation fee which is applicable to both sides of the FoP transaction.</i> <i>Or:</i> <i>Option B for a direct holding market in T2S:</i> <i>a. All retail investor accounts are eligible to be flagged as ‘end-investor account eligible for the account allocation fee’. A retail investor means a ‘retail client’ in the meaning of MiFID (OCJ, L 145 , 30/04/2004). It is noted that it is the responsibility of the respective CSD in a direct holding market in T2S in cooperation with its participants to ensure a proper flagging of accounts.</i> <i>b. DvP and FoP instructions involving at least one account flagged</i>

Currency Participation Agreement

Schedule 7 – Pricing

	<i>as ‘end-investor account eligible for the account allocation fee’ are charged the account allocation fee which is applicable to both sides of the transaction.</i> <i>The following principles apply to account allocations:</i> <i>1. The objective of the fee for account allocations is to ensure a level playing field between direct and indirect holding markets in T2S.</i> <i>2. As a principle, the account allocation fee should not be used for transactions in direct holding markets in T2S that would have been charged the full price in an average indirect holding market or in an average direct holding market opting for a layered model in T2S.</i> <i>3. In line with the transparency principle of T2S, the T2S Board reports on an annual basis about the share of DvP transactions, FoP transactions and Account allocations in each of the respective direct holding markets in T2S. This report includes the share of DvP transactions and FoP transactions of the aggregated indirect holding markets in T2S for comparison.</i>
Fee trigger	<i>The fee trigger depends on which option A or B is chosen by the respective CSD serving a direct holding market in T2S:</i> <i>• Option A. Any FoP instruction involving at least one account flagged as ‘end-investor account eligible for the account allocation fee’ are charged the account allocation fee which is applicable to both sides of the FoP transaction.</i> <i>Or:</i> <i>• Option B. Any DvP or FoP instruction involving at least one account flagged as ‘end-investor account eligible for the account allocation fee’ are charged the account allocation fee which is applicable to both sides of the transaction.</i>

Currency Participation Agreement

Schedule 7 – Pricing

89 Matching

Price	Eurocent 3 per instruction
DvP weight factor	20%
Background	<i>An unmatched instruction will have to pass through the Matching process and will assume additional processing resources of T2S. Therefore, it will attract a standard Matching charge on top of the regular settlement instruction fee. The Matching charge will be 20% of a DvP instruction charge and will be applied to both parties.</i>
Fee trigger	<i>Each successfully completed Matching event.</i>

90 Intra-position movements

Price	Eurocent 6 per transaction
DvP weight factor	40%
Background	<i>All intra-position movements in the case of securities (i.e. blocking/ unblocking/ reservation/ unreservation/ earmarking / unearmarking) will attract an instruction-based fee. Internally generated intra-position movements will also be charged. For example, say a securities position is blocked for a specific DvP transaction. Once the DvP transaction which is using the blocked securities is ready to be settled, T2S will first have to unblock the securities position so the DvP can settle. This unblocking will be charged. For further details, see Example 109 in the UDFS v1.0. No fees are applied for the blocking of static data (i.e. of the Party, Securities Account). The intra-position movement fee will be charged to respective T2S Users via their CSD.</i>
Fee trigger	<i>Any successfully executed intra-position movement.</i>

91

Currency Participation Agreement

Schedule 7 – Pricing

92 Intra-balance movements

Price	Eurocent 6 per transaction
DvP weight factor	40%
Background	<i>All intra-balance movements in the case of cash (i.e. blocking/unblocking) will attract an instruction-based fee. Internally generated intra-balance movements will also be charged. The fees are also applied for the automatic release of cash blockings during end-of-day and the regenerated cash blockings at the next start-of-day in the case of a Conditional Securities Delivery (CoSD). No fees are applied for the blocking of static data (i.e. of the Party, Securities Account). The intra-balance (cash) movement fee will be charged to respective T2S Users via their Central Bank.</i>
Fee trigger	<i>Any successfully executed intra-balance movement.</i>

93 Auto collateralisation service with Payment Bank

Price	Eurocent 15 per transaction
DvP weight factor	100%
Background	<i>The complete auto-collateralisation with a Payment Bank will attract an all-in-one fee of 100% DvP weight factor. Only the collateral provider will get charged.</i>
Fee trigger	<i>Each successfully executed auto-collateralisation transaction with a Payment Bank within the monthly billing period.</i>

94 Fail on Intended Settlement Date

Price	Eurocent 15 per instruction
DvP weight factor	100%
Background	<i>Matched settlement instructions failing to settle on their Intended Settlement Date (ISD) will be re-introduced into all the future settlement cycles until they either settle or are cancelled by the two counterparties. The <u>daily charge</u> will address the resource cost of congestion and of the additional processes required to recycle a failed transaction, e.g. eligibility checking. It is not the task of T2S to apply disciplinary actions. These will need to be applied outside of T2S. Both parties of the failing settlement transaction will attract the</i>

Currency Participation Agreement

Schedule 7 – Pricing

	<i>charge.</i>
Fee trigger	<i>Each Matched DvP, FoP, or PFOD which does not settle on its Intended Settlement Date will attract a surcharge. Furthermore, the surcharge will continue to be applied for every Settlement Day that the instruction fails to settle after the ISD. The charge will be applied to both parties of the transaction.</i>

95 **Daytime settlement process**

Price	Eurocent 3 <u>surcharge</u> per instruction settled during the period 07:00 - 18:00
DvP weight factor	<i>20%</i>
Background	<i>Settlement instructions successfully executed during the period 07:00 – 18:00 will attract a 20% “daytime surcharge”.</i>
Fee trigger	<i>Any DvP, FoP or PFOD instruction successfully settled during the period 07:00 – 18:00 will attract the daytime surcharge.</i>

96

Currency Participation Agreement

Schedule 7 – Pricing

4.3 Information services

On average, 25% of the annual T2S revenues will be recovered via information services.

Reports, queries and messages of Directly Connected Parties (which are entitled to do so by the respective CSD) will be charged to the CSD of the Directly Connected Party. Reports, queries and messages of a Payment Bank will be charged to the Central Bank of the Payment Bank. Reports, queries and messages that are received/generated during peak hours, i.e. the last two hours prior to the DvP cut-off time (i.e. indicatively between 2 p.m. – 4 p.m.), may be subject to the daytime congestion surcharge.

For the purposes of the pricing of information services, the following definitions are used:

- A **‘business item’** is one instance of a business entity defined in the T2S data model (e.g. settlement instruction, securities position, intra-balance movement, liquidity transfer, cash posting, Securities Account, Dedicated Cash Account etc) with all its attributes.
- A **‘message’** is an encrypted inbound/outbound communication used for Application-to-Application (A2A) interactions between T2S and its participants. A definitive list of all messages can be found in Chapter 3 of the User Detailed Functional Specifications (UDFS).
- A **‘file’** is a structured collection of ‘messages’.
- A **‘transmission’** can be any of the following: a ‘message’, a ‘file’, an ‘A2A query request’, ‘A2A query response’ or an ‘A2A report’.

Currency Participation Agreement

Schedule 7 – Pricing

117 A2A reports

Price	Eurocent 0.4 per business item in an A2A report
Background	<i>A2A reports will be charged based on the reported number of business items. The list of A2A reports and associated business item are shown in Annex 1 to Schedule 7.</i>
Fee trigger	<i>Any A2A report generated, with the charge based on the reported number of business items.</i>

118 A2A queries

Price	Eurocent 0.7 per queried business item in an A2A query
Background	<i>A2A queries will be charged based on the number of queried business items. The list of A2A queries and associated business item are shown in Annex 1 to Schedule 7.</i>
Fee trigger	<i>Any A2A query generated, with the charge based on the number of queried business items.</i>

119 U2A queries

Price	Eurocent 10 per executed U2A query
Background	<i>U2A queries are submitted via the GUI and the U2A query response is received by the GUI. U2A queries viewed on the GUI are charged a fixed fee per executed query. If a U2A query were downloaded/exported, then it would be charged in the same manner as for A2A queries (i.e. per business item in the downloaded U2A query). The list of U2A queries and associated business item are shown in Annex 1 to Schedule 7.</i>
Fee trigger	<i>Any executed U2A search function viewed on the GUI would be charged a fixed fee. If a U2A query is downloaded, it would be additionally charged in the same manner as for A2A queries (i.e. per queried business item).</i>

120

Currency Participation Agreement

Schedule 7 – Pricing

121 Messages bundled into a file

Price	Eurocent 0.4 per message in each file containing bundled messages
Background	<i>T2S Actors will have the possibility to send messages to T2S and receive messages from T2S bundled together into a file. Messages received by T2S which are not accepted or not successful authenticated will not be charged for.</i>
Fee trigger	<i>Each file containing bundled messages, with the charge based on the number of messages in the file.</i>

122 Transmissions

Price	Eurocent 1.2 per transmission
Background	<i>All types of transmissions (with the exception of technical acknowledgement messages) will be counted and charged for.</i>
Fee trigger	<i>Each transmission per T2S Party (both inbound and outbound) will be counted and charged for (except for technical acknowledgement messages).</i>

123

Currency Participation Agreement

Schedule 7 – Pricing

124 Some worked examples for the pricing of information services:

Item	Transmission fee (in eurocent)	Business item fee (in eurocent)	Fixed fee	Total charge
A2A report sent to a T2S Actor containing 100 business items	1.2 eurocent (for sending the report)	40 eurocent (100 x 0.4 eurocent for each business item contained in the report)	-	41.2 eurocent
A file containing 100 messages, sent by a T2S Actor to the T2S Platform	1.2 eurocent (for receiving the file)	40 eurocent (100 x 0.4 eurocent for each message bundled into the file)	-	41.2 eurocent
A2A query request and the subsequent response containing 100 business items	2.4 eurocent (1.2 eurocent for the A2A query request message and 1.2 eurocent for the A2A query response)	70 eurocent (100 x 0.7 eurocent for each queried business item)	-	72.4 eurocent
100 (individual) messages sent by T2S to a T2S Actor	120 eurocent (100 x 1.2 eurocent for each message)	-	-	120 eurocent
U2A query on the GUI	-	-	10 eurocent	10 eurocent
U2A query containing 100 business items, viewed on the GUI and then subsequently downloaded	-	70 eurocent (100 x 0.7 eurocent for each queried business item)	10 eurocent (for the initial viewing on the GUI)	80 eurocent

4.4 Tariff items initially priced at zero

126 T2S will be sized in accordance with an expected consumption pattern, i.e. the anticipated
127 distribution of settlement volumes during night-/day-time and peak hours. These items will
128 initially be set at a zero price, presuming that actual usage of T2S will be within this expected
129 consumption pattern. However, should there be a stronger than expected use of T2S resources
130 and the volume distribution pattern be different from expected thus adversely affecting T2S
131 performance, it will be reconsidered to charge for these items. The Eurosystem will regularly
132 review the actual usage of T2S resources against expected consumption patterns.

Currency Participation Agreement

Schedule 7 – Pricing

133 **Daytime congestion charge**

Price	Zero eurocent per instruction
DvP weight factor	0%
Background	<i>An additional congestion surcharge may be applied to settlement instructions successfully executed during the last two hours prior to the DvP cut-off time (i.e. indicatively between 14:00 – 16:00). Initially this “congestion charge” will be set at 0 eurocent but if, once T2S goes live, it is found that too many instructions are executed during the period and hence causing congestion, a fee may be applied.</i>
Fee trigger	<i>Any DvP, FoP or PFOD instruction successfully settled during the last two hours prior to the DvP cut-off time (i.e. indicatively between 14:00 – 16:00) will attract the daytime congestion surcharge.</i>

134 **Auto collateralisation service with a Central Bank**

Price	Zero eurocent per transaction
DvP weight factor	0%
Background	<i>All transactions resulting from auto-collateralisation with a Central Bank will be charged an all-in-one fee. Only the collateral provider will get charged.</i>
Fee trigger	<i>All successfully processed auto-collateralisation transactions with a Central Bank within the monthly billing period.</i>

135 **Daytime settlement of ‘high’ priority and ‘top’ priority instructions**

Price	Zero eurocent per instruction
DvP weight factor	0%
Background	All ‘Top Priority’ and ‘High Priority’ instructions processed during the period 07:00 – 18:00 will be subject to a surcharge. TOP priority = default assigned to instructions of trading platforms (multilateral trading facilities, Stock Exchanges, etc.) with and without a central clearing counterparty (CCP) as well as over the counter (OTC) instructions with a CCP (URD 7.2.2.2). Special instructions assigned by Central Banks or CSDs with a ‘reserved priority’ (e.g. Central Bank monetary policy operations) will attract the same charge. HIGH priority = can be assigned by T2S Users to OTC transactions (without

Currency Participation Agreement

Schedule 7 – Pricing

	<i>CCP) in the relevant settlement instruction. High priority instructions follow in the processing hierarchy after top priority instructions (URD 7.2.2.3).</i>
Fee trigger	<i>Instructions flagged with 'Top Priority' or 'High Priority' which are settled in the period 07:00 – 18:00. If a CSD's priority traffic exceeds 20% of its total settlement volume within the monthly billing period, the Eurosystem will discuss the matter with the respective CSD to assess the reason for such high usage. Should usage not be brought into a range below 20%, the CSD will be billed for the priority fee and charges may apply after a notification period of 60 days.</i>

136 Cancellation

Price	Zero eurocent per instruction
DvP weight factor	0%
Background	<i>The cancellation of a settlement instruction which had been submitted previously will need to be validated and the original settlement instruction will be flagged as successfully cancelled. In cases where the instruction has already been Matched, each side of the cancellation will still get charged. Cancellation instructions which are not successfully executed or have been denied are not charged.</i>
Fee trigger	<i>All instructions that have been successfully cancelled. Successful automatic cancellation of settlement instructions by the Instruction Maintenance Module would also be charged. All previously attracted chargeable status (e.g. Matched, partial settlement, Intended Settlement Date fail) will remain and get charged as well.</i>

137 Settlement modification

Price	Zero eurocent per instruction
DvP weight factor	0%
Background	<i>Settlement instruction modifications include any change of the Hold status (CSD hold status/ CSD validation hold status/ party hold status/ CoSD hold status), all release instructions, change of priority, change of partial settlement indicator and linkage block. All relevant default settings will not attract a charge because they are driven by the relevant static data.</i>

Currency Participation Agreement

Schedule 7 – Pricing

Fee trigger	<i>Any successfully executed settlement modification instruction leading to a change in status.</i>

138 **Fee per T2S Dedicated Cash Account**

Price	Zero euro monthly per T2S Dedicated Cash Account
Background	<i>Monthly fixed fee to cover for the maintenance of the static data. This fee will be charged to respective T2S Users via their Central Bank.</i>
Fee trigger	<i>Any T2S Dedicated Cash Account with the account status 'open' at the end of the monthly billing period or if it was closed during the billing period.</i>

139 **4.5 Tariff items priced at zero at least until end of cost-recover period**

140 **Securities Account fees**

141 Securities Account fees will be set at zero at least until the end of the cost recovery period.

Price	Option a) Zero eurocent monthly per ISIN in a Securities Account Option b) Zero euros monthly per Securities Account
Background	<i>Increased numbers of ISINs in an account in general means more resource associated with maintaining static data for the account. T2S parties will have the choice between: Option a) each Securities Account open in the database of T2S and active during the billing period will attract a monthly fixed fee which will be applied for each ISIN held in the account; or Option b) each Securities Account open in the database of T2S will attract a monthly fixed fee to cover for the maintenance of a Securities Account static data. Should CSDs offer the option. T2S Users can decide which option to be applied but it should be stable in the long term.</i>
Fee trigger	<i><u>Option a)</u> All ISIN positions at the end of the monthly billing period within a Securities Account which was active during the billing period and the account flagged to be charged by ISIN will attract a fix fee per ISIN position in the account <u>Option b)</u> Any Securities Account <u>not</u> flagged to be charged by ISIN with the account status 'open' at the end of the monthly billing period will attract a fix fee. This fixed fee will also be applied to accounts closed during the billing period.</i>

142

Currency Participation Agreement

Schedule 7 – Pricing

5 Inventory of T2S Service Charges

5.1 Introduction

The Inventory of T2S Service Charges (the Inventory) provides T2S Users with a description of how T2S will finance changes (which, depending on the type of change, could potentially result in increases of T2S prices included in the T2S price list), and a number of other services not covered in the T2S price list. The present content of the Inventory is not necessarily exhaustive, but could potentially be expanded to encompass other types of service charges. If the list were to be expanded at a later stage, the general principle of charging at cost shall remain.

5.2 Changes

The process for how changes will be implemented to the T2S Services is described in Schedule 9 on ‘Change and Release Management’. The following section describes how the costs for Common Changes and Specific Changes of the T2S Services will be recovered.

5.2.1 T2S Common Changes

Common Changes are defined as “any new feature, functionality or service – or any amendment of an existing feature, functionality or service – which is implemented for the benefit of all T2S Actors”. Prior to going ahead and implementing a Change Request, the Eurosystem will specify the development and running costs of the change. This will be a binding offer on behalf of the Eurosystem.

Those Common Changes that are classified as “corrective maintenance” (i.e. fixing of errors in coding, design or detailed specifications (bug fixes)” and “technical maintenance” (i.e. software adaptations and/or testing activities imposed by changes of the hardware or the operating system or other infrastructural software packages within certain resource limits) will not be charged separately. Some of these Common Changes might be financed through the T2S Contingency Reserve, within the general rules defined by the Governing Council.

All other Common Changes will first need to be financed by the Eurosystem and the Governing Council needs to decide to increase the financial envelope of T2S by the cost of such a change. Substantial increases in the financial envelope could result in the need to adjust the T2S price list at some stage and/or to lengthen the amortisation period and/or to establish separate amortisation cycles. The development costs, running costs and capital costs associated with these Common Changes will therefore have to be recovered through T2S fees (see T2S price list) over an amortisation period.

Currency Participation Agreement

Schedule 7 – Pricing

CSDs commit to bear any residual costs related to Common Changes requested by them that cannot be recovered through T2S fees.

5.2.2 T2S Specific Changes

Specific Changes are defined as “any new feature, functionality or service – or any amendment of an existing feature, functionality or service – which is not supported by all T2S Actors”. Based on the principle of non-exclusiveness and non-discrimination, the functionality would in principle be available to all initial and future T2S parties. However, those not wishing to use the new functionality would not be impacted and therefore would not bear any of the costs.

Prior to a Specific Change Request being approved, the Eurosystem will specify the full financial consequences associated with the change (e.g. the implementation costs, the running costs, capital costs and potentially lost revenues). The estimate of the implementation costs will be a binding offer on behalf of the Eurosystem.

Once the Specific Change Request has been approved and before the Eurosystem starts development activities, the entities requesting the change (“requesters”) will formally commit to bear the full financial consequences of the change and agree with the T2S Board on the financing of the Specific Change. The financing of Specific Changes may be in the form of either pre-financing, financing via transaction fees levied on the use of the specific functionality or any other recovery method to be agreed between the requesters and the T2S Board.

Entities which have not been part of the original agreement between the Eurosystem and the requesters to develop a specific functionality but decide to use such functionality at a later stage (“late-joiners”) will have to bear an appropriate share of the financial consequences. The requesters that initially requested the specific functionality shall seek an agreement with the late-joiner(s) for the revised allocation of financial consequences of such functionality. If original requesters and the late-joiner(s) cannot find an agreement on the revised allocation of the full financial consequences of that functionality, a panel of experts (nominated by CSDs in line with Arbitration rules) will decide on a revised allocation, using objective criteria in order to ensure non-discrimination, to avoid duplication of Specific Changes and to keep T2S open for new developments. Subject to the late-joiner having paid or committed to pay its share of the full financial consequences of the Specific Change in accordance with the revised allocation, it will be able to use the specific functionality.

5.2.3 Pricing of assessments of Change Requests

Preliminary assessments of a request for a functional change will attract a charge of €2,000. If, based on the results of the preliminary assessment, the party then decides to request a detailed

Currency Participation Agreement

Schedule 7 – Pricing

assessment for the functional change, the detailed assessment will attract an additional charge of €10,000.

If the Change Request is subsequently approved and implemented, either as a Common Change or Specific Change, the costs of the preliminary and detailed assessments will be added to the total cost of the change (and recovered in the manner described in sections 5.2.1 and 5.2.2).

If the change is rejected, the costs of the preliminary and detailed assessment would be charged directly to the requester. In case there is more than one requester, the costs of the preliminary assessments and detailed assessments would be distributed equally.

5.3 RTGS fees for connecting to T2S

If an RTGS system charges T2S a fee for connecting to T2S, T2S will not charge this fee to its Contracting CSDs. T2S will annually charge such fee back to the Central Bank that operates the T2S Dedicated Cash Account in the currency in which the RTGS system operates. As a matter of service, T2S will annually provide each Central Bank operating a T2S Dedicated Cash Account with each Payment Bank's annual share in the total number of postings on that T2S Dedicated Cash Account and the Central Bank might take that into account when allocating the charges.

5.4 Training

The Eurosystem will provide training by qualified trainers to interested parties on the structural and operational aspects of T2S. Such general training which T2S offers to all T2S Stakeholders will be free of charge. Tailor-made training will be charged to the requesting party on a per diem basis. The Eurosystem will charge training services at cost. T2S training course offerings and associated charges will be published on a regular basis.

5.5 Consultancy

The Eurosystem may provide resources on request of a CSD, Central Bank or a Directly Connected Party to provide advice and support improving their technical infrastructure interaction with the T2S platform. Specific consultancy will be charged to the requesting party on a per diem basis. The Eurosystem will charge the consultancy services that it provides at cost.

5.6 Request for an additional test environment

The Eurosystem will be providing two test environments for User Testing during migration and post-migration without charging any additional service charge.

The Eurosystem will provide additional test environments subject to an approved Change Request. If CSDs/Central Bank would require additional test environments, the set-up costs of

Currency Participation Agreement

Schedule 7 – Pricing

the test environment as well as daily maintenance fees will be charged at cost either as a Common or a Specific Change.

If the additional test environment(s) is charged as a Specific Change, the fee will be included in the respective CSD/Central Bank bill as soon as the relevant test environment is ready for testing.

5.7 Securities Reference Data

If the Eurosystem were to provide the securities maintaining services to CSDs, it will charge these services at cost.

5.8 Connectivity Services

[The Eurosystem allows all CSDs and NCBs, and their customers, i.e. Directly Connected Parties and Dedicated Cash Account holders respectively, to connect to T2S via two types of connectivity: (i) a Dedicated Link connection, and (ii) a Value Added Network. The Eurosystem will charge the set-up and operation of its Dedicated Link connection at cost to the Directly Connected Actors using such a connection. In addition, the Eurosystem will charge each Directly Connected Actor with a one-off fee of EUR [...] for the issuance of each requested security certificate and an annual fee of EUR [...] for the annual prolongation of each security certificate.]

5.9 One-off joining fee

A CSD joining T2S will pay a one-off joining fee in the amount of 25% of the annual fee that this CSD will pay to T2S, calculated on the basis of the fee paid in the first full year of T2S operation of the CSD in question. The fee will be calculated and charged one year after the CSD will have started its operations in T2S.

5.10 Exit Management

If a CSD terminates the T2S Framework Agreement for convenience, the Eurosystem will invoice the CSD at cost for all planning, co-ordination and execution of exit activities that go beyond normal operational support. This will also be the case if a CSD decides to exit because the relevant non-euro area NCB no longer outsources its currency.

If a CSD has terminated the Framework Agreement for cause, the Eurosystem will provide the support for exit activities free of charge.

5.11 External Examiner

In accordance with Article 23.7 of the Currency Participation Agreement, the non-euro NCB and/or its auditors shall have the right to propose special examinations to be conducted by the

Currency Participation Agreement

Schedule 7 – Pricing

268 External Examiner directly to the Governing Council provided that the non-euro NCB bears the
269 costs associated with such special examinations.

270 If a regular or special examination is required because of a severe incident or a material and
271 ongoing problem having disrupted the proper functioning of the T2S Platform or the provision of
272 T2S Services, as specified in Article 23.5 of the Currency Participation Agreement, the total cost
273 charged by the External Examiner shall be borne by the Eurosystem.

CURRENCY PARTICIPATION AGREEMENT

ANNEX 1 TO SCHEDULE 7

LIST OF REPORTS AND QUERIES AND ASSOCIATED BUSINESS ITEMS

Currency Participation Agreement

Schedule 7 – Annex 1 – List of reports and queries and associated business items

Table of contents

1. List of A2A reports and business items..... 1

2. List of A2A queries and business items..... 3

3. List of U2A reports and business items..... 6

Currency Participation Agreement

Schedule 7 – Annex 1 – List of reports and queries and associated business items

1. List of A2A reports and business items

Report Name	Business Item
Current Settlement Day Cash Information Report	T2S Dedicated Cash Account
Following Settlement Day Cash Forecast Report	T2S Dedicated Cash Account
Statement of Accounts	Cash Posting
Statement of Settlement Allegements	Allegement
Statement of executed amendment instructions for Intra-Balance Movements	Amendment Instruction
Statement of executed amendment instructions for Intra-Position Movements and Settlement Instructions	Amendment Instruction
Statement of executed cancellation instructions for Intra-Balance Movements	Cancellation Instruction
Statement of executed cancellation instructions for Intra-Position Movements and Settlement Instructions	Cancellation Instruction
Statement of Holdings	Securities Position
Statement of pending amendment instructions for Intra-Balance Movements	Amendment Instruction
Statement of pending amendment instructions for Intra-Position Movements and Settlement Instructions	Amendment Instruction
Statement of pending cancellation instructions for Intra-Balance Movements	Cancellation Instruction
Statement of pending cancellation instructions for Intra-Position Movements and Settlement Instructions	Cancellation Instruction
Statement of Pending Instructions	Settlement Instruction
Statement of pending intra-balance movements	Intra-Balance Movement
Statement of pending intra-position movements	Intra-Position Movement
Statement of settled intra-balance movements	Intra-Balance Movement
Statement of settled intra-position movements	Intra-Position Movement

Currency Participation Agreement

Schedule 7 – Annex 1 – List of reports and queries and associated business items

Statement of Static Data for Party	Party
Statement of Static Data for Securities	Security
Statement of Static Data for Securities Accounts	Securities Account
Statement of Static Data for T2S Dedicated Cash Accounts	T2S Dedicated Cash Account
Statement of Transactions	Settlement Instruction

Currency Participation Agreement

Schedule 7 – Annex 1 – List of reports and queries and associated business items

2. List of A2A queries and business items

Query name	Business Item
Amendment Instruction List Query	Amendment Instruction
Amendment Instruction Query for Intra Balance Movements	Amendment Instruction
Amendment Instruction Query for Intra Position Movements and Settlement Instructions	Amendment Instruction
Cancellation Instructions for Intra Balance Movements Query	Cancellation Instruction
Cancellation Instructions for SI + Intra Position Movements Query	Cancellation Instruction
Cash Forecast Query	T2S Dedicated Cash Account
Collateral Value of a Security Query	T2S Dedicated Cash Account
Collateral Value per T2S Dedicated Cash Account Query	T2S Dedicated Cash Account
Cumulative Billing Data Query	Party
Current Status of the T2S settlement day	Business Day
Immediate Liquidity Transfer Order Detail Query	Immediate Liquidity Transfer Order
Immediate Liquidity Transfer Order List Query	Immediate Liquidity Transfer Order
Intra Balance Movements Query	Intra Balance Movement
Intra Position Movements Query	Intra Position Movement
ISIN List Query	Security
Itemised Billing Data Query	Billing Item
Limit Query	Limit
Limit Utilisation Journal Query	Limit
Limit Utilisation Query	Limit
Liquidity Transfer Order Detail Query	Standing or Predefined Liquidity Transfer Order

Currency Participation Agreement

Schedule 7 – Annex 1 – List of reports and queries and associated business items

Liquidity Transfer Order Link Set Query	Liquidity Transfer Order Link Set
Liquidity Transfer Order List Query	Standing or Predefined Liquidity Transfer Order
Liquidity Transfer Order of a Liquidity Transfer Order Link Set Query	Standing or Predefined Liquidity Transfer Order
Outstanding Auto-Collateralisation Credit Query	T2S Dedicated Cash Account
Party List Query	Party
Party Reference Data Query	Party
Report Details Query	Report
Restricted Party Query	Party
Securities Account List Query	Securities Account
Securities Account Position Query	Securities Position
Securities Account Reference Data Query	Securities Account
Securities CSD Link Query	Security
Securities Deviating Nominal Query	Security
Securities Reference Data Query	Security
Settlement Instruction Audit Trail Query	Settlement Instruction
Settlement Instruction Current Status Query	Settlement Instruction
Settlement Instruction Query	Settlement Instruction
Settlement Instruction Status Audit Trail Query	Settlement Instruction
Static Data Audit Trail Security Query	Security
Static Data Audit Trail Party Query	Party
Static Data Audit Trail Securities Account Query	Securities Account
Static Data Audit Trail T2S DCA Query	T2S Dedicated Cash Account
T2S Calendar Query	Dates
T2S Dedicated Cash Account Balance Query	T2S Dedicated Cash Account

Currency Participation Agreement

Schedule 7 – Annex 1 – List of reports and queries and associated business items

T2S Dedicated Cash Account List Query	T2S Dedicated Cash Account
T2S Dedicated Cash Account Posting Query	Cash Posting
T2S Dedicated Cash Account Reference Data Query	T2S Dedicated Cash Account
T2S Diary Query	Business Day
T2S Overall Liquidity Query	Party
Total amount of standing and predefined orders Query	Party
Total collateral value per T2S Dedicated Cash Account Query	T2S Dedicated Cash Account

Currency Participation Agreement

Schedule 7 – Annex 1 – List of reports and queries and associated business items

3. List of U2A reports and business items

Note: When the Business Item of a U2A query is referred to as “fixed”, it means that only one business item per query will be counted and charged for.

Query name	Business Item
Allegment Instruction Query	Allegement
Amendment Instruction List Query	Amendment Instruction
Amendment Instruction Query for Intra Balance Movements	Amendment Instruction
Amendment Instruction Query for Intra Position Movements and Settlement Instructions	Amendment Instruction
Attribute Domain Details Query	fixed
Attribute Domain List Query	fixed
Attribute Reference Details Query	fixed
Attribute Reference List Query	fixed
Auto-Collateralisation Eligibility Links Query	fixed
Cancellation Instructions for Intra Balance Movements Query	Cancellation Instruction
Cancellation Instructions for SI + Intra Position Movements Query	Cancellation Instruction
Cash Forecast Query	T2S Dedicated Cash Account
Close Links Query	fixed
Closing Day Query	fixed
CMB Details Query	fixed
CMB List Query	fixed
CMB Securities Account Link Details Query	fixed
CMB Securities Account Links List Query	fixed
Collateral Value of a Security Query	T2S Dedicated Cash Account
Collateral Value per T2S Dedicated Cash Account Query	T2S Dedicated Cash Account

Currency Participation Agreement

Schedule 7 – Annex 1 – List of reports and queries and associated business items

Conditional Security Delivery Rule Details Query	fixed
Conditional Security Delivery Rule Query	fixed
Conditional Security Delivery Rule Set Details Query	fixed
Conditional Security Delivery Rule Set Query	fixed
Country Query	fixed
CSD Account Links Query	fixed
Cumulative Billing Data List Query	Party
Cumulative Billing Data Query	Party
Currency Query	fixed
Current Status of the T2S settlement day	Business Day
Data Changes Details Query	fixed
Data Changes Query	fixed
Default Event Schedule Details Query	fixed
Dynamic Data Audit Trail Details Query	fixed
Dynamic Data Audit Trail List Query	fixed
Eligible Counterpart CSD List Query	fixed
Eligible Counterpart CSD Query	fixed
Event Type Details Query	fixed
Event Type List Query	fixed
External RTGS Account Details Query	fixed
External RTGS Account List Query	fixed
Grant/Revoke Privileges List Query	fixed
Grant/Revoke Roles List Query	fixed
Hold/Release Instruction Query	fixed
Immediate Liquidity Transfer Order Detail Query	Immediate Liquidity Transfer Order
Immediate Liquidity Transfer Order List Query	Immediate Liquidity Transfer Order

Currency Participation Agreement

Schedule 7 – Annex 1 – List of reports and queries and associated business items

Inbound Files Details Query	fixed
Inbound Files List Query	fixed
Inbound Message Details Query	fixed
Inbound Message List Query	fixed
Intra Balance Movements Query	Intra Balance Movement
Intra Position Movements Query	Intra Position Movement
ISIN List Query	Security
Itemised Billing Data List Query	Billing Item
Itemised Billing Data Query	Billing Item
Limit List Query	Limit
Limit Query	Limit
Limit Utilisation Journal Query	Limit
Limit Utilisation Query	Limit
Liquidity Transfer Order Detail Query	Standing or Predefined Liquidity Transfer Order
Liquidity Transfer Order Link Set Query	Liquidity Transfer Order Link Set
Liquidity Transfer Order List Query	Standing or Predefined Liquidity Transfer Order
Liquidity Transfer Order of a Liquidity Transfer Order Link Set Query	Standing or Predefined Liquidity Transfer Order
Market-specific Attribute Details Query	fixed
Market-specific Attribute Query	fixed
Market-specific Restriction List Query	fixed
Market-specific Restriction Type Rule Detail Query	fixed
Market-specific Restriction Type Rule Set List Query	fixed
Market-specific Restriction Type Details Query	fixed
Market-specific Restriction Type Rule Sets -Display Rule Sets Matrix Query	fixed

Currency Participation Agreement

Schedule 7 – Annex 1 – List of reports and queries and associated business items

Message Subscription Rule Details Query	fixed
Message Subscription Rule Query	fixed
Message Subscription Rule Set Details Query	fixed
Message Subscription Rule Set Query	fixed
Network Service List query	fixed
Operating Day Type Details Query	fixed
Operating Day Type List Query	fixed
Outbound Message Details Query	Message
Outbound Message List Query	Message
Outstanding Auto-Collateralisation Credit Query	T2S Dedicated Cash Account
Partial Settlement Threshold Group Query	fixed
Party List Query	Party
Party Reference Data Query	Party
Privilege Query	fixed
Report Configuration Detail Query	fixed
Report Configuration List Query	fixed
Report Details Query	Report
Report Query	Report
Restricted Party Query	Party
Role Details Query	fixed
Role Query	fixed
Routing Details Query	fixed
Routing Query	fixed
Secured Group Details Query	fixed
Secured Group List Query	fixed
Secured Object	fixed
Securities Account List Query	Securities Account
Securities Account Position Query	Securities Position

Currency Participation Agreement

Schedule 7 – Annex 1 – List of reports and queries and associated business items

Securities Account Reference Data Query	Securities Account
Securities CSD Link Query	Security
Securities Deviating Nominal Query	Security
Securities Position Detailed Restriction Details Query	Security
Securities Posting Query	Securities Posting
Securities Reference Data Query	Security
Securities Valuations Query	Security
Service Item Details Query	fixed
Service Item Query	fixed
Settlement Instruction Audit Trail Query	Settlement Instruction
Settlement Instruction Current Status Query	Settlement Instruction
Settlement Instruction Query	Settlement Instruction
Settlement Instruction Status Audit Trail Query	Settlement Instruction
Static Data Audit Trail Security Query	Security
Static Data Audit Trail Party Query	Party
Static Data Audit Trail Securities Account Query	Securities Account
Static Data Audit Trail T2S DCA Query	T2S Dedicated Cash Account
SWIFT BIC Query	fixed
System Entity Query	fixed
T2S Calendar Query	Dates
T2S Dedicated Cash Account Balance Detailed Restrictions Query	T2S Dedicated Cash Account
T2S Dedicated Cash Account Balance Query	T2S Dedicated Cash Account
T2S Dedicated Cash Account List Query	T2S Dedicated Cash Account
T2S Dedicated Cash Account Posting Query	Cash Posting
T2S Dedicated Cash Account Reference Data Query	T2S Dedicated Cash Account
T2S Diary Query	Business Day
T2S Overall Liquidity Query	Party

Currency Participation Agreement

Schedule 7 – Annex 1 – List of reports and queries and associated business items

T2S System User Query (T2S Actor Query)	fixed
Technical Addresses Network Services Link Details Query	fixed
Technical Addresses Network Services Links List Query	fixed
Tolerance Amount Query	fixed
Total amount of standing and predefined orders Query	Party
Total collateral value per T2S Dedicated Cash Account Query	T2S Dedicated Cash Account

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 8

GOVERNANCE

Currency Participation Agreement

Schedule 8 – Governance

Table of contents

Preamble.....	1
1 The decision-making process.....	3
1.1 T2S Governance Bodies.....	3
1.2 Decision-making on Change Requests.....	4
1.3 Decision-making on relevant matters other than Change Requests	7
2 Additional Governance arrangements	8
2.1 Prioritisation	8
2.2 Changes driven by Legal and Regulatory Requirements	9
2.3 Transparency	10
2.4 Technical groups supporting the T2S Governance Bodies	10
Annex 1 - Mandate of the NECSG	1
1 Preamble.....	1
2 Objective	1
3 Responsibilities	1
4 Composition	2
5 Term	2
6 Reporting.....	2
7 Working Procedures	3
Annex 2 – Mandate of the Governors’ Forum.....	1
1 Objective	1
2 Responsibilities	1
3 Right to convene	1
4 Composition	2
5 Term	2
6 Endorsement of resolutions	2
7 Working Procedures	2

Currency Participation Agreement

Schedule 8 – Governance

1 **Preamble**

2 This schedule sets out the Governance, i.e. the set of rules and procedures concerning the
3 management of T2S Services, including the related procedures for decision-making and the roles
4 of T2S Stakeholders therein. The Governance applies as of the Agreement Date and shall govern
5 the Development Phase and the Operational Phase of TARGET2-Securities (T2S).

6 The parties agree that:

7 (1) The aim of the Governance principles is to provide each T2S Stakeholder with the level of
8 control necessary in further pursuing its commercial and policy objectives and to seek
9 compliance with Legal and Regulatory Requirements. However, the parties agree that since T2S
10 is a multilateral environment, their level of control is necessarily less than if each T2S signatory
11 had its own environment. Levels of control can vary with the objects of control as described in
12 this Agreement. However, T2S is designed and operated so that the Connected NCBs will
13 exercise full control in real time over the Dedicated Cash Accounts in their respective currency in
14 T2S as described in Article [20 (7) and (8)].

15 (2) Control is necessary to ensure that T2S operates safely and efficiently. Moreover, control
16 shall allow change to be achieved and managed so as to ensure that changes that are proposed by
17 one party/parties can be introduced without unduly affecting the other party/parties.

18 (3) In order to achieve the necessary balance of control, it is very important that transparency is
19 ensured and that all T2S Stakeholders are closely involved in the Governance of T2S. It is
20 essential to ensure that T2S meets the evolving needs of the market in a consensual way.
21 Transparency shall assure the T2S Stakeholders that final decisions will not be taken before their
22 positions are considered by the relevant T2S Governance Body and by the other T2S
23 Stakeholders. For this reason, technical and policy documents, such as the User Requirements
24 Document, the Economic Impact Analysis and the T2S Governance arrangements were
25 extensively discussed with market participants and published on the T2S's website. The
26 Eurosystem intends to continue doing so.

27 (4) The euro area and the Connected NCBs need to maintain control of their respective currencies
28 in T2S. In particular they need to continue to be able to operate the cash accounts they hold for
29 their Dedicated Cash Account Holders, and to be able to safeguard the integrity of their
30 respective currency (which, for the purposes of the CPA, includes the implementation of
31 monetary policy including all central bank credit operations as well as settlement in Central Bank
32 Money in their currency). They also need to maintain or contribute to financial stability in their
33 country and to ensure a level playing field for market participants.

Currency Participation Agreement

Schedule 8 – Governance

34 (5) Users, i.e. the customers of CSDs, and ultimately issuers and investors are the eventual
35 beneficiaries of T2S. Their demands have to be appropriately taken into account when further
36 developing T2S functionalities in order to ensure that T2S continues to meet the needs of the
37 market.

38 On the basis of the above considerations, Section 1 explains the relationship of the different T2S
39 Governance Bodies in the decision-making process. Additional Governance arrangements are
40 outlined in Section 2.

Currency Participation Agreement

Schedule 8 – Governance

41 **1 The decision-making process**

42 **1.1 T2S Governance Bodies**

43 The T2S Governance Bodies are specified in Article [20 (6)] of this Agreement. They are
44 involved in the decision-making process with final decisions being taken by the Governing
45 Council in accordance with Article [20] of this Agreement and in accordance with this Schedule.

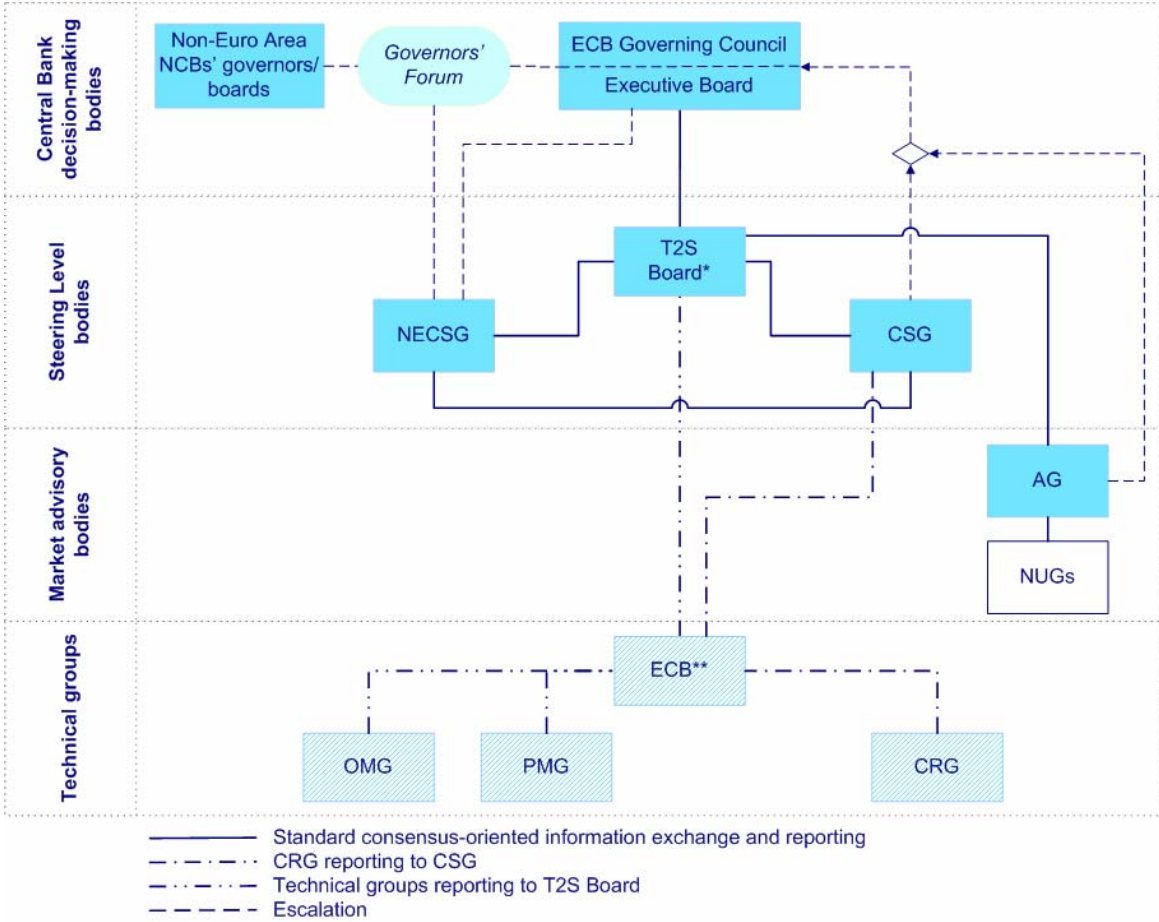
46 The Steering Level consists of the Non-euro Currencies Steering Group (NECSG), the CSD
47 Steering Group (CSG) and the T2S Board. For matters which are referred to the Steering Level in
48 this Agreement and which have not been delegated to the T2S Board by the Governing Council,
49 the Governing Council represents the Eurosystem. Each T2S Governance Body has the
50 possibility to establish substructures, i.e. technical groups (permanent) or task forces (ad-hoc);
51 see also Section 2.4.

52 The resolutions of the Governors' Forum require the endorsement of the Governing Council and
53 the decision-making bodies of each of the Connected NCBs.

Currency Participation Agreement

Schedule 8 – Governance

Figure 1: Bodies involved in the T2S Governance



Note: * The T2S Board is the Eurosystem T2S Governance Body at the Steering Level for matters which have been delegated by the Governing Council. The T2S Board liaises with other Eurosystem internal governance structures for issues of common concern.

** The ECB routes the reporting and the information to the respective addressees.

1.2 Decision-making on Change Requests

- Any individual Participating CSD, User member in the AG, euro area NCB, Connected NCB, the ECB or the 4CB may initiate a Change Request.
- The Change Request is prepared by the Change Review Group (CRG) according to the procedures described in Schedule 9 (Change and Release Management). The CRG submits its deliverables to the CSD Steering Group (CSG) via the ECB. The ECB also provides the CRG deliverables to the T2S Board, the Non-euro Currencies Steering Group (NECSG) and the T2S Advisory Group (AG) and publishes the deliverables on the T2S website. Should any of the before-mentioned T2S Governance Bodies fail to provide its view within a reasonable amount of time, taking into account the urgency of the Change Request, this T2S Governance

Currency Participation Agreement

Schedule 8 – Governance

70 Body is then assumed to have agreed with the Change Request and the decision-making
71 procedure continues.

72 3. If the Change Request was related to safeguarding the integrity of the respective currency
73 (which, for the purposes of the CPA, includes the implementation of monetary policy
74 including all central bank credit operations as well as settlement in Central Bank Money in
75 the respective currency) and/or financial stability as part of crisis management measures,
76 transparency could be limited to the contracting T2S Actors (Participating CSDs and Central
77 Banks) upon request of a Central Bank. Such Change Requests shall be made transparent at
78 the latest when the change is taken up in a release.

79 4. The AG gives its advice on the Change Request within a reasonable amount of time, taking
80 into account the urgency of the Change Request. The advice of the AG is addressed to the
81 T2S Board and it shall be published on the T2S's website.

82 5. The CSG takes a resolution on the Change Request within a reasonable amount of time,
83 taking into account the urgency of the Change Request. The resolution of the CSG is
84 addressed to the T2S Board and shall be published on the T2S's website.

85 6. The NECSG takes a resolution within a reasonable amount of time, taking into account the
86 urgency of the Change Request. If the Connected NCB(s) consider at risk the integrity of the
87 respective currency, the financial stability or the level playing field for market participants,
88 such concern shall be included in the resolution of the NECSG. The resolution of the NECSG
89 is addressed to the T2S Board and it shall be published on the T2S's website.

90 7. A final decision on the Change Request is taken by the Governing Council on the basis of a
91 proposal by the T2S Board within a reasonable amount of time, taking into account the
92 urgency of the Change Request. The T2S Board submits a proposal to the Governing Council
93 after having reached a consensus with the CSG and the NECSG, taking into account the
94 advice of the AG in accordance with paragraph 8.

95 8. If consensus cannot be achieved based on the stakeholders' initial resolutions, the T2S Board
96 aims at reconciling the different views before the Governing Council takes its final decision:

97 a. The T2S Board coordinates discussions with relevant stakeholder groups in order to find
98 a consensual solution. The T2S Board may ask for a re-assessment of the Change
99 Request by the CRG taking into account the views of all relevant stakeholders. Based on
100 the CRG re-assessment, the T2S Board discusses with all relevant stakeholder groups
101 taking into account the respective views and prepares a compromise proposal within a
102 reasonable amount of time, taking into account the urgency of the Change Request. The

Currency Participation Agreement

Schedule 8 – Governance

T2S Board shares this proposal with the CSG, the NECSG and the AG. For issues of key concern, this consensus driven approach to establish a compromise proposal may be a repetitive process. Once consensus is reached within a reasonable amount of time, taking into account the urgency of the Change Request, the AG formally gives its new advice and the CSG and the NECSG take new resolutions on the Change Request.

- b. If such discussions do not lead to consensus, the T2S Board, the CSG or the NECSG may ask for a non-binding external advice except for matters related to safeguarding the integrity of currencies in T2S or to financial stability. The party providing such advice needs to be selected by common agreement of the T2S Board, the CSG and the NECSG and deliver its advice in parallel to the T2S Board, the CSG, the NECSG and the AG. All relevant stakeholder groups review their position on the basis of the non-binding external advice and the T2S Board coordinates discussions with the relevant stakeholder groups in order to find a consensual solution in accordance with paragraph 8a and taking into account paragraph 9 and 10. Within a reasonable amount of time and taking into account the urgency of the Change Request, the AG formally gives its final advice and the CSG and the NECSG take final resolutions on the Change Request before the Governing Council takes the final decision on the basis of a proposal by the T2S Board.

9. If the reconciliation process according to paragraph 8 does not lead to consensus between the Eurosystem and the Connected NCB(s), both Parties have the right to request a review of the issue by the Governors' Forum, in order to find a consensual solution.

10. If no solution for the dispute can be found in the Governors' Forum, the following procedure applies:

- a. the view of the Eurosystem as owner and operator of T2S prevails. If the dispute was based on the refusal of a Change Request because Connected NCB(s) consider that the measure is inappropriate for reasons linked to their responsibilities in terms of safeguarding the integrity of the respective currency or in relation to financial stability, the Eurosystem would have to justify overruling the refusal either (i) with the need to safeguard general Eurosystem central bank functions (safeguarding the euro, financial stability, no distortion of competition) or (ii) with the need to preserve the integrity of the T2S platform for economic, functional or technical reasons.
- b. the concerned Connected NCB(s) shall have the right to terminate the respective bilateral CPA. The concerned Connected NCB(s) shall have the right to require that they can exit T2S within 24 months after the Governing Council's decision, during which period they shall not be affected by a change they rejected. Connected NCBs shall endeavour to limit the exit period to the shortest time possible.

Currency Participation Agreement

Schedule 8 – Governance

11. The final decision of the Governing Council is published on the T2S's website.

1.3 Decision-making on relevant matters other than Change Requests

1. Any individual Participating CSD, euro area NCB, Connected NCB, the ECB, the 4CB or User member in the AG may, outside the scope of Change Requests, propose a resolution or, in particular in the case of the AG, an advice concerning relevant matters of T2S¹ to the T2S Board or, in exceptional circumstances, to the Governing Council.

2. In all T2S Governance Bodies the chairperson may decide that the proposal for a resolution or an advice needs first to be analysed by a substructure, i.e. a technical group (permanent) or by a task force (ad-hoc). The T2S Board or, in exceptional circumstances, the Governing Council organises the procedure in such a way that all T2S Governance Bodies are properly consulted within a reasonable amount of time and without duplicating substructures on similar topics. In case of divergence of views between different T2S Governance Bodies, the T2S Board shall aim at reconciling the different views. The CSG or the NECSG can, upon agreement with the T2S Board, ask for a non-binding external advice for relevant matters of T2S¹ except for matters related to safeguarding the integrity of currencies in T2S or to financial stability. The party providing such advice needs to be selected by common agreement of the T2S Board, the CSG and the NECSG and shall deliver its advice in parallel to the T2S Board, the AG, the CSG and the NECSG.

3. A decision on the proposal is taken by the Governing Council or, for matters which have been delegated by the Governing Council, by the T2S Board after consultation of the AG, the CSG and the NECSG within a reasonable amount of time, taking into account the urgency of the matter.

4. The Eurosystem notifies the relevant parties. For Connected NCBs, the following procedure applies. The Eurosystem notifies the decision to the Connected NCB Governors who, in general, have four weeks to object if they consider that the measure is inappropriate for reasons linked to their responsibilities in term of safeguarding the integrity of the respective currency or in relation to financial stability. The relevant procedure, as defined under Section 1.2, paragraphs 9 and 10 above, applies.

5. The decision of the Governing Council or the T2S Board shall be published on the T2S website.

¹ Such relevant matters include crisis management, risk issues, operational issues, monitoring the T2S Service (in accordance with the Service Level Agreement), pricing issues, acceptance for testing and go-live.

Currency Participation Agreement

Schedule 8 – Governance

2 Additional Governance arrangements

In addition to the general Governance procedures outlined above, this section clarifies a number of specific situations.

2.1 Prioritisation

The Change Review Group shall:

- prepare a proposal for the definition of a release based on procedures described in Schedule 9 (Change and Release Management).

The AG:

- shall submit its advice regarding the prioritisation of Change Requests to the T2S Board;

The CSG:

- shall make a resolution addressed to the T2S Board regarding the prioritisation of Change Requests stemming from the Participating CSDs or in relation to the functioning rules of Securities Accounts;

- may prepare a proposal to the T2S Board on the prioritisation of all Change Requests.

The NECSG:

- shall make a resolution addressed to the T2S Board regarding the prioritisation of Change Requests stemming from the Connected NCBs or in relation to the functioning rules of Dedicated Cash Accounts;

- may prepare a proposal to the T2S Board on the prioritisation of all Change Requests.

The T2S Board:

- shall prepare a proposal for the prioritisation of all T2S Stakeholder Change Requests to be submitted to the Governing Council taking into account the views of the AG, the CSG and the NECSG. If the proposals for prioritisation of Change Requests provided by the T2S Board, the AG, the CSG and the NECSG diverge, the T2S Board shall aim at finding consensus and seeks the views of the AG, the CSG and the NECSG before submitting the final proposal on the prioritisation of Change Requests to the Governing Council.

Currency Participation Agreement

Schedule 8 – Governance

The Governing Council:

- shall prioritise all T2S Stakeholder Change Requests on the basis of a T2S Board proposal, to which the views obtained from the AG, the CSG and the NECSG are attached.

2.2 Changes driven by Legal and Regulatory Requirements

Changes motivated by Legal and Regulatory Requirements shall be dealt with in T2S according to the standard procedure set out in Schedule 9 (Change and Release Management) with high priority, in accordance with the principle that T2S shall support the participating CSDs in complying with oversight, regulatory and supervisory requirements, and following the relevant decision-making process. Such Change Requests have to be initiated by the affected entities.

However, several cases have to be distinguished:

- (a) Changes in European legislation are dealt with as quickly as possible or as required in the legislation. The analysis of the Change Request by the various T2S Governance Bodies mentioned in this note concerns only the modalities of the implementation.
- (b) It is expected that the Participating CSDs and Central Banks inform the T2S Board on any proposed change in national legislation with an impact on T2S as early as reasonably practicable. The relevant Change Requests shall be dealt with according to the standard procedure. The final decision shall be taken by the Governing Council and a potential refusal shall include the reasons why the implementation of the Change Request is not feasible.
- (c) Change Requests resulting from a Relevant Competent Authority request shall follow the standard procedure and the Eurosystem shall involve the AG, the CSG and the NECSG. Should these discussions lead to a disagreement with the Relevant Competent Authority, the Change Request shall be brought to the Governing Council and the Relevant Competent Authority will be invited to submit its written view directly to the Governing Council. The Governing Council would then take due account of the views of the Relevant Competent Authority before making a decision. Should the Governing Council reject the Change Request, it will provide a written explanation of the rationale to the Relevant Competent Authority. The Governing Council can reconsider its decision based on additional information provided by the Relevant Competent Authority. When a Change Request resulting from a Relevant Competent Authority request relates to only one market it shall not be in contradiction with the General Principles of T2S and relevant costs shall be borne by the Participating CSDs, subject to the regulatory decision.

Currency Participation Agreement

Schedule 8 – Governance

(d) Changes under (b) and (c) above which involve legislation or regulatory requirements in a non-euro area country are discussed in the Governors' Forum, if the Governor of the relevant Connected NCB so requests.

The Eurosystem shall aim at finding solutions to the cases outlined above, including the possibility of optional features to the extent that they are technically viable and within the Lean Scope of T2S.

2.3 Transparency

In order to allow a wide range of market participants to remain closely involved in T2S developments, the extensive T2S transparency regime shall be continued and relevant documentation and information shall be made available on the T2S's website. In particular, the Eurosystem's offer of the future updates of the Framework Agreement to all interested CSDs and of the Currency Participation Agreement to all interested non-euro area NCBs shall be made transparent. Furthermore, relevant advice, resolutions and decisions related to changes shall be published. This transparency will allow all T2S Stakeholders to contribute to ongoing T2S discussions and make their views known to relevant T2S Governance Bodies.

2.4 Technical groups supporting the T2S Governance Bodies

Each T2S Governance Body has the possibility to establish technical groups, and to dissolve them, to deal with T2S issues that are within its remit. The T2S Board shall make proposals to avoid duplication of substructures on similar topics.

The technical groups shall in particular:

(a) ensure that T2S and subsequent releases go-live and that CSDs, as well as Central Banks, are duly and timely prepared, including with regard to the relevant aspects of User Testing and Migration;

(b) review, in line with Schedule 2 (T2S Programme Planning and Monitoring), the CSD and/or Central Bank-relevant planning and programme reporting, including risks and issues;

(c) assess Change Requests, as defined in Schedule 9 (Change and Release Management);

(d) develop and maintain the Manual of Operational Procedures; and

(e) meet the Eurosystem to review the T2S service performance against the SLA.

Currency Participation Agreement

Schedule 8 – Governance

The technical groups shall report to the relevant T2S Governance Bodies. The technical groups have the possibility to exchange relevant information directly among themselves. They organise their work in an efficient manner to fulfil their mandates, including the possible creation of their own substructures.

At the time of the signature of the Currency Participation Agreement, the following groups have been considered as technical groups:

(a) PMG: Project Managers Group, established by the Steering Level and consisting of project managers of Participating CSDs, euro area NCBs, non-euro area NCBs, the ECB and 4CB. The T2S Board shall appoint the chairperson of the PMG on the basis of her/his technical expertise after consultation of the CSG and the NECSG. The PMG reports to the T2S Board and keeps the CSG and the NECSG informed of its work. It needs to ensure that T2S and subsequent releases go live and that CSDs as well as Central Banks are duly and timely prepared. Its name, mandate and need for continuation will be reviewed when all CSDs and Central Banks will have migrated to T2S.

(b) CRG: Change Review Group, established by the Steering Level and consisting of product managers and functional experts of Participating CSDs, euro area NCBs, non-euro area NCBs, the ECB and 4CB. User representatives participate in the CRG as observers. The T2S Board shall appoint the chairperson of the CRG on the basis of her/his technical expertise after consultation of the CSG and the NECSG. The CRG reports to the CSG via the ECB. The ECB disseminates the deliverables of the CRG also to the T2S Board, the AG and the NECSG. It assesses Change Requests as defined in Schedule 9 (Change and Release Management). The CRG and the PMG also need to exchange information regarding the impact of changes on the T2S timeline. The CRG continues the work of the AG Sub-Group on User Requirements Management.

(c) OMG: Operations Managers Group, established by the Steering Level and consisting of operations experts of Participating CSDs, euro area NCBs, non-euro area NCBs, the ECB and 4CB. Representatives of Users which are Directly Connected Parties may participate in the OMG as observers for specific agenda items. The T2S Board shall appoint the chairperson of the OMG on the basis of her/his technical expertise after consultation of the CSG and the NECSG. The OMG reports to the T2S Board and informs the AG, the CSG and the NECSG. It develops and maintains the Manual of Operational Procedures, meets to review the T2S service performance against the SLA and coordinates the management of operational incidents. The OMG continues the work of the AG Sub-Group on Operational Framework.

Currency Participation Agreement

Schedule 8 – Annex 1 – Mandate of the NECSG

Annex 1 - Mandate of the NECSG

1 Preamble

TARGET2-Securities (T2S) is a multi-currency system for the whole of Europe. The T2S Services that the Eurosystem offers to Central Securities Depositories (CSDs) in Europe allow for the core, neutral and borderless settlement of securities transactions on a Delivery-versus-Payment basis in Central Bank Money for all participating currencies. The provision of T2S Services in different currencies is based on the cooperation between Central Banks and the equality of all currencies in T2S.

2 Objective

The ECB's Governing Council and the governing bodies of the non-euro area national central banks that signed the Currency Participation Agreement (CPA) (hereinafter the 'Connected NCBs') have established the Non-euro Currencies Steering Group (NECSG). The NECSG discusses all matters of relevance for Connected NCBs in T2S. It is the objective of the NECSG to achieve consensus and to avoid where possible transmitting individual views to the Eurosystem.

The NECSG supports the decision-making process in T2S, which has a multilateral character, by providing the Eurosystem, to the extent possible, with a common position of the Connected NCBs on matters of relevance for Connected NCBs in T2S. The NECSG works within the Governance specified in the corresponding CPA Schedule.

3 Responsibilities

In the T2S Governance, the NECSG is responsible for articulating and coordinating the views of Connected NCBs.

The NECSG may agree on a resolution on any issue in relation to T2S, and in particular on:

- changes to the CPA and its Schedules, in line with the applicable procedures;
- any issue brought to the Governing Council with implications for the CPA;
- issues brought to the attention of the Governing Council in relation to changes to T2S;

Currency Participation Agreement

Schedule 8 – Annex 1 – Mandate of the NECSG

- changes to the T2S Scope Defining Set of Documents, in line with the applicable procedures specified in the CPA Schedules 8 (Governance) and 9 (Change and Release Management);
- the prioritisation of Change Requests stemming from Connected NCBs;
- disputes between the Eurosystem and CSDs upon the invitation of the T2S Board, the Governing Council or the CSD Steering Group;
- any other consultation request of the T2S Board or the Governing Council.

The outcome of a discussion in the NECSG neither restricts the ability of a Central Bank to safeguard the integrity of its currency (which, for the purposes of the CPA, includes the implementation of monetary policy including all credit operations as well as the settlement in Central Bank Money in the respective currency) nor the control over its respective cash accounts (including the exercise of its rights and duties under the CPA), nor pre-empts the right of the Governor of any of the Connected NCBs to request a meeting of the Governors' Forum.

4 Composition

The NECSG is composed of senior managers nominated by the respective Governors of all Connected NCBs. The NECSG Chairperson is elected by the members of the NECSG and appoints a very experienced member of staff of any of the Connected NCBs or the ECB as NECSG Secretary. The NECSG Chairperson may designate an alternate to replace the NECSG Secretary in exceptional circumstances.

The NECSG Chairperson may invite the T2S Board Chairperson to attend their discussions as an observer.

5 Term

The NECSG's mandate starts as of the Agreement Date and expires with the replacement of the CPA with a new agreement and/or with the termination of the CPA by the signatories. The term of the NECSG members begins and ends at the same time as the term of the members of the T2S Board.

6 Reporting

The NECSG provides resolutions to the T2S Board as the managing body of T2S, upon invitation or on its own initiative. The NECSG may transmit its resolutions directly to the Governors'

Currency Participation Agreement

Schedule 8 – Annex 1 – Mandate of the NECSG

Forum and/or the Governing Council if it considers that the control of any one or more of the currencies, the General Principles of T2S or other core elements of T2S are at risk. The NECSG may establish its own procedures on the frequency of this reporting, which may vary over time during the validity of the CPA.

7 Working Procedures

The NECSG meets upon the invitation of the NECSG Chairperson and as frequently as the NECSG decides. The first NECSG meeting takes place within three months after the CPA enters into force.

The NECSG's aim is to adopt resolutions by consensus and to avoid where possible transmitting individual views to the Eurosystem. However each individual member of the NECSG has the right to:

- include an opinion in an NECSG resolution that differs from the view of the other central banks; and
- escalate an issue to the Governors' Forum if they consider that a T2S Board decision negatively affects their ability to safeguard the integrity of their respective national currency.

Any NECSG member may propose a resolution. A disagreement between one or more Connected NCBs and the Eurosystem may be escalated from the technical, expert and sub-structure level to the NECSG. The NECSG may invite the T2S Board Chairperson or another T2S Board member to its discussion. The NECSG may request the advice of the CSD Steering Group and/or the T2S Advisory Group. It is the objective of the NECSG to achieve consensus. However, if the NECSG members and the T2S Board Chairperson cannot reach a mutually agreeable solution, the issue is escalated to the T2S Board and ultimately to the Governors' Forum.

The NECSG may establish sub-structures to support its work if it considers this necessary. It coordinates with the T2S Board who organises work in such a way that all relevant T2S Governance Bodies are properly involved without duplicating sub-structures on similar topics.

Detailed working procedures are specified in the 'Rules of Procedure' to be drafted by the NECSG. The T2S Board has the possibility to express a non-binding opinion on the Rules of Procedure before their entry into force.

As part of the transparency principle of T2S, NECSG resolutions are in principle published on T2S's website.

Currency Participation Agreement

Schedule 8 – Annex 2 – Mandate of the Governors' Forum

Annex 2 – Mandate of the Governors' Forum

1 Objective

The ECB's Governing Council and the governing bodies of the non-euro area national central banks that signed the Currency Participation Agreement (CPA) (hereinafter the 'Connected NCBs') have established the Governors' Forum. The Governors' Forum discusses in exceptional circumstances matters of relevance for Connected NCBs in TARGET2-Securities (T2S) that could not be resolved by other bodies. It is the clear objective of the Governor's Forum to discuss and settle such disputes by agreeing on a common resolution in consensus.

2 Responsibilities

The Governor's Forum deals with all disputes between the Eurosystem and the Connected NCBs arising in relation to the implementation of the CPA and to T2S in non-euro area countries in general when all other methods of reaching a consensus have been exhausted.

Appropriate matters that can be brought to the Governors' Forum include in particular, but not exclusively:

- issues related to safeguarding the integrity of the non-euro area currency (which, for the purposes of the CPA, includes the implementation of monetary policy including all central bank credit operations as well as the settlement in Central Bank Money in their currency) or financial stability;
- issues related to other legal or regulatory responsibilities of the Connected NCBs;
- issues related to the (potential) termination of a CPA and the subsequent exit management procedure for a Connected NCB.

3 Right to convene

The Governors' Forum meets only in the event that:

- (a) one or several members of the NECSG consider that a decision of the T2S Board negatively affects their ability to safeguard the integrity of their respective currency (which, for the purposes of the CPA, includes the implementation of monetary policy including all credit

Currency Participation Agreement

Schedule 8 – Annex 2 – Mandate of the Governors' Forum

401 operations as well as the settlement in Central Bank Money in their respective currency) or
402 financial stability;

403 (b) one or several governors of Connected NCBs wish to discuss any matter that a governor feels
404 appropriate to raise in relation to T2S;

405 (c) the Governing Council wishes to consult the Governor's Forum before taking a decision or to
406 discuss any matter which the Governing Council feels appropriate to raise in relation to T2S.

407 **4 Composition**

408 The Governors' Forum is composed of the governors of the Connected NCBs that have signed
409 the CPA and an equal number of Governing Council members. The Governors' Forum is chaired
410 by the President or the Vice-President of the ECB.

411 **5 Term**

412 The Governors' Forum is established and can be convened as of the Agreement Date until the
413 CPA is terminated or replaced by another contractual arrangement.

414 **6 Endorsement of resolutions**

415 The resolutions of the Governors' Forum require the endorsement of the Governing Council and
416 the decision-making bodies of each of the Connected NCBs.

417 **7 Working Procedures**

418 The Governors' Forum meets only upon the request of one or several Connected NCBs and/or
419 the Governing Council and works based on consensus of its members. The Governing Council
420 and the governors of Connected NCBs can agree to have recourse on an ad-hoc basis to expert
421 panels. Such panels assist the Governors' Forum in finding a compromise solution. This applies
422 in particular to technical issues.

423 Relevant conclusions are made public on T2S's website after the endorsement of the Governing
424 Council and the decision-making bodies of each of the Connected NCBs.

425 The Governors' Forum is an ad-hoc body and therefore does not require specific rules of
426 procedure. The T2S Board Chairperson acts as secretary to the Governor's Forum.

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 9

CHANGE AND RELEASE MANAGEMENT

Currency Participation Agreement

Schedule 9 – Change and Release Management

Table of contents

Introduction	1
1. Objective.....	2
2. Scope.....	3
3. Entities involved in the CRM process.....	5
3.1 Technical level	5
3.1.1 ECB.....	5
3.1.2 4CB.....	5
3.1.3 Participating CSDs and the Central Banks	6
3.1.4 Change Review Group	6
3.2 Steering Level	7
4. Change management	9
4.1 Categorisation of changes	9
4.1.1 Type of change according to urgency	9
4.1.2 Type of change according to beneficiary	9
4.1.3 Parameters of changes.....	10
4.1.3.1. Parameter 1: Legal/business importance.....	10
4.1.3.2. Parameter 2: Market implementation efforts.....	11
4.1.3.3. Parameter 3: Operational/technical impact	11
4.1.3.4. Parameter 4: Financial impact for T2S	12
4.2 Change Management process.....	13
4.2.1 Change Request Initiation and Registration.....	15
4.2.2 Preliminary assessment	16
4.2.3 Detailed assessment and evaluation.....	17
4.2.3.1. Detailed assessment	17
4.2.3.2. Evaluation of the Change Request.....	18
4.2.4 Authorisation	19
5. Release management	21
5.1 Release types and frequency	21
5.2 Release Management process.....	22

Currency Participation Agreement

Schedule 9 – Change and Release Management

5.2.1	Preparation of the list of authorised changes and defect resolutions	24
5.2.2	Definition of release.....	24
5.2.3	Release approval.....	26
5.2.4	Release planning and monitoring	26
5.2.5	Implementation.....	27
5.2.5.1.	Design, building and configuration	27
5.2.5.2.	Testing of a new release by the Participating CSDs and the CBs	28
5.2.5.3.	Roll- out and communication	30
5.2.5.4.	Delivery – Go-live	31
5.2.6	Post implementation review	31
Annex 1:	Change Request Form	1
Annex 2:	Change Request Form	1
Annex 3:	Indicative timeline for the T2S Release Management	1
Annex 4:	Scoring mechanism	1

Currency Participation Agreement

Schedule 9 – Change and Release Management

1 **Introduction**

2 There will be changes in T2S for a variety of reasons. Due to the fact that these changes need to
3 be translated in a timely and consistent way into functional, legal, operational or technical
4 specifications, with the involvement of (and impact on) all relevant T2S Stakeholders, a proper
5 Change and Release Management process (CRM) must be defined and implemented. In addition,
6 the implementation of any of these changes can risk damaging the service's availability or
7 integrity, and may require changes (or specific monitoring efforts) on the part of entities
8 connected to, or relying on, T2S. The CRM process is thus essential in order to efficiently track
9 and manage changes to T2S and to mitigate the risks associated with these changes.

10 The definition of a release will follow a demand driven model, meaning that a priority rating is
11 used to establish the order in which the authorised changes should be considered for a particular
12 T2S release, and also taking into consideration the available capacity and the resources for
13 implementing the change.

14 The CRM process is based on the ITIL (Information Technology Infrastructure Library)
15 framework version 3.0 for IT service management.

16 **The CRM process will apply before and after T2S Go-Live Date, for all Change Requests**
17 **(falling within the scope of this document) that are initiated as from the entry into force of**
18 **the Framework Agreement respectively the Currency Participation Agreement.**

19 The Eurosystem, the CSDs that have signed the Framework Agreement (FA) ('Participating
20 CSDs') and the non-euro area NCBs that have signed the Currency Participation Agreement
21 (CPA) ('Connected non-euro area NCBs') will be entitled to participate in the CRM process as
22 full members of the Change Review Group (CRG) in accordance with the T2S Governance. User
23 representatives participate in the CRG as observers.

24 Meanwhile, the CSDs and non-euro area NCBs which have not yet entered into an agreement
25 with the Eurosystem by the agreed date will have no right of co-decision in the CRM process
26 until they sign. They will be kept informed about the changes to the T2S Services via T2S
27 communication channels.

28

Currency Participation Agreement

Schedule 9 – Change and Release Management

1. Objective

The objectives of the CRM process are to:

- Respond to the relevant T2S Stakeholders' changing business requirements while maximising value and minimise the risk of change related incidents;
- Ensure that Change Requests falling within the scope of this document will be managed within the Lean Scope of T2S;
- Ensure that Change Requests are managed in an efficient and controlled manner from the initiation until implementation (recorded and then evaluated, authorized, and that the resulting changes are prioritized, planned, tested, implemented, documented and reviewed in a controlled manner);
- Ensure that Change Requests falling within the scope of this document are communicated to all relevant T2S Stakeholders in accordance with the rules laid down in this Schedule and in Schedule 8 (Governance);
- Agree on the exact T2S release content and plan the successful rollout of a release into the production environment; and
- Ensure that all changes are traceable, secure and that only correct, authorised and tested versions are installed on the T2S production environment.

Currency Participation Agreement

Schedule 9 – Change and Release Management

2. Scope

The CRM process applies to all functional changes which trigger any addition to, deletion from or modification of any item in T2S as defined in the T2S Scope Defining Set of Documents¹, as well as to changes to these documents, even if they do not have an impact on the T2S functionality. In addition, the CRM process applies to the requirements to be fulfilled by NSPs, as laid down in – and taking into account the provisions of – the Licence Agreement, and to the specifications for the Value-added Connectivity Services necessary to implement the Dedicated Link Connections.

The General Principles of T2S in Section 1.2 of the User Requirements Document cannot be changed as a by-product of another Change Request, but only by a separate Change Request to the General Principles of T2S, which follows the decision-making process in this Schedule and respecting the Eurosystem rights as described in Schedule 8 (Governance). If any other Change Request falling within the scope of this Schedule is not in line with the General Principles of T2S as they read from time to time in the User Requirements Document, the CRG will immediately report such inconsistency to the Steering Level and wait for guidance before continuing the assessment of that Change Request.

Any change subject to the CRM process must be undertaken following the process outlined in this document.

Corrections/changes covered by maintenance activities for fixing errors, mistakes, failures or faults in the software system, which produce an incorrect or unexpected result, or cause it to behave in unintended ways (e.g. fixing errors in coding, design or detailed specification, performing changes to the system caused by an incident/problem) will be managed according to the procedures defined in the Manual of Operational Procedures. However, although these corrections/changes do not need assessment and authorisation in the context of Change Management process, they follow the Release Management process as described in chapter 5.2.

The following changes are not subject to the CRM process:

- Technical changes to hardware/infrastructure components (i.e. non-functional changes) under the control of the Eurosystem that are necessary to sustain the daily operation of T2S in accordance with the Service Levels specified in Schedule 6 (T2S Service Level Agreement). The respective arrangements/procedures for handling these changes are

¹ The T2S Scope Defining Set of Documents as defined in the Schedule 1 (Definitions) to the FA and the CPA.

Currency Participation Agreement

Schedule 9 – Change and Release Management

- 77 covered in Schedule 6 (T2S Service Level Agreement) and will be detailed in the Manual
78 of Operational Procedures. The operational body/team responsible for managing and
79 implementing the technical changes should liaise closely with the Change Review Group
80 (as defined in section 3.1.3) to ensure a smooth implementation, in particular in case of
81 technical changes that may have an impact on the service delivered (based on the risk
82 assessment);
- 83 ▪ Business configuration changes related to market parameters that can be done by the
84 Participating CSDs²/ CBs or by the Eurosystem in accordance with the procedures
85 defined in the Manual of Operational Procedures;
- 86 ▪ Changes related to non-functional and non-technical documentation e.g. Manual of
87 Operational Procedures, Registration and Connectivity Guides, training materials, etc;
- 88 ▪ Updates of the baseline version of T2S Specification and T2S Operational Phase
89 Documents³, which follow a Deliverable Change Process. The process and the
90 substructure involved are defined in Schedule 2 Annex 8 (T2S Deliverables list and
91 management process) to the FA and CPA;
- 92 ▪ Other changes related to the FA and its annexes, respectively to the CPA and its annexes
93 that will be managed according to the relevant procedure as set out in the FA,
94 respectively the CPA or the relevant annex following the applicable Governance regime.
- 95

² In accordance with the Preamble D of the Framework Agreement, the Participating CSDs shall retain full control of the parameter of its business operations. This applies e.g. for Participating CSDs for setting up the T2S Securities Accounts for their customers including all needed access rules , granting of access privileges, etc Setting up of these parameters and rules should be done according to the best market practices and the relevant regulatory requirements.

³ T2S Specification and T2S Operational Phase Documents as defined in the Schedule 1 (Definitions) to the FA and the CPA and in the Schedule 2 Annex 8 (T2S Deliverables list and management process).

Currency Participation Agreement

Schedule 9 – Change and Release Management

3. Entities involved in the CRM process

There are two levels differentiated in the CRM process: a “technical” level and a “Steering” Level. The Participating CSDs and the Central Banks are expected to organise themselves according to these two levels.

3.1 Technical level

3.1.1 ECB

The T2S Team of the ECB supports the T2S Board in the CRM process. The roles and responsibilities of the ECB at the different stages of the CRM process are described in the chapters 4.2 and 5.2 of this Schedule. They include inter alia:

- being the entry point for all Change Requests;
- keep a register of all Change Requests;
- manage their processing as described in this document;
- monitor Change Requests during their entire lifecycle, from the initiation until they have reached their end status (i.e. authorization or rejection);
- monitor the release definition and its implementation;
- track progress and issues that may influence decision-making and report them inter alia to the Change Review Group as defined in chapter 3.1.3;
- ensure availability of the relevant information to the relevant T2S Stakeholders.

3.1.2 4CB

4CB means the Deutsche Bundesbank, the Banco de España, the Banque de France and the Banca d'Italia, collectively, in their capacity as NCBs responsible for building, maintaining and running the T2S Platform based on the respective contractual arrangements and on decisions of the Governing Council. In the context of CRM process, the 4CB is entrusted with different roles and responsibilities as described in the chapters 4.2 and 5.2 of this Schedule. They include inter alia:

- assess the impact stemming from requests for new functionalities or technical

Currency Participation Agreement

Schedule 9 – Change and Release Management

122 enhancements from a technical, functional and operational point of view (feasibility,
123 planning, budget);

124 ▪ building, configuration and delivery of a release into production;

125 ▪ propose the time-frame for implementing a change or a release;

126 ▪ examine the impact on the system security and provide a security impact assessment;

127 3.1.3 Participating CSDs and the Central Banks

128 The euro area NCBs, the Participating CSDs and the Connected non-euro area NCBs are entitled
129 to participate in the CRM process. Their roles and responsibilities at different stages of the CRM
130 process are described in the chapters 4.2 and 5.2 of this Schedule. They include inter alia:

131 ▪ act as full members of the Change Review Group (CRG);

132 ▪ initiate Change Requests on their own or customers' behalf;

133 ▪ evaluate and monitor Change Requests;

134 ▪ monitor release definition and implementation;

135 ▪ test and verify releases;

136 ▪ involve their respective user communities in the process.

137 3.1.4 Change Review Group

138 At the technical level, a “Change Review Group” (CRG) will be created. It will be composed of
139 representatives from each CSD that has signed the FA, each non-euro area NCB that has signed
140 the CPA, each euro area NCBs, the ECB and the 4CB. User representatives participate in the
141 CRG as observers. The members of the CRG shall have a product manager profile having the
142 required functional and business expertise.

143 The CRG will be responsible, inter alia for/ in charge of:

144 ▪ reviewing Change Requests on regular basis, evaluate the information provided in the
145 Change Request and in the assessment (checking its consistency and completeness across
146 all Change Requests) and making proposals for decision making at the Steering Level.

147 ▪ building and maintaining the scoring mechanism according to which authorised changes
148 will be prioritised in view of their implementation in (one of) the next release(s).

Currency Participation Agreement

Schedule 9 – Change and Release Management

- making proposals for, reviewing and monitoring the content of each release as well as any changes to the agreed release.

As regards the interactions with the Steering Level, the role of the CRG is limited to the managing the process (i) from reviewing and evaluating the Change Request to making proposal for its approval/ rejection and (ii) from ranking the authorised changes based on the scoring mechanism to preparing the proposal for the content of future T2S releases. The CRG will aim at reaching a common agreement in making a proposal to the Steering Level for their decision-making. In case of disagreement, both majority and minority views will be reported to the Steering Level. Once the decision to authorise⁴ a change or to define the content of a T2S release has been taken, the decision is binding for the CRG's further work.

The CRG reports to the CSG via the ECB. The ECB also provides the deliverables of the CRG to the T2S Board, the AG and the NECSG.

The CRG will be informed and – to the extent possible and relevant – consulted on technical changes and changes that need to be implemented urgently in order to restore and continue the provision of T2S Services, by the relevant operational groups responsible for handling these changes, in accordance with the procedures defined in the Manual of Operational Procedures.

The CRG will schedule regular meetings, typically every 2 months, but meetings can also be organised more frequently if deemed necessary. The CRG should have face-to-face meetings, however some of the assessment process can be handled in written procedure if this process is accepted by the CRG in advance.

3.2 Steering Level

Without prejudice to the role of the Governing Council, the governance bodies at the Steering Level are (i) the T2S Board, (ii) the CSD Steering Group (CSG) and (iii) the Non-euro Currencies Steering Group (NECSG) as defined in the FA and the CPA.

Their roles and responsibilities in the decision-making process of changes and in the prioritisation of Change Requests for defining the content of the next T2S releases, as well as the escalation and dispute resolution procedure in case of disagreement between the Participating CSDs and the Eurosystem, or between the non-euro area NCBs and the Eurosystem are described in the FA, the CPA and Schedule 8 (Governance).

⁴ The authorisation of a Change Request is covered in the chapter 4.2.4

Currency Participation Agreement

Schedule 9 – Change and Release Management

178 Each governance body at the Steering Level will receive information from the CRG via the ECB
179 with respect to the CRM process. In the spirit of transparency, this information will also be
180 shared with the Advisory Group in accordance with Schedule 8 (Governance). The CRG will act
181 as a single joint technical group supporting these three governance bodies for the purpose of the
182 CRM process.
183

Currency Participation Agreement

Schedule 9 – Change and Release Management

4. Change management

4.1 Categorisation of changes

4.1.1 Type of change according to urgency

According to its level of urgency, a change falls under one of the following categorises:

- **Normal changes:** changes that can be planned without time constraints and will go through the CRM process before being implemented into the production environment.
- **Fast-track Changes:** changes that are imposed by Legal and Regulatory Requirements, or by CSG resolutions related to risk management, or changes that are critical for the stability of the T2S Platform or imposed by Central Bank decisions related to safeguarding the currency/-ies or related to crisis management measures to ensure financial stability and that, owing to the time constraints, have to be implemented in a shorter timeframe than normal, which will be decided on an ad-hoc basis. These changes will also go through the CRM process, however, the length of the different process steps will be shortened on an ad-hoc basis, in particular for preliminary and detailed assessment.

4.1.2 Type of change according to beneficiary

Irrespective of the urgency, all changes subject to the CRM process fall into one the following categories:

- **Common Changes:** any new feature, functionality or service – or any amendment of an existing feature, functionality or service – which is implemented for the benefit of all T2S Actors.
- **Specific Changes:** any new feature, functionality or service – or any amendment of an existing feature, functionality or service – which is not implemented as a Common Change (within the applicable Governance arrangements), but which some Participating CSDs and/or CBs wish to implement, provided that it is compliant with the Lean Scope of T2S, and for which they jointly accept to bear the investment and running costs. In case of Specific Change i) the unauthorised use should be either prevented or monitored (as agreed in the request); ii) in order to avoid any impact on non-supporting Participating CSDs/CBs, the implementation mechanism will be based – if possible – on

Currency Participation Agreement

Schedule 9 – Change and Release Management

213 the approach that the functionality will be made available to all parties, but that those not
214 wishing to use it, are not impacted by the change. iii) If this backward compatibility
215 cannot be ensured, the change can only be authorised upon agreement of each non-
216 supporting CSD/CB. These changes may be triggered by:

- 217 ○ market-specific regulatory, legal, fiscal or market-specific requirements or,
- 218 ○ innovation or improvement considered useful by one or more Participating CSDs or
- 219 CBs.

220 4.1.3 Parameters of changes

221 Each change is categorised based on a number of parameters which are used to indicate how
222 important or delicate a change is relative to others changes.

223 4.1.3.1. Parameter 1: Legal/business importance

224 The importance of a Change Request derives from the business need for a change and should be
225 part of the business justification. From an importance viewpoint, the Change Requests will be
226 classified into one of four categories as defined below:

Category	Definition
Critical	1) A change required by the Eurosystem or by a Connected non-euro area NCB to implement its statutory tasks. 2) A change relating to an area which would - if the change is not implemented - prevent Participating CSDs or CBs or their customers from connecting to and/or using T2S or put the requester in non-compliance (after implementing any work-arounds) with legal, regulatory (including, among others, unacceptable operational risks), or fiscal requirements. 3) Changes to preserve security, systems availability and stability etc.
High	1) A change that would offer a significant enhancement and benefits to the T2S Service or the T2S Actors. 2) A change to embody agreed harmonisation in T2S where there is a high efficiency benefit. 3) A change to significantly improve safety or stability. 4) A change to remove major ambiguity or inconsistency in the T2S Scope Defining Set of Documents or the T2S Documentation.

Currency Participation Agreement

Schedule 9 – Change and Release Management

Medium	1) A change with moderate efficiency benefits, but which does not have an important harmonisation dimension. 2) A change to improve the usability of the system. 3) A change to remove minor ambiguity or inconsistency in the technical and functional documentation.
Low	1) Changes that are “nice to have” and are useful to pad out a release. 2) A change to improve clarity of the technical and functional documentation.

227 4.1.3.2. Parameter 2: Market implementation efforts

228 Change Requests will be classified into three categories on the basis of the effort required by the
229 market to properly implement and timely absorb the change (i.e. implement the necessary IT
230 changes, adapt the operational procedures, integrate the change into the service offerings, adapt
231 the legal arrangements, etc.)

Category	Definition
High	Changes that require high efforts (a long implementation time and significant resources) on the side of the majority of Participating CSDs, CBs and/or their communities in order for them to be able to implement the change and take full benefit of it.
Medium	Changes that require high efforts (a long implementation time or significant resources) on the side of a minority of Participating CSDs, CBs and/or their communities or medium efforts on the side of the majority of Participating CSDs, CBs and/or their communities in order for them to be able to implement the change and take full benefit of it.
Low	Changes that do not require a long implementation time and any significant resources on the side of Participating CSDs, CBs and their communities in order for them to be able to take full benefit of the change

232 4.1.3.3. Parameter 3: Operational/technical impact

233 Change Requests will be classified into three categories on the basis of the operational/technical
234 impact if the change is undertaken, i.e. the risk that a change might trigger (some) instability on
235 the T2S Platform. The technical/operational risk of a change is its potential
236 undesirable/unexpected adverse impact on the T2S Platform and on the CSD/CBs.

237

Currency Participation Agreement

Schedule 9 – Change and Release Management

Category	Definition
High	Changes that have the potential to significantly threaten the Service Level for a significant part of T2S Services or have a significant operational impact on the Participating CSDs, CBs or 4CB, because insufficient mitigating measures can be taken.
Medium	Changes that have the potential to significantly threaten the Service Level for a minor part of T2S Services or have a limited operational impact on the Participating CSDs, CBs or 4CB, because insufficient mitigating measures can be taken.
Low	Changes that are expected not to threaten the Service Level for Participating CSDs or CBs or to have no or insignificant operational impact on the Participating CSDs, CBs or 4CB.

4.1.3.4. Parameter 4: Financial impact for T2S

An indication of the impact of the change on the required cost will be provided by the 4CB during the preliminary assessment phase. During the detailed assessment phase, the 4CB will provide the precise investment cost and the annual running cost, including a breakdown on costs for hardware, software and telecommunication.

Change Requests will be classified into three categories on the basis of the cost impact for the implementation of the Change Request.

Category	Definition
High	Changes with an investment cost of more than 500 000 EUR
Medium	Changes with an investment cost of less than 500 000 EUR, but more than 100 000 EUR
Low	Changes with an investment cost of less than 100 000 EUR

Currency Participation Agreement

Schedule 9 – Change and Release Management

4.2 Change Management process

All changes defined in chapter 2 as falling within the scope of the CRM process are subject to the Change Management (CM) process described in this chapter.

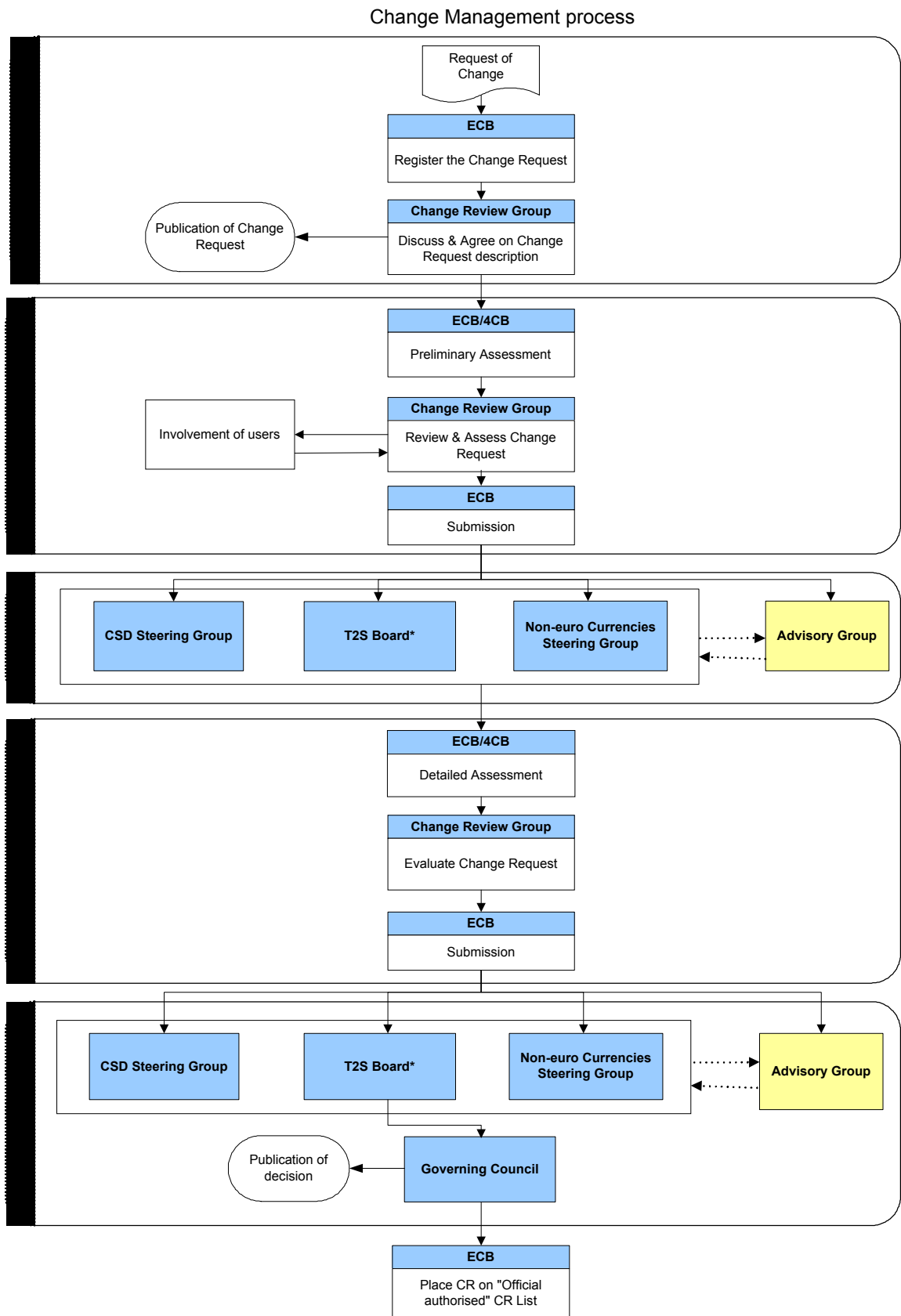
Depending on the urgency of the change, the length of the process may be different. In case of Fast-track Changes, the length of the process steps will be decided on ad-hoc basis (in particular for the preliminary and detailed assessments) considering the time that is available to implement each individual change.

In order to ensure transparency and facilitate a degree of monitoring by all relevant T2S Stakeholders, the Change Requests will be published on the website and shared with the AG according to the provisions outlined in Schedule 8 (Governance) and in this chapter.

The overall information flow of the CM process is presented in the following diagram:

Currency Participation Agreement

Schedule 9 – Change and Release Management



Note: * The T2S Board is the Eurosystem Governance body at the Steering Level for matters which have been delegated by the Governing Council. The T2S Board liaises with other Eurosystem internal governance structures for issues of common concern.

Currency Participation Agreement

Schedule 9 – Change and Release Management

4.2.1 Change Request Initiation and Registration

The requester, i.e. Participating CSDs, euro area NCBs, Connected non-euro area NCBs, the ECB or the 4CB, can submit a Change Request to the ECB using the standard form attached in Annex 1 (Change Request Form) and supply key information such as the title of the requested change, its description (changes in the existing features and functionalities, new features and functionalities in T2S), its business motivation (including the legal/regulatory requirement⁵), the urgency of the change, the categorisation of change, the date of the request, etc.

Users will always initiate Change Requests indirectly via a Participating CSD or a Central Bank. If this is not successful, Users can propose the initiation of a Change Request as a resolution in the AG. Then upon agreement of the AG, the Change Request is submitted for registration to the ECB who will submit it to the CRG for consideration according to the process described in this chapter.

The requester should clearly state in the description of the change whether the change should be implemented as a Specific Change and whether the unauthorised use of the Specific Change should be prevented or monitored. In addition, the requester will allocate the relevant parameters as defined in Chapter 4.1.3 to each Change Request in order to indicate its importance relative to the other changes, except the parameter 4 which will be allocated by the 4CB.

Upon receipt of the Change Request, the ECB will check whether the proposed Change Request is formally complete and unambiguous.

The ECB will then register the Change Request in a log and confirm its registration back to the requester. Upon registration, the Change Request receives a unique identifier.

In order to ensure transparency of Change Requests, the change log will be available to the Participating CSDs and CBs showing all requested changes according to their status and – where relevant – their assigned release.

The ECB will submit the registered Change Request to the CRG. The CRG will consider whether the categorisation of the change is correct or may – in liaison with the requester of the change – modify any parameter of the request to ensure that the change is adequately classified according to the parameters described in chapter 4.1.2. The CRG will check whether the change concerns only Dedicated Cash Accounts, only Securities Accounts or both. The CRG will also check the clarity and completeness of the request, that no complementary changes will be required for its implementation, confirm if the change should be assessed as a Specific Change and/or as a

⁵ Changes which are motivated by Legal and Regulatory Requirements will be implemented according to chapter 2.2. of Schedule 8 (Governance).

Currency Participation Agreement

Schedule 9 – Change and Release Management

Common Change considering the interest expressed by the other Participating CSDs/ CBs and agree carrying on with the preliminary assessment.

After the CRG's validation, the Eurosystem will publish the registered Change Request on the website. If the Change Request relates to safeguarding the integrity of the currency and/or financial stability as part of the crisis management measures, the Change Request will not be published on the website or shared with the user community of the Participating CSDs and CBs upon the request of a Central Bank until no later than the point in time the change has been formally taken up in a release.

4.2.2 Preliminary assessment

Upon the agreement of the CRG to carry out the preliminary assessment, the ECB will prepare – in co-operation with the requester and 4CB– the preliminary assessment of the Change Request. The preliminary assessment includes:

- compliance check: whether it falls within the Lean Scope of T2S and does not conflict with another Change Request already submitted;
- functional assessment: how does it affect the functionality as described in the T2S Scope Defining Set of Documents;
- technical assessment: evaluate the technical feasibility and complexity, analyse which domains, business sub-areas or other RTGS and /or CMS systems will be impacted. If necessary, the ECB will cooperate with the relevant non-euro area NCBs and consult the relevant ESCB committees or business areas that are responsible for these Eurosystem services;
- cost assessment: preliminary indication of the impact of the change from a cost perspective (see Parameter 4 in chapter 4.1.3.4 above);
- risk assessment: whether it could trigger instability to the T2S Platform or create performance problems.

The ECB and the 4CB will provide the information necessary for the preliminary and detailed assessment (see chapter 4.2.3.) that is required for the CRG to evaluate the CR. In case of changes to the T2S Scope Defining Set of Documents, a confirmation will be given by the ECB and 4CB– as part of the preliminary assessment – whether these changes in the documents have also an impact on the T2S Platform or not. If no impact exists on the T2S functionality, these changes can go directly to the authorisation phase (chapter 4.2.4).

Currency Participation Agreement

Schedule 9 – Change and Release Management

The result of the preliminary assessment will be provided by the ECB to the CRG for evaluation, in average 6 weeks and maximum 8 weeks from the agreement of the CRG to carry out the preliminary assessment.

While preliminary assessment is conducted by the ECB and 4CB, the Participating CSDs and CBs will consult their user communities in order to collect information on the change benefits and its impact on the process on the Users' side. This will allow the Users to provide their input and ensure that T2S provides functionality according to the needs of the market.

Upon the receipt of the preliminary assessment, the CRG will review and consider it from the potential impact of the change on their business or user community, with the aim of finding an agreement whether the Change Request should undertake the further steps of the process or not. Based on the categorisation of the change, the CRG will also analyse and assess the importance/impact of a change from/on all the T2S Actors' perspective, as well as any potential negative impact on another category of T2S Stakeholders.

The CRG will then finalise the preliminary assessment and will agree to propose one of the following actions:

1. Rejecting the Change Request. This requires the agreement of the requester, in which case the process stops at this stage. The governance bodies at the Steering Level will be informed accordingly. If there is a disagreement from the requester, the issue is escalated to the Steering Level for guidance; or
2. launching the detailed assessment of the Change Request and submit the preliminary assessment to the ECB who disseminates it to the Steering Level i.e. the CSG, the NECSG, the AG and the T2S Board for consideration.

Those Change Requests related to safeguarding the integrity of the currency and/or financial stability as part of the crisis management measures, that are not made transparent upon request of a Central Bank are not yet submitted to the AG.

4.2.3 Detailed assessment and evaluation

4.2.3.1. Detailed assessment

All changes reaching this process step will be subject to a full impact analysis.

The ECB and 4CB will evaluate the impact of the Change Request based on the following dimensions:

Currency Participation Agreement

Schedule 9 – Change and Release Management

Functional impact – to evaluate the functional consequences of a change, which function(s) it impacts.

Technical impact – to evaluate the technical consequences of a change, which module it impacts, the possible impacts on market participants, the complexity of the change, etc.

Cost impact - the assessment of the costs in order to implement the feature. The financial impact will cover the precise investment cost and the annual running costs as well as a breakdown of costs for hardware, software and telecommunication.

Legal impact - to evaluate possible impact of the Change Request on the legal construction of T2S and to assess any legal, regulatory or fiscal requirements – particularly on the Participating CSDs and CBs concerned, as well as Intellectual Property Rights-related issues.

Service Level impact – to evaluate the impact on the Service Level, including the KPIs agreed with the Participating CSDs, CBs and the other T2S Users.

Documentation impact - assessment of the documents that will need to be modified as a result of the Change Request. This can be the URD, GFS, UDFS, GS, GTD, Service Description, the GUI Business Functionality, User Handbooks, SLA, MOP etc.

Impact on the security of the system – to examine the impact on the system security and draw the attention to any risk that the Change Request would create;

Impact on operations – to highlight any constraint that the Change Request may impose directly or indirectly on IT operations and the possible resulting technical, operational or financial impacts.

As an outcome of the detailed evaluation step, the ECB will prepare a dossier for each Change Request which will be submitted to the CRG. This takes a maximum 10 weeks for the ECB and 4CB after the decision to conduct the detailed evaluation has been taken. Each Change Request shall be analysed without undue delay and assuring the quality.

4.2.3.2. Evaluation of the Change Request

Upon the receipt of the dossier with the detailed assessment, the CRG will review and evaluate it with the aim of finding a common agreement. The CRG members will also evaluate any potential impact on the economic, functional and technical viability and assess the cost and benefit of implementation for different stakeholders and the risks for their communities or the wider T2S. If needed, the CRG may modify any attribute of the Change Request as a result of the information provided in the detailed assessment.

Currency Participation Agreement

Schedule 9 – Change and Release Management

For Change Requests which have been assessed as common and specific, the CRG will evaluate and agree whether the change should be implemented as common or specific based on the information provided in the detailed assessment.

During its evaluation, the CRG may request the ECB and 4CB to conduct further detailed analysis. If the CRG requires further detailed analysis also from the CSDs' and CBs' perspective, the CSDs and CBs will have the opportunity to consult their user communities in order to collect further information on the change's benefits and its impact on the process on the Users's side.

If a Change Request has been assessed as a Common Change but it is supported only by some CRG members which have expressed their interest in implementing the change as a Specific Change (i.e. the change is rejected by the CRG as a Common Change), the change is submitted for re-assessment. The same rule will apply in case of a Change Request which is assessed as specific but, after the evaluation, the CRG members support its implementation as a Common Change.

Upon the finalisation of its evaluation, the CRG will prepare and submit its proposal on the draft resolution to the CSG via the ECB. The ECB will disseminate the evaluation of the CRG also to the T2S Board, the AG and the NECSG. Where necessary, the CRG will indicate those Change Requests that are uncontroversial and the issues that the Steering Level needs to be aware of, including diverging views of CRG members.

4.2.4 Authorisation

The authorisation process of a change is carried out by the Steering Level in accordance with Schedule 8 (Governance).

During the authorisation, the Steering Level may request further evaluation to be conducted by the CRG in order to complement the overall picture. In that case, the impacts of the Change Request will be re-assessed/evaluated as described in chapter 4.2.3.

The final decision on the Change Request may be:

1. To reject the Change Request. If all Participating CSDs and CBs agree on this decision then the process stops at this stage.
2. To authorise the change, as well as its cost recovery method, according to the principles specified in Schedule 7 (Pricing) to the FA and the CPA.

If a change is authorised after a failed dispute resolution in the Governors' Forum, which triggers the termination of the CPA by a non-euro area NCB, the latter has the right to exit T2S within a

Currency Participation Agreement

Schedule 9 – Change and Release Management

415 maximum period of 24 months. During this time and to the extent relevant for the operation of
416 T2S, the non-euro area NCB shall not be affected by the change that triggered their termination.
417 If such a change is imposed by a competent EU authority (i.e. any organization that
418 has regulatory, supervisory or oversight authority over the NCB, or a Connected NCB or a
419 Participating CSD (as required by the context) with cross-border competences), the concerned
420 CB will either make its best endeavours for a quicker exit, or will make the necessary changes in
421 its system so that T2S can implement the change.

422 The final decision of the Governing Council shall be published on the T2S website. Once
423 authorised, the Change Request will become part of the list of authorised changes, and hence
424 become eligible for implementation in (one of) the next T2S release(s), as explained in chapter 5
425 on the Release Management process.

426

Currency Participation Agreement

Schedule 9 – Change and Release Management

5. Release management

The Release Management (RM) process ensures that all aspects of a change, technical and non-technical, are considered together. The main objective is to deliver, distribute and track one or more changes intended for simultaneous release into the live environment while protecting the integrity of the production environment and its services.

The RM process covers the planning, design, build, configuration and testing of software and hardware to create a set of release components for the production environment. The term “Release” is used to describe a collection of authorised changes which typically consist of enhancements to the T2S Service (i.e. new and/or changed software required and any new or changed hardware needed for the implementation of the changes) and a number of defect resolutions which are implemented into the production environment.

The goal of the RM process is to ensure that authorised changes and the defect resolutions that have been agreed as part of a release are secure and traceable, and that only correct, tested and authorised versions are installed into the production environment.

All authorised changes initiated via a Change Management process and the defect resolutions shall follow the RM process.

5.1 Release types and frequency

As of the T2S Go-Live Date the releases can be classified as follows:

- Major release: a release where a large proportion of functionality provided by the T2S Service is affected or significant new functionality is added. This typically covers software changes containing substantially new functionality and defect resolutions.
- Minor release: a release that should contain, to the extent possible, changes that are less impacting for the T2S Users or for which backward compatibility is ensured. A minor release is only executed in case of need if the major release could not include the whole range of changes necessary to be implemented in the respective year or in cases where a business-critical change can not be bundled with the next major release.
- Fast-track release: if T2S is confronted with changes that are imposed by Legal and Regulatory Requirements, or by CSG resolutions related to risk management, or changes that are critical for the stability of the T2S Platform or imposed by Central Bank

Currency Participation Agreement

Schedule 9 – Change and Release Management

456 decisions related to safeguarding the currency/-ies or related to crisis management
457 measures to ensure financial stability that cannot be bundled into the next major or
458 minor release due to the time constraints, T2S will have to comply with these
459 requirements, possibly with an additional release, typically containing only the relevant
460 change(s).

461 ▪ Hot-fix release: it covers software corrections that need to be performed before the next
462 regular release, as otherwise the defect concerned could lead to substantial operational
463 problems, require heavy workarounds and/or lead to any other clear increase in the
464 operational risk level.

465 After the T2S Go-Live Date given the active involvement required from various relevant T2S
466 Stakeholders over a certain period of time, the frequency of releases should be minimised in
467 order to be able to manage risks adequately. The optimum frequency of releases should be
468 balanced between the business requirements and the relative impact, risk and cost of the release.
469 Consequently, depending on needs and resource allocation, and without prejudice to the need for
470 any fast-track and hot-fix releases, the Eurosystem can support 2 releases every year: one major
471 and - in case of need - one minor release⁶.

472 An indicative timeline showing the interaction between the RM and its milestones, the CM and
473 the meetings of the bodies are presented in Annex 3 (Indicative timeline for the T2S Release
474 Management).

475 The Participating CSDs and CBs will have the possibility to monitor the release implementation
476 and to carry out the testing according to the provisions currently described in Schedule 2 (T2S
477 Programme Planning and Monitoring) and 3 (User Testing) to the FA and to the CPA⁷.

478 5.2 Release Management process

479 The activities to be carried out during the RM process are depicted in the following diagram:

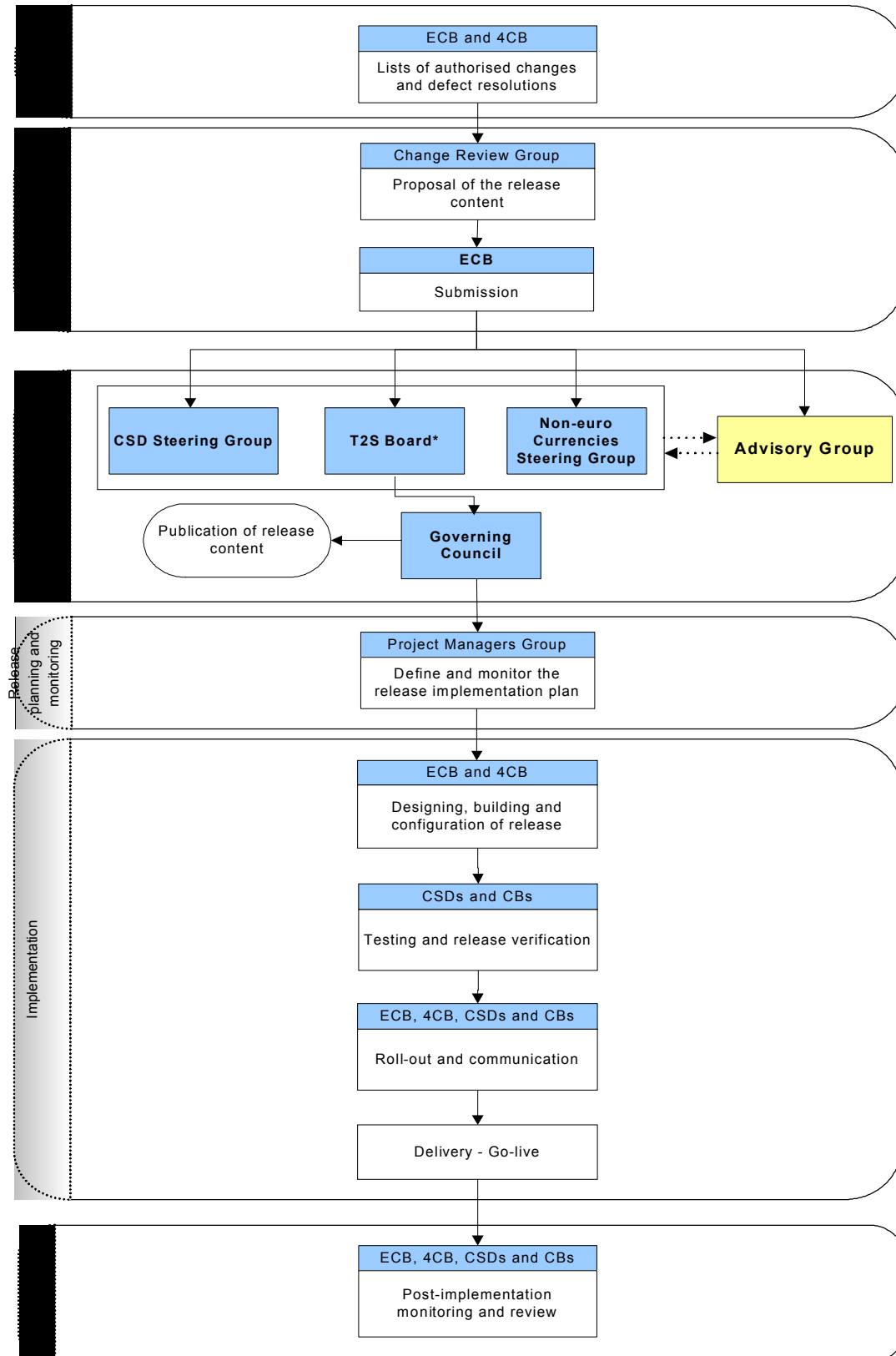
⁶ The date of the yearly major release is still to be defined, however it will be agreed by the governance bodies at the steering level taking into account the interdependencies with the other interconnected Eurosystem systems or with the release of a new version of messaging standards. The minor releases are planned on the basis of their size and urgency.

⁷ The Schedule 2 and 3 will be reviewed and amended after the T2S Go-Live Date release in order to adapt them to the upcoming releases.

Currency Participation Agreement

Schedule 9 – Change and Release Management

Release Management process



Currency Participation Agreement

Schedule 9 – Change and Release Management

Note: * The T2S Board is the Eurosystem Governance body at the Steering Level for matters which have been delegated by the Governing Council. The T2S Board liaises with other Eurosystem internal governance structures for issues of common concern.

5.2.1 Preparation of the list of authorised changes and defect resolutions

In view of defining the content of a release, the ECB and 4CB prepares a list of all authorised changes⁸ and all pending defect resolutions to be implemented prior to the start of the release definition (i.e. “cut-off time”). Separate lists will be prepared according to the different categories of T2S Stakeholders (i.e. Participating CSDs, CBs) and their business requirements.

The lists of authorised changes together with all the relevant information on each individual change and the list of defect resolutions that need to be implemented will be submitted to the CRG by the ECB.

5.2.2 Definition of release

Based on the lists of authorised changes and defect resolutions prepared by the ECB and 4CB, the CRG will examine each Common and Specific Change in detail and will propose a ranking of these changes based on a scoring mechanism (Annex 4 Scoring Mechanism)⁹. Similarly, the CRG will consider all defect resolutions that are pending for implementation, prioritise them and make a proposal on those defect resolutions to be embedded in the next release.

It is under the CRG’s responsibility to develop, implement and carry out the scoring mechanism as a tool for facilitating the definition of the content of a release by balancing criticality and risk, as well as Common and Specific Changes. This priority rating is used to establish the order in which the authorised changes should be considered for a particular T2S release taking into consideration its business/legal importance and the associated risks and budgetary implications. The Common and Specific Changes must be subject to a separate prioritisation process.

The results of the prioritisation exercise carried out by the CRG, as well as the available capacity and resources for implementing the changes will be used to find an appropriate balance for deciding which changes should be included in the next release. The Eurosystem will make best efforts to adapt its capacity to manage the demand for Change Requests as soon as possible. The Eurosystem will provide a justification when a Change Request is not implemented in a release due to lack of adapting its capacity. When conducting the prioritisation exercise and establishing the content of a release, the CRG should consider the following criteria for Common Changes:

⁸ Excluding those changes that are frozen during the exit time of a non-euro area NCB (see chapter 4.2.4)

⁹ Annex 4 (Scoring Mechanism) will be prepared by the CRG as soon as possible after signature of the Framework Agreement respectively the Currency Participation Agreement.

Currency Participation Agreement

Schedule 9 – Change and Release Management

- 511 ▪ to ensure a level playing field for all T2S Stakeholders in order to create the highest
512 possible level of satisfaction throughout all T2S Actors/for each type of stakeholders’
513 point of view;
- 514 ▪ to consider those changes that bring benefits to the wide majority of the Participating
515 CSDs and CBs;
- 516 ▪ to select those changes which in total serve the interest of all Participating CSDs and
517 CBs;
- 518 ▪ to cluster the changes if they are interlinked or relate to the same service or there is a
519 need to implement them together in order to reduce cost or complexity;

520 The CRG should also consider the following criteria for Specific Changes:

- 521 ▪ to assess the changes with the aim of balancing the ratio of Common and Specific
522 Changes;
- 523 ▪ to select those Specific Changes requested by the Participating CSDs/CBs that do not
524 benefit to a large extend from the Common Changes that are part of the same release;
- 525 ▪ to increase the priority of Specific Changes in proportion to the time they are waiting to
526 be implemented.

527 Based on the outcome of the prioritisation exercise for defining the content of the next release,
528 the CRG will prepare its recommendation on the content of the next T2S release containing the
529 Common and Specific Changes, as well as the defect resolutions. The CRG submits its report on
530 the definition of a new release to the CSG via the ECB¹⁰. The ECB disseminates the deliverables
531 of the CRG also to the T2S Board, the AG and the NECSG. In case of agreement in the CRG, the
532 report will contain the common proposal on the content of the next T2S release. In case of
533 disagreement in the CRG, the report will draw the attention of each group to the changes relevant
534 for them, outline the reasons for disagreement and if possible suggest a few variants/options with
535 respect to the release content.

536 Those changes which have not been selected for implementation due to insufficient priority will
537 be parked and will be further considered in the prioritisation exercise for the next T2S release.

¹⁰ The report shall contain a reference to the initiator of the change as well as a reference as to whether the functioning of cash accounts, of Securities Accounts or both are affected.

Currency Participation Agreement

Schedule 9 – Change and Release Management

5.2.3 Release approval

All governance bodies at the Steering Level will review the CRG proposal/report on the content of the release including the related costs and will focus on the changes in their remit and prioritise them. At the end, the Governing Council of the ECB shall prioritise all Change Requests, on the basis of a T2S Board proposal, to which the views obtained from the CSG, the NECSG and the AG are attached. The information on changes selected for the next T2S release will be published on the website.

5.2.4 Release planning and monitoring

Upon approval of the content of the next release, the Project Managers Group (PMG) will prepare a detailed release implementation plan that will ensure synchronisation with the Participating CSDs /CBs planning, in particular if changes are required in their own internal systems. The release planning will ensure that a reasonable freeze period is respected around Christmas and the summer holidays. Once the release implementation plan is finalised and agreed, the PMG will manage and monitor this plan as much as possible – and as far as relevant – in accordance with the provisions of Schedule 2 (T2S Programme Planning and Monitoring) to the FA and the CPA.

Due to the involvement of a large number of parties, a successful implementation and delivery of the release into production requires agreement between the parties on their roles and responsibilities as well as the expectations and commitments during the release implementation.

In accordance with the roles and responsibilities defined in Schedule 2 (T2S Programme Planning and Monitoring) of the FA and CPA, the following key principles will be followed in the context of release planning, monitoring and reporting:

- A common release implementation plan will be defined and maintained based upon clearly identified deliverables and synchronisation points taking into account all the respective constraints and dependencies of the involved parties;
- A regular and close monitoring of the release plan , with decisions committing all parties will be undergone based on a comprehensive framework established to manage events that may affect the release deliverables and milestones;
- Relevant documentation and necessary information will be provided by the Eurosystem to all involved parties as background information for supporting release planning and reporting;
- Regular meetings will be organised between the Eurosystem and the Participating CSDs/

Currency Participation Agreement

Schedule 9 – Change and Release Management

570 CBs to review and discuss the overall status assessment of the T2S release
571 implementation, to discuss progress and any risks and issues that might jeopardize the
572 release, and recommend mitigation measures/corrective actions;

573 ▪ A reporting framework will be established by the Eurosystem to inform regularly all
574 involved parties at the various levels of Governance about the status assessment of the
575 release implementation, including the progress against the plan, to provide status
576 assessment of each deliverable relevant for Participating CSDs and CBs and to ensure
577 that the planning issues and risks are identified, discussed and addressed in a timely and
578 appropriate manner.

579 ▪ A T2S risk and issue management and reporting framework will be established by the
580 Eurosystem to identify, manage and report of risks and issues, affecting the successful
581 delivery of the release;

582 ▪ A comprehensive framework will be established to allow the Eurosystem to monitor the
583 readiness status of all involved parties to deliver the release into production;

584 ▪ The Participating CSDs and CBs will ensure their own readiness and coordinate the
585 readiness of their clients to be ready to use the T2S release, i.e. ensuring planning
586 feasibility and monitoring progress.

587 **5.2.5 Implementation**

588 The implementation phase starts with the designing, building and configuration through the final
589 testing and verification stages and ends with the actual release into the production environment.

590 The full length of a major release cycle will be up to 12 months from the moment when the
591 content has been defined and agreed until the deployment into the production environment (i.e.
592 1 year for the implementation period). The minor release cycle will depend on the size of the
593 release, but typically will not exceed half of the length of the major release one.

594 **5.2.5.1. Design, building and configuration**

595 Once the approved content of the release is communicated to the 4CB, the latter will be
596 responsible for designing, building and configuring the release. This process includes, inter alia,
597 the following activities:

598 ▪ Creating a new version of one or more software modules;

599 ▪ Purchasing equipment or services externally;

Currency Participation Agreement

Schedule 9 – Change and Release Management

- Preparing a hardware modification;
- Updating all relevant documentation or producing new one;
- Providing training to the Participating CSDs and the CBs, if required¹¹.

All relevant documents are updated by the ECB and 4CB and will be provided to the T2S Stakeholders as specified hereafter:

- URD, GFS, UDFS, Service Description and GUI Business Functionality – five months prior to the User Testing at the latest point in time; and
- GS, GTD, User handbooks, SLA, MOP – one month prior to the User Testing at the latest point in time.

The ECB and 4CB will ensure consistency across all documentation, including legal agreements and operational procedures.

5.2.5.2. Testing of a new release by the Participating CSDs and the CBs

The Eurosystem will conduct a Eurosystem Acceptance Testing before the start of User Testing thereby ensuring that the T2S test environments and T2S Platform meet the functional and non-functional requirements (including performance testing - if there is a potential impact on the performance) by the change in order for the users to successfully carry out their User Testing. Once the Eurosystem internal tests are finalised, the Eurosystem confirms the readiness of the T2S testing environments for the T2S User Testing via a release note. The test calendar is communicated to the Participating CSDs and the CBs providing information on the testing activities, the availability of the testing environments and any other relevant information for performing the testing. This test calendar and the test activities will follow as much as possible – and where relevant – the approach defined in Schedule 3 (User Testing).

The Participating CSDs and CBs start testing the new release once all the entry criteria for the User Testing are met. A stability period is envisaged in the pre-production where the system should be tested while running according to the Service Level Agreement. The length of this period will be decided by the CRG on a case-by-case basis. The aim of the User Testing is to ensure that the new T2S release delivers the expected services as described in the User Requirements Document, as well as the functional and non-functional specifications and to

¹¹ The Participating CSDs, respectively the CBs are responsible for the providing training to their users. On Participating CSDs/ CBs' request, the Eurosystem should agree on providing trainings for Participating CSDs' respectively CBs' users for topics selected by Participating CSDs/CBs.

Currency Participation Agreement

Schedule 9 – Change and Release Management

628 guarantee the readiness of the Participating CSDs and CBs and their communities for the
629 migration/operation to/of the new release.

630 The User Testing activities are performed according to the framework agreed between the
631 Participating CSDs/ CBs and the Eurosystem, which may include a set of user certification tests
632 to ensure that T2S Stakeholders are able to use the new or amended functionality correctly. As a
633 matter of fact, the verification of the release is given by the Participating CSDs and CBs once the
634 exit criteria of the verification process have been completed successfully.

635 The security impact of all proposed changes to the T2S Platform should be assessed prior to
636 delivery into production in order to check that they do not compromise the security of the T2S
637 Platform. In this respect it is noteworthy that security should be planned and integrated from the
638 start of development. This ensures that risk factors are adequately considered in a timely manner
639 and prevents unnecessary costly security measures to be implemented only once the new system
640 is operational.

641 The testing and release verification process by the Participating CSDs and CBs will typically take
642 up to 3 months (i.e. for a major release).

643 The following principles will be applied during User Testing phase of a release:

- 644 ▪ The scope of release User Testing covers both functional and non-functional testing;
- 645 ▪ The preparation of non-functional release user test activities is done jointly by the
646 Eurosystem and the Participating CSDs/CBs;
- 647 ▪ The Participating CSDs and CBs shall appoint a CSD respectively CB Test Manager who
648 will be the primary contact point for the Eurosystem for all discussions about user release
649 testing;
- 650 ▪ The Eurosystem shall appoint a T2S Test Manager who will ensure proper co-ordination
651 and exchange of information with the CSD's and CB's Test Manager;
- 652 ▪ The execution of non-functional release user test activities is the primary responsibility
653 of the Eurosystem;
- 654 ▪ The Eurosystem will report to the Participating CSDs/CBs about the results of non-
655 functional release testing;
- 656 ▪ User Testing of a new release aims at ensuring compliance of T2S with the T2S Scope
657 Defining Set of Documents;

Currency Participation Agreement

Schedule 9 – Change and Release Management

- 658 ▪ The Participating CSDs and CBs define their acceptance tests and agree these with the
659 Eurosystem;
- 660 ▪ The Eurosystem defines certification tests and agrees these with the Participating CSDs
661 and CBs;
- 662 ▪ User Testing of a new release is organised in different stages: interoperability testing
663 (both bilateral and multilateral), acceptance testing, community testing and business day
664 testing, based on the concept and the principles laid down in Schedule 3 (User Testing);
- 665 ▪ The Participating CSDs and CBs are responsible for the co-ordination of user test
666 activities of a new release with their communities;
- 667 ▪ The Eurosystem is responsible for the co-ordination of user test activities of a new
668 release between all T2S Actors, including the organisation of a central repository for test
669 sets, test cases and test scenarios related to the certification tests for T2S User Testing;
- 670 ▪ The Eurosystem will support the User Testing activities of a new release through the
671 implementation of incident and problem management procedures as described in the
672 Manual of Operational Procedures;
- 673 ▪ The Participating CSDs and CBs shall inform the Eurosystem of any incident they
674 experience during the execution of their user tests of a new release;
- 675 ▪ In particular, the Eurosystem shall undertake all necessary corrective measures to resolve
676 all defects discovered during the User Testing activities of a new release and caused by
677 T2S;
- 678 ▪ All decisions related to (un)successful completion of the test stages, as well as the
679 implementation of the release in the production environment will be prepared under the
680 responsibility of the Project Managers Group (PMG) and will be made in accordance
681 with the Governance arrangements laid down in Schedule 8 (Governance).

682 **5.2.5.3. Roll- out and communication**

683 The release plan drawn up during the preceding phases will be complemented with information
684 about the exact installation process and the agreed implementation activities and delivery of the
685 release into production.

686 The ECB in collaboration with the 4CB, Participating CSDs and CBs will agree on the rollout
687 planning which includes the following:

Currency Participation Agreement

Schedule 9 – Change and Release Management

- 688 ▪ Producing an exact, detailed timetable of events, as well as who will do what i.e.
689 resource plan;
- 690 ▪ Producing the release note and communication to the Users;
- 691 ▪ Planning communication;
- 692 ▪ Incident management.

693 All the impacted T2S Stakeholders will be informed on what is planned and how it might affect
694 them. The responsibilities of the interested parties in the implementation of the release will be
695 communicated by the ECB ensuring that everyone is aware of them. This will be accomplished
696 via the release communication/notes.

697 **5.2.5.4. Delivery – Go-live**

698 Bringing the application software release into the production environment is the final step in the
699 Release Management process.

700 To ensure a smooth roll-out of the release, the checklist and procedures agreed between the
701 Eurosystem, 4CB, the Participating CSDs and CBs need to be followed by all the involved
702 parties.

703 The Governing Council shall give the formal and final acceptance of the release for the go-live
704 based on the successful completion of the user testing of the new release and after obtaining the
705 views of the CSG, and the NECSG. The release is delivered into the production environment on
706 the agreed date following the agreed procedures.

707 **5.2.6 Post implementation review**

708 A post implementation review will take place periodically in order to evaluate the change/release
709 performance and to verify the effectiveness of the change/release package implementation.

710 These review meetings will provide an opportunity to assess and review the efficiency and
711 effectiveness of the Change and Release Management Process, as well as to identify any potential
712 improvement to the overall process flow.

Currency Participation Agreement

Schedule 9 – Annex 1 – Change Request Form

713 Annex 1: Change Request Form

General Information		
CR raised by:	Institute:	Date raised:
Change Request title:		CR ref. no: <i>(to be filled in by the ECB)</i>
Change Request type <i>(Common, Specific, if specific unauthorised use to be controlled or monitored?)</i> : <i>(to be filled in by the requester)</i>	Urgency <i>(Normal, Fast-track)</i> <i>(to be filled in by the requester)</i>	
1. Legal/business importance parameter (C, H, M, L): <i>(to be filled in by the requester)</i>	2. Market implementation efforts parameter (H, M, L): <i>(to be filled in by the requester)</i>	
3. Operational/Technical risk parameter (H, M, L): <i>(to be filled in by the requester)</i>	4. Financial impact parameter (H, M, L): <i>(to be filled in by the 4CB)</i>	
Requester Category <i>(CSD, CB, ECB, 4CB)</i> <i>(to be filled in by the requester)</i>	Status: <i>(to be filled in by the CRG)</i>	
Description of requested change:		
Reason for change and expected benefits/business motivation:		
Submitted annexes / related documents:		

Currency Participation Agreement

Schedule 9 – Annex 1 – Change Request Form

Proposed wording for the Change Request:

Currency Participation Agreement

Schedule 9 – Annex 2 – Change Request Form

Annex 2: Change Request Form

At any time, a Change Requests will have one of the following statuses:

Registered – The Change Request was registered by the ECB.

Rejected by Change Review Group – When the Change Review Group has agreed with the requester that the change should be dropped.

Under preliminary Assessment – The ECB/4CB is conducting the preliminary assessment.

Pending with Change Review Group – The ECB has submitted the preliminary assessment to the Change Review Group to review it and consult their communities.

Under Detailed Assessment – The ECB/4CB is conducting the detailed assessment of the Change Request.

Being evaluated by the Change Review Group – The ECB has submitted the detailed assessment to the CRG and they are evaluating it.

Pending at Steering Level – The Change Request with the assessment is submitted to the Steering Level for a formal authorisation.

Authorised at Steering Level – The Steering Level has authorised the change and it was placed on the official list of changes.

Rejected at Steering Level – The Steering Level has rejected the change.

Allocated to a release – The change is allocated to a release.

Under implementation – The change is under implementation but not yet delivered to test

Delivered to test – The change is being tested by the CSDs and CBs

Verified – The change was successfully tested and verified by the CSDs and CBs

Parked – Change Request is parked for the next T2S release (s).

Frozen – The implementation of the change is frozen for max. 24 months due to the exit period of a non-euro area NCB

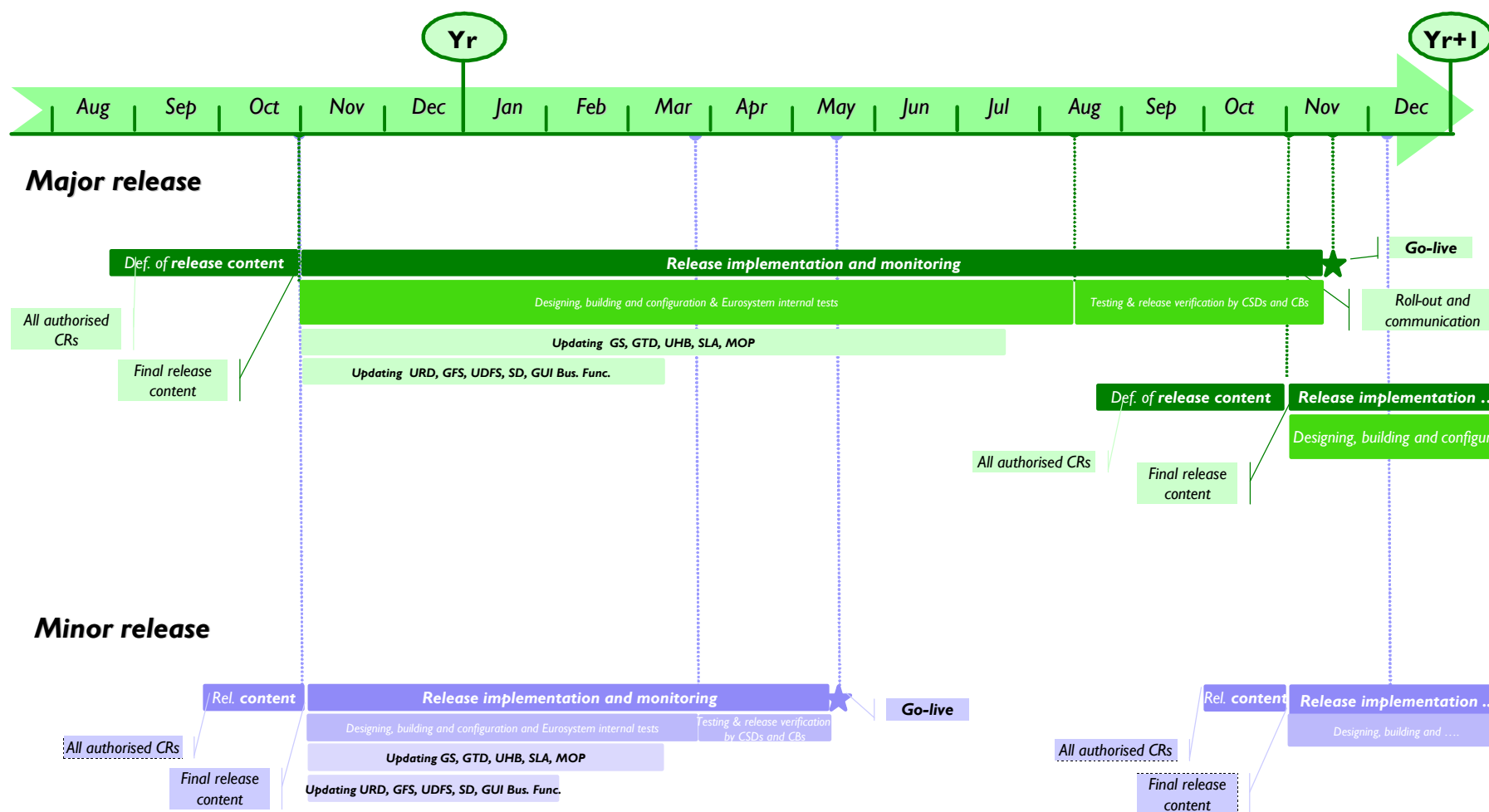
Closed – The Change Request has been implemented in T2S and all relevant documentation has been updated and all other impacted documents have been aligned.

Currency Participation Agreement

Schedule 9 – Annex 3 – Indicative timeline for the T2S Release Management

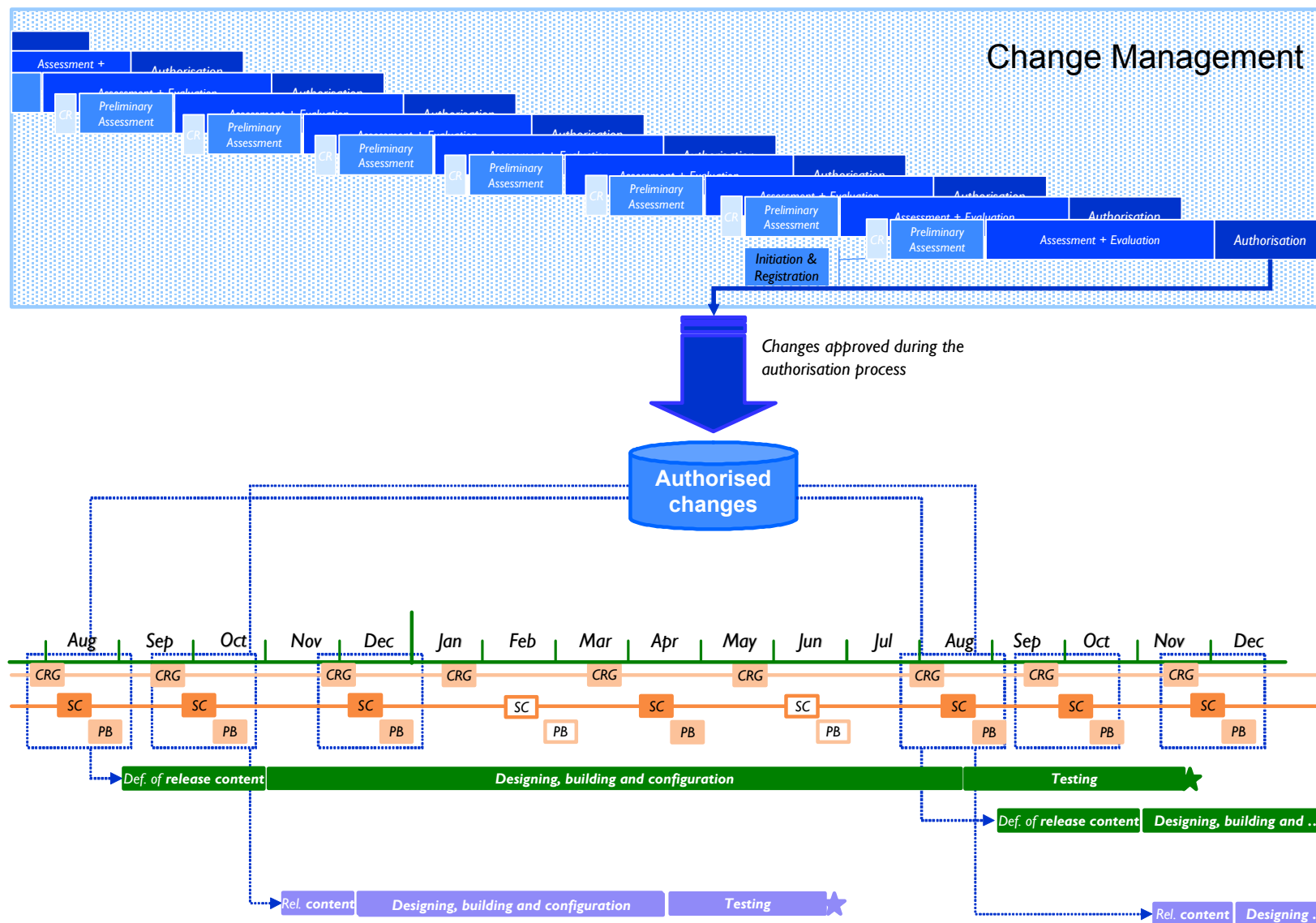
Annex 3: Indicative timeline for the T2S Release Management

Indicative timeline for the T2S Release Management process



Currency Participation Agreement

Schedule 9 – Annex 3 – Indicative timeline for the T2S Release Management



Currency Participation Agreement

Schedule 9 – Annex 4 – Scoring mechanism

Annex 4: Scoring mechanism

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 10

INFORMATION SECURITY

Currency Participation Agreement

Schedule 10 – Information Security

Table of contents

Introduction	1
1 Objective and scope of T2S Information Security	2
1.1 Objective	2
1.2 Scope	2
2 General responsibilities of the Contracting Parties	4
2.1 General responsibilities of the Eurosystem.....	4
2.2 General responsibilities of the [NCB]	5
3 The T2S Information Security management framework.....	6
3.1 The Information Security Policy for T2S.....	6
3.2 The T2S Information Security Requirements and Controls.....	6
3.3 The T2S Information Security risk management process	6
4 The T2S Information Security risk management process	7
4.1 Risk management methodology.....	8
4.1.1 Business impact analysis	8
4.1.2 The T2S Information Security Requirements and Controls	9
4.1.3 The T2S Threat Catalogue	9
4.1.4 The T2S Information Security risk management process	10
4.1.4.1 T2S Information Security management framework review process	11
4.1.4.2 Compliance and risk assessment process.....	12
4.2 Deliverables to the [NCB].....	12
4.2.1 T2S Information Security Risk Evaluation Table	12
4.2.2 T2S Information Security Risk Treatment Plan	13
4.3 Co-operation and escalation procedures	14
4.4 Examples for the Shared Documents	15
4.4.1 T2S Information Security Risk Evaluation Table	15
4.4.2 T2S Information Security Risk Treatment Plan	16

Currency Participation Agreement

Schedule 10 – Information Security

1 Introduction

2 This document aims at presenting the provisions related to the framework to ensure that the
3 requirements concerning Information Security in T2S are met and kept up-to-date. In addition the
4 document defines the involvement of the Connected NCB in the Information Security Management
5 Process, in accordance with the applicable governance arrangements, as well as the Eurosystem's
6 reporting obligations towards the Connected NCB.

7 The management of Information Security for T2S is largely based on the ISO/IEC standards
8 27001:2005 and 27002:2005. This Schedule and the related Annexes therefore use the terms and
9 definitions of these standards, if applicable, and in such case prevail over the terms defined in
10 Schedule 1. A definition of the relevant terms is included in chapter 2 of Annex 2 (T2S Security
11 Requirements and Controls) to this Schedule.

12 The document is divided into four chapters, corresponding to the major aspects identified as relevant
13 for T2S Information Security: i) objective and scope of T2S Information Security; ii) general
14 responsibilities of the Contracting Parties; iii) the T2S Information Security Management
15 Framework, and iv) the T2S Information Security Risk Management Process.

16

Currency Participation Agreement

Schedule 10 – Information Security

1 Objective and scope of T2S Information Security

1.1 Objective

The objective of T2S Information Security is to protect T2S business processes and its information from a wide range of threats, whether internal or external, deliberate or accidental, and to minimise the impact on the continuity of T2S business of any threats, that, despite all measures taken, do materialise.

ISO 27001 defines Information Security as “preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved”¹.

For the avoidance of doubt, it is acknowledged that “*the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events*” (i.e. operational risk as defined in the report entitled “*International Convergence of Capital Measurement and Capital Standards*”, published by the Basel Committee on Banking Supervision, June 2006), is covered by the T2S Information Security Policy, to the extent such risk may have an impact on the confidentiality, integrity and availability of T2S information. Operational risks that are not covered by the T2S Information Security Policy are covered in the SLA reports as specified in Schedule 6 (T2S Service Level Agreement).

1.2 Scope

The scope of the T2S Information Security Schedule covers all arrangements aiming at fulfilling the T2S Information Security Requirements as specified in Annex 2 (T2S Security Requirements and Controls) to this Schedule, as well as to the relevant principles to conduct the initial risk analysis before go-live and all subsequent risk analyses during the production phase. These risk analyses focus on the proper implementation of the agreed security controls. Furthermore, all reporting obligations and the activities to keep the T2S Information Security Management Framework up-to-date are covered by this Schedule as well.

The perimeter of the T2S Information Security Management Framework is limited to the T2S Platform and does not extend to the system(s) in place on the side of the [NCB]. Nevertheless, the

¹ ISO 27001:2005 (chapter 3.4)

Currency Participation Agreement

Schedule 10 – Information Security

44 Eurosystem commits to provide the [NCB] with all information necessary to allow the latter to
45 perform its own risk management obligations. Network Service Providers are also out of scope for
46 the T2S Information Security Management Framework managed by the Eurosystem, but the
47 Eurosystem imposes certain requirements, comparable to those for third party service providers, via
48 the agreements.
49

Currency Participation Agreement

Schedule 10 – Information Security

2 General responsibilities of the Contracting Parties

As an overarching principle, the Eurosystem and the [NCB] shall co-operate in good faith in order to allow both parties to fulfil their commitments with respect to Information Security.

2.1 General responsibilities of the Eurosystem

The Eurosystem shall:

- a) implement the T2S Information Security Management Framework in accordance with this Schedule, in particular by designing, developing and operating the system with the objective that each T2S Actor has access to T2S information according to the confidentiality, integrity and availability requirements described in this Schedule and its Annexes;
- b) implement a process to manage Information Security in T2S according to the process described in section 4 of this Schedule:
 - a. regularly reviewing the implementation;
 - b. regularly updating the T2S Security Requirements to keep them in line with technical developments;
 - c. regularly assess the effectiveness of the process and update it if necessary;
- c) share the Asset Classification Scheme and Likelihood and Impact Grading Scales used in the risk management process for information;
- d) report the results of Information Security reviews to the [NCB] (according to section 4.3 of this Schedule);
- e) report Information Security incidents (according to the definition in Annex 2 [T2S Security Requirements and Controls] to this Schedule) to the Connected NCB;
- f) report to the Connected NCB newly identified threats or detected gaps that might threaten T2S Information Security;

Currency Participation Agreement

Schedule 10 – Information Security

- g) provide all other relevant information to the Connected NCB to allow the latter to fulfil its own risk management obligations.

2.2 General responsibilities of the [NCB]

In view of ensuring Information Security for T2S, the Connected NCB shall:

- a) ensure its own compliance with Information Security requirements according to its internal standards, regulatory requirements and/or best practices;
- b) report Information Security incidents (according to the definition in Annex 2 [T2S Security Requirements and Controls] to this Schedule) to the Eurosystem, if T2S or other T2S Parties might be impacted by such incidents; and
- c) report to the Eurosystem newly identified threats or detected gaps that might threaten T2S Information Security.

Currency Participation Agreement

Schedule 10 – Information Security

3 The T2S Information Security management framework

This chapter describes the documents that specify the Eurosystem's commitments in the Information Security management process.

To ensure Information Security the related requirements and implemented measures need to evolve over time to accommodate for new threats and to adapt to the technical development. All the annexes will therefore regularly be reviewed and if need be updated according to the arrangements defined in the Currency Participation Agreement.

3.1 The Information Security Policy for T2S

The Information Security Policy for T2S – attached as Annex 1 (Information Security Policy for T2S) to this Schedule – is a high-level document embracing, at a generic level, a definition of the scope of Information Security for T2S, the security policy principles, allocation of responsibilities and other relevant aspects related to information security in the T2S environment.

The Information Security Policy for T2S focuses on the Eurosystem's responsibilities only. Any Information Security requirements to be applied to the [NCB] are covered in the Service Level Agreement (SLA).

3.2 The T2S Information Security Requirements and Controls

The purpose of the T2S Security Requirements and Controls – attached as Annex 2 to this Schedule – is to specify which conditions are to be fulfilled (i.e. the requirements) for establishing information security for T2S, as well as to indicate how these conditions can be met (i.e. the controls). The requirements and controls are based directly on ISO standard 27002.

3.3 The T2S Information Security risk management process

The T2S Information Security risk management process – described in chapter 4 of this Schedule – specifies the approach for managing Information Security for T2S and the related reporting of the risk situation and planned risk treatment to the [NCB].

Currency Participation Agreement

Schedule 10 – Information Security

4 The T2S Information Security risk management process

This chapter outlines the approach to ensure the continuous process of managing Information Security in T2S. This approach is established under the umbrella of the Information Security Policy for T2S (Annex 1 to Schedule 10) which embraces at a generic level a definition of the scope of T2S, the information security policy principles, the allocation of responsibilities and summarises the information security management domains.

The main goal of information security in T2S is to protect T2S information from a wide range of threats and to minimise the impact of any threats on T2S operations, which, despite all measures taken, do materialise. In particular, T2S Information Security aims at avoiding any propagation of Information Security incidents, whether caused endogenously in T2S or by a T2S Actor, to other T2S Actors. To accomplish this, the T2S risk management process defines two main processes. One process (i.e. the “review” process) ensures that the T2S Information Security management framework is kept up to date and effective, while the other process (the “core” process) focuses on the implementation of this framework and the assessment of any remaining risks.

A full risk assessment is performed before the initial go-live of T2S (pre-production security assessment). Moreover, the process interfaces with the change management and with the incident management processes to guarantee that the security requirements and controls are in place and that the risk is continuously monitored and maintained at an appropriate level. In addition to these event-driven assessments, a time-driven mechanism ensures a complete security compliance checking and risk assessment every three years also for parts that have not been subject to a change.

This chapter is structured as follows:

- Section 4.1 puts the T2S Information Security risk management process into the perspective of the complete T2S Information Security management framework;
- Section 4.2 places emphasis on the information flow exchanged between the Eurosystem and the [NCB] during the T2S risk assessment process cycle;
- Section 4.3 describes the co-ordination and escalation process for T2S Information Security issues and in particular how the [NCB] will be involved in the T2S Information Security Management Process;
- Section 4.4 provides examples on how the information shared with the [NCB] is going to be structured.

Currency Participation Agreement

Schedule 10 – Information Security

4.1 Risk management methodology

The information security risk management methodology applied by the Eurosystem for T2S is defined as the series of interlinked components, which provide the common methodological foundation for delivering, maintaining and governing the information security and related internal controls for the Eurosystem.

4.1.1 Business impact analysis

Risk management commonly starts with a criticality assessment of the information system as a whole determining the business impact for the Eurosystem in relation to the three security aspects: confidentiality, integrity and availability. Since T2S plays a vital role in the post-trade services chain, and has cross-system relationships to systems at many CSDs as well as RTGS and collateral management systems of the Central Banks, it is a systemically important system. Undoubtedly, the protection needs, in terms of confidentiality, integrity and availability would reach the highest score. However, even for a highly critical system not all components are of the same criticality level. Therefore, the Eurosystem categorises the individual assets using the following inventory classification principles.

The rules being that

- an owner is identified/nominated for each asset;
- the criticality for each asset is identified taking confidentiality, integrity and availability aspects into account;
- all the security requirements and controls (see section 4.1.2) are considered as applicable to T2S;
- deviations from this general rule is under the owner² responsibility according to the asset classification's criticality and the applicability of the control;

² In accordance with ISO 27002, the term 'asset owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has any property rights to the asset, but refers rather to "stewardship" or "custody" of assets, in particular for data.

Currency Participation Agreement

Schedule 10 – Information Security

- deviations must be justified and argued during the compliance checking phase performed by Information Security experts who have no direct or indirect conflict of interest in the performance or outcome of this compliance.

The list of assets and their categorisation are subject to change. If changes are required to T2S due to changes in the list of assets (or their categorisation), then these updates will be performed as part of the Change and Release Management process. On top of that, the asset inventory will be subject to a complete review every three years.

4.1.2 The T2S Information Security Requirements and Controls

The list of controls taken into account for the individual assets is derived from the following different sources:

- ISO/IEC standard 27002:2005 as mentioned in the URD;
- URD chapter 18;
- Experience from Target2.

When compiling this list, all controls from all listed sources were taken into account. Only those controls that are obviously not applicable to T2S have been dropped from these inputs.

By coordinating this effort with the work done for Target2 and CCBM2, the Eurosystem ensures that a common approach for these three core systems is followed to ensure an appropriate high level of information security for all three interconnected systems.

4.1.3 The T2S Threat Catalogue

The T2S Threat Catalogue listing all threats that have been considered for T2S is compiled out of input taken from the Information Security Forum.

The Eurosystem consolidated the input by differentiating between threats and root causes, which in itself are not a threat but can allow several threats to become imminent.

The T2S Threat Catalogue provides information on relevant threats to the system (internal or external/accidental or deliberate) and serves as the basis for the identification of the impact, the appropriate security controls and (later) evaluation of potential residual risks.

Currency Participation Agreement

Schedule 10 – Information Security

The purpose of the T2S Threat Catalogue is twofold; it helps to identify all potential threats to T2S without overlooking any and to ensure that all threats are addressed properly by mapping the security requirements and controls to the threats they address.

4.1.4 The T2S Information Security risk management process

Information Security risk management for T2S is based on two main processes:

- The T2S Information Security management framework review process ensures that the T2S Information Security management framework continues to adequately address the risks, as they change over time by ensuring a timely update and approval of documents. The T2S Information Security management framework review process consists in identifying new and changed threats deriving from system changes and new business requirements, incidents and security developments, as well as Legal and Regulatory Requirements. In addition to this continuous, event driven process, the Eurosystem will review all documents of the T2S Information Security management framework on a yearly basis.
- The compliance and risk assessment process is used to assess the overall T2S Information Security risk situation. This includes the security compliance check to identify deviations from the T2S Information Security Requirements and Controls as well as their assessment and reporting to the CSDs and NCBs. The process applied to the whole T2S scope is triggered every three years, the first before the go-live of T2S (the pre-production security assessment). In between these full verifications, any changes to T2S or any security related incident will trigger a partial verification for the relevant parts.

Currency Participation Agreement

Schedule 10 – Information Security

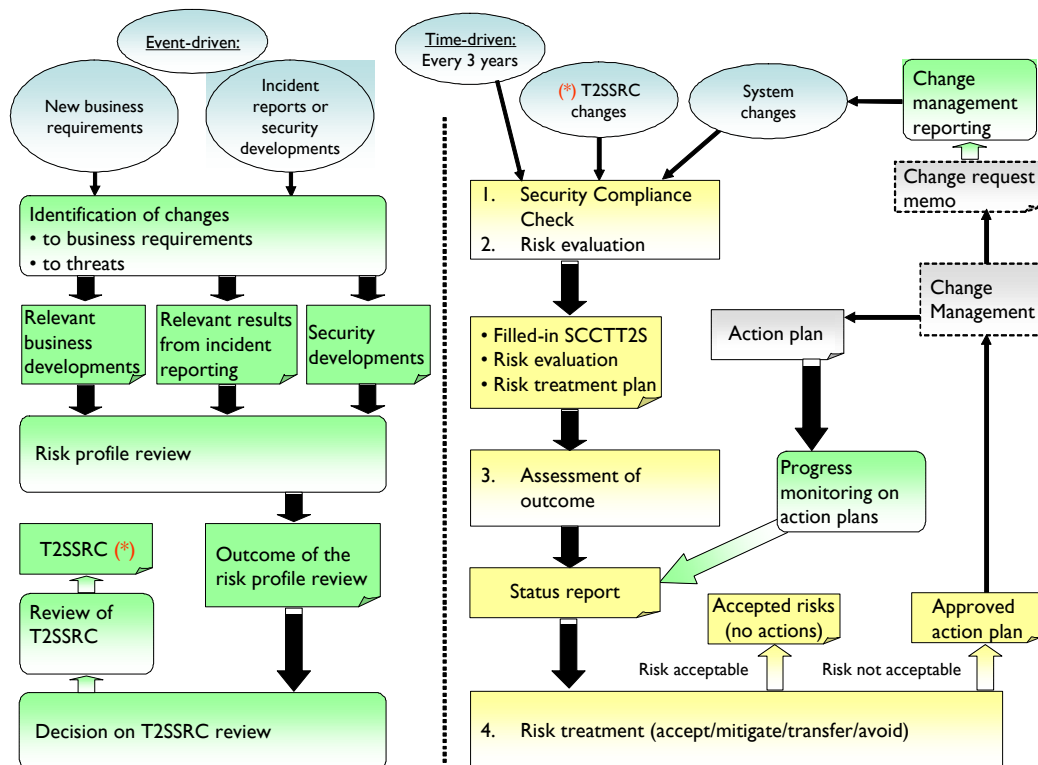


Figure 1: The two risk management processes and their interaction

4.1.4.1 T2S Information Security management framework review process

The T2S Information Security management framework review process ensures that the T2S Information Security management framework continues to adequately address the risks that T2S is exposed, as they change over time. The findings resulting from change requests, incidents and security developments provides the Eurosystem with information on which to base a sound decision on whether the relevant documents, i.e. the Information Security Policy for T2S, the T2S Threat Catalogue and the T2S Security Requirements and Controls, should be updated.

In addition to this continuous, event driven process, the Eurosystem will review all documents of the T2S Information Security management framework on a yearly basis.

If the need for an update is identified, an updated version of the documents is proposed to the relevant governance body (as defined in Schedule 8 [Governance]) for approval.

Currency Participation Agreement

Schedule 10 – Information Security

4.1.4.2 Compliance and risk assessment process

The compliance and risk assessment is a multi-step process to assess the overall risk situation.

In a first step (security compliance check), it takes the defined security requirements and controls and performs a compliance check by validating the completeness and effectiveness of the actual implementation of these controls within the scope of T2S.

In a second step (risk assessment), all threats addressed by non-compliant controls are assessed (based on grading scales) concerning likelihood of the risk materialising and its associated impact.

In a third step, the risk situation of T2S concerning each threat is determined by aggregating the results of the individual assessments for those controls that are relevant for this threat into an overall likelihood and potential impact. The result is represented using a grading scale.

In a fourth step, the Eurosystem will make a proposal for the treatment of all identified risks based on their potential impact on the Eurosystem as provider of the T2S Services. Available options to treat risks are acceptance, avoidance, mitigation or transfer of risks.

In a final step, for all risks that cannot be or are not accepted, actions plans for avoiding, mitigating or transferring the risks will be defined and implemented (T2S Information Security Risk Treatment Plan – see section 4.2.2).

4.2 Deliverables to the [NCB]

The Eurosystem drives the process described in section 4.1. However, the assessment of the risk impacts can only be based on the impact on T2S and/or the Eurosystem. This section therefore focuses on the information the Eurosystem will share with the [NCB] and their options to use this as input to their own business risk assessment processes in order to meet their regulatory requirements and to get evidence that the security requirements are addressed properly by the Eurosystem.

4.2.1 T2S Information Security Risk Evaluation Table

The ‘T2S Information Security Risk Evaluation Table’ (ISRET) is generated as part of the risk assessment. It provides the likelihood for each threat for which not all the relevant controls are implemented and effective, as well as the impact of the threat, taking into account the non-compliant controls. The ISRET includes the following information:

Currency Participation Agreement

Schedule 10 – Information Security

- 249 1. ID: Threat identification number
- 250 2. Threat: Threat description (from the Threat Catalogue)
- 251 3. Current likelihood (based on a likelihood grading scale)
- 252 4. Likelihood explanation: explanation of the likelihood scoring
- 253 5. Current impact (based on an impact grading scale)
- 254 6. Impact explanation: explanation of the impact scoring
- 255 7. Risk Treatment Plan ID: reference to the appropriate treatment plan mitigating the risk, as
256 described in the T2S Information Security Risk Treatment Plan (see section 4.2.2)
- 257 Based on this ISRET, the [NCB] has the necessary information to evaluate its own business risk.
- 258 Section 4.4.1 shows the template and an example of this table.
- 259 The Eurosystem will share with the [NCB] the ISRET whenever it is updated, but at least on a yearly
260 basis.

261 **4.2.2 T2S Information Security Risk Treatment Plan**

- 262 Together with each ISRET, the Eurosystem will share the proposal for the ‘T2S Information Security
263 Risk Treatment Plan’ (IS RTP).
- 264 This plan proposes a treatment (i.e. a mitigation measure or acceptance) for all the risks listed in the
265 ISRET.
- 266 The IS RTP includes the following information:
- 267 1. Risk Treatment Plan ID: Risk Treatment Plan identification
- 268 2. Proposed treatment: information on the planned safeguard measures or proposal to accept
269 the risk together with an explanation why it is recommended to accept the risk
- 270 3. Current likelihood of residual risk: likelihood of the residual risk before the implementation
271 of the plan (as it appears in the ISRET)

Currency Participation Agreement

Schedule 10 – Information Security

- 272 4. Likelihood of residual risk after fix: likelihood of the residual risk after the implementation
273 of the safeguard measures
- 274 5. Current impact of residual risk: impact of the residual risk before the implementation of the
275 plan (as it appears in the ISRET)
- 276 6. Impact of residual risk after fix: impact of the residual risk after the implementation of the
277 safeguard measures
- 278 7. Planned implementation date: a deadline by when these measures will be implemented
- 279 8. Status: Progress of the action plan implementation (not started, in progress, closed)
280 including the date

281 Mitigation measures that imply a functional change to T2S will be processed according to Schedule 9
282 (Change and Release Management Procedure), while mitigation measures that imply a non-
283 functional change will be processed according to Schedule 6 (Service Level Agreement – Annex 1
284 [Management of non-functional changes]). Should the [NCB] see the need for additional mitigation
285 measures, they can as well raise change requests to implement these measures in T2S.

286 Those risks appearing in subsequent ISRTPs that require follow-up are consolidated in a single
287 Action Plan in order to monitor whether the action plans are delivered on time. Progress monitoring
288 on the action plans will be delivered to the [NCB] at least on an annual basis, and whenever there is
289 an update to the plan or a change of status of a risk treatment (e.g. it is successfully implemented).

290 4.3 Co-operation and escalation procedures

291 The Eurosystem shall set up a multilateral co-ordination substructure, in accordance with the T2S
292 governance, for the coordination and monitoring of the T2S Information Security risk management
293 activities. This substructure shall meet on a regular basis and shall consist of a limited number of
294 representatives from the Eurosystem, 4CB, CSDs that have signed the Framework Agreement and
295 Connected NCBs.

296 The role of the substructure in charge of T2S Information Security Risk management shall be to:

- 297 ▪ Coordinate and review T2S Information Security Risk management activities;
- 298 ▪ Monitor the implementation of the ISRTP;

Currency Participation Agreement

Schedule 10 – Information Security

- 299 ▪ Review the ISRET;
- 300 ▪ Discuss issues raised by the members of the substructure, including Information Security
301 issues emerging outside the scope T2S Information Security;
- 302 ▪ Prepare communications related to Information Security risks to the various T2S
303 Stakeholders and the public at large.
- 304 If a new information security risk is identified, or if an existing information security risk obtains a
305 higher likelihood or impact score, the Eurosystem will communicate such changes to the [NCB] in
306 accordance with the incident response times specified in Schedule 6 (T2S Service Level Agreement).
- 307 Upon reception of such communication, or if another information security issue requires urgent
308 attention:
- 309 ▪ The [NCB] may request a conference call with the Eurosystem, at the latest during the next
310 business day, or at its earliest convenience;
- 311 ▪ The issue shall be discussed during the conference call;
- 312 ▪ The Eurosystem shall summarize the outcome of the conference call and distribute it to the
313 members of the substructure in charge of Information Security risk management.
- 314 In case no agreement can be reached in the substructure, each party shall be entitled to escalate the
315 problem to the Project Managers Group (PMG), where the situation shall be discussed and rapidly
316 assessed.
- 317 If a mutually agreeable solution cannot be found in the PMG, then the general T2S escalation process
318 shall apply whereby the issue is escalated to the T2S Steering Level in order to receive guidance to
319 resolve the issue. The escalation process shall be in accordance with the general T2S governance
320 arrangements, as specified in the Schedule 8 (Governance).
- 321 Ultimately there shall be recourse to the dispute resolution process as described in the provisions of
322 the relevant Articles in the core Currency Participation Agreement.

323 **4.4 Examples for the Shared Documents**

324 **4.4.1 T2S Information Security Risk Evaluation Table**

Currency Participation Agreement

Schedule 10 – Information Security

Example of the T2S Information Security Risk Evaluation Table that the Eurosystem will share with the [NCB].

ID	Threat	Risk Likelihood Score	Risk Likelihood Explanation	Risk Impact Score	Risk Impact Explanation	Risk Treatment Plan ID
23	Loss of historical information	3		2		RTP #1
28	External staff dependency	1		3		RTP #2
88	Eavesdropping	2		1		RTP #3
93	Intentional security loopholes	2		2		No additional measure can be applied efficiently

4.4.2 T2S Information Security Risk Treatment Plan

Example for the Risk Treatment Plan the Eurosystem will propose to the [NCB].

Risk Treatment Plan ID	Description of Planned Actions / Proposal to accept the risk	Current Likelihood ³	Likelihood after fix ⁴	Current Impact ⁵	Impact after fix ⁶	Planned Implementation Date	Status
RTP #1	Description of Risk Treatment Plan #1	3	3	2	1	Planned date for RTP#1	Ongoing
RTP #2	Description of Risk Treatment Plan #2	1	1	3	2	Planned date for RTP#2	Not started due to XXX
RTP #3	Description of Risk Treatment Plan #3	2	1	1	1	Planned date for RTP#3	Not started

³ This column provides for each threat, its likelihood for materializing before the action plan implementation

⁴ This column provides the likelihood of materialising for each threat influenced by the action plan (after the action plan implementation)

⁵ This column provides the impact of each threat before the action plan implementation

⁶ This column provides the impact of each threat after the action plan implementation

CURRENCY PARTICIPATION AGREEMENT

ANNEX 1 TO SCHEDULE 10

INFORMATION SECURITY POLICY FOR T2S

Currency Participation Agreement

Schedule 10 – Annex 1 – Information security policy for T2S

Table of contents

1. Information Security management.....	2
2. Purpose of the T2S Information Security Policy	3
3. Objective.....	4
4. Scope of the T2S Information Security Policy	5
5. Management domains of Information Security	7
5.1 Organization of Information Security	7
5.2 Asset management	7
5.3 Human resources security	7
5.4 Physical and environmental security	7
5.5 Communications and operations management.....	8
5.6 Access control	8
5.7 Information systems acquisition, development and maintenance	8
5.8 Information Security incident management	8
5.9 Business continuity management	8
5.10 Compliance	8
6. Responsibilities for Information Security management in T2S	10
6.1 The Eurosystem.....	10
6.1.1 Governing Council of the ECB	10
6.2 External stakeholders.....	10
6.2.1 Central Banks	10
6.2.2 Central Securities Depositories (CSDs).....	11
6.2.3 Third Party service providers	11

INFORMATION SECURITY POLICY FOR T2S

T2S is a service to support Central Securities Depositories (CSDs) by providing core, borderless and neutral settlement of securities transactions. The objective is to achieve harmonised and commoditised Delivery-versus-Payment settlement in Central Bank Money in substantially all securities in Europe.

Through its direct cross-system relationship with RTGS systems and collateral management systems, a T2S security failure might have systemic implications at a global scale. T2S is a critical IT platform supporting systemically important systems and services and should consequently be designed and operated with a high degree of security and operational reliability. Hence information security is a vital and integral part of T2S.

The main objective of information security is to protect T2S information from a wide range of threats and to minimise the impact of any threats on the continuity of T2S operations, which, despite all measures taken, do materialise. In particular, T2S Information Security aims at avoiding any propagation of Information Security incidents, whether caused endogenously in T2S or by a T2S Actor, to other T2S Actors.

Any non-compliance with the security objectives defined in the present policy note may have serious business, financial and/or reputational consequences for the Eurosystem.

Currency Participation Agreement

Schedule 10 – Annex 1 – Information security policy for T2S

1. Information Security management

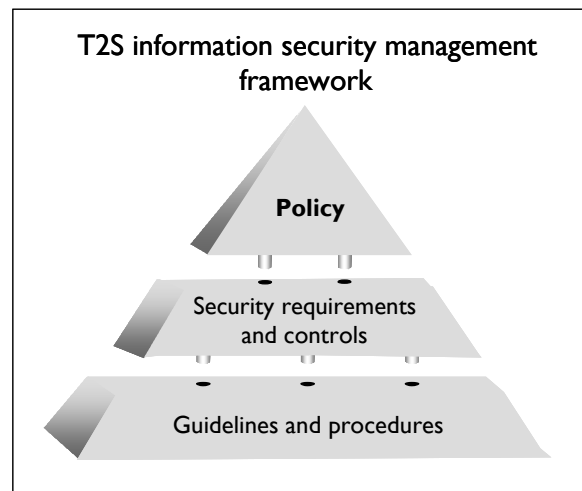
Information Security management shall mean the continuous process of identifying potential threats, verifying whether security controls are comprehensive and effective and minimising or addressing security risks in line with a pre-defined risk tolerance.

Security controls selected to reduce the risk situation must be understandable, effective and appropriate from a cost-benefit perspective. In this respect the task of Information Security management is to find an adequate balance between expenditure on controls and the business harm likely to result from security failures.

Information Security is achieved by implementing suitable security controls. In this context it is important to note that Information Security is not only based on technical solutions. The organisational framework is equally important.

In order to meet these basic principles a comprehensive T2S risk management framework has been developed. This framework has a hierarchical, three-layer structure ranging from a high-level policy to

operational procedures. The first layer comprises an Information Security Policy for T2S (i.e. the present document, in the following referred to as '*the policy*'), which embraces at a generic level the security principles and further relevant aspects related to information security management. In the second layer, the T2S Security Requirements and Controls are specified. In the third layer, the T2S Information Security risk management manual describes in detail the risk management processes.



Currency Participation Agreement

Schedule 10 – Annex 1 – Information security policy for T2S

2. Purpose of the T2S Information Security Policy

The policy¹ represents the first layer of a comprehensive T2S Information Security management framework. It is a high-level document embracing, at a generic level, a definition of the scope of T2S, the security policy principles, allocation of responsibilities and other relevant aspects related to Information Security in the T2S environment.

By approving the policy, the Eurosystem, in its role as owner of T2S, sets a clear direction and demonstrates its support for and commitment to Information Security. Moreover, the importance and value of T2S and its processing resources, both human and technical, are being acknowledged.

¹ The policy for T2S takes into account the “Recommendations for securities settlement systems” (Recommendation XI) published by the Committee on Payment and Settlement Systems and the Technical Committee of the International Organization of Securities Commissions in November 2001, the ISO/IEC standard 27002:2005 and the ESCB information systems security policy .

Currency Participation Agreement

Schedule 10 – Annex 1 – Information security policy for T2S

3. Objective

The main objective of Information Security is to protect T2S business processes and its information from a wide range of threats, whether internal or external, deliberate or accidental, and to minimise the impact on the continuity of T2S business of any threats that, despite all measures taken, do materialise.

ISO 27001 defines Information Security as “preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved”.

The terms “confidentiality”, “integrity” and “availability” are then further specified as follows:²

- **Confidentiality:** the property that the asset information is not made available or disclosed to unauthorized individuals, entities, or processes;
- **Integrity:** the property of safeguarding the accuracy and completeness of information assets;
- **Availability:** the property of the asset information being accessible and usable upon demand by an authorized individual, entity, or process.

Any non-compliance with these objectives might prevent the Eurosystem from meeting its statutory business goals and/or have serious financial and/or reputational consequences. Through its direct cross-system relationship with RTGS systems and collateral management systems, a T2S security failure might, in the worst case, even have systemic risk implications at a global scale.

In order to meet the key objectives an effective Information Security management framework shall be in place.

² Definitions based on ISO/IEC standard 27001:2005.

Currency Participation Agreement

Schedule 10 – Annex 1 – Information security policy for T2S

4. Scope of the T2S Information Security Policy

The scope of this policy comprises all assets (including human resources) needed to develop, implement, maintain and operate T2S. T2S can in principle be subdivided into the following three main layers:

1. The *infrastructure* layer, consisting of all hardware components (including interfaces), required for the development, implementation, maintenance and operation of T2S, even if these components are used, in whole or in part, for the provision of IT services outside the T2S context.³
2. The *application* layer consisting of all software components necessary to develop, implement, maintain and operate T2S. The software component essentially consists of “the” T2S application, which is subdivided into six functional domains: Interface, Static Data Management, Settlement, Life Cycle Management and Matching, Liquidity Management and, SQRA⁴.
3. The *data* layer consisting of all configuration data, as well as static and transactional data necessary to run T2S.
4. The *operational* layer, consisting of all procedures to be applied by and between all relevant stakeholders in order to run and complete the T2S business day in a sound and safe manner.

The smooth operation of T2S as a whole relies to some extent on secure and resilient services provided by entities which are outside the T2S boundaries. These are:

- Central Securities Depositories (CSDs).
- Central Banks allowing their currency to be settled in T2S (through the connection with their RTGS and, where relevant, collateral management systems);
- Third Party service providers (such as Network Service Providers), although the agreements between the Eurosystem and Third Party service providers are subject to the

³ It is important to note that, in accordance with the ECB Governing Council’s decision of 8 March 2007, “*the T2S service will be developed internally within the Eurosystem and operated on the TARGET2 platform in order to exploit synergies with TARGET2 to the fullest extent*”. Because of this so-called “T2S on TARGET2” concept T2S infrastructure assets will exploit full benefits from the information security features already in place for TARGET2.

⁴ Statistics, Queries, Reports and legal Archiving

Currency Participation Agreement

Schedule 10 – Annex 1 – Information security policy for T2S

84 requirements specified in section 5.2.3 of Annex 2 to Schedule 10 (Information
85 Security);

86 The ultimate responsibility to apply this policy to all T2S assets rests with the Eurosystem (as
87 defined in chapter 6.1). For the assets under the control of external stakeholders (as defined in
88 chapter 6.2) specific arrangements apply, which are established, implemented and maintained
89 under their full responsibility (without prejudice to any minimum requirements agreed between
90 these external stakeholders and the Eurosystem).

91

Currency Participation Agreement

Schedule 10 – Annex 1 – Information security policy for T2S

5. Management domains of Information Security

In the following sections the management domains of Information Security are presented. These represent at a high level the security requirements that shall be implemented in T2S in order to preserve confidentiality, integrity and availability.⁵ The specific control objectives and the security controls that shall be implemented to meet these objectives are specified in the “T2S Security Requirements and Controls” document (Annex 2 of Schedule 10).

5.1 Organization of Information Security

In order to ensure that Information Security is adequately managed an organisational framework shall be established to address Information Security related issues in a comprehensive and effective manner.

5.2 Asset management

All T2S information assets shall be identified, classified and prioritised in order to indicate the required level of protection. The responsibilities for maintaining these assets shall be clearly assigned to ensure that information assets receive an appropriate level of protection.

5.3 Human resources security

Personnel (including external party staff) shall be informed about their Information Security responsibilities, made aware about security rules and procedures and their obligation to adhere to them.

5.4 Physical and environmental security

Critical and sensitive information processing facilities shall be housed in secure areas physically protected to prevent unauthorised access to business premises, damage or compromise of information assets, interruption to business activities and theft.

⁵ They are aligned with the high-level security requirements defined in the T2S user requirements (Chapter 18) approved by the Governing Council in July 2008.

Currency Participation Agreement

Schedule 10 – Annex 1 – Information security policy for T2S

5.5 Communications and operations management

Responsibilities shall be clearly allocated and procedures for the management and operation of T2S information processing facilities established in order to ensure the correct and secure operation.

5.6 Access control

Information shall be protected against unauthorised access. Access to information, information processing facilities and business processes shall be granted and controlled on the basis of business and security requirements according to the “business-need-to-know” principle.

5.7 Information systems acquisition, development and maintenance

Security requirements shall be identified and agreed prior to the development of or changes to T2S. Adequate security controls shall be in place to prevent loss, modification or misuse of information in applications systems.

5.8 Information Security incident management

Effective Information Security incident management procedures shall be in place to ensure that security events and weaknesses associated with T2S are communicated in a manner allowing timely corrective actions to be taken.

5.9 Business continuity management

A business continuity management programme shall be implemented to ensure that necessary steps are taken to identify the potential impact of security failures on the business, maintain viable recovery strategies and plans, and ensure continuity of services through training, exercising, maintenance and review.

5.10 Compliance

All relevant statutory, regulatory and contractual requirements applicable to the T2S shall be identified, documented and compliance with these arrangements shall be checked in order to avoid a breach of any criminal or civil law.

Currency Participation Agreement

Schedule 10 – Annex 1 – Information security policy for T2S

- 139 CSDs outsource a critical part of their business operations to T2S. Hence it shall be ensured that
140 T2S is operated in compliance with the jurisdiction of the countries where the CSDs are located.
- 141 Tools and measures to ensure auditability shall be implemented.
- 142

Currency Participation Agreement

Schedule 10 – Annex 1 – Information security policy for T2S

6. Responsibilities for Information Security management in T2S

Information Security management is a key element of any sound governance structure. ,

The common governance structure of T2S comprises a number of different stakeholders whose roles and responsibilities with respect to information security are outlined in the following. In this regard, these stakeholders are either the Eurosystem or external entities (namely, the non-euro NCBs, the Central Securities Depositories, and Third Party service providers).

6.1 The Eurosystem

6.1.1 Governing Council of the ECB

The TS2 Platform is fully owned and operated by the Eurosystem [see T2S user requirements - Principle 1]. The Eurosystem is responsible for safeguarding the public function of T2S and has consequently the ultimate responsibility for deciding on the general security policy and framework for T2S Information Security management (in accordance with the User Requirements), and the definition of the risk tolerance.

In accordance with ISO 27002, the term ‘asset owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets.⁶ Consequently, and without prejudice to the provisions of section 4.3 of Schedule 10 (Information Security), the Eurosystem is also responsible for defining and implementing an effective organisational framework to address Information Security issues, and for the acceptance of remaining risks. Furthermore it is responsible for verifying that all requirements specified in the Information Security policy for T2S are fulfilled in T2S.

6.2 External stakeholders

6.2.1 Central Banks

Central Banks operating national infrastructure used as interface to the T2S and providers of cash accounts are directly responsible for ensuring that Information Security is properly addressed,

⁶ The term ‘owner’ does not mean that the person actually has any property rights to the asset, but refers rather to “stewardship” or “custody” of assets, in particular for data.

Currency Participation Agreement

Schedule 10 – Annex 1 – Information security policy for T2S

security controls are effective, and their personnel adhere to their internal security rules and procedures.

6.2.2 Central Securities Depositories (CSDs)

From an Information Security perspective the roles and responsibilities of CSDs are twofold.

First, an operational failure at a CSD could have a significant adverse effect on the smooth functioning of T2S. Consequently it shall be the responsibility of the CSD to ensure that their internal systems (incl. interfaces) are operated with a high degree of security and operational reliability. The relevant provisions must be addressed in the corresponding Service Level Agreement (SLA).

Second, CSDs are subject to a regulatory framework. In this respect CSDs shall seek assurance that T2S is providing settlement services in a secure and robust manner in compliance with applicable regulatory arrangements. To the extent that an evolution in regulatory arrangements has an impact on the T2S Platform, on the T2S Scope Defining Set of Documents, or on the T2S Specifications, these should be managed through the Change Management procedure laid down in Schedule 9.

6.2.3 Third Party service providers

Bound by contract Third Party service providers shall implement appropriate measures designed to protect against risks that could potentially result in substantial harm in terms of confidentiality, integrity and availability to any T2S services. The relevant provisions must be addressed in the contract.

CURRENCY PARTICIPATION AGREEMENT

ANNEX 2 TO SCHEDULE 10

SECURITY REQUIREMENTS AND CONTROLS

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Table of contents

1. Introduction	1
2. Terms and definitions	2
2.1 Terms	2
2.2 Definitions	6
3. Structure of the security requirements and controls	9
4. Security policy	11
4.1 Information security policy	11
4.1.1 Information security policy document	11
4.1.2 Review of the information security policy	12
5. Organising information security	13
5.1 Internal organisation	13
5.1.1 Management commitment to information security	13
5.1.2 Information security co-ordination	13
5.1.3 Allocation of information security responsibilities	14
5.1.4 Confidentiality agreements	15
5.1.5 Contact with authorities	15
5.1.6 Contact with special interest groups	16
5.1.7 Independent review of information security	16
5.1.8 Authorisation process for information processing facilities	17
5.2 External parties	17
5.2.1 Identification of risks related to external parties	17
5.2.2 Addressing security when dealing with the customer	19
5.2.3 Addressing security in third party agreements	19
6. Asset management	22
6.1 Responsibility for assets	22
6.1.1 Inventory of assets	22
6.1.2 Ownership of assets	23
6.1.3 Acceptable use of assets	23
6.2 Information classification	23
6.2.1 Classification guidelines	24

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

6.2.2	Information labelling and handling.....	24
7.	Human resources security	25
7.1	Prior to employment	25
7.1.1	Roles and responsibilities.....	25
7.1.2	Screening.....	25
7.1.3	Terms and conditions of employment.....	26
7.2	During employment.....	27
7.2.1	Management responsibilities	27
7.2.2	Information security awareness, education, and training	28
7.2.3	Disciplinary process.....	28
7.3	Termination or change of employment.....	28
7.3.1	Termination responsibilities	28
7.3.2	Return of assets.....	29
7.3.3	Removal of access rights.....	29
8.	Physical and environmental security.....	30
8.1	Secure areas.....	30
8.1.1	Physical security perimeter	30
8.1.2	Physical entry controls	31
8.1.3	Securing offices, rooms, and facilities	31
8.1.4	Protecting against external and environmental threats.....	32
8.1.5	Working in secure areas.....	32
8.1.6	Public access, delivery, and loading areas	33
8.2	Equipment security	33
8.2.1	Equipment siting and protection.....	33
8.2.2	Supporting utilities.....	34
8.2.3	Cabling security.....	35
8.2.4	Equipment maintenance.....	35
8.2.5	Security of equipment off-premises	36
8.2.6	Secure disposal or re-use of equipment	36
8.2.7	Removal of property	37
9.	Communications and operations management.....	38
9.1	Operational procedures and responsibilities.....	38
9.1.1	Documented operating procedures	38
9.1.2	Change management.....	39
9.1.3	Segregation of duties.....	39
9.1.4	Separation of development, test, and operational facilities	39

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

9.2	Third party service delivery management.....	40
9.2.1	Service delivery	40
9.2.2	Monitoring and review of third party services	40
9.2.3	Managing changes to third party services	41
9.3	System planning and acceptance	41
9.3.1	Capacity management	42
9.3.2	System acceptance	42
9.4	Protection against malicious and mobile code	43
9.4.1	Controls against malicious code	43
9.4.2	Controls against mobile code	44
9.5	Back-up	45
9.5.1	Information backup	45
9.6	Network security management	46
9.6.1	Network controls	46
9.6.2	Security of network services	46
9.7	Media handling.....	47
9.7.1	Management of removable media.....	47
9.7.2	Disposal of media	48
9.7.3	Information handling procedures	48
9.7.4	Security of system documentation	49
9.8	Exchange of information and software	49
9.8.1	Information exchange policies and procedures	49
9.8.2	Exchange agreements.....	51
9.8.3	Physical media in transit	51
9.8.4	Electronic messaging	52
9.8.5	Business Information Systems	52
9.9	Electronic commerce services	53
9.9.1	Publicly available information.....	53
9.10	Monitoring	54
9.10.1	Audit logging.....	54
9.10.2	Monitoring system use.....	55
9.10.3	Protection of log information	56
9.10.4	Administrator and operator logs	56
9.10.5	Fault logging	56
9.10.6	Clock synchronisation.....	57
10.	Access control.....	58
10.1	Business requirement for access control	58
10.1.1	Access control policy.....	58

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

10.2	User access management	59
10.2.1	User registration	59
10.2.2	Privilege management.....	60
10.2.3	User password management.....	60
10.2.4	Review of user access rights.....	61
10.3	User responsibilities.....	61
10.3.1	Password use	61
10.3.2	Unattended user equipment	62
10.3.3	Clear desk and clear screen policy.....	62
10.4	Network access control	63
10.4.1	Policy on use of network services.....	63
10.4.2	User authentication for external connections	64
10.4.3	Equipment identification in networks	65
10.4.4	Remote diagnostic and configuration port protection.....	65
10.4.5	Segregation in networks	65
10.4.6	Network connection control	65
10.4.7	Network routing control.....	66
10.5	Operating system access control	66
10.5.1	Secure log-on procedures	66
10.5.2	User identification and authentication	67
10.5.3	Password management system	67
10.5.4	Use of system utilities	68
10.5.5	Session time-out	68
10.5.6	Limitation of connection time	69
10.6	Application and information access control.....	69
10.6.1	Information access restriction.....	69
10.6.2	Sensitive system isolation	70
10.7	Mobile computing and teleworking.....	70
10.7.1	Mobile computing and communications	70
10.7.2	Teleworking	71
11.	Information systems acquisition, development and maintenance.....	73
11.1	Security requirements of information systems	73
11.1.1	Security requirements analysis and specification	73
11.2	Correct processing in applications.....	73
11.2.1	Input data validation	74
11.2.2	Control of internal processing	74
11.2.3	Message integrity.....	75
11.2.4	Output data validation.....	75

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

11.3	Cryptographic controls	76
11.3.1	Policy on the use of cryptographic controls	76
11.3.2	Key management	77
11.4	Security of system files	78
11.4.1	Control of operational software	78
11.4.2	Protection of system test data	79
11.4.3	Access control to program source code	79
11.5	Security in development and support processes	80
11.5.1	Change control procedures	80
11.5.2	Technical review of applications after operating system changes	81
11.5.3	Restrictions on changes to software packages	82
11.5.4	Outsourced software development	82
11.5.5	Information leakage	83
11.6	Technical Vulnerability Management	83
11.6.1	Control of technical vulnerabilities	83
12.	Information security incident management	85
12.1	Reporting information security events and weaknesses	85
12.1.1	Reporting information security events	85
12.1.2	Reporting security weaknesses	86
12.2	Management of information security incidents and improvements	86
12.2.1	Responsibilities and procedures	86
12.2.2	Learning from information security incidents	87
12.2.3	Collection of evidence	87
13.	Business continuity management	89
13.1	Information security aspects of business continuity management	89
13.1.1	Including information security in the business continuity management process	89
13.1.2	Business continuity and risk assessment	90
13.1.3	Developing and implementing continuity plans including information security	91
13.1.4	Business continuity planning framework	92
13.1.5	Testing, maintaining and re-assessing business continuity plans	93
14.	Compliance	95
14.1	Compliance with legal requirements	95
14.1.1	Identification of applicable legislation	95
14.1.2	Intellectual property rights (IPR)	95
14.1.3	Protection of records	96
14.1.4	Data protection and privacy of personal information	97

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

14.1.5 Prevention of misuse of information processing facilities	97
14.1.6 Regulation of cryptographic controls.....	97
14.2 Compliance with security policies and technical compliance.....	97
14.2.1 Compliance with security policies and security requirements.....	98
14.2.2 Technical compliance checking.....	98
14.3 Information systems audit considerations	99
14.3.1 Information systems audit controls	99
14.3.2 Protection of information systems audit tools	99

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

1. Introduction

The purpose of the T2S security requirements and controls (T2SSRC) is to specify the security requirements for TARGET2 Securities (T2S) as laid down in the information security policy for T2S.

The T2SSRC are derived from the Information security policy for T2S and represent the *second layer* of the comprehensive T2S risk management framework depicted in the following exhibit.

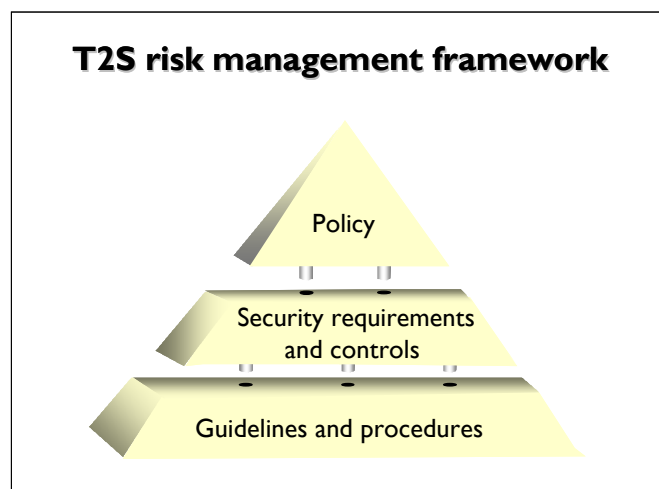


Exhibit 1: T2S risk management framework

As a general rule, the implementation of the security controls specified in this document is mandatory¹. However, it might be that due to specific technical and/or environmental circumstances (e. g. contradicting national legislation) the application of a particular security control is not feasible. If this was the case, it will have to be justified in the context of the security assessment, more specifically when the compliance of T2S with the T2SSRC is checked, why it is not possible to implement this particular security control. The associated residual risk must then be accepted.

In addition to the requirements specified in the present document, good information systems security measures and routines corresponding to best practice (such as ISF, NIST, SANS, the German BSI) should be applied.

All security requirements and controls included in this document are specified from a business perspective and have to be implemented by the service provider (4CB) responsible for designing, building and operating T2S.

¹ In the following document the words 'must' and 'should' are used for better readability but have the same meaning in the sense as being mandatory.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

2. Terms and definitions

2.1 Terms

For the purpose of this document, the terms listed in the following table have the meaning as specified in that table. If this document is part of a set of documents, the same terms have the meaning as specified in such other documents. Conversely, the definition of these terms in such other documents does – for the purpose of this document – not affect their meaning as specified in the following table.

Term	Definition
Asset	Anything that has a value to the organisation, like for instance information (e.g. databases, data files), software (e.g. system software, application software), physical assets (e.g. processors, tapes, power supply), services (e.g. computing services, heating, air-conditioning) and people (e.g. users, consultants).
Business transaction	All types settlement instructions, settlement restrictions and maintenance instructions as well as liquidity transfers processed by T2S.
Customer	Customer is defined as any entity that has a business relationship with the Eurosystem under the Framework Agreement or under the Currency Participation Agreement.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Term	Definition
Disaster [Major operational disruption]	A high-impact disruption of normal business operations affecting a large metropolitan or geographic area and the adjacent communities that are economically integrated with it. In addition to impeding the normal operation of financial industry participants and other commercial organisations, major operational disruptions typically affect the physical infrastructure. Disasters (Major operational disruptions) can result from a wide range of events, such as earthquakes, hurricanes and other weather-related events, biological incidents (e.g. epidemics), terrorist attacks, and other intentional or accidental acts that cause widespread damage to the physical infrastructure. The most significant in terms of their impact are referred to as extreme events, which typically cause the destruction of, or severe damage to, physical infrastructure and facilities, the loss or inaccessibility of personnel, and restricted access to the affected area. [Taken from the BIS “High level principles for business continuity” published in August 2006]
External Party	Any entity different from the Eurosystem (including the Central Banks it is composed of) and its Contractual Parties under the Framework Agreement or the Currency Participation Agreement
Impact	The result of an unwanted incident.
Impact analysis	The process of identifying the threats to the assets and the impact such threats could have, if the threat resulted in a genuine incident. Such analysis should quantify the value of the assets being protected to decide on the appropriate level of safeguards.
Information	The meaning that is currently assigned to data by means of the conventions applied to those data.
Information processing facilities	Any information processing system, service or infrastructure, or the physical locations housing them [ISO/IEC 27002:2005].
Information security	Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved [ISO/IEC 27002:2005].

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Term	Definition
Information security event	An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant [ISO/IEC TR 18044:2004].
Information security incident	An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [ISO/IEC TR 18044:2004].
Inherent risk	The risk before risk treatment.
Policy	Overall intention and direction as formally expressed by management.
Recovery	Recovery (or recover) refers to the restoration of the processing service and settlement activities after a disruption including the processing of pending payment transactions.
Residual risk	The risk remaining after risk treatment.
Risk	Combination of the probability of an event and its consequence [ISO Guide 73:2002]. In other words, the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of or damage to the assets.
Risk analysis	Systematic use of information to identify sources and to estimate the risk [ISO Guide 73:2002].
Risk assessment	The overall process of risk analysis and risk evaluation [ISO Guide 73:2002].
Risk evaluation	The process of comparing the estimated risk against given risk criteria to determine the significance of the risk [ISO Guide 73:2002].
Risk management	Coordinated activities to direct and control an organization with regard to risk. [ISO Guide 73:2002]. Risk management is the ongoing process of risk assessment (evaluation of the impact or system criticality, and the likelihood of loss/damage occurring) leading to the definition of security requirements and the additional mitigation (by safeguards) and/or acceptance of remaining risks .
Risk treatment	The process of selection and implementation of measures to modify risk [ISO Guide 73:2002].

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Term	Definition
Risk Profile	Having a different risk profile shall mean that the <i>alternate site</i> must be sufficiently remote from, and does not depend on the same <i>physical infrastructure</i> components as the primary business location. This minimises the risk that both could be affected by the same event. For example, the <i>alternate site</i> should be on a different power grid and central telecommunication circuit from the primary business location. [Derived from the BIS “High level principles for business continuity” published in August 2006]
Security assessment	A documented process reflecting the risk management procedure and presenting prevailing status of risks in relation to the security requirements, i.e. remaining risks for the security aspects such as: availability, integrity, confidentiality, authentication, authorisation, auditability and non-repudiation.
Security control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature NOTE: Security control is also used as a synonym for control, safeguard (measure), or countermeasure.
Security requirements	The types and levels of protection necessary to meet the security of the assets. The security requirements result from the security risks and are addressed by implementing suitable security controls.
Security risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of or damage to the assets.
Senior management	This is the highest decision making body of the service providing organisation (4CB).
Service	The term “Service” refers to all the T2S services as defined in the T2S Service Description document.
Service providing organisation	This term refers to all parts of the service provider’s (4CB) organisation that are involved in the T2S activities (design, build, test, operate, maintain, support T2S).
Service perimeter	This encompasses all infrastructural and technical components, business/organisational procedures and rules, human resources that are used to provide the T2S service.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Term	Definition
Third party	A company or individual recognized as being independent of the Contractual Parties, and that provides services generally covered by a Service Level Agreement.
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization [ISO/IEC 13335-1:2004]
User	A user is an individual that can log into the service with a login name and requests or uses the services provided. As this document only applies to internal stakeholders (see T2S Information Security Policy), this term only refers to those users designing, building, testing (internal), operating (business and technical), maintaining and supporting (business and technical) T2S.
Vulnerability	A weakness of an asset or group of assets that can be exploited by a threat [ISO/IEC 13335-1:2004]

29 2.2 Definitions

30 Specific values defined for T2S are listed in the following table:

Value Name	Description	Value	Referencing Control
Policy Review Interval	The planned interval for reviewing the Information Security Policy.	Three years	4.1.2
Confidentiality Agreement Review Interval	The planned interval for reviewing confidentiality agreements.	Three years	5.1.4
Independent Security Review Interval	The planned interval for an independent review of the approach to managing information security and its implementation.	Three years	5.1.7
Physical Entry Controls Review Interval	The planned interval for reviewing physical entry controls.	Three months	8.1.2

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Support Utilities Review Interval	The planned interval for reviewing support utilities.	Six months	8.2.2
Restoration Check Interval	The planned interval for checking the system restoration from backup.	One year	9.5.1
Distribution List Review Interval	The planned interval for the review of distribution list recipients.	Six months	9.7.3
Audit Logging Period	The period for keeping technical audit logs of the service.	Two years	9.10.1
Privileged Activities Review Interval	The planned interval for reviewing privileged activities on the service.	One business day	9.10.2
Administrator Log Review Interval	The planned interval for reviewing system administrator and operator logs.	One week	9.10.4
User Access Control Policy Review Interval	The planned interval for reviewing the User Access Control Policy.	Three years	10.1.1
User Access Rights Review Interval	The planned interval for reviewing the user access rights.	Six months	10.2.4
Privileged User Access Rights Review Interval	The planned interval for reviewing the privileged user access rights.	Three months	10.2.4
Privileged Account Changes Logging Period	The period for keeping audit logs of changes to privileged accounts.	One year	10.2.4
Minimum Password Length	The minimum length for user passwords.	Eight characters	10.3.1
Password Expiry Period	The expiry period for passwords after which a change is required.	Sixty days	10.3.1
Maximum Logon Attempts	The maximum number of failed logon attempts for a user before the account is disabled.	Three attempts	10.3.1

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Remote Connections Idle Interval	The idle time after which a re-authentication of a remotely connected user is required.	10 minutes	10.4.2
Period for Keeping Previous Passwords	The period to keep previously used passwords to prevent reuse.	One year	10.5.3
Session Time-out	The period of inactivity before a user session is closed.	15 minutes	10.5.5
Information Access Restriction Review Interval	The planned interval for the review of the service's output to remove redundant information.	Three years	10.6.1
Business Continuity Test Interval	The planned interval for testing business continuity.	Six months	13.1.5
Business Continuity Review Interval	The planned interval for reviewing the business continuity plan.	Six months	13.1.5
Compliance Review Interval	The planned interval for a full compliance review of the service with security policies and requirements.	Three years	14.2.1
Technical Compliance Check Interval	The planned interval for checking the technical compliance of the platform.	One year	14.2.2

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

3. Structure of the security requirements and controls

The document consists of 11 *Information Security Management Domains* which mainly serve the purpose of structuring the broad field of information security. On a second layer the *Security Requirements* specifying the objectives that should be achieved are defined. Finally on a third layer the (benchmark) *Security Controls* are specified.

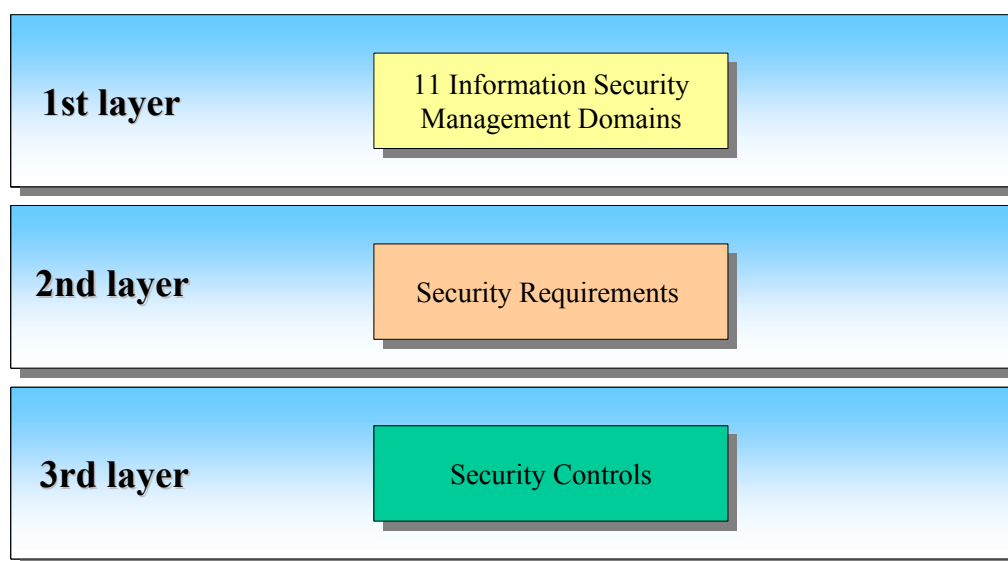


Exhibit 2: Structure of the security requirements and controls

The eleven information security management domains are listed in the following (the number in brackets indicates the number of main security requirements included within each clause):

- a) Security Policy (1) – see chapter 4;
- b) Organising Information Security (2) – see chapter 5;
- c) Asset Management (2) – see chapter 6;
- d) Human Resources Security (3) – see chapter 7;
- e) Physical and Environmental Security (2) – see chapter 8;
- f) Communications and Operations Management (10) – see chapter 9;
- g) Access Control (7) – see chapter 10;
- h) Information Systems Acquisition, Development and Maintenance (6) – see chapter 11;
- i) Information Security Incident Management (2) – see chapter 12;
- j) Business Continuity Management (1) – see chapter 13;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

50 k) Compliance (3) – see chapter 14.

51 *Note: The order of the clauses does not imply their importance.*

52 Under each information security management domain the security requirements are specified.

53 Each requirement section contains:

54 a) a control objective stating what is to be achieved, i.e. the actual security requirement; and

55 b) one or more security controls that should be implemented to meet the security
56 requirements.

57 The security controls are the processes and measures that should be implemented within the
58 service perimeter to meet the security requirements.

59

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

4. Security policy

4.1 Information security policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

4.1.1 Information security policy document

Control: An information security policy document² must be approved, by senior management published and communicated to all relevant parties (including users and external parties).

The senior management must be named in the information security policy document. The policy document must state the commitment to information security and set out the approach to managing information security. It must contain statements concerning:

- a) a definition of information security, its overall objectives and scope and the importance of information security;
- b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;
- c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;
- d) a brief explanation of the security policies, principles, and compliance requirements including:
 - 1) compliance with legislative, regulatory, and contractual requirements;
 - 2) security education, training, and awareness requirements;
 - 3) business continuity management;
 - 4) consequences of information security policy violations;
- e) a definition of responsibilities for information security management, including reporting information security incidents;
- f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules that users should comply with.

² This refers to a specific information security policy defined by the Service providing organisation

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

87 This information security policy must be communicated to all users in a form that is accessible
88 and understandable to the intended reader.

89 4.1.2 Review of the information security policy

90 Control: The information security policy must be reviewed at planned intervals and/or when
91 significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

92 The information security policy must have an owner who has approved management
93 responsibility for the development, review, and evaluation of the information security policy.

94 The review of the information security policy must take account of the results of other
95 management processes, like for instance change and incident management. The information
96 security policy must be reviewed at planned intervals (*Policy Review Interval*) and/or when
97 significant changes occur.

98 The input to the review of the information security policy should include information on:

- 99 a) feedback from interested parties;
- 100 b) results of independent reviews;
- 101 c) status of preventive and corrective actions;
- 102 d) results of previous management reviews;
- 103 e) process performance and information security policy compliance;
- 104 f) changes that could affect the approach to managing information security, including
105 changes to the organisational environment, business circumstances, resource availability,
106 contractual, regulatory, and legal conditions, or to the technical environment;
- 107 g) trends related to threats and vulnerabilities;
- 108 h) reported information security incidents;
- 109 i) recommendations provided by relevant authorities.

110 The output from the review must include any decisions and actions related to:

- 111 a) improvement of the approach to managing information security and its processes;
- 112 b) improvement of control objectives and controls;
- 113 c) improvement in the allocation of resources and/or responsibilities.

114 A record of the review must be maintained.

115 The approval for the revised policy must be obtained from the senior management.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

5. Organising information security

5.1 Internal organisation

Objective: To manage information security effectively.

A management framework must be established to initiate and control the implementation of information security.

The senior management must approve the information security policy, assign security roles and co-ordinate and review the implementation of security.

5.1.1 Management commitment to information security

Control: The senior management must actively and visibly support security through clear direction, demonstrated commitment, explicit assignment of roles and responsibilities, and acknowledgment of information security responsibilities.

The senior management must:

- a) ensure that information security goals are identified, meet the organisational requirements, and are integrated in relevant processes;
- b) formulate, review, and approve an information security policy;
- c) review the effectiveness of the implementation of the information security policy;
- d) provide clear direction and visible management support for security initiatives;
- e) provide the resources needed for information security;
- f) approve assignment of specific roles and responsibilities for information security;
- g) initiate plans and programs to maintain information security awareness;
- h) ensure that the implementation of information security controls is co-ordinated.

The needs for internal or external specialist information security advice must be identified, and results of the advice must be reviewed and coordinated throughout the service perimeter.

5.1.2 Information security co-ordination

Control: Information security activities must be co-ordinated by representatives from different parts within the service perimeter with relevant roles and job functions.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Typically, information security co-ordination should involve the co-operation and collaboration of managers, users, administrators, application designers, auditors and security personnel, and specialist skills in areas such as insurance, legal issues, human resources, IT or risk management.

This activity must:

- a) ensure that security activities are executed in compliance with the information security policy;
- b) identify how to handle non-compliances;
- c) approve methodologies and processes for information security, e.g. risk assessment, information classification;
- d) identify significant threat changes and exposure of information and information processing facilities to threats;
- e) assess the adequacy and co-ordinate the implementation of information security controls;
- f) effectively promote information security education, training and awareness;
- g) evaluate information received from the monitoring and reviewing of information security incidents, and recommend actions in response to identified information security incidents.

5.1.3 Allocation of information security responsibilities

Control: All information security responsibilities must be clearly defined.

Allocation of information security responsibilities must be done in accordance with the information security policy (see clause 4). Responsibilities for the protection of individual assets and for carrying out specific security processes must be clearly identified. This responsibility must be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities.

The senior management may delegate security tasks to others. Nevertheless senior management remains responsible and must determine that any delegated tasks have been correctly performed.

Areas for which individuals are responsible must be clearly stated; in particular the following must take place:

- a) the assets and security processes associated with each particular system must be identified and clearly defined;
- b) the entity responsible for each asset or security process must be assigned and the details of this responsibility must be documented;
- c) authorisation levels must be clearly defined and documented.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

The allocation of roles and responsibilities in the risk management process are described in the risk management manual.

5.1.4 Confidentiality agreements

Control: Requirements for confidentiality or non-disclosure agreements for the protection of information must be identified and regularly reviewed at planned intervals.

Confidentiality or non-disclosure agreements must address the requirement to protect confidential information using legally enforceable terms. To identify requirements for confidentiality or non-disclosure agreements, the following elements must be implemented:

- a) a definition of the information to be protected (e.g. confidential information);
- b) expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;
- c) required actions when an agreement is terminated;
- d) responsibilities and actions of signatories to avoid unauthorised information disclosure (such as ‘need to know’);
- e) ownership of information and intellectual property, and how this relates to the protection of confidential information;
- f) the permitted use of confidential information, and rights of the signatory to use information;
- g) the right to audit and monitor activities that involve confidential information;
- h) process for notification and reporting of unauthorised disclosure or confidential information breaches;
- i) terms for information to be returned or destroyed at agreement cessation; and
- j) expected actions to be taken in case of a breach of this agreement.

Confidentiality and non-disclosure agreements must comply with all applicable laws and regulations for the jurisdiction to which it applies.

Requirements for confidentiality and non-disclosure agreements must be regularly reviewed at planned intervals (*Confidentiality Agreement Review Interval*) and/or when changes occur that influence these requirements.

5.1.5 Contact with authorities

Control: Contacts with relevant authorities must be maintained.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Procedures must be in place that specify who (e.g. law enforcement, fire department, supervisory authorities) and when and by whom authorities should be contacted. Procedures must also be in place depicting how identified information security incidents should be reported in a timely manner if it is suspected that laws may have been broken.

5.1.6 Contact with special interest groups

Control: Contacts with special interest groups or other specialist security forums and professional associations must be maintained in order to ensure that:

- a) knowledge about best practices is improved and to stay up to date with relevant security information;
- b) the understanding of the information security environment is current and complete;
- c) early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities are received;
- d) access to specialist information security advice is gained;
- e) information about new technologies, products, threats, or vulnerabilities is shared and exchanged;
- f) suitable liaison points when dealing with information security incidents are provided.

5.1.7 Independent review of information security

Control: The approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) must be reviewed independently by recognised experts at planned intervals, and/or when significant changes to the security implementation occur.

Such an independent review³ is necessary to ensure the continuing suitability, adequacy, and effectiveness to managing information security.

Information security review activities are carried out at planned intervals (*Independent Security Review Interval*) and/or when significant changes to the security implementation occur by individuals independent of the area under review, e.g. the T2S Board, internal audit function, an independent manager or a third party organisation specialising in such reviews. Individuals carrying out these reviews must have the appropriate skills and experience.

The results of the independent review are recorded and reported to the T2S Board. These records must be maintained.

³ This independent review is usually triggered by the Level 2 Governance.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

If the independent review identifies that the approach and implementation to managing information security is inadequate or not compliant with the direction for information security stated in the information security policy document, the senior management will be informed and should consider corrective actions.

5.1.8 Authorisation process for information processing facilities

Control: A management authorisation process shall be defined and implemented.

This control is not applicable for the time being, as all changes are covered by the change management process.

5.2 External parties

Objective: To maintain the security of the service's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

The security of the service's information and information processing facilities must not be reduced by the introduction of external party products or services.

Any access to the service's information processing facilities and processing and communication of information by external parties must be controlled. Where there is a business need for working with external parties that may require access to the service's information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment must be carried out to determine security implications and control requirements. Controls must be agreed and defined in an agreement with the external party.

5.2.1 Identification of risks related to external parties

Control: The risks to the service's information and information processing facilities from business processes involving external parties must be identified and controls implemented before granting access.

Where there is a need to allow an external party access to the information processing facilities or information, a risk assessment must be carried out to identify any requirements for specific controls. The identification of risks related to external party access must take into account the following issues:

- a) the information processing facilities an external party is required to access;
- b) the type of access the external party will have to the information and information processing facilities, e.g.:
 - 1) physical access, e.g. to offices, computer rooms, filing cabinets;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 266 2) logical access, e.g. to databases, information systems;
- 267 3) network connectivity between the service and the external party's network(s), e.g.
- 268 permanent connection, remote access;
- 269 4) whether the access is taking place on-site or off-site;
- 270 c) the value and the classification level of the information involved, and its criticality for
- 271 business operations;
- 272 d) the controls necessary to protect information that is not intended to be accessible by
- 273 external parties;
- 274 e) the external party personnel involved in handling the service's information;
- 275 f) how the personnel authorised to have access can be identified, the authorisation verified,
- 276 and how often this needs to be reconfirmed;
- 277 g) the different means and controls employed by the external party when storing,
- 278 processing, communicating, sharing and exchanging information;
- 279 h) the impact of access not being available to the external party when required, and the
- 280 impact of the external party entering or receiving inaccurate or misleading information;
- 281 i) practices and procedures dealing with information security incidents and potential
- 282 damages, and the terms and conditions for the continuation of external party access in the
- 283 case of an information security incident;
- 284 j) legal and regulatory requirements and other contractual obligations relevant to the
- 285 external party that should be taken into account.
- 286 Access by external parties to the service's information must not be provided until the controls
- 287 have been implemented and, where feasible, a contract has been signed defining the terms and
- 288 conditions for the connection or access and the working arrangement. Generally, all security
- 289 requirements resulting from work with external parties or internal controls should be reflected by
- 290 the agreement with the external party.
- 291 It must be ensured that the external party is aware of their obligations, and accepts the
- 292 responsibilities and liabilities involved in accessing, processing, communicating, or managing the
- 293 service's information and information processing facilities.
- 294 The controls 5.2.2 and 5.2.3 cover different external party arrangements, e.g. including:
- 295 a) service providers, such as ISPs, network providers, telephone services, maintenance and
- 296 support services;
- 297 b) managed security services;
- 298 c) customers;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- d) outsourcing of facilities and/or operations, e.g. IT systems, data collection services, call centre operations;
- e) management and business consultants, and auditors;
- f) developers and suppliers, e.g. of software products and IT systems;
- g) cleaning, catering, and other outsourced support services;
- h) temporary personnel, student placement, and other casual short-term appointments.

5.2.2 Addressing security when dealing with the customer

Control: All identified security requirements must be addressed using a defined process with documented results, before giving customers access to the service's information or assets.

The following terms must be implemented to address security prior to giving customers access to any of the assets (depending on the type and extent of access given, not all of them might apply):

- a) the product or service to be provided;
- b) a description of each service to be made available;
- c) the target level of service and unacceptable levels of service;
- d) the respective liabilities of the service providing organisation and the customer;
- e) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with customers in other countries.

5.2.3 Addressing security in third party agreements

Control: Agreements with third parties involving accessing, processing, communicating or managing the service's information or information processing facilities, or adding products or services to information processing facilities must cover all relevant security requirements.

The following terms should be included in the agreement in order to satisfy the identified security requirements:

- a) The information security policy;
- b) controls to ensure asset protection, including:
 - 1. procedures to protect assets, including information, software and hardware;
 - 2. any required physical protection controls and mechanisms;
 - 3. controls to ensure protection against malicious software;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 329 4. procedures to determine whether any compromise of the assets, e.g. loss or
330 modification of information, software and hardware, has occurred;
- 331 5. controls to ensure the return or destruction of information and assets at the end
332 of, or at an agreed point in time during, the agreement;
- 333 6. confidentiality, integrity, availability, and any other property of the assets;
- 334 7. restrictions on copying and disclosing information, and using confidentiality
335 agreements;
- 336 c) user training in methods, procedures, and security;
- 337 d) ensuring user awareness for information security responsibilities and issues;
- 338 e) provision for the transfer of personnel, where appropriate;
- 339 f) responsibilities regarding hardware and software installation and maintenance;
- 340 g) a clear reporting structure and agreed reporting formats;
- 341 h) a clear and specified process of change management;
- 342 i) access control policy, covering:
- 343 1. the different reasons, requirements, and benefits that make the access by the third
344 party necessary;
- 345 2. permitted access methods, and the control and use of identifiers such as user IDs
346 and passwords;
- 347 3. an authorisation process for user access and privileges;
- 348 4. a requirement to maintain a list of individuals authorised to use the services
349 being made available, and what their rights and privileges are with respect to
350 such use;
- 351 5. a statement that all access that is not explicitly authorised is forbidden;
- 352 6. a process for revoking access rights or interrupting the connection between
353 systems;
- 354 j) arrangements for reporting, notification, and investigation of information security
355 incidents and security breaches, as well as violations of the requirements stated in the
356 agreement;
- 357 k) a description of the product or service to be provided, and a description of the
358 information to be made available along with its security classification;
- 359 l) the target level of service and unacceptable levels of service;
- 360 m) the definition of verifiable performance criteria, their monitoring and reporting;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- n) the right to monitor, and revoke, any activity related to the assets;
- o) the right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors;
- p) the establishment of an escalation process for problem resolution;
- q) service continuity requirements, including measures for availability and reliability, in accordance with business priorities;
- r) the respective liabilities of the parties to the agreement;
- s) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with organisations in other countries;
- t) intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work;
- u) involvement of the third party with subcontractors, and the security controls these subcontractors need to implement;
- v) conditions for renegotiation/termination of agreements:
 - 1. a contingency plan must be in place in case either party wishes to terminate the relation before the end of the agreements;
 - 2. renegotiation of agreements if the security requirements change;
 - 3. change of current documentation of asset lists, licences, agreements or rights relating to them.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

6. Asset management

6.1 Responsibility for assets

Objective: To achieve and maintain protection of assets.

All assets must be accounted for and have a nominated owner.

Owners must be identified for all assets and the responsibility for the maintenance of controls must be assigned. The implementation of specific controls may be delegated by the asset owner as appropriate but the owner remains responsible for the proper protection of the assets.

6.1.1 Inventory of assets

Control: All assets must be clearly identified and an inventory of all important (its business value and its security classification) assets drawn up and maintained. Regular audits of the asset inventory must be performed.

All assets must be identified and the importance of these assets must be documented. The asset inventory must include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. The inventory should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned.

However, in order to reduce the work associated with drawing up the inventory grouping of assets is allowed. Criteria for grouping are:

- a) *similar assets*;
- b) *similar security requirements*;
- c) *assets are used in the same process and protection requirements are valid throughout*;
- d) *assets can be considered as a unit*.

Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets must be identified and documented.

There are many types of assets, including:

- a) information: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;
- b) software assets: application software, system software, development tools, and utilities;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- c) physical assets: computer equipment, communications equipment, removable media, and other equipment;
- d) services: computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning;
- e) people, and their qualifications, skills, and experience.

6.1.2 Ownership of assets

Control: All information and assets associated with information processing facilities must have for security purposes a designated asset owner⁴.

The asset owner is responsible for:

- a) ensuring that information and assets associated with information processing facilities are classified;
- b) defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies.

6.1.3 Acceptable use of assets

Control: Rules for the acceptable use of information and assets associated with information processing facilities must be identified, documented, and implemented.

All employees, contractors and third party users must follow rules for the acceptable use of information and assets associated with information processing facilities, including:

- a) rules for electronic mail and Internet usages;
- b) guidelines for the use of mobile devices, especially for the use outside the premises;

Specific rules or guidance must be provided by the senior management. Employees, contractors and third party users using or having access to assets must be aware of the limits existing for their use of the information and assets associated with information processing facilities, and resources. They must be responsible for their use of any information processing resources and of any use carried out under their responsibility.

6.2 Information classification

Objective: To ensure that information receives an appropriate level of protection.

⁴ The term 'asset owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has any property rights to the asset.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Information must be classified to indicate the need, priorities, and expected degree of protection when handling the information.

6.2.1 Classification guidelines

Control: Information must be classified in terms of criticality, value and sensitivity (level of confidentiality) taking legal requirements into account as well.

Classifications and associated protective controls for information must take account of business needs for sharing or restricting information and the business impacts associated with such needs.

Classification guidelines must include conventions for initial classification and reclassification over time; in accordance with some predetermined access control policy.

6.2.2 Information labelling and handling

Control: A set of procedures for information labelling and handling must be developed and implemented in accordance with the classification scheme⁵ adopted by the service.

Procedures for information labelling need to cover information assets in physical and electronic formats.

Output from systems containing information that is classified as being sensitive or critical must carry a classification label (in the output). The labelling must reflect the classification according to the rules established in 6.2.1.

For each classification level, handling procedures including the secure processing, storage, transmission, declassification, and destruction must be defined. This should also include the procedures for chain of custody and logging of any security event.

Agreements with other organisations that include information sharing must include procedures to identify the classification of that information and to interpret the classification labels from other organisations.

⁵ The ECB classification scheme should be used as reference document as long as a common ESCB scheme is not deployed.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

7. Human resources security

7.1 Prior to employment⁶

Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles for which they are considered, and to reduce the risk of theft, fraud or misuse of facilities.

7.1.1 Roles and responsibilities

Control: Security roles and responsibilities of employees, contractors and third party users must be defined and documented in accordance with the information security policy.

Security roles and responsibilities must include the requirement to:

- a) implement and act in accordance with the information security policies;
- b) protect assets from unauthorised access, disclosure, modification, destruction or interference;
- c) execute particular security processes or activities;
- d) ensure responsibility is assigned to the individual for actions taken;
- e) report security events, potential events or security risks.

Security roles and responsibilities must be defined and clearly communicated to job candidates during the pre-employment process.

7.1.2 Screening

Control: Background verification checks on all candidates for employment, contractors, and third party users must be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

Verification checks must take into account all relevant privacy, protection of personal data and/or employment based legislation, and should, where permitted, include the following:

- a) availability of satisfactory character references, e.g. one business and one personal;

⁶ Explanation: The word 'employment' is meant here to cover all of the following different situations: employment of people, appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- b) a check (for completeness and accuracy) of the applicant's curriculum vitae;
- c) confirmation of claimed academic and professional qualifications;
- d) independent identity check (passport or similar document);
- e) more detailed checks, such as credit checks or checks of criminal records.

Procedures must define criteria and limitations for verification checks, e.g. who is eligible to screen people, and how, when and why verification checks are carried out.

A screening process must also be carried out for contractors, and third party users. Where contractors are provided through an agency the contract with the agency must clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern. In the same way, the agreement with the third party must clearly specify all responsibilities and notification procedures for screening.

Information on all candidates being considered for positions within the organisation must be collected and handled in accordance with any applicable legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates should be informed beforehand about the screening activities.

7.1.3 Terms and conditions of employment

Control: As part of their contractual obligation, employees, contractors and third party users must agree and sign the terms and conditions of their employment contract, which must state the responsibilities of both sides concerning information security. Terms and conditions must be in accordance with any applicable legislation existing in the relevant jurisdiction.

The terms and conditions of employment must reflect the security policy in addition to clarifying and stating:

- a) that all employees, contractors and third party users who are given access to sensitive information must sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities;
- b) the employee's, contractor's and third party user's legal responsibilities and rights, e.g. regarding copyright laws, data protection legislation;
- c) responsibilities for the classification of information and management of assets associated with information systems and services handled by the employee, contractor or third party user;
- d) responsibilities of the employee, contractor or third party user for the handling of information received from other companies or external parties;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- e) responsibilities for the handling of personal information, including personal information created as a result of, or in the course of, employment with the respective central bank;
- f) responsibilities that are extended outside the hosting premises and outside normal working hours, e.g. in the case of home-working;
- g) actions to be taken if the employee, contractor or third party user disregards the security requirements.

It must be ensured that employees, contractors and third party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the assets associated with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment.

7.2 During employment

Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support the information security policy in the course of their normal work, and to reduce the risk of human error.

7.2.1 Management responsibilities

Control: Management must require employees, contractors and third party users to apply security in accordance with established policies and procedures of the service providing organisation.

Management responsibilities must include ensuring that employees, contractors and third party users:

- a) are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information;
- b) are provided with guidelines to state security expectations of their role;
- c) are motivated to fulfil the security policies set-up by the senior management;
- d) achieve a level of awareness on security relevant to their roles and responsibilities;
- e) conform to the terms and conditions of employment, which includes the information security policy and appropriate methods of working;
- f) continue to have the appropriate skills and qualifications.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

7.2.2 Information security awareness, education, and training

Control: All employees, contractors and third party users must receive appropriate awareness training and regular updates on the policies and procedures, as relevant for their job function.

Awareness training must commence with a formal induction process designed to introduce the information security policy, procedures and expectations before access to information or services is granted.

Ongoing training must include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages and information on the disciplinary process.

7.2.3 Disciplinary process

Control: There must be a formal disciplinary process in accordance with any applicable legislation existing in the relevant jurisdiction for employees⁷ who have committed a security breach.

The disciplinary process must not commence without prior verification that a security breach has occurred.

7.3 Termination or change of employment

Objective: To ensure that employees, contractors and third party users exit or change employment in an orderly manner (as defined in the following control sections).

7.3.1 Termination responsibilities

Control: Responsibilities for performing employment termination or change of employment must be clearly defined and assigned.

The communication of termination responsibilities must include ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement, and the terms and conditions of employment continuing for a defined period after the end of the employee's, contractor's or third party user's employment.

Responsibilities and duties still valid after termination of employment must be contained in employee's, contractor's or third party user's contracts.

⁷ Appropriate contractual remedies against contractors and third-party users who have committed a security breach are covered as part of the third party agreements as described in chapter 5.2.3.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Changes of responsibility or employment must be managed as the termination of the respective responsibility or employment, and the new responsibility or employment must be controlled as described in clause 7.1.

7.3.2 Return of assets

Control: All employees, contractors and third party users must return all assets in their possession upon termination of their employment, contract or agreement.

The termination process must be formalised to include the return of all previously issued software, corporate documents, and equipment. Other assets such as mobile computing devices, access cards, software, manuals, and information stored on electronic media also need to be returned.

In cases where an employee, contractor or third party user purchases equipment or uses their own personal equipment, procedures must be followed to ensure that all relevant information is returned and securely erased from the equipment.

In cases where an employee, contractor or third party user has knowledge that is important to ongoing operations, that information must be documented and transferred to the appointed people.

7.3.3 Removal of access rights

Control: The access rights of all employees, contractors and third party users to information and information processing facilities must be removed upon termination of their employment, contract or agreement or adjusted upon change.

Changes of an employment must be reflected in removal of all access rights that were not approved for the new employment. The access rights that must be removed or adapted include physical and logical access, keys, identification cards, information processing facilities, subscriptions, and removal from any documentation that identifies them as a current member of the respective central bank. If a departing employee, contractor or third party user has known passwords for accounts remaining active, these must be changed upon termination or change of employment, contract or agreement.

Access rights for information assets and information processing facilities must be reduced or removed at the time the employment terminates or changes.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

8. Physical and environmental security

8.1 Secure areas

Objective: To prevent unauthorised physical access, damage, and interference to the hosting premises and information.

Critical or sensitive information processing facilities must be housed in secure areas, protected by defined security perimeters, with security barriers and entry controls. They must be physically protected from unauthorised access, damage, and interference.

The protection provided must be commensurate with the identified risks.

8.1.1 Physical security perimeter

Control: Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) must be used to protect areas that contain the service's information and information processing facilities.

The following must be implemented for physical security perimeters:

- a) security perimeters must be clearly defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;
- b) perimeters of a building or site containing information processing facilities must be physically sound (i.e. there must be no gaps in the perimeter or areas where a break-in could easily occur); the external walls of the site should be of solid construction and all external doors must be suitably protected against unauthorised access with control mechanisms, e.g. bars, alarms, locks etc; doors and windows should be locked when unattended and external protection should be implemented for windows;
- c) a manned reception area or other means to control physical access to the site or building must be in place;
- d) access to sites and buildings must be restricted to authorised personnel only;
- e) physical barriers should, where applicable, be built to prevent unauthorised physical access and environmental contamination;
- f) all fire doors on a security perimeter should be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance to

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

suitable regional, national, and international standards; they must operate in accordance with local fire code in a failsafe manner;

- g) intruder detection systems must be installed to national, regional or international standards and tested (at least once a year) to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms;
- h) information processing facilities managed by the service providing organisation should be physically separated⁸ from those managed by third parties.

8.1.2 Physical entry controls

Control: Secure areas must be protected by entry controls to ensure that only authorised personnel are allowed access.

The following must be implemented:

- a) the date and time of entry and departure of visitors must be recorded;
- b) visitors must be supervised unless their access has been previously approved; they must only be granted access for specific, authorised purposes and must be provided with instructions on the security requirements of the area and on emergency procedures;
- c) access to the areas (e.g. computer rooms and office rooms) must be controlled and restricted to authorised persons only; authentication controls, e.g. access control card plus PIN, must be used to authorise and validate all access;
- d) an audit trail of all access must be maintained (see 14.1.3);
- e) all employees, contractors, third party users and visitors must be required to wear some form of visible identification and must immediately notify security personnel if they encounter unescorted visitors not wearing visible identification;
- f) third party support service personnel must be granted restricted access to secure areas only when required; this access must be authorised and monitored;
- g) access rights to secure areas must be reviewed at planned intervals (*Physical Entry Controls Review Interval*) and updated, and revoked when necessary.

8.1.3 Securing offices, rooms, and facilities

Control: Physical security for offices, rooms, and facilities must be designed and applied.

⁸ Physical separation in this context is not required if third party support personnel is always supervised by internal staff.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

The following must be implemented to secure offices, rooms, and facilities:

- a) account must be taken of relevant health and safety regulations and standards;
- b) key facilities must be sited to avoid access by the public;
- c) where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities;
- d) directories and internal telephone books identifying locations of sensitive information processing facilities must not be readily accessible by the public.

8.1.4 Protecting against external and environmental threats

Control: Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster must be designed and applied.

Consideration must be given to any security threats presented by neighbouring premises, e.g. a fire in a neighbouring building, water leaking from the roof or in floors below ground level or an explosion in the street.

The following guidelines must be implemented to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster:

- a) hazardous or combustible materials must not be stored within a secure area;
- b) bulk supplies such as stationery must not be stored within a secure area;
- c) fallback equipment and back-up media must be sited at a secondary site with a different risk profile to avoid damage from a disaster affecting the main site;
- d) fire fighting equipment must be provided and suitably placed.

8.1.5 Working in secure areas

Control: Physical protection and guidelines for working in secure areas must be designed and applied.

The following must be implemented:

- a) personnel must only be aware of the existence of, or activities within, a secure area on a need to know basis;
- b) unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- c) vacant secure areas (i.e. rooms containing critical components but not permanently staffed) must be physically locked and periodically checked;
- d) photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorised.

8.1.6 Public access, delivery, and loading areas

Control: Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises must be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

The following must be implemented:

- a) access to a delivery and loading area from outside of the building should be restricted to identified and authorised personnel;
- b) the delivery and loading area must be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building;
- c) the external doors of a delivery and loading area must be secured when the internal doors are opened;
- d) incoming material should be inspected for potential threats before this material is moved from the delivery and loading area to the point of use;
- e) incoming material should be registered in accordance with asset management procedures on entry to the site.

8.2 Equipment security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the service providing organisation's activities.

Equipment must be protected from physical and environmental threats.

8.2.1 Equipment siting and protection

Control: Equipment must be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

The following must be implemented to protect equipment:

- a) equipment must be sited to minimise unnecessary access into work areas;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- b) information processing facilities handling sensitive data must be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorised persons during their use, and storage facilities secured to avoid unauthorised access;
- c) items requiring special protection must be isolated to reduce the general level of protection required;
- d) controls must be adopted to minimise the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism;
- e) environmental conditions, such as temperature and humidity, must be monitored for conditions, which could adversely affect the operation of information processing facilities;
- f) lightning protection must be applied to all buildings and lightning protection filters must be fitted to all incoming power and communications lines.

8.2.2 Supporting utilities

Control: Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.

All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning must be adequate for the systems they are supporting. At regular intervals (*Support Utilities Review Interval*) the support utilities must be inspected and tested to ensure their proper functioning and to reduce any risk from their malfunction or failure. An electrical supply must be provided that conforms to the equipment manufacturer's specifications.

An uninterruptible power supply (UPS) to support orderly close down or continuous running must be in place for equipment supporting critical business operations. Power contingency plans must cover the action to be taken on failure of the UPS. A back-up generator must be in place if processing is required to continue in case of a prolonged power failure. An adequate supply of fuel must be available to ensure that the generator can perform for a prolonged period. UPS equipment and generators must be checked at least twice a year to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations. In addition, consideration should be given to using multiple power sources or, if the site is large a separate power substation.

Emergency power off switches must be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting must be provided in case of main power failure.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

The water supply must be stable and adequate to supply air conditioning, humidification equipment and fire suppression systems (where used).

Malfunctions in the water supply system may damage equipment or prevent fire suppression from acting effectively. Therefore an alarm system to detect malfunctions in the supporting utilities must be installed.

Telecommunications equipment must be connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services. Voice services must be adequate to meet local legal requirements for emergency communications.

8.2.3 Cabling security

Control: Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage.

The following must be implemented:

- a) power and telecommunications lines into information processing facilities must be underground, where possible, or subject to adequate alternative protection;
- b) network cabling must be protected from unauthorised interception or damage, for example by using a conduit or by avoiding routes through public areas;
- c) power cables should be segregated from communications cables to prevent interference;
- d) clearly identifiable cable and equipment markings should be used to minimise handling errors, such as accidentally patching of wrong network cables;
- e) a documented patch list should be used to reduce the possibility of errors;
- f) installation of armoured conduit and locked rooms or boxes at inspection and termination points;
- g) use of alternative routings and/or transmission media providing security;
- h) controlled access to patch panels and cable rooms.

8.2.4 Equipment maintenance

Control: Equipment must be correctly maintained to ensure its continued availability and integrity.

The following must be implemented:

- a) equipment must be maintained in accordance with the supplier's recommended service intervals and specifications;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- b) only authorised maintenance personnel must carry out repairs and service equipment;
- c) records must be kept of all suspected or actual faults, and all preventive and corrective maintenance;
- d) all requirements imposed by insurance policies must be complied with.

8.2.5 Security of equipment off-premises

Control: Security must be applied to off-site equipment taking into account the risks of it being outside of the hosting premises.

Regardless of ownership, the use of any information processing equipment outside the hosting premises must be authorised by responsible management.

The following guidelines must be implemented for the protection of off-site equipment:

- a) equipment and media⁹ taken off the hosting premises must not be left unattended in public places;
- b) portable computers should be carried as hand luggage;
- c) manufacturers' instructions for protecting equipment must be observed at all times, e.g. protection against exposure to strong electromagnetic fields;
- d) home-working controls must be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office;
- e) adequate insurance cover must be in place to protect equipment off-site.

8.2.6 Secure disposal or re-use of equipment

Control: All items of equipment containing storage media must be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

Devices containing sensitive information must be physically destroyed or the information must be destroyed, deleted or securely overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

Damaged devices containing sensitive data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded.

⁹ Information storing and processing equipment includes all forms of personal computers, organisers, mobile phones, smart cards, paper or other form, which is held for home working or being transported away from the normal work location

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

8.2.7 Removal of property

Control: Equipment, information or software must not be taken off-site without prior authorisation.

The following guidelines must be implemented:

- a) equipment, information or software must not be taken off-site without prior authorisation;
- b) employees, contractors and third party users who have authority to permit off-site removal of assets must be clearly identified;
- c) time limits for equipment removal should be set and returns checked for compliance;
- d) equipment must be recorded as being removed off-site and recorded when returned to the issuing department.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

9. Communications and operations management

9.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

Responsibilities and procedures for the management and operation of all information processing facilities must be established. This includes the development of operating procedures.

Segregation of duties must be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

9.1.1 Documented operating procedures

Control: Operating procedures must be documented, maintained, and made available to all users who need them.

Documented procedures must be prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, media handling, computer room and mail handling management, and safety.

The operating procedures must specify the instructions for the detailed execution of each job including:

- a) processing and handling of information;
- b) backup (see 9.5);
- c) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;
- d) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;
- e) support contacts in the event of unexpected operational or technical difficulties;
- f) special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs;
- g) system restart and recovery procedures for use in the event of system failure;
- h) the management of audit-trail and system log information (see 9.10).

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Operating procedures, and the documented procedures for system activities, must be treated as formal documents and changes authorised by management as part of the change management process.

9.1.2 Change management

To avoid redundancies this control has been merged with control 11.5.1.

9.1.3 Segregation of duties

Control: Duties and areas of responsibility must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of assets.

Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Care must be taken that no single person can access, modify or use assets without authorisation or detection. The initiation of an event should be separated from its authorisation for example by implementing the four-eye principle. The possibility of collusion must be implemented in designing the controls.

The initiation of an event must be separated from its authorisation meaning segregation of activities which require collusion in order to defraud (critical business functions), i.e. features must be in place in order to ensure that no person is in a position to alter sensitive business data single-handed, e.g. dispatching of a payment.

9.1.4 Separation of development, test, and operational facilities

Control: Development, test, and operational facilities must be separated to reduce the risks of unauthorised access or changes to the operational system.

The following must be implemented:

- a) rules for the transfer of software from development to operational status must be defined and documented;
- b) development and operational software must run on different systems or computer processors and in different domains or directories;
- c) compilers, editors, and other development tools or system utilities should not be accessible from operational systems when not required;
- d) the test system environment should emulate the operational system environment as closely as possible;
- e) users should use different user profiles for operational and test systems;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- f) menus should display identification messages to reduce the risk of error;
- g) sensitive data should not be copied into the test system environment (see 11.4.2).

9.2 Third party service delivery management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

The senior management must check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.

9.2.1 Service delivery

Control: It must be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

Service delivery by a third party must include the agreed security arrangements, service definitions, and aspects of service management. In case of outsourcing arrangements, the senior management must plan the necessary transitions (of information, information processing facilities, and anything else that needs to be moved), and must ensure that security is maintained throughout the transition period.

The senior management must ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

9.2.2 Monitoring and review of third party services

Control: The services, reports and records provided by the third party must be regularly monitored and reviewed, and audits (where applicable) must be carried out regularly.

Monitoring and review of third party services must involve a service management relationship and process between the service providing organisation and the third party to:

- a) monitor service performance levels to check adherence to the agreements;
- b) review service reports produced by the third party and arrange regular progress meetings as required by the agreements;
- c) receive information about information security incidents and review of this information conducted jointly;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

d) review third party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

e) resolve and manage any identified problems.

The responsibility for managing the relationship with a third party should be assigned to a designated individual or service management team. In addition, it should be ensured that the third party assigns responsibilities for checking for compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources must be made available to monitor the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action must be taken when deficiencies in the service delivery are observed.

9.2.3 Managing changes to third party services

Control: Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, must be managed, taking into account the criticality of business systems and processes involved after a thorough re-assessment of risks.

The process of managing changes to a third party service must include rules for:

a) changes requested by the service providing organisation impacting the third party:

1. enhancements to the current service offered;
2. development of any new applications and systems;
3. modifications or updates of policies and procedures;
4. new controls to resolve information security incidents and to improve security.

b) changes in the third party services that impact the service providing organisation:

1. changes and enhancement to networks;
2. use of new technologies;
3. adoption of new products or newer versions/releases;
4. new development tools and environments;
5. changes to physical location of service facilities;
6. change of vendors.

9.3 System planning and acceptance

Objective: To minimise the risk of systems failures.

Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance. Projections of future capacity requirements

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

must be made, to reduce the risk of system overload. The operational requirements of new systems must be established, documented, and tested prior to their acceptance and use.

9.3.1 Capacity management

Control: The use of resources must be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

For each new and ongoing activity, capacity requirements must be identified. System tuning and monitoring must be applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls must be put in place to indicate problems in due time. Projections of future capacity requirements must take account of new business and system requirements and current and projected trends in the information processing capabilities.

Particular attention needs to be paid to any key resources in order to avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.

9.3.2 System acceptance

Control: Acceptance criteria for new information systems, upgrades, and new versions must be established, and suitable tests of the system(s) carried out during development and prior to acceptance.

It must be ensured that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested. New information systems, upgrades, and new versions must only be migrated into production after obtaining formal acceptance. The following must be established prior to formal acceptance being provided:

- a) performance and computer capacity requirements;
- b) error recovery and restart procedures, and contingency plans;
- c) preparation and testing of routine operating procedures;
- d) agreed set of security controls in place;
- e) effective manual procedures;
- f) business continuity arrangements;
- g) evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end;
- h) evidence that consideration has been given to the effect the new system has on the overall security of the service;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

i) training in the operation or use of new systems;

j) ease of use, as this affects user performance and avoids human error.

Tests involving the operations function and users must be carried out to confirm that all acceptance criteria have been fully satisfied. Testing activities and results must be properly documented.

9.4 Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

Precautions are required to prevent and detect the introduction of malicious code and unauthorised mobile code.

Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users must be made aware of the dangers of malicious code.

9.4.1 Controls against malicious code

Control: Detection, prevention, and recovery controls to protect against malicious code and user awareness procedures must be implemented.

Protection against malicious code must be based on malicious code detection and repair software, security awareness, system access and change management controls. The following must be implemented:

a) establishing a formal policy prohibiting the use of unauthorised software;

b) establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken;

c) conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorised amendments should be formally investigated (optional);

d) installation and maintenance of up-to-date malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the checks carried out must include:

1. checking any files on electronic or optical media, and files received over networks, for malicious code before use;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 1004 2. checking electronic mail attachments and downloads for malicious code before use;
1005 this check must be carried out at different places, e.g. at electronic mail servers,
1006 desk top computers and when entering the internal network;
- 1007 3. checking web pages for malicious code;
- 1008 e) defining management procedures and responsibilities to deal with malicious code
1009 protection on systems, training in their use and reporting;
- 1010 f) preparing plans for recovering from malicious code attacks, including all necessary data
1011 and software back-up and recovery arrangements;
- 1012 g) implementing procedures to regularly collect information, such as subscribing to mailing
1013 lists and/or checking web sites giving information about new malicious code;
- 1014 h) implementing procedures to verify information relating to malicious code, and ensure
1015 that warning bulletins are accurate and informative; managers should ensure that
1016 qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing
1017 software protecting against malicious code, are used to differentiate between hoaxes and
1018 real malicious code; all users must be made aware of the problem of hoaxes and what to
1019 do on receipt of them.

1020 **9.4.2 Controls against mobile code**

1021 Control: Where the use of mobile code¹⁰ is authorised, the configuration must ensure that the
1022 authorised mobile code operates according to a clearly defined security policy, and unauthorised
1023 mobile code must be prevented from executing.

1024 The following should be implemented to protect against mobile code performing unauthorised
1025 actions:

- 1026 a) executing mobile code in a logically isolated environment;
- 1027 b) blocking any use of mobile code;
- 1028 c) blocking receipt of mobile code;
- 1029 d) activating technical measures as available on a specific system to ensure mobile code is
1030 managed;
- 1031 e) control the resources available to mobile code access;
- 1032 f) cryptographic controls to uniquely authenticate mobile code.

¹⁰ Mobile code is software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction (e.g. ActiveX, Java applets, JavaScript). Mobile code is associated with a number of middleware services.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

9.5 Back-up

Objective: To maintain the integrity and availability of information and information processing facilities.

Routine procedures must be established to implement the agreed back-up policy and strategy for taking back-up copies of data and rehearsing their timely restoration.

9.5.1 Information backup

Control: Backup copies of information and software must be taken and tested regularly in accordance with the agreed backup policy.

Adequate backup facilities must be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

The following items for information backup must be implemented:

- a) the necessary level of backup information must be defined in a backup policy;
- b) accurate and complete records of the back-up copies and documented restoration procedures must be produced;
- c) the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements, the security requirements of the information involved, and the criticality of the information to the continued operation of the service;
- d) the backups must be stored in a remote location with a different risk profile to escape any damage from a disaster at the main site;
- e) backup information must be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the backup site;
- f) backup media must be tested to ensure that they can be relied upon for emergency use when necessary;
- g) restoration procedures must be regularly checked and tested (*Restoration Check Interval*) to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery;
- h) in situations where confidentiality is of importance, backups should be protected by means of encryption;
- i) the retention period for essential business information, and also any requirement for archive copies to be permanently retained must be determined.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

9.6 Network security management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

The secure management of networks, which may span the boundaries of the service providing organisation, requires careful consideration to dataflow, legal implications, monitoring, and protection.

Additional controls may also be required to protect sensitive information passing over public networks.

9.6.1 Network controls

Control: Networks must be adequately managed and controlled in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

Network managers must implement controls to ensure the security of information in networks, and the protection of connected services from unauthorised access. The following items must be implemented:

- a) operational responsibility for networks should be separated from computer operations where appropriate;
- b) responsibilities and procedures for the management of remote equipment, including equipment in user areas, must be established;
- c) logging and monitoring should be applied to enable recording of security relevant actions;
- d) management activities should be closely co-ordinated both to optimise the service and to ensure that controls are consistently applied across the information processing infrastructure.

9.6.2 Security of network services

Control: Security features, service levels, and management requirements of all network services¹¹ must be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

¹¹ Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and intrusion detection systems. Network services are for example SWIFT, Internet access, mail service provider, etc.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

The ability of the network service provider to manage agreed services in a secure way must be determined and monitored, and the right to audit must be agreed.

The security arrangements necessary for particular services, such as security features, service levels, and management requirements, must be identified and included in the contract.

9.7 Media handling

Objective: To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.

Media must be controlled and physically protected.

Operating procedures must be established to protect documents, computer media (e.g. tapes, disks, memory sticks, CDs, DVDs), input/output data and system documentation from unauthorised disclosure, modification, removal, and destruction.

9.7.1 Management of removable media

Control: There must be procedures in place for the management of removable media¹².

The following measures for the management of removable media must be implemented:

- a) if no longer required, the contents of any re-usable media that are to be removed from the hosting premises must be made unrecoverable;
- b) where necessary and practical, authorisation should be required for media removed from the hosting premises and a record of such removals must be kept in order to maintain an audit trail;
- c) all media must be stored in a safe, secure environment, in accordance with manufacturers' specifications;
- d) information stored on media that needs to be available longer than the media lifetime (in accordance with manufacturers' specifications) must be also stored elsewhere to avoid information loss due to media degradation;
- e) registration of removable media must be implemented to limit the opportunity for data loss.
- f) all procedures and authorisation levels must be clearly documented.

¹² Removable media include e.g. tapes, disks, flash disks, removable hard drives, CDs, DVDs, and printed media.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

9.7.2 Disposal of media

Control: Media must be disposed of securely and safely when no longer required, using formal procedures.

Formal procedures for the secure disposal of media should minimise the risk of sensitive information leakage to unauthorised persons. The procedures for secure disposal of media containing sensitive information must be commensurate with the sensitivity of that information. The following items must be implemented:

- a) media containing sensitive information must be stored and disposed of securely and safely, e.g. by incineration or shredding, or erased of data for use by another application;
- b) procedures must be in place to identify the items that might require secure disposal;
- c) care must be taken in selecting a contractor that provide disposal services for papers, equipment and media;
- d) disposal of sensitive items must be logged in order to maintain an audit trail.

9.7.3 Information handling procedures

Control: Procedures for the handling and storage of information¹³ must be established to protect this information from unauthorised disclosure or misuse.

Procedures must be drawn up for handling, processing, storing, and communicating information consistent with its classification. The following items must be implemented:

- a) handling and labelling of all media to its indicated classification level;
- b) access restrictions to prevent access from unauthorised personnel;
- c) maintenance of a formal record of the authorised recipients of data;
- d) protection of spooled data awaiting output to a level consistent with its sensitivity;
- e) storage of media in accordance with manufacturers' specifications;
- f) keeping the distribution of data to a minimum (need-to-know principle);
- g) clear marking of all copies of media for the attention of the authorised recipient;
- h) review of distribution lists and lists of authorised recipients at planned intervals (*Distribution List Review Interval*).

¹³ These procedures apply to information in documents, computing systems, networks, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities, use of facsimile machines.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

9.7.4 Security of system documentation

Control: System documentation¹⁴ must be protected against unauthorised access.

To secure system documentation, the following items must be implemented:

- a) system documentation must be stored securely;
- b) access to system documentation must be limited to authorised persons;
- c) system documentation held on a public network, or supplied via a public network, must be protected.

9.8 Exchange of information and software

Objective: To maintain the security of information and software exchanged within the service providing organisation and with any external entity.

Exchange of information and software between the service providing organisation and an external entity must be based on a formal exchange policy, carried out in line with exchange agreements, and must be compliant with any relevant legislation.

Procedures must be established to protect information and physical media containing information in transit.

9.8.1 Information exchange policies and procedures

Control: Formal exchange policies, procedures, and controls must be in place to protect the exchange of information through the use of all types of communication facilities.

The procedures and controls to be followed when using electronic communication facilities for information exchange should consider the following items:

- a) procedures designed to protect exchanged information from interception, copying, modification, mis-routing, and destruction;
- b) procedures for the detection of and protection against malicious code that may be transmitted through the use of electronic communications;
- c) procedures for protecting communicated sensitive electronic information that is in the form of an attachment;
- d) policy or guidelines outlining acceptable use of electronic communication facilities;

¹⁴ System documentation may contain a range of sensitive information, e.g. descriptions of applications processes, procedures, data structures, authorisation processes.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 1173 e) procedures for the use of wireless communications, taking into account the particular
1174 risks involved;
- 1175 f) employee, contractor and any other user's responsibilities not to compromise the service
1176 providing organisation, e.g. through defamation, harassment, impersonation, forwarding
1177 of chain letters, unauthorised purchasing, etc.;
- 1178 g) use of cryptographic techniques e.g. to protect the confidentiality, integrity and
1179 authenticity of information;
- 1180 h) retention and disposal guidelines for all business correspondence, including messages, in
1181 accordance with relevant national and local legislation and regulations;
- 1182 i) not leaving sensitive or critical information on printing facilities, e.g. copiers, printers,
1183 and facsimile machines, as these may be accessed by unauthorised personnel;
- 1184 j) controls and restrictions associated with the forwarding of communication facilities, e.g.
1185 automatic forwarding of electronic mail to external mail addresses;
- 1186 k) reminding personnel that they should take precautions, e.g. not to reveal sensitive
1187 information to avoid being overheard or intercepted when making a phone call by:
- 1188 1. people in their immediate vicinity particularly when using mobile phones;
- 1189 2. wiretapping, and other forms of eavesdropping through physical access to the phone
1190 handset or the phone line, or using scanning receivers;
- 1191 3. people at the recipient's end;
- 1192 l) not leaving messages containing sensitive information on answering machines since
1193 these may be replayed by unauthorised persons, stored on communal systems or stored
1194 incorrectly as a result of misdialling;
- 1195 m) reminding personnel about the problems of using facsimile machines, namely:
- 1196 1. unauthorised access to built-in message stores to retrieve messages;
- 1197 2. deliberate or accidental programming of machines to send messages to specific
1198 numbers;
- 1199 3. sending documents and messages to the wrong number either by misdialling or
1200 using the wrong stored number;
- 1201 n) reminding personnel not to register demographic data, such as the e-mail address or other
1202 personal information, in any software to avoid collection for unauthorised use;
- 1203 o) reminding personnel that modern facsimile machines and photocopiers have page caches
1204 and store pages in case of a paper or transmission fault, which will be printed once the
1205 fault is cleared.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

1206 In addition, personnel should be reminded that they should not have confidential conversations in
1207 public places or open offices and meeting places with non-sound proofed-walls.

1208 Information exchange facilities must comply with any relevant legal requirements.

1209 9.8.2 Exchange agreements

1210 Control: Agreements must be established for the exchange of information and software between
1211 the service providing organisation and external parties (see also control 5.2.1).

1212 Exchange agreements should, if applicable, consider the following security conditions:

1213 a) management responsibilities for controlling and notifying transmission, dispatch, and
1214 receipt;

1215 b) procedures for notifying sender of transmission, dispatch, and receipt;

1216 c) procedures to ensure traceability and non-repudiation;

1217 d) minimum technical standards for packaging and transmission;

1218 e) escrow agreements¹⁵;

1219 f) courier identification standards;

1220 g) responsibilities and liabilities in the event of information security incidents, such as loss
1221 of data;

1222 h) use of an agreed labelling system for sensitive or critical information, ensuring that the
1223 meaning of the labels is immediately understood and that the information is protected;

1224 i) ownership and responsibilities for data protection, copyright, software license
1225 compliance and similar considerations;

1226 j) technical standards for recording and reading information and software;

1227 k) any special controls that may be required to protect sensitive items, such as cryptographic
1228 keys.

1229 9.8.3 Physical media in transit

1230 Control: Media containing information must be protected against unauthorised access, misuse or
1231 corruption during transportation outside the hosting premises.

¹⁵ A legal provision whereby, in the event of a developer/supplier failing or otherwise ceasing to trade, the source code for their packaged software is made available to licensed / registered users, thereby enabling its ongoing maintenance.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

The following measures must be implemented to protect information media being transported between sites:

- a) reliable transport or couriers must be used;
- b) a list of authorised couriers must be established;
- c) procedures to check the identification of couriers must be developed;
- d) packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting software against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields;
- e) controls should be adopted, where necessary, to protect sensitive information from unauthorised disclosure or modification; examples include:
 1. use of locked containers;
 2. delivery by hand;
 3. tamper-evident packaging (which reveals any attempt to gain access);
 4. in exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.

9.8.4 Electronic messaging

Control: Information involved in electronic messaging must be protected.

Security considerations for electronic messaging must include the following:

- a) protecting messages from unauthorised access, modification or denial of service;
- b) ensuring correct addressing and transportation of the message;
- c) general reliability and availability of the service;
- d) legal considerations, for example requirements for electronic signatures;
- e) obtaining approval prior to using external public services such as instant messaging or file sharing;
- f) stronger levels of authentication controlling access from publicly accessible networks.

9.8.5 Business Information Systems

Control: Policies and procedures must be developed and implemented to protect the service's information associated with the interconnection of business/office information systems.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Office information systems are opportunities for faster dissemination and sharing of service related information using a combination of: documents, computers, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities and facsimile machines. Consideration given to the security and business implications of interconnecting such facilities must include:

- a) vulnerabilities in systems where information extracted from the service (e.g. statistical data) is shared between different parts of the service providing organization;
- b) vulnerabilities of information in business communication systems, e.g. recording phone calls or conference calls, confidentiality of calls, storage of facsimiles, opening mail, distribution of mail;
- c) policy and appropriate controls to manage information sharing within the service providing organisation;
- d) restricting access to diary information relating to selected individuals, e.g. personnel working on sensitive projects;
- e) restricting selected facilities (e.g. functional mail boxes, document management systems) to specific categories of user;
- f) identifying the status of office information system users, e.g. employees of the organization or contractors in directories for the benefit of other users;

9.9 Electronic commerce services

Objective: To ensure that the integrity and availability of information electronically published through publicly available systems is considered.

9.9.1 Publicly available information

Control: The integrity of information being made available on a publicly available system must be protected to prevent unauthorised modification.

Software, data, and other information requiring a high level of integrity, being made available on a publicly available system (e.g. information on a Web server accessible via the Internet), must be protected by appropriate mechanisms, e.g. digital signatures. The publicly accessible system must be tested against weaknesses and failures prior to information being made available.

There must be a formal approval process before information is made publicly available. In addition, all input provided from the outside to the system must be verified and approved.

Electronic publishing systems, especially those that permit feedback and direct entering of information, must be carefully controlled so that:

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 1294 a) information is obtained in compliance with any data protection legislation;
- 1295 b) information input to, and processed by, the publishing system will be processed
- 1296 completely and accurately in a timely manner;
- 1297 c) sensitive information will be protected during collection, processing, and storage;
- 1298 d) access to the publishing system does not allow unintended access to networks to which
- 1299 the system is connected.

1300 **9.10 Monitoring**

1301 Objective: To detect unauthorised information processing activities.

1302 Systems must be monitored and information security events must be recorded. Operator logs and

1303 fault logging must be used to ensure information system problems are identified.

1304 The service providing organisation must comply with all relevant legal requirements applicable

1305 to its monitoring and logging activities.

1306 **9.10.1 Audit logging**

1307 Control: Audit logs recording user activities, exceptions, and information security events must be

1308 produced and kept for an agreed period (*Audit Logging Period*) to assist in future investigations

1309 and access control monitoring.

1310 Audit logs must include:

- 1311 a) user IDs;
- 1312 b) dates, times, and details of key events, e.g. log-on, failed log-on attempts and log-off;
- 1313 c) terminal identity or location if possible;
- 1314 d) records of rejected data and other resource access attempts;
- 1315 e) changes to system configuration;
- 1316 f) use of privileges;
- 1317 g) use of system utilities and applications (if such features are provided);
- 1318 h) files accessed and the kind of access according to the classification;
- 1319 i) network addresses and protocols according to the classification;
- 1320 j) alarms raised by the access control system;
- 1321 k) activation and de-activation of protection systems, such as anti-virus systems and
- 1322 intrusion detection systems.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

9.10.2 Monitoring system use

Control: Procedures for monitoring use of information processing facilities must be established by senior management and the results of the monitoring activities reviewed regularly.

The level of monitoring required and the intervals for individual facilities must be determined by a risk assessment. The service providing organisation must comply with all relevant legal requirements applicable to its monitoring activities. Events that must be monitored are:

a) authorised access to critical data such as:

- 1) the user ID;
- 2) the date and time of key events;
- 3) the types of events;
- 4) the files accessed;
- 5) the program/utilities used;

b) all privileged operations such as:

- 1) use of privileged accounts, e.g. supervisor, root, administrator;
- 2) system start-up and stop;
- 3) I/O device attachment/detachment;

c) unauthorised access attempts such as:

- 1) failed or rejected user actions;
- 2) failed or rejected actions involving data and other resources;
- 3) access policy violations and notifications for network gateways and firewalls;
- 4) alerts from proprietary intrusion detection systems;

d) system alerts or failures such as:

- 1) console alerts or messages;
- 2) system log exceptions;
- 3) network management alarms;
- 4) alarms raised by the access control system;

e) changes to, or attempts to change, system security settings and controls.

The above events must be reviewed at planned intervals (*Privileged Activities Review Interval*).

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

9.10.3 Protection of log information

Control: Logging facilities and log information must be protected against tampering and unauthorised access.

Controls should aim to protect against unauthorised changes and operational problems with the logging facility including:

- a) alterations to the message types that are recorded;
- b) log files being edited or deleted;
- c) storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence.

9.10.4 Administrator and operator logs

Control: System administrator and system operator activities must be logged.

Logs should include:

- a) the time at which an event (success or failure) occurred;
- b) information about the event (e.g. files handled) or failure (e.g. error occurred and corrective action taken);
- c) which account and which administrator or operator was involved;
- d) which processes were involved.

System administrator and operator logs must be reviewed at planned intervals (*Administrator Log Review Interval*).

9.10.5 Fault logging

Control: Faults must be logged, analysed, and appropriate action taken.

Faults reported by users or by system programs related to problems with information processing or communications systems must be logged. There must be clear rules for handling reported faults including:

- a) review of fault logs to ensure that faults have been satisfactorily resolved;
- b) review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorised.

It must be ensured that error logging is enabled, if this system function is available.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

1381 The level of logging required for individual systems must be determined by a risk assessment,
1382 taking performance degradation into account.

1383 **9.10.6 Clock synchronisation**

1384 Control: The clocks of all information processing systems (belonging to the service) must be
1385 synchronised with an agreed accurate time source.

1386 For computers or communication devices which have the capability to operate a real-time clock,
1387 this clock must be set to an agreed standard, e.g. Coordinated Universal Time (UTC) or local
1388 standard time. As some clocks are known to drift with time, there must be a procedure that
1389 checks for and corrects any significant variation.

1390

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

10. Access control

10.1 Business requirement for access control

Objective: To control access to information.

Access to information, information processing facilities, and business processes must be controlled on the basis of business and security requirements. Access control rules must take account of policies for information dissemination and authorisation.

10.1.1 Access control policy

Control: An access control policy must be established, documented, and reviewed based on business and security requirements for access.

Access control rules and rights for each user or group of users must be clearly stated in an access control policy. Access controls are both logical and physical and these should be implemented together since they complement each other. Users and service providers must be given a clear statement of the business requirements to be met by access controls.

The policy must take account of the following:

- a) security requirements of individual business applications;
- b) identification of all information related to the business applications and the risks the information is facing;
- c) policies for information dissemination and authorisation, e.g. the need to know principle and security levels and classification of information;
- d) consistency between the access control and information classification policies of different systems and networks;
- e) relevant legislation and any contractual obligations regarding protection of access to data or services;
- f) standard user access profiles for common job roles;
- g) management of access rights in a distributed and networked environment which recognises all types of connections available;
- h) segregation of access control roles, e.g. access request, access authorisation, access administration;
- i) requirements for formal authorisation of access requests;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

j) requirements for periodic review of access controls;

k) removal of access rights.

The policy should be reviewed at planned intervals (*User Access Control Policy Review Interval*).

10.2 User access management

Objective: To ensure authorised user access and prevent unauthorised access to information systems.

Formal procedures must be in place to control the allocation of access rights to information systems and services.

The procedures must cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given to the need to control the allocation of privileged access rights, which allow users to override system controls.

10.2.1 User registration

Control: There must be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems (belonging to the service) and services.

The access control procedure for user registration and de-registration must include:

a) using unique user IDs to enable users to be linked to and held responsible for their actions; the use of group IDs should only be permitted where they are necessary for business or operational reasons, and must be approved and documented;

b) checking that the user has authorisation from relevant management for the use of the information system or service;

c) checking that the level of access granted is appropriate to the business purpose and is consistent with organisational security policy, e.g. it does not compromise segregation of duties;

d) giving users a written statement of their access rights;

e) requiring users to sign statements indicating that they understand the conditions of access;

f) ensuring service providers do not provide access until authorisation procedures have been completed;

g) maintaining a formal record of all persons registered to use the service;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- h) immediately removing or blocking access rights of users who have changed roles or jobs or have left;
- i) checking for, and removing or blocking, redundant user IDs and accounts;
- j) ensuring that redundant user IDs are not issued to other users.

10.2.2 Privilege management

Control: The allocation and use of privileges must be restricted and controlled.

The allocation of privileges must be controlled through a formal authorisation process. The following steps must be implemented:

- a) the access privileges associated with each system product, e.g. operating system, database management system and each application, and the users to which they need to be allocated must be identified and documented;
- b) Privileges must be allocated to individuals on a need-to-use basis for the normal operating and on an event-by-event basis for exceptional situations;
- c) an authorisation process and a record of all privileges allocated must be maintained. Privileges must not be granted until the authorisation process is complete;
- d) privileges should be assigned to a different user ID from those used for normal business use.

10.2.3 User password management

Control: The allocation of passwords must be controlled through a formal management process.

The process must include the following requirements:

- a) users must be required to sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group;
- b) when users are required to maintain their own passwords they must be provided initially with a secure temporary password, which they are forced to change immediately;
- c) establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password;
- d) temporary passwords must be given to users in a secure manner;
- e) temporary passwords must be unique to an individual and should not be guessable;
- f) users must acknowledge receipt of passwords;
- g) passwords must never be stored on computer systems in an unprotected form;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- h) default vendor passwords must be altered following installation of systems or software.

10.2.4 Review of user access rights

Control: Management must review users' access rights at regular intervals using a formal process.

The review of access rights according to the following points must be in place:

- a) users' access rights must be periodically reviewed (*User Access Rights Review Interval*);
- b) user access rights must be reviewed and re-allocated when moving from one employment to another within the same central bank;
- c) authorisations for special privileged access rights must be periodically reviewed (*Privileged User Access Rights Review Interval*);
- d) changes to privileged accounts must be logged for periodic review (*Privileged Account Changes Logging Period*).

10.3 User responsibilities

Objective: To prevent unauthorised user access, and compromise or theft of information and information processing facilities.

As the co-operation of authorised users is essential for effective security they must be made aware of their responsibilities for maintaining effective access controls.

A clear desk and clear screen policy must be implemented to reduce the risk of unauthorised access or damage to papers, media, and information processing facilities.

10.3.1 Password use

Control: Users must be required to follow the password policy and good security practices in the selection and use of passwords. The software providing the authentication facilities should support parameters¹⁶ to ensure strong passwords.

All users must at least:

- a) keep passwords confidential;

¹⁶ Authentication parameters define settings required for login security. Examples are: Password Expiry (defining the maximum number of calendar days a password is valid), Minimum Account Name / Password Length (minimum number of characters allowed for a account name/password), Password Complexity (defining the minimum complexity of the password – e.g. at least one uppercase character, one symbol and one number), Password Reuse (defines the number of password changes before an old password can be reused), Maximum Login Attempts (maximum number of failed login attempts before a user account is locked by the system)

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- b) avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved;
- c) change passwords whenever there is any indication of possible system or password compromise;
- d) not include passwords in any automated log-on process, e.g. stored in a macro or function key;
- e) not share individual user passwords.

In accordance with the password policy the service must ensure that:

- a) user account names have at least the minimum length;
- b) quality passwords with sufficient complexity and minimum length (*Minimum Password Length*) are selected;
- c) password change is enforced after expiry (*Password Expiry Period*) and at the first log-on for temporary passwords;
- d) reuse or recycle a certain number of old passwords is prevented;
- e) user accounts are locked after a certain number of failed login attempts (*Maximum Logon Attempts*).

10.3.2 Unattended user equipment

Control: Users must ensure that unattended equipment has appropriate protection.

All users must be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users must be advised to:

- a) terminate active sessions when finished, unless they can be secured by a locking mechanism, e.g. a password protected screen saver;
- b) log-off from mainframe computers, servers, and office PCs when the session is finished (i.e. not just switch off the PC screen or terminal);
- c) secure PCs or terminals from unauthorised use by a key lock or an equivalent control, e.g. password access, when not in use.

10.3.3 Clear desk and clear screen policy

Control: A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities must be adopted.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

The clear desk and clear screen policy must take into account the information classifications, legal and contractual requirements, and the corresponding risks and cultural aspects. The following measures must be implemented:

- a) sensitive or critical business information, e.g. on paper or on electronic storage media, must be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated;
- b) computers and terminals must be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and must be protected by key locks, passwords or other controls when not in use;
- c) incoming and outgoing mail points and unattended facsimile machines must be protected;
- d) unauthorised use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) should be prevented;
- e) documents containing sensitive or classified information must be removed from printers immediately.

10.4 Network access control

Objective: To prevent unauthorised access to networked services.

Access to both internal and external networked services must be controlled.

User access to networks and network services must not compromise the security of the network services by ensuring:

- a) appropriate interfaces are in place between the network supporting the service and networks operated by other organisations, and public networks;
- b) appropriate authentication mechanisms are applied for users and equipment;
- c) control of user access to information services is enforced.

10.4.1 Policy on use of network services

Control: Users must only be provided with access to those services that they have been specifically authorised to use.

A policy must be formulated concerning the use of networks and network services. This policy must cover:

- a) the networks and network services which are allowed to be accessed;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- b) authorisation procedures for determining who is allowed to access which networks and networked services;
- c) management controls and procedures to protect access to network connections and network services;
- d) the means used to access networks and network services (e.g. the conditions for allowing dial-up access to an Internet service provider or remote system).

The policy on the use of network services must be consistent with the business access control policy.

10.4.2 User authentication for external connections

Control: Strong authentication methods (e.g. hardware token, certificates) must be used to control access by remote users¹⁷.

A formal procedure for managing and controlling remote connections must be established. Following controls must be in place:

- a) Remote connections must only be activated when absolutely necessary and ask for re-authentication after a defined period of inactivity (*Remote Connections Idle Interval*);
- b) authentication by the use of cryptographic techniques and two-factor authentication;
- c) If used, call-back facilities, must follow strict controls and procedures; call forwarding processes should only be used if absolutely necessary;
- d) A logging of all remote connections must be in place.

If remote connections are used for Third Party/vendor support

- a) the decision to allow remote access by TP/vendors is made case by case by the senior management and substantiated by a risk analysis;
- b) remote access must be allowed only for a limited period of time and only in case support can not be provided on site in time;
- c) contractual provisions for remote access must exist and must also be laid down as regards the commitment of vendors' personnel to the secrecy of data;
- d) access should be limited to read-only for diagnostic purposes. However, if more privileged access is required (e.g. in emergency cases) then the remote connection activity related to critical functions must be monitored;

¹⁷ a user trying to establish a connection from a location outside of the information processing facilities

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- e) if used, call-back facilities, must follow strict controls and procedures; call forwarding processes should only be used if absolutely necessary;
- f) a logging of all remote connections must be in place.

10.4.3 Equipment identification in networks

Control: Automatic equipment identification must be implemented as a means to authenticate connections from specific locations and equipment.

10.4.4 Remote diagnostic and configuration port protection

Control: Physical and logical access to diagnostic and configuration ports must be controlled.

Potential controls for the access to diagnostic and configuration ports include the use of a key lock and supporting procedures to control physical access to the port.

Ports, services, and similar facilities installed on a computer or network facility, which is not specifically required for business functionality, must be disabled or removed.

10.4.5 Segregation in networks

Control: Groups of information services, users, and information systems must be segregated from a logical point of view.

The security of the network must be controlled by dividing it into separate (physical or logical) network domains. The domains should be defined based on a risk assessment and the different security requirements within each of the domains.

The criteria for segregation of networks into domains must be based on the access control policy and access requirements, and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology.

In addition, segregation of networks must be based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption.

10.4.6 Network connection control

Control: The capability of users to connect to the network must be restricted, in line with the access control policy and requirements of the business applications.

The network access rights of users must be maintained and updated as required by the access control policy.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

1625 Linking network access rights to certain times of day or dates should be implemented.

1626 **10.4.7 Network routing control**

1627 Control: Routing controls must be implemented for networks to ensure that computer connections
1628 and information flows do not breach the access control policy of the business applications.

1629 Routing controls must be based on positive checks of source and destination address.

1630 **10.5 Operating system access control**

1631 Objective: To prevent unauthorised access to operating systems.

1632 Security facilities must be used to restrict access to operating systems to authorised users. Access
1633 must be granted based on the “need-to-have” principle.

1634 **10.5.1 Secure log-on procedures**

1635 Control: Access to operating systems must be controlled by a secure log-on procedure.

1636 The procedure for logging into an operating system must be designed to minimise the opportunity
1637 for unauthorised access. The log-on procedure must therefore disclose the minimum of
1638 information about the system, in order to avoid providing an unauthorised user with any
1639 unnecessary assistance. A good log-on procedure must:

- 1640 a) not display system or application identifiers until the log-on process has been
1641 successfully completed;
- 1642 b) display a general notice warning that the computer should only be accessed by authorised
1643 users;
- 1644 c) not provide help messages during the log-on procedure that would aid an unauthorised
1645 user;
- 1646 d) validate the log-on information only on completion of all input data. If an error condition
1647 arises, the system should not indicate which part of the data is correct or incorrect;
- 1648 e) limit the number of unsuccessful log-on attempts allowed, to four bad log-on attempts,
1649 and consider:
 - 1650 1. recording unsuccessful and successful attempts;
 - 1651 2. disconnecting connections;
 - 1652 3. sending an alarm message to the system console if the maximum number of log-
1653 on attempts is reached.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- f) limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on;
- g) display the following information on completion of a successful log-on:
 - 1. date and time of the previous successful log-on;
 - 2. details of any unsuccessful log-on attempts since the last successful log-on;
- h) not display the password being entered or consider hiding the password characters by symbols;
- i) not transmit passwords in clear text over a network.
- j) forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorisation.

10.5.2 User identification and authentication

Control: All users must have a unique identifier (user ID) for their personal use only, and a suitable authentication technique must be chosen to substantiate the claimed identity of a user.

This control must be applied for all types of users (including technical support personnel, operators, network administrators, system programmers, and database administrators).

In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used. Approval by management must be documented for such cases. Additional controls are required to maintain accountability.

Generic IDs for use by an individual should only be allowed either where the functions accessible or actions carried out by the ID do not need to be traced (e.g. read only access), or where there are other controls in place (e.g. password for a generic ID only issued to one staff at a time and logging such instance).

Strong authentication and identity verification is required for staff having access to processing facilities via a remote connection (i.e. via unsecured networks), authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, must be used.

10.5.3 Password management system

Control: Systems for managing passwords must be interactive and must ensure quality passwords in line with the security control 10.3.1.

A password management system must:

- a) enforce the use of individual user IDs to maintain accountability;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- b) allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;
- c) enforce a choice of quality passwords;
- d) enforce password changes;
- e) force users to change temporary passwords at the first log-on;
- f) maintain a record of previous user passwords for a defined minimum period of time and prevent re-use (*Period for Keeping Previous Passwords*);
- g) not display passwords on the screen when being entered;
- h) store password files separately from application system data;
- i) store and transmit passwords in protected (e.g. encrypted or hashed) form.

10.5.4 Use of system utilities

Control: The use of utility programs (e. g. security tools, SQL, QMF, APF) that might be capable of overriding system and application controls must be restricted and tightly controlled.

The following measures for the use of system utilities must be implemented:

- a) use of identification, authentication, and authorisation procedures for system utilities;
- b) segregation of system utilities from applications software;
- c) limitation of the use of system utilities to the minimum practical number of trusted, authorised users;
- d) authorisation for ad hoc use of systems utilities;
- e) logging of all use of system utilities;
- f) defining and documenting of authorisation levels for system utilities;
- g) removal or disabling of all unnecessary software based utilities and system software;
- h) not making system utilities available to users who have access to applications on systems where segregation of duties is required.

10.5.5 Session time-out

Control: Inactive sessions must shut down after a defined period of inactivity to prevent unauthorised access.

A time-out facility must clear the session screen and also, possibly later, close both application and network sessions after a defined period of inactivity (*Session Time-out*).

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

10.5.6 Limitation of connection time

Control: Restrictions on connection times must be considered to provide additional security for high-risk applications.

Connection time controls should be considered, especially from high risk locations, e.g. external areas that are outside the organization's security management. Examples of such restrictions include:

- a) using predetermined time slots;
- b) restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation;
- c) considering re-authentication at timed intervals.

10.6 Application and information access control

Objective: To prevent unauthorised access to information held in application systems.

Security facilities must be used to restrict access to and within application systems.

Logical access to application software and information must be restricted to authorised users.

10.6.1 Information access restriction

Control: Access to information and application system functions must be restricted in accordance with the defined access control policy.

Restrictions to access must be based on individual business application requirements. The access control policy must also be consistent with the organisational access policy.

The following measures must be implemented in order to support access restriction requirements:

- a) providing menus to control access to application system functions;
- b) controlling the access rights of users, e.g. read, write, delete, and execute;
- c) controlling access rights of other applications;
- d) ensuring that outputs from application systems handling sensitive information contain only the information relevant to the use of the output and are sent only to authorised terminals and locations; this must include periodic reviews of such outputs to ensure that redundant information is removed (*Information Access Restriction Review Interval*).

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

10.6.2 Sensitive system isolation

Control: The service must be operated in a dedicated (isolated) computing environment.

A dedicated environment could be achieved using physical or logical methods.

10.7 Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

The protection required must be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of teleworking the respective site must be appropriately protected and it must be ensured that suitable arrangements are in place for this way of working.

10.7.1 Mobile computing and communications

Control: A formal policy must be in place, and security measures must be adopted to protect against the risks of using mobile computing and communication facilities.

The mobile computing policy must include the requirements for physical protection, access controls, cryptographic techniques, backups, and virus protection. This policy must also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places.

Procedures against malicious software must be in place and be kept up to date.

Backups of critical business information must be taken regularly. Equipment must be available to enable the quick and easy backup of information. These backups must be given adequate protection against, e.g., theft or loss of information.

Suitable protection must be given to the use of mobile facilities connected to networks. Remote access to business information across public network using mobile computing facilities must only take place after successful identification and two-factor authentication.

Mobile computing facilities must also be physically protected against theft especially when left outside the hosting premises, for example, in cars and other forms of transport, hotel rooms, conference centres, and meeting places. A specific procedure taking into account legal, insurance and other security requirements of the service providing organisation must be established for cases of theft or loss of the mobile computing facilities. Equipment carrying important, sensitive, and/or critical business information must not be left unattended and, where possible, should be physically locked away, or have special locks (e. g. putting it in a safe) that secure the equipment.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

1774 Training must be arranged for personnel using mobile computing to raise their awareness on the
1775 additional risks resulting from this way of working and the controls that should be implemented.

1776 10.7.2 Teleworking

1777 Control: A policy, operational plans and procedures must be developed and implemented for
1778 teleworking activities.

1779 Teleworking activities must both be authorised and controlled by management, and it must be
1780 ensured that suitable arrangements are in place for this way of working.

1781 The following matters should be considered:

- 1782 a) the existing physical security of the teleworking site, taking into account the physical
1783 security of the building and the local environment;
- 1784 b) the proposed physical teleworking environment;
- 1785 c) the communications security requirements, taking into account the need for remote
1786 access, the sensitivity of the information that will be accessed and pass over the
1787 communication link and the sensitivity of the internal system;
- 1788 d) the threat of unauthorised access to information or resources from other persons using the
1789 accommodation, e.g. family and friends;
- 1790 e) the use of home networks and requirements or restrictions on the configuration of
1791 wireless network services;
- 1792 f) policies and procedures to prevent disputes concerning rights to intellectual property
1793 developed on privately owned equipment;
- 1794 g) access to privately owned equipment (to check the security of the machine or during an
1795 investigation), which may be prevented by legislation;
- 1796 h) software licensing agreements that are such that the service providing organisation may
1797 become liable for licensing for client software on workstations owned privately by
1798 employees, contractors or third party users;
- 1799 i) anti-virus protection and firewall requirements.

1800 The guidelines and arrangements to be implemented should include:

- 1801 a) the provision of suitable equipment and storage furniture for the teleworking activities,
1802 where the use of privately owned equipment that is not under the control of the service
1803 providing organisation is not allowed;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 1804 b) a definition of the work permitted, the hours of work, the classification of information
1805 that may be held and the internal systems and services that the teleworker is authorised to
1806 access;
- 1807 c) the provision of suitable communication equipment, including methods for securing
1808 remote access;
- 1809 d) physical security;
- 1810 e) rules and guidance on family and visitor access to equipment and information;
- 1811 f) the provision of hardware and software support and maintenance;
- 1812 g) the provision of insurance;
- 1813 h) the procedures for backup and business continuity;
- 1814 i) audit and security monitoring;
- 1815 j) revocation of authority and access rights, and the return of equipment when the
1816 teleworking activities are terminated.
- 1817

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

11. Information systems acquisition, development and maintenance

11.1 Security requirements of information systems

Objective: To ensure that security is an integral part of information systems.

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements must be identified, agreed prior to the development and/or implementation of information systems and documented as part of the overall business case for an information system.

11.1.1 Security requirements analysis and specification

Control: Statements of business requirements for new information systems, or enhancements to existing information systems must specify the requirements for security controls.

Security requirements and controls must reflect the business value of the information assets involved, and the potential business damage, which might result from a failure or absence of security.

System requirements for information security and processes for implementing security must be integrated in the early stages of information system projects. Controls introduced at the design stage are significantly cheaper to implement and maintain than those included during or after implementation.

If products are purchased, a formal testing and acquisition process must be followed. Contracts with the supplier must address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement then the risk introduced and associated controls must be reconsidered prior to purchasing the product. Where additional functionality is supplied and causes a security risk, this must be disabled or the proposed control structure must be reviewed to determine if advantage can be taken of the enhanced functionality available.

11.2 Correct processing in applications

Objective: To prevent errors, loss, unauthorised modification or misuse of information in applications.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Controls must be designed into applications, including user developed applications to ensure correct processing. These controls must include the validation of input data, internal processing and output data.

Additional controls may be required for components of the service that process, or have an impact on, sensitive, valuable or critical information. Such controls must be determined on the basis of a risk assessment.

11.2.1 Input data validation

Control: Data input to applications must be validated to ensure that this data is correct and appropriate.

Checks must be applied to the input of business transactions, standing data (e.g. names and addresses, credit limits, customer reference numbers), and parameter tables (e.g. opening hours). The following checks should be implemented:

- a) dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors:
 1. out-of-range values;
 2. invalid characters in data fields;
 3. missing or incomplete data;
 4. exceeding upper and lower data volume limits;
 5. unauthorised or inconsistent control data;
- b) periodic review of the content of key fields or data files to confirm their validity and integrity;
- c) procedures for responding to validation errors;
- d) procedures for testing the plausibility of the input data;
- e) creating a log of the activities involved in the data input process.

11.2.2 Control of internal processing

Control: Validation checks must be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

The design and implementation of applications should ensure that the risks of processing failures leading to a loss of integrity are minimised. Specific areas to consider include:

- a) the use of add, modify, and delete functions to implement changes to data;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- b) the procedures to prevent programs running in the wrong order or running after failure of prior processing;
 - c) the use of appropriate programs to recover from failures to ensure the correct processing of data;
 - d) protection against attacks using buffer overruns/overflows.
- A checklist must be prepared, activities documented, and the results must be kept secure. Examples of checks that can be incorporated include the following:
- a) session or batch controls, to reconcile data file balances after transaction updates;
 - b) balancing controls, to check opening balances against previous closing balances, namely:
 - 1. run-to-run controls;
 - 2. file update totals;
 - 3. program-to-program controls;
 - c) validation of system-generated input data;
 - d) checks on the integrity, authenticity or any other security feature of data or software downloaded, or uploaded, between central and remote computers;
 - e) hash totals of records and files;
 - f) checks to ensure that application programs are run at the correct time;
 - g) checks to ensure that programs are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved;
 - h) creating a log of the activities involved in the processing.

11.2.3 Message integrity

Control: Requirements for ensuring authenticity and protecting message integrity in applications must be identified, and controls identified and implemented.

An assessment of security risks must be carried out to determine if message integrity is required and to identify the most appropriate method of implementation.

11.2.4 Output data validation

Control: Data output from an application must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

Output validation may include:

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 1906 a) plausibility checks to test whether the output data is reasonable;
- 1907 b) reconciliation control counts to ensure processing of all data;
- 1908 c) procedures for responding to output validation tests;
- 1909 d) creating a log of activities in the data output validation process.

1910 **11.3 Cryptographic controls**

1911 Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic
1912 means.

1913 A policy must be developed on the use of cryptographic controls¹⁸. Key management must be in
1914 place to support the use of cryptographic techniques.

1915 **11.3.1 Policy on the use of cryptographic controls**

1916 Control: A policy on the use of cryptographic controls for protection of information must be
1917 developed and implemented.

1918 When developing a cryptographic policy the following measures must be implemented:

- 1919 a) the management approach towards the use of cryptographic controls across the service,
1920 including the general principles under which business information must be protected;
- 1921 b) based on a risk assessment, the required level of protection should be identified taking
1922 into account the type, strength, and quality of the encryption algorithm required;
- 1923 c) the use of encryption for protection of sensitive information transported by mobile or
1924 removable media, devices or across communication lines;
- 1925 d) the approach to key management, including methods to deal with the protection of
1926 cryptographic keys and the recovery of encrypted information in the case of lost,
1927 compromised or damaged keys;
- 1928 e) roles and responsibilities, e.g. who is responsible for:
- 1929 1. the implementation of the policy;
- 1930 2. the key management, including key generation;
- 1931 f) the standards to be adopted for the effective implementation throughout the service
1932 (which solution is used for which business processes);

¹⁸ Cryptographic controls can be used to achieve different security objectives, e.g.: a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted; b) integrity/authenticity: using digital signatures or message authentication codes to protect the authenticity and integrity of stored or transmitted sensitive or critical information; c) non-repudiation: using cryptographic techniques to obtain proof of the occurrence or non occurrence of an event or action.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- g) the impact of using encrypted information on controls that rely upon content inspection (e.g. virus detection).

When implementing the cryptographic policy for the service, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of Europe and to the issues of trans-border flow of encrypted information.

11.3.2 Key management

Control: Key management must be in place to support the use of cryptographic techniques.

All cryptographic keys must be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorised disclosure. Equipment used to generate, store and archive keys must be physically protected.

A key management system must be based on an agreed set of standards, procedures, and secure methods for:

- a) generating keys for different cryptographic systems and different applications;
- b) generating and obtaining public key certificates;
- c) distributing keys to intended users, including how keys should be activated when received;
- d) storing keys, including how authorised users obtain access to keys;
- e) changing or updating keys including rules on when keys should be changed and how this will be done;
- f) dealing with compromised keys;
- g) revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves (in which case keys should also be archived);
- h) recovering keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information;
- i) archiving keys, e.g. for information archived or backed up;
- j) destroying keys;
- k) logging and auditing of key management related activities.

In order to reduce the likelihood of compromise, activation, and deactivation dates for keys must be defined so that the keys can only be used for a limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used, and the perceived risk.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

1965 In addition to securely managing secret and private keys, the authenticity of public keys must
1966 also be implemented.

1967 **11.4 Security of system files**

1968 Objective: To ensure the security of system files.

1969 Access to system files and program source code must be controlled. Ensure that IT projects and
1970 support activities conducted in a secure manner. Care must be taken to avoid exposure of
1971 sensitive data in test environments.

1972 **11.4.1 Control of operational software**

1973 Control: There must be procedures in place to control the installation of software components on
1974 operational systems.

1975 To minimise the risk of corruption to operational systems, the following measures must be
1976 implemented to control changes:

- 1977 a) the updating of the operational software, applications, and program libraries must only be
1978 performed by trained administrators upon management authorisation;
- 1979 b) operational systems should only hold approved executable code, and not development
1980 code or compilers;
- 1981 c) applications and operating system software must only be implemented after extensive
1982 and successful testing; the tests must include tests on usability, security, effects on other
1983 systems and user-friendliness, and should be carried out on separate systems; it must be
1984 ensured that all corresponding program source libraries have been updated;
- 1985 d) a configuration control system must be used to keep control of all implemented software
1986 as well as the system documentation;
- 1987 e) a rollback strategy must be in place before changes are implemented;
- 1988 f) an audit log must be maintained of all updates to operational program libraries;
- 1989 g) the previous version of application software must be retained as a contingency measure;
- 1990 h) old versions of software (including system management software, scripts) must be
1991 archived, together with all required information and parameters, procedures,
1992 configuration details, and supporting software for as long as the data is retained in
1993 archive.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

Vendor supplied software used in operational systems must be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The senior management must consider the risks of relying on unsupported software.

Any decision to upgrade to a new release must take into account the business requirements for the change, and the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version. Software patches must be applied when they can help to remove or reduce security weaknesses.

Physical or logical access must only be given to suppliers for support purposes when necessary, and with management approval. The supplier's activities must be monitored.

11.4.2 Protection of system test data

Control: Test data must be selected carefully. If sensitive information is used for testing purposes, it must be protected and controlled.

The use of operational databases containing personal information or any other sensitive information for testing purposes should be avoided. If personal or otherwise sensitive information is used for testing purposes, all sensitive details and content must be removed or modified beyond recognition before use. The following guidelines must be applied to protect operational data, when used for testing purposes:

- a) the access control procedures, which apply to operational application systems, should also apply to test application systems;
- b) there must be separate authorisation each time operational information is copied to a test application system;
- c) operational information must be erased from a test application system immediately after the testing is complete;
- d) the copying and use of operational information must be logged to provide an audit trail.

11.4.3 Access control to program source code

Control: Access to program source code must be restricted according to the senior management's decision.

Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) must be strictly controlled, in order to prevent the introduction of unauthorised functionality and to avoid unintentional changes. The following measures must then be implemented to control access to such program source libraries/directories in order to reduce the potential for corruption of computer programs:

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 2026 a) where possible, program source libraries/directories should not be held in operational
2027 systems;
- 2028 b) the program source code and the program source libraries/directories must be managed
2029 according to established procedures;
- 2030 c) support personnel must not have unrestricted access to program source
2031 libraries/directories;
- 2032 d) the updating of program source libraries/directories and associated items, and the issuing
2033 of program sources to programmers must only be performed after authorisation has been
2034 received;
- 2035 e) program listings must be held in a secure environment;
- 2036 f) an audit log must be maintained of all access to program source libraries/directories;
- 2037 g) maintenance and copying of program source libraries/directories must be subject to strict
2038 change control procedures.

2039 **11.5 Security in development and support processes**

2040 Objective: To maintain the security of application system software and information. Project and
2041 support environments must be strictly controlled.

2042 **11.5.1 Change control procedures**

2043 Control: The implementation of changes¹⁹ must be controlled by the use of formal change control
2044 procedures.

2045 Formal change control procedures must be documented and enforced in order to minimise the
2046 corruption of information systems. Introduction of new systems and major changes to existing
2047 systems must follow a formal process of documentation, specification, testing, quality control,
2048 and managed implementation.

2049 This process must include a risk assessment, analysis of the impacts of changes, and specification
2050 of security controls needed. This process must also ensure that existing security and control
2051 procedures are not compromised, that support programmers are given access only to those parts
2052 of the system necessary for their work, and that formal agreement and approval for any change is
2053 obtained.

2054 The change procedures must include:

- 2055 a) identification and recording of changes;

¹⁹ These changes include not only software, but hardware and procedures as well.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 2056 b) planning and testing of changes;
- 2057 c) assessment of the potential impacts, including security impacts, of such changes;
- 2058 d) maintaining a record of agreed authorisation levels;
- 2059 e) ensuring change requests are submitted by authorised users;
- 2060 f) reviewing controls and integrity procedures to ensure that they will not be compromised
- 2061 by the changes;
- 2062 g) identifying all software, information, database entities, and hardware that require
- 2063 amendment;
- 2064 h) obtaining formal approval for detailed proposals before work commences;
- 2065 i) ensuring authorised users accept changes prior to implementation;
- 2066 j) ensuring that the system documentation set is updated on the completion of each change
- 2067 and that old documentation is archived or disposed of;
- 2068 k) ensuring that operating documentation and user procedures are changed as necessary to
- 2069 remain appropriate;
- 2070 l) maintaining an audit trail of all change requests;
- 2071 m) maintaining a version control for all software updates;
- 2072 n) ensuring that the implementation of changes takes place at the right time and does not
- 2073 disturb the business processes involved;
- 2074 o) planning for recovery and fallback;
- 2075 p) ensuring that documentation describing how to proceed in the event an emergency
- 2076 change/patch has to be implemented is in place;
- 2077 q) ensuring that all people that might be affected by or involved in implementing a change
- 2078 are informed about the implementation date.

2079 11.5.2 Technical review of applications after operating system changes

2080 Control: Before operating system software is changed, all business-critical applications must be

2081 reviewed and tested to ensure that there is no adverse impact on business operations or security.

2082 This process must cover:

- 2083 a) review of application control and integrity procedures to ensure that they have not been
- 2084 compromised by the operating system changes;
- 2085 b) ensuring that the annual support plan and budget will cover reviews and system testing
- 2086 resulting from operating system changes;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 2087 c) ensuring that notification of operating system changes is provided in time to allow tests
2088 and reviews to take place before implementation;
2089 d) ensuring that appropriate changes are made to the business continuity plans.

2090 11.5.3 Restrictions on changes to software packages

2091 Control: Modifications to software packages must be discouraged, limited to necessary changes,
2092 and all changes must be strictly controlled.

2093 As far as possible, and practicable, vendor-supplied software packages should be used without
2094 modification. Where a software package needs to be modified the following points must be
2095 considered:

- 2096 a) the risk of built-in controls and integrity processes being compromised;
2097 b) whether the consent of the vendor should be obtained;
2098 c) the possibility of obtaining the required changes from the vendor as standard program
2099 updates;
2100 d) the impact if the service providing organisation becomes responsible for the future
2101 maintenance of the software as a result of changes.

2102 If changes are necessary the original software must be retained and the changes applied to a
2103 clearly identified copy. A software update management process must be implemented to ensure
2104 the most up-to-date approved patches and application updates are installed for all authorised
2105 software. All changes must be fully tested and documented, so that they can be reapplied if
2106 necessary to future software upgrades.

2107 11.5.4 Outsourced software development

2108 Control: Outsourced software development must be supervised and monitored

2109 Where software development is outsourced, the following points must be considered:

- 2110 a) licensing arrangements, code ownership, and intellectual property rights;
2111 b) certification of the quality and accuracy of the work carried out;
2112 c) escrow arrangements in the event of failure of the third party;
2113 d) rights of access for audit of the quality and accuracy of work done;
2114 e) If open source software is used the following controls must be applied:
2115 1. downloaded from a trusted source
2116 2. integrity check, e. g. MD5 verification

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

2117 3. verifying the general licensing arrangements (e.g. GNU license)

2118 f) contractual requirements for quality and security functionality of code;

2119 g) testing before installation to detect malicious and Trojan code.

2120 11.5.5 Information leakage

2121 Control: Opportunities for information leakage must be prevented.

2122 As far as possible, and practicable, is has to be ensured that covert channels²⁰ and Trojan codes²¹
2123 are not introduced into a new or upgraded system.

2124 This control is redundant with 11.5.1 Change control procedures, 9.4.1 Controls against
2125 malicious code and 9.4.2 Controls against mobile code.

2126 11.6 Technical Vulnerability Management

2127 Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

2128 Technical vulnerability management must be implemented in an effective, systematic, and
2129 repeatable way with measurements taken to confirm its effectiveness. These considerations must
2130 include operating systems, and any other applications in use.

2131 11.6.1 Control of technical vulnerabilities

2132 Control: Timely information about technical vulnerabilities of information systems being used
2133 must be obtained, the exposure of the service to such vulnerabilities evaluated, and appropriate
2134 measures taken to address the associated risk.

2135 A current and complete inventory of assets is a prerequisite for effective technical vulnerability
2136 management. Specific information needed to support technical vulnerability management
2137 includes the software vendor, version numbers, current state of deployment (e.g. what software is
2138 installed on what systems), and the person(s) within the organisation responsible for the software.

2139 Timely action must be taken in response to the identification of potential technical vulnerabilities.
2140 The following measures must be implemented to establish an effective management process for
2141 technical vulnerabilities:

2142 a) roles and responsibilities associated with technical vulnerability management, including
2143 vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any
2144 other coordination activities must be clearly defined and established;

²⁰ A covert channel can expose information by some indirect and obscure means.

²¹ Trojan code is designed to affect a system in a way that is not authorised.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 2145 b) information resources that will be used to identify technical vulnerabilities and to
2146 maintain awareness about them must be identified for software and other technology
2147 (based on the asset inventory list); these information resources must be updated based on
2148 changes in the inventory, or when other new or useful resources are found;
- 2149 c) a timeline must be defined to react to notifications of potential technical vulnerabilities;
- 2150 d) once a potential technical vulnerability has been identified, the senior management must
2151 identify the associated risks and the actions to be taken; such action could involve
2152 patching of vulnerable systems and/or applying other controls;
- 2153 e) depending on how urgently a technical vulnerability needs to be addressed, the action
2154 taken must be carried out according to the controls related to change management or by
2155 following information security incident response procedures;
- 2156 f) if a patch is available, the risks associated with installing the patch must be assessed (the
2157 risks posed by the vulnerability should be compared with the risk of installing the patch);
- 2158 g) patches must be tested and evaluated before they are installed to ensure they are effective
2159 and do not result in side effects that cannot be tolerated; if no patch is available, other
2160 controls should be implemented, such as:
- 2161 1. turning off services or capabilities related to the vulnerability;
- 2162 2. adapting or adding access controls, e.g. firewalls, at network borders;
- 2163 3. increased monitoring to detect or prevent actual attacks;
- 2164 4. raising awareness of the vulnerability;
- 2165 h) an audit log must be kept for all procedures undertaken;
- 2166 i) the technical vulnerability management process must be monitored and evaluated in
2167 order to ensure its effectiveness and efficiency;
- 2168 j) system components at high risk must be addressed first.
- 2169

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

12. Information security incident management

12.1 Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Formal event reporting and escalation procedures must be in place. All employees, contractors and third party users must be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of assets. They are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

12.1.1 Reporting information security events

Control: Information security events must be reported through appropriate management channels as quickly as possible.

A formal information security event reporting procedure must be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event. A point of contact must be established for the reporting of information security events. It must be ensured that this point of contact is well known, is always available and is able to provide adequate and timely response.

All employees, contractors and third party users must be made aware of their responsibility to report any information security events as quickly as possible. They must also be aware of the procedure for reporting information security events and the point of contact. The reporting procedures must include:

- a) suitable feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed;
- b) information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in case of an information security event;
- c) the correct behaviour to be undertaken in case of an information security event, i.e.:
 - 1. noting all important details (e.g. type of non-compliance or breach, occurring malfunction, messages on the screen, strange behaviour) immediately;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

2199 2. not carrying out any own action, but immediately reporting to the point of
2200 contact;

2201 d) reference to an established formal disciplinary process for dealing with employees,
2202 contractors or third party users who commit security breaches.

2203 **12.1.2 Reporting security weaknesses**

2204 Control: All employees, contractors and third party users must be required to note and report any
2205 observed or suspected security weaknesses in systems or services.

2206 All employees, contractors and third party users must report these matters either to the
2207 appropriate point of contact as quickly as possible in order to prevent information security
2208 incidents. The reporting mechanism should be easy, accessible, and available. They must be
2209 informed that they should not, in any circumstances, attempt to prove a suspected weakness.

2210 **12.2 Management of information security incidents and improvements**

2211 Objective: To ensure a consistent and effective approach is applied to the management of
2212 information security incidents.

2213 Responsibilities must be clearly allocated and procedures must be in place to handle information
2214 security events and weaknesses effectively once they have been reported. A process of continual
2215 improvement must be applied to the response to, monitoring, evaluating, and overall management
2216 of information security incidents.

2217 Where evidence is required, it must be collected to ensure compliance with legal requirements.

2218 **12.2.1 Responsibilities and procedures**

2219 Control: Management responsibilities and procedures must be established to ensure a quick,
2220 effective, and orderly response to information security incidents.

2221 In addition to reporting of information security events and weaknesses, the monitoring of
2222 systems, alerts, and vulnerabilities must be used to detect information security incidents. The
2223 following measures for information security incident management procedures must be
2224 implemented:

2225 a) procedures must be established to handle different types of information security incident,
2226 including:

2227 1. information system failures and loss of service;

2228 2. malicious code;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 2229 3. denial of service;
- 2230 4. errors resulting from incomplete or inaccurate business data;
- 2231 5. breaches of confidentiality and integrity;
- 2232 6. misuse of information systems.
- 2233 b) in addition to normal contingency plans, the procedures must also cover:
- 2234 1. analysis and identification of the cause of the incident;
- 2235 2. containment;
- 2236 3. planning and implementation of corrective action to prevent recurrence, if
- 2237 necessary;
- 2238 4. communication with those affected by or involved with recovery from the
- 2239 incident;
- 2240 5. reporting the action to the appropriate authority;
- 2241 c) audit trails and similar evidence must be collected and secured, as appropriate, for:
- 2242 1. internal problem analysis;
- 2243 2. use as forensic evidence in relation to a potential breach of contract breach or
- 2244 regulatory requirement or in the event of civil or criminal proceedings, e.g. under
- 2245 computer misuse or data protection legislation;
- 2246 3. negotiating for compensation from software and service suppliers;
- 2247 d) action to recover from security breaches and correct system failures must be carefully
- 2248 and formally controlled.

2249 12.2.2 Learning from information security incidents

2250 Control: There must be mechanisms in place to enable the types, volumes, and impacts of

2251 information security incidents to be quantified and monitored.

2252 The information gained from the evaluation of information security incidents must be used to

2253 identify recurring or high impact incidents.

2254 12.2.3 Collection of evidence

2255 Control: Where a follow-up action against a person or organisation after an information security

2256 incident could lead to legal action (either civil or criminal), evidence must be collected, retained,

2257 and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

2258 Internal procedures must be developed and followed when collecting and presenting admissible
2259 evidence for the purposes of disciplinary action.

2260 Any forensics work must only be performed on copies of the evidential material. The integrity of
2261 all evidential material must be protected. Copying of evidential material must be supervised by
2262 trustworthy personnel and information on when and where the copying process was executed,
2263 who performed the copying activities and which tools and programs have been utilised must be
2264 logged.

2265

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

13. Business continuity management

13.1 Information security aspects of business continuity management

Objective: To counteract interruptions to the service and to protect critical business processes from the effects of major failures of information systems or disasters, and to ensure their timely resumption.

A business continuity management process must be implemented to minimise the impact on the service and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process must identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

The consequences of disasters, security failures, loss of service, and service availability must be subject to a business impact analysis. Business continuity plans must be developed and implemented to ensure timely resumption of essential operations. Information security must be an integral part of the overall business continuity process, and other management processes of the service providing organisation.

Business continuity management must include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

13.1.1 Including information security in the business continuity management process

Control: A managed process must be developed and maintained for business continuity that addresses the information security requirements needed to ensure business continuity of the service.

The process must bring together the following key elements of business continuity management:

- a) understanding the risks the service is facing in terms of likelihood and impact in time, including an identification and prioritisation of critical business processes;
- b) identifying all the assets involved in critical business processes;
- c) understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 2297 incidents causing smaller impact, as well as serious incidents that could threaten the
2298 viability of the service), and establishing the business objectives of information
2299 processing facilities;
- 2300 d) identifying sufficient financial, organisational, technical, environmental and human
2301 resources to address the identified information security requirements;
- 2302 e) ensuring the safety of personnel and the protection of information processing facilities
2303 and property;
- 2304 f) formulating and documenting business continuity plans addressing information security
2305 requirements in line with the agreed business continuity strategy;
- 2306 g) regular testing and updating of the plans and processes put in place;
- 2307 h) ensuring that the management of business continuity is incorporated in the overall
2308 processes and structure of the respective central bank; responsibility for the business
2309 continuity management process must be assigned at an appropriate level;
- 2310 i) ensuring that business continuity arrangements are able to cope with a major loss or
2311 inaccessibility of critical staff.

2312 13.1.2 Business continuity and risk assessment

2313 Control: Events that can cause interruptions to business processes must be identified, along with
2314 the probability and impact of such interruptions and their consequences for information security.

2315 Information security aspects of business continuity must be based on identifying events (or
2316 sequence of events) that can cause interruptions to the service, e.g. equipment failure, human
2317 errors, theft, fire, natural disasters and acts of terrorism. This must be followed by a risk
2318 assessment to determine the probability and impact of such interruptions, in terms of time,
2319 damage scale and recovery period.

2320 Business continuity risk assessments must be carried out with full involvement from owners of
2321 business resources and processes. This assessment must consider all business processes and must
2322 not be limited to the information processing facilities, but must include the results specific to
2323 information security. It is important to link the different risk aspects together, to obtain a
2324 complete picture of the business continuity requirements of the service providing organisation.
2325 The assessment must identify, quantify, and prioritise risks against criteria and objectives
2326 relevant to the service providing organisation, including critical resources, impacts of disruptions,
2327 allowable outage times, and recovery priorities.

2328 Depending on the results of the risk assessment, a business continuity strategy must be developed
2329 to determine the overall approach to business continuity. Once this strategy has been created,

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

endorsement must be provided by senior management, and a plan created and endorsed to implement this strategy.

13.1.3 Developing and implementing continuity plans including information security

Control: Plans must be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time-scales following interruption to, or failure of, critical business processes.

The business continuity planning process must consider the following:

- a) identification and agreement of all responsibilities and business continuity procedures;
- b) identification of the acceptable loss of information and services;
- c) implementation of the procedures to allow recovery and restoration of business operations and availability of information in required time-scales; particular attention needs to be given to the assessment of internal and external business dependencies and the contracts in place;
- d) definition of procedures for both internal and external communication described in a crisis communication plan;
- e) operational procedures to follow pending completion of recovery and restoration;
- f) documentation of agreed procedures and processes;
- g) education of staff in the agreed procedures and processes, including crisis management;
- h) testing and updating of the plans.

The planning process must focus on the following business objectives:

- a) Business continuity measures must ensure that all business transactions can be processed with the 'same day value' and the business day can be finalised with a defined maximum delay;
- b) In a 'disaster situation'²² it must be possible to recover operations from a remote secondary site in line with the recovery times stated in the Service Level Agreement.

The services and resources facilitating this must be identified, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities. Such

²² Major failure or disaster is understood to mean a serious service interruption which is solved by relocation of the service operations to a second site, physically separate from the primary site. Causes for a major failure can be technical faults, such as lengthy hardware, software or communication failures. Disaster events are fire, flood, explosions, sabotage, evacuation, blockade, terrorist attacks etc.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services.

Business continuity plans must address vulnerabilities and therefore may contain sensitive information that needs to be protected. Copies of business continuity plans must be stored in a remote location with a different risk profile to escape any damage from a disaster at the main site. Management must ensure copies of the business continuity plans are up-to-date and protected with the same level of security as applied at the main site. Other material necessary to execute the business continuity plans must also be stored at the remote location.

If alternative temporary locations are used, the level of implemented security controls at these locations must be equivalent to the main site.

13.1.4 Business continuity planning framework

Control: A single framework of business continuity plans must be maintained to ensure that all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

The business continuity plan must describe the approach for continuity, for example the approach to ensure information or information system availability and security. The plan must also specify the escalation plan and the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, any existing emergency procedures, e.g. evacuation plans or fallback arrangements, must be amended as appropriate. Procedures must be included within the change management programme to ensure that business continuity matters are always addressed appropriately.

The business continuity plan must have a specific owner. Emergency procedures, manual fallback plans, and recovery plans must be within the responsibility of the owners of the appropriate business resources or processes involved.

A business continuity planning framework must address the identified information security requirements and consider the following:

- a) the conditions for activating the plans which describe the process to be followed (e.g. how to assess the situation, who is to be involved) before each plan is activated;
- b) emergency procedures, which describe the actions to be taken following an incident, which jeopardises business operations;
- c) fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time-scales;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 2391 d) temporary operational procedures to follow pending completion of recovery and
2392 restoration;
- 2393 e) recovery procedures which describe the actions to be taken to return to normal business
2394 operations;
- 2395 f) a maintenance schedule which specifies how and when the plan will be tested;
- 2396 g) a process for maintaining the plan;
- 2397 h) awareness, education, and training activities which are designed to create understanding
2398 of the business continuity processes and ensure that the processes continue to be
2399 effective;
- 2400 i) the responsibilities of the individuals, describing who is responsible for executing which
2401 component of the plan. Alternatives must be nominated as required;
- 2402 j) the critical assets and resources needed to be able to perform the emergency, fallback and
2403 recovery procedures.

2404 **13.1.5 Testing, maintaining and re-assessing business continuity plans**

2405 Control: The business continuity plans must be tested and updated regularly to ensure that they
2406 are up to date and effective.

2407 Business continuity plan tests should ensure that all members of the recovery team and other
2408 relevant staff are aware of the plans and their responsibility for business continuity and
2409 information security and know their role when a plan is invoked.

2410 The test schedule for business continuity plan(s) must indicate how and when each element of the
2411 plan should be tested. Each element of the plan(s) should be tested at planned intervals (*Business*
2412 *Continuity Test Interval*).

2413 A variety of techniques should be used in order to provide assurance that the plan(s) will operate
2414 in real life. These should include:

- 2415 a) table-top testing of various scenarios (discussing the business recovery arrangements
2416 using example interruptions);
- 2417 b) simulations (particularly for training people in their post-incident/crisis management
2418 roles);
- 2419 c) technical recovery testing (ensuring information systems can be restored effectively);
- 2420 d) testing recovery at an alternate site (running business processes in parallel with recovery
2421 operations away from the main site);

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 2422 e) tests of supplier facilities and services (ensuring externally provided services and
2423 products will meet the contracted commitment);
- 2424 f) complete rehearsals (testing that personnel, equipment, facilities, and processes can cope
2425 with interruptions).
- 2426 The results of tests must be recorded and actions taken to improve the plans, where necessary.
- 2427 Responsibility must be assigned for reviews of each business continuity plan. The identification
2428 of changes in business arrangements not yet reflected in the business continuity plans must be
2429 followed by an appropriate update of the plan. This formal change control process should ensure
2430 that the updated plans are distributed and reinforced by regular reviews of the complete plan
2431 (*Business Continuity Review Interval*).
- 2432

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

14. Compliance

14.1 Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements.

Advice on specific legal requirements should be sought from legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).

14.1.1 Identification of applicable legislation

Control: All relevant and applicable statutory, regulatory, and contractual requirements and the approach to meet these requirements must be explicitly defined, documented, and kept up to date for the service and the service providing organisation.

The specific controls and individual responsibilities to meet these requirements must be similarly defined and documented.

14.1.2 Intellectual property rights (IPR)

Control: Procedures must be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

The following guidelines should be considered:

- a) publishing an intellectual property rights compliance policy which defines the legal use of software and information products;
- b) acquiring software only through known and reputable sources, to ensure that copyright is not violated;
- c) maintaining awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against personnel breaching them;
- d) maintaining asset registers, and identifying all assets with requirements to protect intellectual property rights;

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

- 2462 e) maintaining proof and evidence of ownership of licenses, master disks, manuals, etc;
- 2463 f) implementing controls to ensure that any maximum number of users permitted is not
- 2464 exceeded;
- 2465 g) carrying out checks that only authorised software and licensed products are installed;
- 2466 h) providing a policy for maintaining licence conditions;
- 2467 i) providing a policy for disposing or transferring software to others;
- 2468 j) using appropriate audit tools;
- 2469 k) complying with terms and conditions for software and information obtained from public
- 2470 networks;
- 2471 l) not duplicating, converting to another format or extracting from commercial recordings
- 2472 (film, audio) other than permitted by copyright law;
- 2473 m) not copying in full or in part, books, articles, reports or other documents, other than
- 2474 permitted by copyright law.

2475 14.1.3 Protection of records

2476 Control: Important records must be protected from loss, destruction, and falsification, in
2477 accordance with statutory, regulatory, contractual, and business requirements.

2478 Records must be categorised into record types, e.g. accounting records, database records,
2479 transaction logs, audit logs, and operational procedures, each with details of retention periods and
2480 type of storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic
2481 keying material and programs associated with encrypted archives or digital signatures, must also
2482 be stored to enable decryption of the records for the length of time the records are retained.

2483 To meet the record safeguarding objectives, the following steps must be taken:

- 2484 a) guidelines must be issued on the retention, storage, handling, and disposal of records and
- 2485 information;
- 2486 b) a retention schedule must be drawn up identifying records and the period of time for
- 2487 which they should be retained;
- 2488 c) an inventory of sources of key information must be maintained;
- 2489 d) controls must be implemented to protect records and information from loss, destruction,
- 2490 and falsification.

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

14.1.4 Data protection and privacy of personal information

Control: Data protection and privacy must be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

A data protection and privacy policy must be developed and implemented. This policy must be communicated to all persons involved in the processing of personal information.

14.1.5 Prevention of misuse of information processing facilities

Control: Users must be deterred from using information processing facilities for unauthorised purposes.

The senior management must approve the use of information processing facilities. Any use of these facilities for non-business purposes without management approval, or for any unauthorised purposes, should be regarded as improper use of the facilities. If any unauthorised activity is identified by monitoring or other means, this activity should be brought to the attention of the individual manager concerned for consideration of appropriate disciplinary and/or legal action.

Legal advice must be taken before implementing monitoring procedures.

All users should be aware of the precise scope of their permitted access and of the monitoring in place to detect unauthorised use.

At log-on, a warning message should be presented to indicate that the information processing facility being entered is under the responsibility of the respective part of the service providing organisation and that unauthorised access is not permitted. The user has to acknowledge and react appropriately to the message on the screen to continue with the log-on process.

14.1.6 Regulation of cryptographic controls

Control: Cryptographic controls must be used in compliance with all applicable agreements, laws, and regulations.

Legal advice must be sought to ensure compliance with national laws and regulations. Before encrypted information or cryptographic controls are moved to another country, legal advice should also be taken.

14.2 Compliance with security policies and technical compliance

Objective: To ensure compliance of the service with security policies and standards.

The compliance of information systems with security policies must be reviewed at least every three years and/ or when significant changes occur. Such reviews must be performed against the

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

existing security policies and the technical platforms. The service must be checked for compliance with applicable security implementation standards and documented security controls.

14.2.1 Compliance with security policies and security requirements

Control: Managers must ensure that all security procedures are carried out correctly to achieve compliance with security policies and standard based security requirements.

At planned intervals (*Compliance Review Interval*) and/or when significant changes occur, the compliance of information processing with the existing security policies and any other security requirements must be reviewed.

If any non-compliance is found as a result of the review:

- a) determine the causes of the non-compliance;
- b) evaluate the need for actions to ensure that non-compliance do not recur;
- c) determine and implement appropriate corrective action;
- d) review the corrective action taken.

Results of reviews and corrective actions carried out must be recorded and these records must be maintained. The results must be reported to the persons carrying out the independent reviews, when the independent review takes place.

14.2.2 Technical compliance checking

Control: Information systems must be regularly checked for compliance with the security policy and standard based security requirements.

Technical compliance checking²³ must be performed either manually (supported by appropriate software tools, if necessary) by an experienced system engineer, and/or with the assistance of automated tools, which generate a technical report for subsequent interpretation by a technical specialist. It must be performed on a regular basis (*Technical Compliance Check Interval*) and/or when significant technical changes occur. Such tests must be planned and documented.

Any technical compliance check must only be carried out by competent, authorised persons, or under the supervision of such persons.

²³ e.g. penetration tests and/or vulnerability assessments

Currency Participation Agreement

Schedule 10 – Annex 2 – Security requirements and controls

14.3 Information systems audit considerations

Objective: To maximise the effectiveness of, and to minimise interference to/from the information systems audit process.

There must be controls to safeguard operational systems and audit tools during information systems audits.

Protection is also required to safeguard the integrity and prevent misuse of audit tools.

14.3.1 Information systems audit controls

Control: Audit requirements and activities involving checks on operational systems must be carefully planned and agreed to minimise the risk of disruptions to business processes.

The following points must be observed:

- a) audit requirements must be agreed with appropriate management;
- b) the scope of the checks must be agreed and controlled;
- c) the checks should be limited to read-only access to software and data;
- d) access other than read-only are only allowed for isolated copies of system files, which must be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;
- e) resources for performing the checks must be explicitly identified and made available;
- f) requirements for special or additional processing should be identified and agreed;
- g) all access must be monitored and logged to produce a reference trail;
- h) all procedures, requirements, and responsibilities must be documented;
- i) the person(s) carrying out the audit must be independent of the activities audited.

14.3.2 Protection of information systems audit tools

Control: Access to information systems audit tools must be protected to prevent any possible misuse or compromise.

Information systems audit tools, e.g. software or data files, must be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 11

EXIT MANAGEMENT

Currency Participation Agreement

Schedule 11 – Exit Management

Table of contents

1	Introduction	1
2	Scope and general approach of Exit Management.....	2
2.1	Scope	2
2.2	General approach of Exit Management.....	2
3	Exit of the [NCB]	3
3.1	General responsibilities of the parties	3
3.2	Responsibilities of the [NCB]	4
3.3	Responsibilities of the Eurosystem	4

Currency Participation Agreement

Schedule 11 – Exit Management

1 Introduction

This Schedule sets out the provisions related to preparing and supporting the exit of the [NCB] and its Dedicated Cash Accounts Holders, as well as the roles and responsibilities of the parties during the exit process.

This Schedule does not cover the possible causes of termination and their consequences, nor the decision-making process, including arbitration and escalation, which will take place in case one contracting party does not accept the other contracting party's termination of the Currency Participation Agreement for cause.

The Schedule is divided into two chapters i) scope and general approach of the Exit Management; ii) exit of a Connected NCB to T2S addressing the responsibilities of the Parties.

Currency Participation Agreement

Schedule 11 – Exit Management

2 Scope and general approach of Exit Management

2.1 Scope

This Schedule describes the operational and mutual support principles that will apply from the moment the [NCB] has formally notified the Eurosystem of its decision to exit T2S, either for convenience or for cause, or from the moment the Eurosystem has formally notified the [NCB] that it wishes to terminate the Currency Participation Agreement. Notifications are given by way of an official termination notice, either from the [NCB] to the Eurosystem, or from the Eurosystem to the [NCB].

2.2 General approach of Exit Management

Unless otherwise agreed between the Parties in writing, the exit of [NCB] from T2S will consist of a full de-migration of the [NCB]’s business on a given date (i.e. “big-bang” approach) from the T2S Platform. Such exit shall take place over a weekend, targeting to avoid sensitive weekends (e.g. end-of-month, end-of quarter).

Currency Participation Agreement

Schedule 11 – Exit Management

3 Exit of the [NCB]

3.1 General responsibilities of the parties

- a) It is the responsibility of the Eurosystem to co-ordinate, steer and monitor the exit process. In agreement with the [NCB], it establishes the exit plan, the tasks and the milestones for the exit process and monitors compliance with the agreed procedures, tasks and milestones.
- b) It is the responsibility of the [NCB] to ensure its own readiness for the exit from T2S by the committed date according to the procedures and processes agreed with the Eurosystem and other T2S Actors.
- c) As soon as the formal termination notice has been sent and acknowledged, both the Eurosystem and the exiting [NCB] shall start work to provide for a smooth exit. Both parties shall appoint an “Exit Manager”, whose main responsibility consists in co-ordinating the exit activities and acting as liaison for the other party.
- d) To the extent possible, the parties shall use all reasonable endeavor to minimize the effects of the exit on T2S and on the CSDs whose participants make use of the [NCB], in particular on the national market of the [NCB].
- e) When the [NCB] exits T2S, settlement in its currency in T2S will no longer be possible and the CSD settling transactions in that currency can no longer make the same use of T2S.
- f) It is the responsibility of the [NCB] to co-ordinate all exit activities with its DCA Holders. The Eurosystem will co-ordinate with those CSDs whose participants make use of funds on those accounts for the settlement of securities transactions.
- g) Unless otherwise agreed between the parties, the time between the termination of the Agreement and the actual exit weekend shall not exceed a period of 2 years. If the [NCB] or the relevant CSD(s) are not prepared to exit T2S within this period, then the [NCB] shall in good faith negotiate a solution on the extended usage of the T2S Services, as well as on the remaining time until exit is possible. The [NCB] may choose a shorter exit period, provided all relevant CSDs have been informed about the exit procedures and have had sufficient time to prepare for the simultaneous exit of T2S in relation to settlement of the currency of the [NCB].
- h) For the purpose of the Currency Participation Agreement, the exit process ends when the adaptations are completed so that there are no more funds on the DCAs managed by the [NCB] and the currency no longer can be settled in T2S. Unless otherwise agreed between the parties, the exit of [NCB] from T2S will take the form of a simultaneous inactivation of all Dedicated Cash Accounts operated by the [NCB], so as to prevent any further transfers of funds between the RTGS system and T2S. These activities will take place during a week-end

Currency Participation Agreement

Schedule 11 – Exit Management

58 agreed upon by both parties and called the exit week-end.

- 59 i) After the completion of the exit process, and until the end of the legal archiving period, the
60 Eurosystem shall continue to provide information – including but not limited to transaction
61 data – to the [NCB], upon the latter's request, with respect to the services provided by the
62 Eurosystem to the [NCB] in the context of the Currency Participation Agreement. Upon the
63 [NCB]'s request, access to such information shall be provided by other means – to be agreed
64 between the Eurosystem and the [NCB] – than using the T2S Network Service Provider.

65 3.2 Responsibilities of the [NCB]

66 In view of ensuring a successful exit from T2S, the [NCB] shall:

- 67 a) deliver to the Eurosystem, at the latest one month after the official termination notice, a high-
68 level exit plan clearly defining all activities that the [NCB] itself, its DCA Holders, the
69 Eurosystem, and, where relevant, any CSD are to perform;
- 70 b) deliver to the Eurosystem, at the latest two months after the delivery of the high-level Exit
71 Plan, an overview of the required support for the execution of all exit activities, which the
72 [NCB] expects from the Eurosystem;
- 73 c) monitor and take all necessary measures to facilitate the readiness of its DCA Holders for the
74 exit from T2S;
- 75 d) co-operate with the Eurosystem in preparation of the exit plan and the detailed exit weekend
76 script;
- 77 e) co-ordinate all exit activities with its community, and confirm the successful completion of
78 the activities to the Eurosystem;
- 79 f) inform the Eurosystem of any unexpected event or delay of a planned activity, which may
80 affect the execution of the Eurosystem's support activities or the exit plan.

81 3.3 Responsibilities of the Eurosystem

82 In view of ensuring a successful exit from T2S, the Eurosystem shall:

- 83 a) continue to provide all services and support as specified in the Currency Participation
84 Agreement, until the exit weekend;
- 85 b) provide reasonable support to the [NCB] in preparing its high-level exit plan;
- 86 c) indicate to the [NCB] within one month after the receipt of the high-level exit plan, any
87 constraints and conditions applicable to the support it can provide;
- 88 d) assist the [NCB] in preparing its detailed support request to the Eurosystem, in particular by
89 indicating specific areas where the Eurosystem can offer such support;

Currency Participation Agreement

Schedule 11 – Exit Management

- 90 e) agree with the [NCB] within one month after the receipt of the detailed support request the
91 precise activities that the Eurosystem will conduct, and their timing;
- 92 f) support the [NCB] in establishing the exit plan, including aspects related to its Dedicated
93 Cash Accounts, major project milestones, as well as checkpoints to be met before the start of
94 the exit weekend;
- 95 g) inform the [NCB] within one month after reaching an agreement on the exit plan of the
96 amount of any costs for planning, coordination and execution of exit activities – beyond the
97 normal operational support, which it expects the [NCB] to reimburse, unless the [NCB] has
98 terminated the agreement for cause, in which case the Eurosystem will provide such support
99 free of charge;
- 100 h) upon agreement with the [NCB] on the costs the latter will reimburse, make all reasonable
101 efforts to conduct the agreed activities, including communication and coordination with other
102 T2S Actors, and where relevant confirm their successful completion to the [NCB];
- 103 i) establish the detailed exit weekend script which provides the [NCB] with the required
104 information to execute the tasks and/or to carry out the actions required during the exit
105 weekend;
- 106 j) provide all reasonable support to the [NCB] to address any unexpected events during the exit
107 process;
- 108 k) establish the fall-back arrangements and roll-back procedures specific for the exit, in order to
109 manage the necessary processes if the exit needs to be deferred to a later stage due to
110 predictable or unforeseen circumstances, and/or if the activities already performed during the
111 exit weekend need to be unwound if the exit has to be stopped.

CURRENCY PARTICIPATION AGREEMENT

SCHEDULE 12

PROCEDURE FOR PAYMENT OF CLAIMS

Currency Participation Agreement

Schedule 12 – Procedure for Payment of Claims

Table of contents

1. PROCEDURE IN RESPECT OF ARTICLE 28 (LIABILITY RULES).....	1
2. PROCEDURE IN RESPECT OF CLAIMS PURSUANT TO ARTICLE 29(1).....	2
3. PROCEDURE IN RESPECT OF ARTICLE 33(4) (INFRINGEMENT OF IPR).....	4

Currency Participation Agreement

Schedule 12 – Procedure for Payment of Claims

For the purposes of this Schedule, either Party asserting a claim against the other Party is referred to as “Claimant”, while the other Party is referred to as “Respondent”.

1. Procedure in respect of Article 28 (Liability rules)

The following procedure applies to the handling of any claim pursuant to Article 28 of this Agreement:

(a) The Claimant shall, without undue delay, notify the Respondent of the occurrence of any event which the Claimant reasonably believes may give rise to a claim based on Article 28 of this Agreement, and in any case no later than within [30] calendar days from the occurrence of such event or, in the event the Claimant did not know that an event would give rise to a claim, as from the moment it has the relevant knowledge that such event would give rise to a claim.

(b) The Claimant shall submit its claim against the Respondent without undue delay, and in any case no later than within 12 months from the occurrence of the event which gave rise to the claim or, if the Claimant did not know that an event gave rise to a claim for liability or indemnification, , within 12 months from the moment it knew or should reasonably have known of such a claim. After the expiry of this period, the Respondent shall be entitled to reject the claim.

(c) The Claimant shall submit its claim to the Respondent in writing, specifying its basis, its justification and, to the extent known, the claimed amount, to allow the Respondent to assess the merits of the submitted claim.

(d) The Respondent may request any additional information from the Claimant as may be reasonably required for assessing the merits of the claim. The Claimant shall cooperate in good faith and in a timely manner with the Respondent.

(e) The Respondent shall, without undue delay, notify the Claimant in writing if it accepts the claim or rejects it in whole or in part, in the latter case giving reasons for the rejection.

(f) In case of dispute as to the merits of the claim, the Parties shall make any effort to find an amicable arrangement. As the case may be, the Parties shall take recourse to Article 47 of this Agreement.

(g) If the Respondent has accepted the claim as merited, in whole or in part, or if it was settled either by an amicable arrangement between the Parties or through court proceedings pursuant to Article 47, the Respondent shall, subject to paragraphs (b), (h) and (i), pay out the claim as soon as reasonably practicable and at the latest within 90 calendar days after the end of this calendar year. Any payment pursuant to Article 28 of this Agreement is subject to the limitations of Article 28(5)(a) of this Agreement and shall be made on a

Currency Participation Agreement

Schedule 12 – Procedure for Payment of Claims

provisional basis subject to the reservations of paragraphs (h) and (i). The Claimant shall not be entitled to claim interest or damages for late payment in relation to the time elapsed prior to the expiry of the period of 90 calendar days.

(h) If the liability of the Eurosystem vis-à-vis the [NCB] is limited in accordance with Article 28(5)(a) of this Agreement and the amounts payable to the [NCB] and, as the case may be, to other Connected NCBs are reduced accordingly, the Eurosystem shall notify all Claimants as soon as practicably possible after the end of the relevant calendar year referred to in paragraph (g); the notification shall give sufficient evidence of the reasons for, and the calculation of, the reduced compensation amounts in relation to the amounts that had been claimed.

(i) If a claim is accepted as merited by the Eurosystem after the end of the calendar year in which the event occurred that caused the claim or settled by an amicable arrangement between the Parties, or settled in accordance with Article 47 of this Agreement after the end of this calendar year, the Eurosystem shall pay such claim as soon as reasonably practicable. If such a claim should be subject to a reduction in accordance with Article 28(5)(a) of this Agreement, the Claimant shall be notified in accordance with paragraph (h) prior to the payment. To the extent that a claim to paid after the end of the relevant calendar year referred to in paragraph (g) is subject to a reduction in accordance with Article 28(5)(a) of this Agreement, all payments previously made to the [NCB] or Connected NCBs with regard to the relevant calendar year referred to in paragraph (g) shall be recalculated in accordance with Article 28(5)(a) of this Agreement and the paid amounts shall be adjusted. With regard to this adjustment, the Eurosystem is entitled to claim back any compensation payment made in excess of the adjusted pro rata entitlement in accordance with to Article 28(5)(a) of this Agreement.

2. Procedure in respect of claims pursuant to Article 29(1)

The following procedure applies in addition to Article 29(1) if a DCA Holder has caused a Direct Loss to the Eurosystem in relation to T2S.

(a) The Eurosystem shall notify the [NCB] of the fact that an act or omission of one of the [NCB's] DCA Holders in relation to T2S has caused a Direct Loss to the Eurosystem. The notification shall be sent by the Eurosystem in writing as soon as reasonably practicable but in no case later than [90] calendar days after the loss has occurred.

(b) The notification shall contain a preliminary indication of the amount and composition of the claim against the [NCB].

(c) A delay shall not relieve the [NCB] of its obligation to reimburse the Eurosystem, except to the extent that the [NCB] can demonstrate that the delay caused damages.

Currency Participation Agreement

Schedule 12 – Procedure for Payment of Claims

- 70 (d) The Eurosystem shall precisely set out the amount and the various components of the loss
71 caused by the DCA Holder and for which it claims reimbursement from the [NCB]. The
72 [NCB] may request any additional information from the Eurosystem as may be reasonably
73 required for assessing the merits of the submitted claim. The Eurosystem shall cooperate in
74 good faith with any such request by the [NCB].
- 75 (e) The [NCB] shall notify the Eurosystem in writing within [90] calendar days from the day
76 of the receipt of the claim if it accepts the claim or rejects it in whole or in part, in the latter
77 case giving the reasons for the rejection as set out in paragraph [1] of Article 29. If it
78 accepts the claim, the [NCB] shall reimburse the Eurosystem within [30] calendar days.
- 79 (f) In case of dispute as to the extent and/or proportion of the Eurosystem's contribution to the
80 Eurosystem's loss, the Parties shall take recourse to the Dispute Resolution and Escalation
81 Procedure set out in Article 37 in order to settle the issue in an amicable way.
- 82 (g) As soon as the dispute has been settled, the [NCB] shall reimburse the net amount due to
83 the Eurosystem within [30] calendar days.
- 84 (h) The Eurosystem shall subrogate the [NCB] to any rights it may have against a DCA Holder
85 in relation to the reimbursed claim.

Currency Participation Agreement

Schedule 12 – Procedure for Payment of Claims

3. Procedure in respect of Article 33(4) (Infringement of IPR)

The following procedure applies in addition to Article 33(4) of this Agreement if legal action is commenced or threatened against the [NCB].

(a) If the [NCB] allows the Eurosystem to control the defence against the Third Party claimant, the Eurosystem shall keep the [NCB] informed in all material matters at all times. Notwithstanding such agreement regarding the control over the defence, the [NCB], being the formal party to the legal proceedings, and the Eurosystem shall agree on the way in which the proceedings are conducted. For this purpose, and in due consideration of the agreement to give the Eurosystem control over the defence, the [NCB] shall be entitled to object to legal submissions proposed by the Eurosystem that it considers harmful to the outcome of such proceedings and to make its own counterproposals towards the Eurosystem. Expenses of the [NCB] in the context of such involvement shall be borne by the [NCB].

(b) At the request of the Eurosystem the [NCB] shall give all reasonable assistance and provide all relevant documents and data which are under its control, to the extent permissible under the applicable statutory and contractual law. The Eurosystem shall indemnify the [NCB] for all reasonable cost the latter incurred in that context.

The following applies in addition to Article 33(4)(b) of this Agreement if the [NCB] is held legally liable for an infringement.

(c) The [NCB] shall notify the Eurosystem of the fact that it is held liable to the Third Party pursuant to an Enforceable Judgement. The notification shall be sent as soon as reasonably practicable but in no case later than 30 days after the full text of the court ruling was available to the [NCB].

(d) The notification shall contain a statement to the effect that the [NCB] intends to claim reimbursement from the Eurosystem, the text of the Enforceable Judgement (to the extent available) and a preliminary indication of the amount and composition of the claim to reimbursement.

(e) The [NCB] shall submit its claim to the Eurosystem in writing and without undue delay and in any case no later than 90 calendar days after the full text of the Enforceable Judgement was made available to the [NCB]. A delay shall not relieve the Eurosystem of its obligation to reimburse the [NCB], except to the extent that the Eurosystem can demonstrate that the delay caused damages.

(f) The [NCB] shall precisely set out the amount and the various components of the payment it owes to the Third Party and for which it claims reimbursement from the Eurosystem. The

Currency Participation Agreement

Schedule 12 – Procedure for Payment of Claims

- 120 Eurosystem may request any additional information from the [NCB] as may be reasonably
121 required for assessing the merits of the submitted claim. The [NCB] shall cooperate in
122 good faith with any such request by the Eurosystem.
- 123 (g) The Eurosystem shall notify the [NCB] in writing within 90 calendar days from the day of
124 the receipt of the claim if it accepts the claim or rejects it in whole or in part, in the latter
125 case giving reasons for the rejection.
- 126 (h) In case of dispute as to the merits of the reimbursement claim, the Parties shall take
127 recourse to Article 47 of this Agreement.
- 128 (i) The [NCB] shall subrogate the Eurosystem to any rights it may have against Third Parties
129 in relation to the reimbursed claim.