Information guide

for TARGET2 users

Version 5.0

November 2011

Infoguide

Table of contents

Information guide for TARGET2 users

Table of contents

Table of contents

Table of contents

List of diagrams, tables and boxes

Diagrams

Tables

Boxes

1. Introduction

This “Information guide for TARGET2 users” (hereafter “Infoguide”) aims to provide credit institutions and ancillary systems using TARGET2 with a standard set of information in order to give them a better understanding of the overall functioning of the system and to enable them to make use of it as efficiently as possible. In addition, the Infoguide gives users a clear understanding of which features are common and which are specific to each country. Documentation on country-specific features can be found on the websites of the respective national central banks.

The Infoguide has been drafted specifically with a view to being updated when necessary and as a document to which national central banks (NCBs), the European Central Bank (ECB), the 3CB[1] and TARGET2 users can contribute. It is intended to serve as a dynamic tool, incorporating updates that may emerge either from the national TARGET2 User Groups or from meetings organised for TARGET2 users at the euro area level by the European System of Central Banks (ESCB). The contents of this document confer no legal rights on TARGET2 users, operations or any person or entity.
All times in this document refer to the local time at the seat of the ECB.

1.1. What is TARGET2

TARGET2 (the second-generation Trans-European Automated Real-time Gross settlement Express Transfer system) is the Eurosystem’s interbank funds transfer system, which is designed to support the Eurosystem’s objectives of defining and implementing the monetary policy of the euro area and promoting the smooth operation of payment systems, thus contributing to the integration and stability of the euro area money market. TARGET2 is a single centralised system, offering the same level of service to all TARGET2 users. It has been designed and built to meet the highest standards of robustness and operational reliability.

The system has been designed in such a way that it is able to process cross-border payments denominated in euro as smoothly as if they were domestic payments.

TARGET2 processes only transfers denominated in euro. The aim is to allow payments – especially large-value payments such as those relating to foreign exchange and money market transactions – to

[1] The 3CB comprises the Banca d’Italia, the Banque de France and the Deutsche Bundesbank, the technical providers of the Single Shared Platform (SSP).

be made throughout the euro area at low cost with high security and very short processing times.

As it is a real-time gross settlement (RTGS) system, payments are handled individually. Unconditional payment orders are automatically processed one at a time on a continuous basis. Thus, TARGET2 provides immediate and final settlement of all payments, provided that there are sufficient funds or overdraft facilities available on the payer's account with its central bank.[2] There is no set minimum amount for a payment made through TARGET2.

1.2. How to use the Information guide for TARGET2 users

The Infoguide is a reference guide to assist TARGET2 users during daily operations. It also contains information about which other documents are of high relevance for the users and where these can be found.

The part on "Fundamentals" in Chapter 2 describes the TARGET2 structure, the organisational structure at central bank level, the TARGET2 business days, the TARGET2 transactions, the settlement of ancillary systems and the operational communication.

The part on "Participation" in Chapter 3 describes the access criteria, the static data collection, the TARGET2 directory, the certification testing, the measures to ensure security and operational reliability, the termination or suspension of TARGET2 users and the TARGET2 billing.

Then, in Chapter 4, the procedures in the different phases of a normal business day are described. Chapters 5, Chapter 6 and Chapter 7 describe the procedures to be followed in the event of contingency. These parts (Chapters 4 to 7) are described in the chronological order of a TARGET2 business day, i.e. commencing with the start-of-day procedures (on the evening of the previous working day), then moving on to the night-time settlement phase and the day trade phase, before finishing with the end-of-day procedures.

Chapter 8 describes the testing requirements for contingency arrangements and business continuity. Chapter 9 deals with the change management for the yearly releases as well as for the emergency changes and the so-called hot fixes. There is a description of the TARGET2 compensation scheme in Chapter 10.

Finally, the Annexes provide a detailed description of an inter-regional failover with loss of data (Annex I), an incident report form (Annex II) and self-certification statement for use by critical participants (Annex III), the template to be used for Change Requests (Annex IV), and a glossary (Annex V).

[2] With some exceptions e.g. warehoused payments and payments to an "excluded" participant.

1.3. Scope of the Information guide for TARGET2 users

The Infoguide is intended to cover all those operational matters which concern the TARGET2 users in their daily use of TARGET2.

1.4. Further relevant documentation

Legal documentation

- **Guideline on TARGET2**

The Guideline on TARGET2 is the legal framework for TARGET2 with which the Infoguide has to be fully compliant.

- **Harmonised Conditions**

Each participating NCB adopts arrangements implementing the Harmonised Conditions for participation in TARGET2[3] that are laid down in Annex II of the Guideline on TARGET2. These arrangements shall exclusively govern the relationship between the relevant NCB and its TARGET2 users in respect of the processing of payments in the payments module (PM).

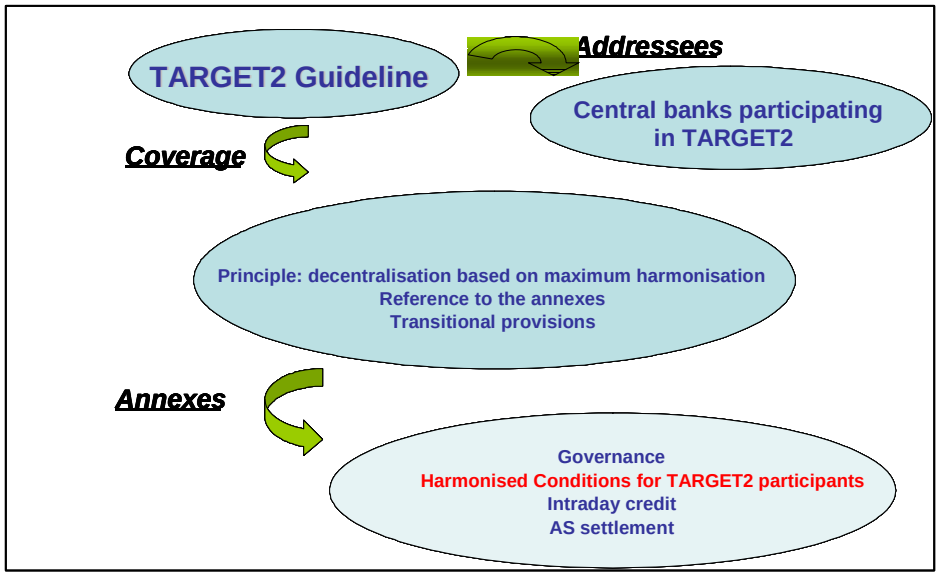


Diagram 1: Legal documentation I

[3] For internet-based participants, supplemental and modified Harmonised Conditions have been agreed.

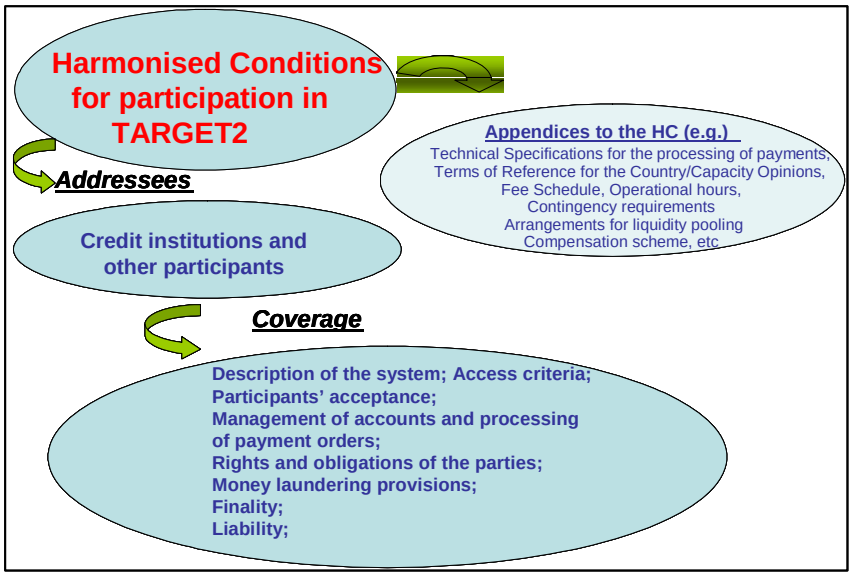


Diagram 2: Legal documentation II

Other relevant documentation

- **User guide for the TARGET2 Information System (T2IS)**

This document provides information on how to access and read information provided in T2IS.

- **User guide for static data collection**

The aim of this document is to provide future TARGET2 users with all the information needed to complete the registration forms.

- **TARGET2 pricing guide for users**

This document provides detailed information on the pricing and billing scheme of TARGET2.

- **General Functional Specifications (GFS) and User Detailed Functional Specifications (UDFS)**

These documents provide the technical details on the functioning of the single shared platform (SSP).

- **ICM handbook**

This document provides details on the functioning of the information and control module (ICM).

- **User Manual Internet Access for the public key certification service**

The manual establishes the procedures followed by the Banca d'Italia as Accredited Certification Authority for the issue and utilisation of electronic certificates in the context of internet access to the TARGET2 system. The service is provided by Banca d'Italia on behalf of the Eurosystem.

- **Settlement times of ancillary systems**

This document provides information in particular about the settlement times of ancillary systems.

- **SWIFT documentation**

The SWIFT documentation provides details of the different SWIFT standards.

All the above-mentioned documents are available in their most recent version on the TARGET2 website under “Documentation”, except the SWIFT documentation, which is available on the SWIFT website. In addition, the NCBs provide further information on specific national characteristics and procedures.

2. Fundamentals

2.1. TARGET2 structure

2.1.1. Governance structure

The management of TARGET2 is based on a three-level governance scheme. The tasks are assigned to the Governing Council (Level 1), the Eurosystem central banks (Level 2) and the SSP-providing central banks (Level 3). The Governing Council is responsible for the general management of TARGET2. The tasks assigned to Level 1 fall within the exclusive competence of the Governing Council. The ESCB's Payment and Settlement Systems Committee (PSSC) assists the Governing Council as an advisory body in all matters relating to TARGET2. The Eurosystem central banks are responsible for the tasks assigned to Level 2, within the general framework defined by the Governing Council. In addition to its advisory role, the PSSC performs the tasks assigned to Level 2. The SSP-providing central banks (Level 3) take decisions on the daily running of the single shared platform on the basis of a predefined service level agreement.

Level 1 – Governing Council	Level 2 – Eurosystem central banks	Level 3 – SSP-providing central banks
Operation		
– Managing severe crisis situations – Authorising establishment and operation of TARGET2 Simulator – Appointing certification authorities for internet-based access – Specifying security policies, requirements and controls for the SSP – Specifying principles for security of certificates used for internet-based access	– Management with regard to system-owner responsibilities, including crisis situations – Maintaining contacts with users at European level (subject to the sole responsibility of central banks for the business relationship with their TARGET2 users) and monitoring daily user activity from a business perspective (central bank task) – Monitoring business developments – Budgeting, financing, invoicing (central bank task) and other administrative tasks	– Managing the SSP on the basis of the agreement referred to in the Guideline on TARGET2

Table 1: TARGET2 governance structure

2.1.2. Technical structure

From a technical point of view, TARGET2 is structured as described below:

- the single shared platform (SSP) with the payment and accounting processing services systems (PAPSS) and the customer-related services systems (CRSS);
- the PAPSS with the payments module (PM), the standing facilities module (SF), the reserve management module (RM), the home accounting module (HAM), the static data module (SD), the contingency module (CM) and the information and control module (ICM);
- the customer-related services systems for central banks only (CROSS, CRAKS and CRISP);
- the central banks with a proprietary home account (PHA), reserve management and intraday credit;
- the banks are connected via SWIFT or internet;
- the ancillary systems are connected via SWIFT.

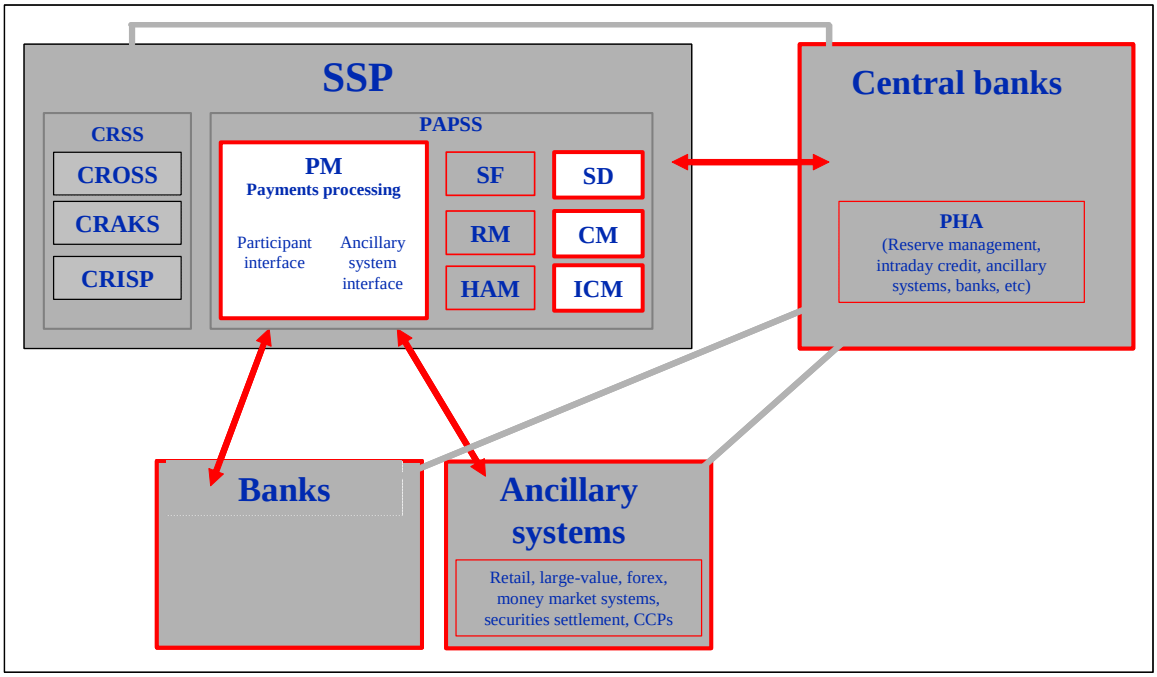


Diagram 3: TARGET2 structure

2.2. Organisational structure at central bank level

The sole contact point for TARGET2 users is the national service desk at their respective national central bank. Within the Eurosystem, the national service desk is represented by the settlement manager. All settlement managers are interlinked by means of a standing teleconference facility. Each NCB also has a crisis manager who is informed via the respective settlement manager and is involved in the case of problem escalation. The crisis managers are also interlinked via a standing teleconference facility.

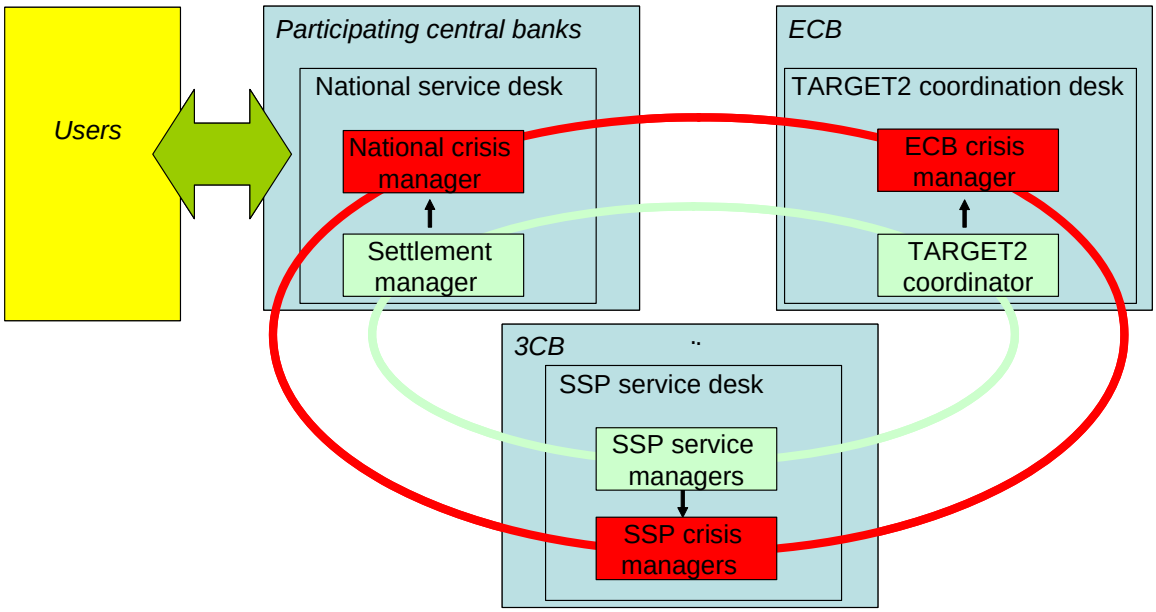


Diagram 4: Overview of TARGET2 actors

2.3. TARGET2 business days

TARGET2 is open on all days, except Saturdays, Sundays, New Year's Day, Good Friday and Easter Monday (according to the calendar applicable at the seat of the ECB), 1 May, Christmas Day and 26 December. TARGET2 business days are the de facto settlement days for the financial markets in euro, as well as for foreign exchange transactions involving the euro.

The table below shows the different phases of the TARGET2 business day.

	Time	Description
Start of day D-1	18:45[a] – 19:00[a]	Start-of-day processing
Night-time settlement	19:00[a] – 19:30[a]	Provision of liquidity to the PM (SF to HAM, SF to PM, HAM to PM, PHA to PM)
	19:30[a] – 22:00	Start-of-procedure message, setting aside of liquidity on the basis of standing orders and ancillary system (AS) night-time processing (AS settlement procedure 6)
Technical window	22:00[b] – 01:00	Technical maintenance window
Night-time settlement	01:00 – 07:00	Night-time processing (AS settlement procedure 6)
Business window	06:45 – 07:00	Business window to prepare daylight operations
Day trade	07:00 – 18:00	Day trade phase
	17:00	Cut-off for customer payments
	18:00	Cut-off for interbank payments
End of day	18:15[a]	Cut-off for use of SF
	18:30[a]	Central bank accounting

Table 2: TARGET2 business day

[a] Plus 15 minutes on the last day of the minimum reserve period.

[b] Over a weekend or on a TARGET2 holiday, the technical window lasts from 22:00 on the last business day until 01:00 on the next business day.

2.4. TARGET2 transactions

In TARGET2, messages can be generally separated into SWIFT FIN messages (in particular customer and interbank payments) and XML traffic (InterAct and FileAct messages).

The payments module (PM) of the SSP uses the SWIFTNet FIN Y-Copy[4] service for the processing of all payments within a dedicated SWIFT Closed User Group (CUG). The PM receives a full copy of each payment to allow settlement and an efficient and comprehensive provision of information in the information and control module (ICM).

[4] In the HAM, V-shape is used.

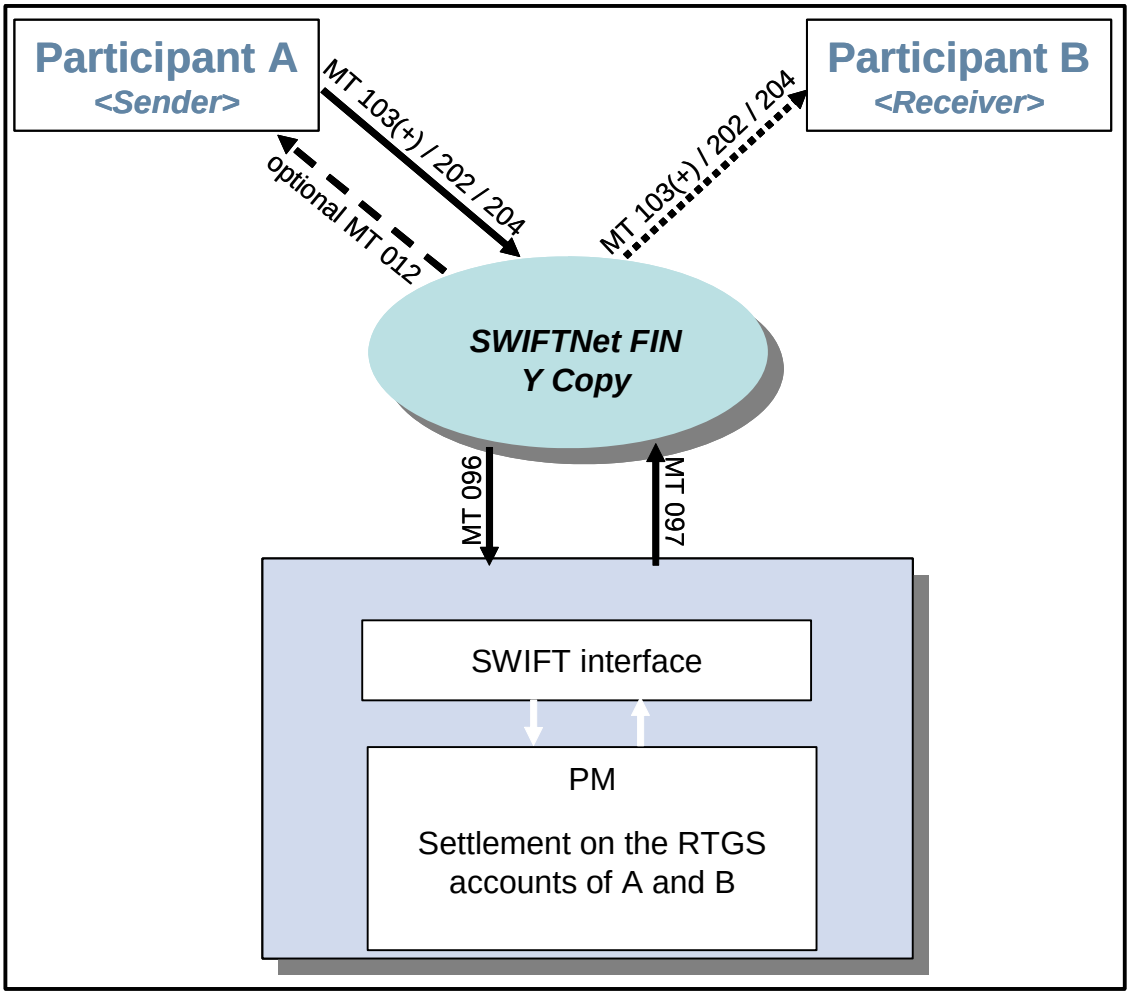


Diagram 5: Y-copy transaction flows

If the participant connects to the ICM in application-to-application mode, SWIFTNet InterAct and SWIFTNet FileAct are used. The various information and control options are set up as XML messages[5]. SWIFTNet Browse allows the initiation of InterAct or FileAct exchanges via a secure browser link.

Users connected to the SSP via internet-based access do not send and receive messages to and from the SSP via the SWIFT network but can create and display them via ICM screens. Connection to the ICM is possible for such users in user-to-application mode only (see also Chapter 3.1.2., "Indirect participation")

[5] Detailed descriptions of XML messages can be found in UDFS Book 4.

2.4.1. Customer payments

Customer payments are defined as credit payments in the SWIFT MT103 and SWIFT MT103+ formats (standard and STP). Customer payments can be processed in TARGET2 from 07:00 until 17:00.

2.4.2. Interbank payments

Interbank payments are defined as credit payments in the SWIFT MT202 format and in MT202COV format, and direct debit payments in the SWIFT MT204 format. These messages are sent by or on behalf of the ordering institution either directly or through any correspondent(s) to the financial institution of the beneficiary institution.

Interbank credit payments MT202 are payments, such as the payment leg of money market, foreign exchange and derivatives transactions, which take place between credit institutions or between NCBs/the ECB and credit institutions.

MT202COV are interbank payments that “cover” underlying customer payments and contain fields for the originator and beneficiary of the credit transaction.

Direct debits MT204 in TARGET2 are intended for wholesale purposes only and are restricted to interbank transactions. In any case, the respective TARGET2 users have to agree with the parties allowing the debiting of their accounts on the terms and conditions for using this service. The TARGET2 user authorises another TARGET2 user to issue a direct debit order. The TARGET2 user also has to inform its central bank, which is responsible for recording and administrating the pre-agreements. Participants using internet-based access are not able to initiate direct debits.

Interbank payments can be processed in TARGET2 from 07:00 until 18:00. Outside this period payments can be submitted and are retained at the SSP level outside settlement.

2.4.3. Liquidity transfers

Liquidity holdings in central bank money can be held in the PM of the SSP but also in home accounts at the respective central banks (proprietary home accounts) or in the HAM (Home Account Module). It is possible to transfer liquidity between the different accounts via the ICM, as well as via SWIFTNet FIN. Liquidity transfers via SWIFTNet FIN can be processed via TARGET2 from 07:00 until 18:00. Liquidity transfers via the ICM are initiated via SWIFTNet InterAct. Basically, manual liquidity transfers transmitted via the ICM are executed immediately after transmission during the operating

hours of the PM until the cut-off time for interbank payments (18:00) and from the start of night-time processing (19:30), except in specific time windows which are used for the SSP maintenance period.[6]

The UDFS 1st book (see 9.1.2.1.1.3 SWIFTNet FIN messages- User header – "Structure when sending a message" and "Structure when receiving a message") provides information on tag 113 "Banking priority". As it is explained there, the third and fourth characters of the field 113 are not used (and not checked by the SSP). TARGET2 users should be aware of national arrangements on the use of the tag.

2.4.4. SWIFTNet FileAct

SWIFTNet FileAct allows the transfer of files and is typically used to exchange batches of structured financial messages and large reports. FileAct messages are accepted whenever the PM is open, except in the following specific time windows:

- SSP maintenance period;
- end-of-day processing, start-of-day processing, provisioning of liquidity.

2.4.5. SWIFTNet InterAct

SWIFTNet InterAct allows the transfer of XML requests via the Secure IP Network (SIPN) by SWIFT to the ICM and the ancillary systems interface (ASI). XML messages are used for requests and responses related to the ICM (in A2A mode) and for ancillary system business. Concerning ancillary system business, the messages are accepted as explained in Section 2.5. With regard to ICM (A2A) business, the messages are accepted depending on the underlying business case. During the SSP maintenance period, no InterAct messages are accepted at all.

2.5. Settlement of ancillary systems[7]

For an ancillary system, access to settlement within the SSP will be possible both via the standard participant interface (PI) and the ancillary systems interface (ASI). In the first case, ancillary systems which fulfil the participation criteria to become a direct participant can use the functionalities of the system as any other direct participant, and will in particular have an RTGS account on the platform. In the second case, the ancillary systems will access the SSP via a specific interface (the ASI), which includes a number of specific features specially designed to facilitate AS settlement, such as

6 See UDFS Book 1 for the processing times of standing orders.

7 For further information, see UDFS, section 2.8 (Settlement of ancillary systems).

centralised control of the authorisation to debit a given account, use of mandated payments, specific settlement procedures, optional mechanisms and the use of specific kinds of accounts (technical account, mirror account, guarantee account). An ancillary system which uses the ASI can, if it fulfils the participation criteria, in parallel become a direct participant and open an RTGS account. Thus, it could be using the ASI for its settlement activities and the RTGS account for other purposes. To support different business cases related to the various types of ancillary systems, six generic settlement procedures are provided by the PM via the ASI.

Settlement procedure[8]	**PM generic settlement procedure**	**Description**
Procedure 1	Liquidity transfer	Transfer between the cash position of a direct participant in the AS and in the PM through a mirror account. Settlement occurs in the AS itself.
Procedure 2	Real-time settlement	Transfer between the accounts of two direct participants, aiming at finalising a transaction already able to settle in the AS.
Procedure 3	Bilateral settlement	AS sends simultaneously debits and credits to the PM. Each transaction (both the debit and the credit leg) is processed independently from the other one.
Procedure 4	Standard multilateral settlement	Debits and credits are posted simultaneously in the PM but all debits have to be settled before credits are made.
Procedure 5	Simultaneous multilateral settlement	Debits and credits are posted simultaneously in the PM but all debits and credits are simultaneously checked for settlement and can only be settled on an all-or-nothing basis.
Procedure 6	Dedicated liquidity and cross system settlement	Direct participants dedicate liquidity for the settlement of the AS transactions, either on

[8] Integrated model: The final settlement of the cash leg takes place in the SSS itself.
Interfaced model: The final settlement of the cash leg takes place in the PM.

		specific sub-accounts or on the mirror account. Settlement occurs either on the sub-accounts (interfaced model) or in the AS itself (integrated model). Such a settlement procedure can be used especially for night-time business, but also in daylight.

Table 3: Settlement procedures

In addition, the above-mentioned mandatory settlement procedures can be adjusted to the specific needs of each ancillary system through the following mechanisms:

- an information period for pre-announcing the settlement of AS procedures 3, 4 and 5;
- a settlement period for the settlement of ancillary systems, in order not to prevent the settlement of other operations; if the ancillary system transactions are not settled at the end of this period, either the respective balances will be rejected or, if chosen by the AS for procedures 4 and 5, a guarantee mechanism will be activated;
- a guarantee fund mechanism provides the complementary liquidity needed in case ancillary system transactions cannot be settled using the liquidity of participants;
- scheduled time is a mechanism which stores the ancillary system transactions until the scheduled settlement time is reached.

Ancillary systems using the settlement procedures 3, 4, 5 and 6 can use FileAct to settle the cash leg of the AS transactions. Basically, FileAct messages based on settlement procedure 6 can be processed during the whole time the PM is open, i.e. until the cut-off time for interbank payments (18:00), and from the start of night-time processing (19:30), except in the specific time windows used for SSP maintenance. FileAct messages based on settlement procedures 3, 4 and 5 can be processed during the day trade phase from 07:00 until 18:00.

2.6. Operational communication

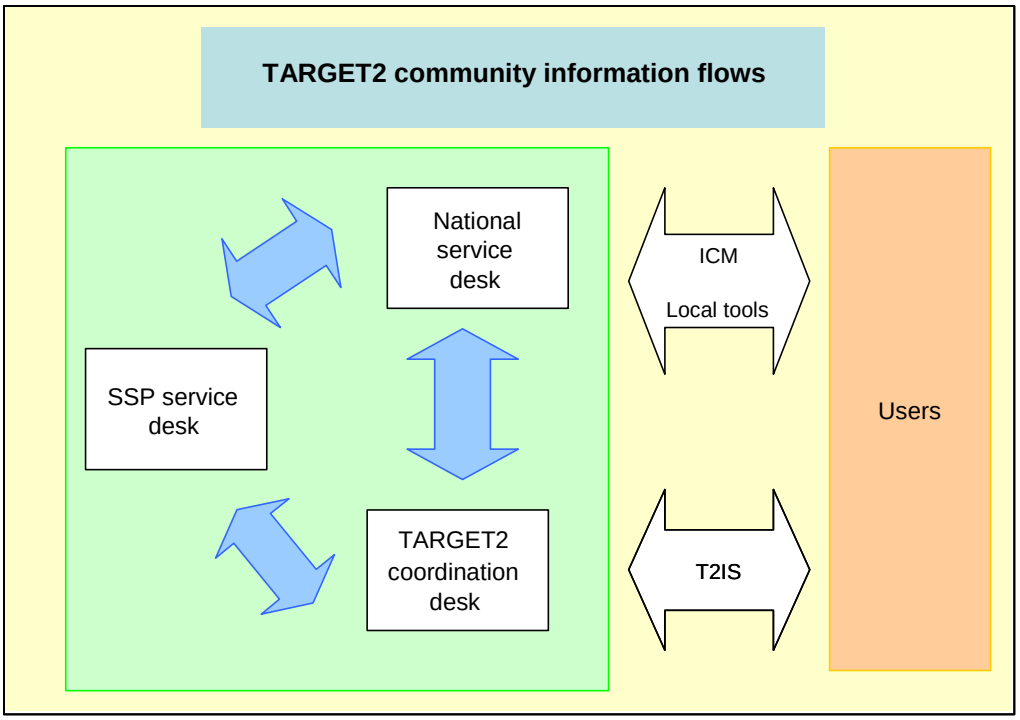


Diagram 6: Information flows

2.6.1. Information and control module

The functionality of the information and control module (ICM) gives direct participants access to a wide range of general information, e.g. on account balances or transactions. It also allows the national service desks to broadcast messages to their national banking community. If necessary, a broadcast message can be sent to all direct participants. In addition, a "ticker" is available for disseminating important information. These tools can only be used if access to the ICM is available. Accordingly, it may not be possible to use them in the event of" SWIFTNet connectivity problems or an SSP failure.

2.6.2. Local tools

Local tools refer to national communication means. The respective national service desk is the contact point for the TARGET2 users. The national service desks are interconnected via an internal ESCB teleconference system. A teleconference of the settlement managers also includes SSP service managers and is coordinated by the TARGET2 coordination desk at the ECB. In the event of a crisis, the settlement managers will escalate the problem to the crisis managers, who are also interconnected

via an internal ESCB teleconference system, including the SSP crisis managers.

The relevant NCB will inform its TARGET2 users about the available local communication channels. National contact details are available in the ICM, together with other national information, under *Contact Items*.

2.6.3. TARGET2 information system

The TARGET2 information system (T2IS) gives up-to-date information on the operational status of the TARGET2 system. It is used by news agencies to receive and disseminate information on the TARGET2 system to external parties. Hence, parties with access to the news agencies have access to this information, e.g. money market traders and the media. In addition, the T2IS information is also available via the ECB website on the sheet “Payments & Markets” in the section “TARGET2”.

In the event that TARGET2 is not fully operational, the T2IS is used to provide information about the type of failure, its impact and the measures envisaged to solve the problem.

3. Participation

3.1. Access criteria

The Eurosystem has developed the general legal structure and principles of participation in TARGET2, which should allow TARGET2 users to decide on the form of their participation in the system. TARGET2 provides a number of possibilities to access the system. These include direct and indirect participation, "addressable BICs" and "multiple-addressee access" to the system. TARGET2 users must meet the TARGET2 security requirements and controls as described in section 3.5 below.

3.1.1. Direct participation

The following types of entities are eligible for direct participation in TARGET2:

(a) credit institutions established in the European Economic Area (EEA), including when they act through a branch established in the EEA;

(b) credit institutions established outside the EEA, provided that they act through a branch established in the EEA; and

(c) NCBs of EU Member States and the ECB.

The respective central bank may, at its discretion, also admit the following entities as direct participants:

(a) treasury departments of central or regional governments of Member States active in the money markets;

(b) public sector bodies of Member States authorised to hold accounts for customers;

(c) investment firms established in the EEA;

(d) organisations providing clearing or settlement services that are established in the EEA and are subject to supervision and/or oversight by a competent authority and comply with the oversight requirements for the location of infrastructures offering services in euro, as amended from time to time and published on the ECB website, in which payments or financial instruments are exchanged and/or cleared while the resulting monetary obligations are settled in TARGET2 in accordance with the Guideline on TARGET2 and a bilateral arrangement between such organisation and the relevant Eurosystem central bank ("ancillary systems"); and

(e) credit institutions or any of the entities of the types listed under (a) to (d), in both cases where these are established in a country with which the European Community has entered into a

monetary agreement allowing access by any such entities to payment systems in the European Community, subject to the conditions set out in the monetary agreement and provided that the relevant legal regime applying in the country is equivalent to the relevant Community legislation.

Direct participants hold at least one account in the payments module of the single shared platform and are able to: (i) submit/receive payments directly to/from the system; and (ii) settle directly with their central bank. Direct participants are responsible for all payments sent from or received on their account by any entity registered through them in TARGET2 (indirect participants, multi-addressee access entities and addressable BICs as described below).

In addition, the direct participants are able to open special-purpose accounts for non-payment activity in the PM. These special-purpose accounts will be identified by a separate BIC11.

3.1.2. Indirect participation

Credit institutions established in the EEA can enter into a contract with only one direct participant that is either a credit institution or a central bank, in order to submit payment orders and/or receive payments, and to settle them via the PM account of that direct participant. TARGET2 central banks recognise indirect participants by registering such indirect participation in the TARGET2 directory.

Where a direct participant which is a credit institution and an indirect participant belong to the same group, the direct participant can expressly authorise the indirect participant to use the direct participant's PM account directly to submit payment orders and/or receive payments by way of group-related multi-addressee access.

3.1.3. Multi-addressee access

In the TARGET2 system, direct participants are able to authorise their branches and credit institutions belonging to their group, located in EEA countries, to channel payments through the direct participant's PM account without its involvement by submitting/receiving payments directly to/from the system. This offers affiliate banks or a group of banks efficient features for liquidity management and payments business.

More precisely, multi-addressee access through branches can be provided as follows:

(a) a credit institution which has been admitted as a direct participant can grant access to its PM account to one or more of its branches established in the EEA in order to submit payment orders and/or receive payments directly, provided that the respective central bank has been informed accordingly;

(b) where a branch of a credit institution has been admitted as a direct participant, the other branches of the same legal entity and/or its head office, in both cases provided that they are established in the EEA, can access the branch's PM account, provided that it has informed the respective central bank.

In practice, a multi-addressee bank is able to send and receive payments from/at its own BIC address. The payments, however, are booked on the account of its direct participant.

3.1.4. Addressable BICs

The TARGET2 addressable BICs are not subject to any system rules. Any direct participant's correspondent or branch that holds a BIC is eligible to be listed in the TARGET2 directory, irrespective of its place of establishment. Moreover, no financial or administrative criteria have been established by the Eurosystem for such addressable BICs, meaning that it is up to the direct participant to define a marketing strategy for offering such status. It is the responsibility of the direct participant to forward the relevant information to the respective central bank for inclusion in the TARGET2 directory.

Payment orders to/from addressable BICs are always sent and received via a direct participant. Their payments are settled in the account of the direct participant in the PM of the SSP.

	Account in PM	**Way to submit /receive payments**	**Settlement of Payments**	**Subject to the system rules**	**Listed in TARGET2 directory**
Direct participation	Yes	Directly	Own account in the PM	Yes	Yes
Multi-addressee access	No	Directly	Account of the direct participant	Yes	Yes
Indirect participation	No	Via direct participant	Account of the direct participant	Yes	Yes
Addressable BICs	No	Via direct participant	Account of the direct participant	No	Yes

Table 4: TARGET2 participation structure

3.1.5. Group of accounts

Different categories exist for receiving the group of accounts status:

Category 1: credit institutions that consolidate according to IAS 27;

Category 2: credit institutions that do not consolidate or consolidate according to other standards but which are in line with the definition provided under IAS 27; and

Category 3: bilateral and multilateral networks of savings and cooperative banks based on statutory/cooperation rules in line with national legal requirements.

Accordingly, the procedures for submitting an application for group status are as follows:

Category 1: submit an extract from the official consolidated statement of accounts or a certified declaration from an external auditor specifying which entities are included in the consolidation;

Category 2: submit a statement from an external auditor demonstrating to the NCB that the consolidation is equivalent to IAS 27; and

Category 3: the NCB will first prepare an assessment demonstrating that the "group" is in accordance with the national legal requirements and/or the statutory framework and that it fulfils the policy requirements as specified in the TARGET2 legal framework. In addition, the ECB Governing Council has to approve an application to be considered as constituting a group.

3.2. Internet-based access

Internet-based access to TARGET2 is an alternative mode of connection to the SSP that offers direct access to the main TARGET2 services[9] without requiring a connection to the SWIFT network. Accordingly, participants with internet access do not send and receive message via the SWIFT network but use the ICM to initiate payments in the SSP and to receive information about payments addressed to them, as well as account statements.

Internet-based access supports the following functionalities.

- Monitoring an RTGS account via the ICM, including online information on inward and outward (final and pending) transactions and on ancillary system settlement and liquidity positions.
- Initiating TARGET2 credit transfers via specific ICM screens, including MT103(+), MT202(COV) and liquidity transfers to both SWIFT-based and internet-based participants.

[9] A bank can use internet-based access to access a PM account or a HAM account.

- Displaying inward TARGET2 credit transfers from both SWIFT-based and internet-based participants, including MT103(+), MT202(COV) and liquidity transfers, and MT204 from SWIFT-based participants.
- Displaying notifications, broadcasts and end-of-day reporting messages on the ICM. An account statement can be downloaded at the start of the next business day.
- Managing limits and reservations; managing queues, including changing priorities, reordering items, changing execution times and revoking queued payments.
- Settling a participant's position in ancillary system settlement, including procedure 6 of the ancillary system settlement, for which sub-accounts can be created.
- Settling payments in relation to Eurosystem open market operations.
- Consulting the TARGET2 directory online.

Internet-based participants can access the ICM in user-to-application (U2A) mode only. It is not possible to include an internet-based account in a group of accounts arrangement or multi-addressee access arrangement, or to have addressable BICs linked to it.

The internet connection is closed for security reasons between 22:00 and 6:30. In addition, no payments can be entered between 19:30 and 22:00 or between 06:30 and 6:45, with the exception of liquidity transfers.

3.3. Static data collection

Registering in TARGET2 requires that direct participants register separately with the SSP and with SWIFT, in the case of SWIFT-based participants, or with an Accredited Certification Authority, for internet-based participants[10]. For payments purposes only BICs published in the TARGET2 directory can be used.

Registration with an Accredited Certification Authority should be carried out following the procedures specified in the "User Manual Internet Access for the public key certification service", available on the TARGET2 website. For registration with SWIFT, see below.

3.3.1. SWIFT registration process

The SWIFT registration allows participants to get the appropriate SWIFT services for TARGET2. It is

[10] Internet-based participants need a BIC1, which is an unpublished BIC.

done electronically via the SWIFT website, based on an electronic form developed by SWIFT and customised for TARGET2 (the so-called "e-ordering"). Publication in the BIC directory will only become effective on one day per month. For the e-ordering process, central banks will first validate and approve all registration requests and the SSP service desk (3CB) will make the second approval. The full process, including validations and implementation by SWIFT, can take two to five weeks. To ensure the consistency of static data between SWIFT and the SSP the TARGET2 users should use the e-ordering via www.swift.com for any modification, especially for the ones related to Message Routing Rules (MRR). In case the participant uses "myswift.com", which is a SWIFT customer relationship management website, the change should be made in coordination with the NCB. The NCB has to be informed, before the implementation date. Further information on the SWIFT registration is available at www.swift.com.

3.3.2. SWIFT authentication

Direct PM participants need to have a SWIFT Relationship Management Application (RMA) authorisation in place with TRGTXEPM, HAM participants with TRGTXEHM, the HAM co-manager with TRGTXEPM and TRGTXEHM, and central bank customers with TRGTXECB. This step is compulsory for all direct PM, HAM or central bank customers.

3.3.3. SSP registration process

The collection of static data for the SSP is a prerequisite for TARGET2 users to access the SSP. The collection of static data is paper-based via the TARGET2 forms. Central banks will key in the information from the forms via the ICM.[11] From a procedural point of view, there are four steps to be followed.

- **Analysis**

The participant performs its analysis of the changes needed according to its change management procedure and fills in the necessary forms. The forms are then submitted to the respective central bank.

The processing of changes to the static data is mainly driven by the TARGET2 user. The TARGET2 user defines its requirements; often in contact with SWIFT and/or the central bank to get information on the feasibility, in particular for complex changes, a prior communication with the central bank is necessary. TARGET2 users may start with a business description of their future organisation/change.

11 A detailed description of the forms can be found in "User guide for the collection of static data".

The time required for the analysis depends on the TARGET2 user's organisation. For some changes, the related tasks might require some time (e.g. new BIC, legal opinion, certification phases, etc.), while for minor static data changes this phase should be short.

As a result, the TARGET2 user submits to its central bank:

- where applicable, a business description of the change and the process (e.g. account set-up, technical changes, need for specific testing and support);
- where applicable, relevant legal documentation (e.g. country opinion);
- where applicable, technical documentation (e.g. on resiliency information); and
- SSP registration forms.

- **Assessment and validation**

At the legal and technical levels, the central bank checks the forms according to its local rules. In case of significant changes, the above-mentioned analysis should involve the central bank. Additionally, the central bank checks if the SWIFT registration is consistent with the static data collection forms.

The checks by the central bank aim at maintaining legal and operational safety for the whole TARGET2 system.

The central bank has to check that the certification of the TARGET2 user will still be valid under the new conditions. Otherwise a new certification phase (the content of which depends on the current certification status and the nature of the change to be made) has to be planned[12] and successfully performed. A TARGET2 user can also request testing activities before moving to the live environment. The checks also include the validation of the registration forms.

As a result, the central bank either validates or rejects the request.

- **Processing of the static data collection**

After validation, the central bank keys in the data from the forms via the ICM. If there is an impact on the TARGET2 directory, the weekly deadline for updates of the TARGET2 directory has to be taken into account.

- **Final check**

The TARGET2 users should check the validity of the modification using the ICM.

[12] According to the change, the modification planned could have to be also implemented in the testing environment.

3.3.4. Conflicting registration

The TARGET2 directory allows only one registration per participant BIC (direct or indirect) and only a single relationship between an addressable BIC/indirect participant and the direct participant which provides the access to TARGET2. It is therefore possible that two or more participants will send conflicting registration forms to their central banks. Therefore, banks should check in the TARGET2 directory whether or not the BIC they wish to register as an addressable BIC/indirect participant is already registered with another direct participant before they send a registration form to their central bank for the registration of addressable BICs.

If the addressable BIC/indirect participant (bank X) is already registered in the TARGET2 directory in connection with another direct participant B, the requesting direct participant A will have to contact the other direct participant B to inform it that the routing instructions for the addressable BIC/indirect participant (bank X) will change.

The direct participant B which is currently the relationship of Bank X, will then have to fill in a form to request the deletion of the existing relationship and will submit this form to its central bank and to the direct participant A.

The direct participant A will then forward to its central bank its own form for the registration of the addressable BIC/indirect participant (bank X) together with a copy of the form for deletion of the former relationship signed by the other participant B.

In the event that the addressable BIC/indirect participant is not in the TARGET2 directory at the time when the participant makes the check, but during the same week another participant requests the registration of the same BIC as an addressable BIC/indirect participant, one central bank request to create the new record would be rejected. That central bank would have to inform the banks about the conflicting registration request. It is up to the banks to reach an agreement on which bank should be the direct participant representing the correspondent.

3.4. TARGET2 directory

To support the routing of payment instructions, the TARGET2 directory is available. The TARGET2 directory uses SWIFT-related information in combination with TARGET2-specific information provided by the TARGET2 users during the SSP registration. The TARGET2 directory is the database of BICs used for the routing of payment orders.

Unless otherwise requested by the TARGET2 user, BICs shall be published in the TARGET2

directory.[13]

The content of the TARGET2 directory is based on the SSP static data, as collected from direct participants on designated forms. The forms will be used by direct participants to request the opening of their account(s) and to collect all other information required by the system. In particular, the direct participant is responsible for the registration of its indirect participants, multi-addressee access entities or addressable BICs and is liable for any mistakes or misuse during this process.

The TARGET2 directory contains information on each institution that can be addressed in TARGET2. Apart from the participant's BIC (bank identifier code), it also contains the addressee BIC (i.e. the BIC to be used to receive and send payments), account holder (i.e. the BIC of the RTGS account), institution name, city heading and national sorting code (if available). The following is an example of an entry for a direct participant in the TARGET2 directory:

BIC	BANKBEBBXXX
Addressee	BANKBEBBXXX
Account holder	BANKBEBBXXX
Institution name	Bank S.A. Brussels
City heading	Brussels
National sorting code	-
Main BIC flag	Yes
Type of change	A
Valid from	20080218
Valid until	99991231
Type of participation	01

Table 5: TARGET2 directory

The TARGET2 directory is distributed[14] only to direct participants. Distribution takes place via SWIFTNet FileAct (pull mode only for the full directory; pull mode and push mode for updates).

[13] BICs that are unpublished in the TARGET2 directory are still published in SWIFT's BIC directory.

[14] Internet-based participants can consult the TARGET2 directory online.

Downloading the full content might mainly be envisaged for the initial loading of the directory or where there is a need to rebuild it. Owing to the size of the file, the use of compression is strongly recommended. Furthermore, direct participants might download the TARGET2 directory at a central point and distribute it internally. Direct participants may only distribute the TARGET2 directory to their branches and entities with multi-addressee access. They are not allowed to forward the TARGET2 directory to any other third parties via any other means.

There is no paper version of the TARGET2 directory. The TARGET2 directory is updated on a weekly basis. Updates are delivered overnight, between Thursday and Friday, for activation the following Monday. The full version is available from Friday morning. It is highly recommended that the TARGET2 users submit change requests to their central banks well in advance, possibly indicating a future activation date. For static data changes impacting the TARGET2 directory it is advisable to choose a Monday as activation date to ensure consistency between static data and the TARGET2 directory. Furthermore it is suggested to choose the first Monday after the monthly update of the SWIFT BICPlusIBAN Directory, in order to be consistent with it.

3.5. Certification testing

Each TARGET2 user must undergo a number of certification testing activities depending on the SSP modules chosen by the respective central bank and the functionalities chosen by the TARGET2 user. Another factor having an impact on the type and number of tests to be performed is, for example, the participation in different ancillary systems. Certification can be split into technical certification, which will consist of the successful individual completion of a number of connectivity and interoperability test cases, and operational certification, which will be assessed based on the participation in country and business day testing.

The test environment of the TARGET2 user should be as similar to the future live environment as possible. Any component used should have already undergone an internal acceptance test procedure.

The respective central bank must be informed in writing about any changes in the test environment and/or the future live environment of the TARGET2 user during or after the certification testing. That includes any technical change (e.g. to technical components or software) as well as any business change related to the interaction with TARGET2. By business change is meant a change of the account structure or specifically the use of optional functions which were not used in the past and therefore were not part of a previous certification process. Besides clearly describing the nature and scope of the change and the associated risks, this information should contain a proposal with regard to the test cases to be re-run due to the change (non-regression testing). The central bank will assess the

proposal made. In principle, changes during the technical certification (i.e. connectivity and interoperability tests) are possible, changes during the business certification (i.e. country and business day tests) should be avoided and changes after a TARGET2 user's certification are not allowed and would require a new certification process. Nevertheless, to keep the necessary flexibility, exemptions to these principles can be granted by central banks if duly justified.

The technical set-up of the SSP and/or the PHA can change following yearly releases, emergency changes and "hot fixes"(e.g. bug fixing). For such cases, the central banks will assess the impact of the changes on the certification process already carried out by TARGET2 users and will inform them accordingly. In some cases, users may be required to re-run a limited number of certification test cases (non-regression testing). Such requests to run non-regression tests will be kept to the strict minimum.

3.6. Measures to ensure the security and operational reliability of TARGET2 users

3.6.1. Tasks and responsibilities

In order to ensure the security and operational reliability of TARGET2 users, the following four main tasks and responsibilities can be distinguished:

- framework setting by the Eurosystem: producing guidelines to be followed by all actors involved and specifying common requirements that should be met by the TARGET2 users;
- compliance check by central banks: checking whether the TARGET2 users are in compliance with the measures laid down in the framework;
- provision of information by the TARGET2 users: providing central banks with the relevant information as specified in the framework; and
- monitoring and follow-up activities by central banks: identification of weaknesses and monitoring of follow-up activities initiated to address these weaknesses.

In order to ensure that all TARGET2 users will have to meet the same criteria and to facilitate that the compliance checks are carried out in a harmonised manner, consistent and effective guidelines and procedures have to be in place. The responsibility for establishing and maintaining this framework is assumed by the Eurosystem.

As regards compliance checks, the guiding principle is that the customer relationship remains under the full responsibility of the NCB with which the TARGET2 user has a legal relationship. In this context, it must be stressed that the decisive criterion is not whether the TARGET2 user is located

inside or outside the euro area. Rather, it has to be considered whether a central bank is within the TARGET2 area[15].

> **Examples:** Denmark has not adopted the euro, but the Danish central bank is participating in TARGET2. Consequently, direct participants with their head office located in Denmark will typically establish a legal relationship with the Danish central bank. The situation is different for direct participants with their head office located in the United Kingdom. The Bank of England has decided not to participate in TARGET2. Therefore, any UK-based direct participant will have to select a TARGET2 central bank with which it will establish the legal relationship.

From a central bank perspective, the following questions should be asked in order to identify whether it is responsible for collecting the relevant information from a particular TARGET2 user.

Does the TARGET2 user manage its own technical infrastructure used for routing payments to TARGET2?

- If the answer is "Yes": the central bank of this direct participant is the responsible central bank.
- If the answer is "No": is the infrastructure used for routing payments to TARGET2 managed by another direct participant based in a different country (e.g. member/concentrator, branch/subsidiary, head office of a direct participant)?
  - ➢ If the answer is "Yes": the central bank of the direct participant managing the technical infrastructure is the responsible one.
  - ➢ If the answer is "No": does the institution managing the infrastructure offer the same service to other direct participants (e.g. service bureau)?
    - o If the answer is "Yes": the central bank having the legal relationship with the biggest direct participant in terms of value using this infrastructure is responsible.
    - o If the answer is "No": the central bank having the legal relationship with the direct participant is responsible.

If a direct participant wants to determine which central bank is responsible for its institution the following table provides some guidance by describing different possible combinations.

15 The TARGET2 area comprises the countries of all central banks participating in TARGET2.

Description of the situation	Central bank responsible
Head office located inside/outside[16] the TARGET2 area; no branches/subsidiaries.	Central bank having the legal relationship with the head office.
Head office and branches/subsidiaries located inside/outside the TARGET2 area; both are direct participants and payments traffic is routed to TARGET2 via the technical infrastructure of the head office.	Central bank having the legal relationship with the head office.
Head office and branches/subsidiaries located inside/outside the TARGET2 area; both are direct participants but have their own technical infrastructure used for routing payments to TARGET2.	Each individual central bank having the legal relationship with the head office and the branches/subsidiaries.
Head office located inside/outside the TARGET2 area not having a legal relationship with a TARGET2 central bank but payments traffic is routed via a branch/subsidiary which is a direct participant (no matter where the technical infrastructure is located).	Central bank having the legal relationship with the branch/subsidiary.
Service provider not having a legal relationship (no matter whether located inside or outside the TARGET2 area) is managing the technical infrastructure for financial institutions which are direct participants.	Central bank having the legal relationship with the financial institution generating the biggest turnover in terms of value when routing payments to TARGET2 using the technical infrastructure of a service provider.

Table 6: Central bank responsibility for direct participants

As suggested by the table above, there might be an exception to the rule as regards service bureaus (see the section entitled "Service bureau and member/concentrator"). It is conceivable that a number of (low-volume) direct participants located in different countries share the technical infrastructure provided by such an organisation. However, service bureaus do not establish a legal relationship with a central bank. Rather, they maintain a legal relationship only with customers using their technical infrastructure for routing transactions to TARGET2. However, direct participants using a service

[16] In case the head office is located outside the TARGET2 area, it needs to be within the EEA.

bureau are legally bound by the Harmonised Conditions to provide their central bank with information about a failure of such an organisation.[17] In such a case and in order to avoid the collection of identical information via different direct participants, it is the task of the central bank maintaining the legal relationship with the biggest direct participant[18] in terms of value of those participants using the same service bureau to check whether it is in compliance with the measures laid down in the framework for ensuring the security and operational reliability of TARGET2 users (see the section on "Critical participants and normal participants").

When direct participants use a member/concentrator[19], two possibilities exist: either the member/concentrator is a direct participant itself, in which case the central bank that has the legal relationship with this direct participant will assume the responsibilities set out in this Infoguide; or the member/concentrator is only a connectivity service provider (not having a legal relationship with a central bank), in which case the central bank maintaining the legal relationship with the biggest direct participant[20] in terms of value of those participants using the same member/concentrator is responsible for checking compliance with the relevant security requirements.

To ensure that these checks can be effectively performed, the direct participants will have to provide their central bank, upon request, with the necessary information and documentation.

Any weakness identified will have to be carefully evaluated, based on a harmonised approach. Follow-up action to address these weaknesses will have to be agreed and their implementation will have to be monitored. This is also a task to be performed by the central banks.

Finally, there should be no overlap between the tasks performed by central banks in the context of this framework and the activities carried out by other regulatory bodies, e.g. banking supervisors or overseers.

3.6.2. Critical participants and normal participants

Notwithstanding the overarching requirement to ensure a level playing-field between TARGET2 users, all stakeholders recognise that the impact of a security failure affecting the systems of financial institutions can vary depending on the market share in terms of value and/or the type of transactions

17 Harmonised Conditions, Article 28 (2): *"Participants shall inform the [central bank responsible] of any security-related incidents in their technical infrastructure and, where appropriate, security-related incidents that occur in the technical infrastructure of the third party providers."*

18 The biggest direct participant using a service bureau might change, for example following a merger. If such a situation arises, it will have to be considered how to proceed.

19 The same principle applies when TARGET2 users establish other arrangements for sharing IT infrastructure, e.g. by outsourcing the processing of payments to a specialised company (in some cases a joint venture with other TARGET2 users).

20 See footnote 14.

processed (e.g. settlement transactions of systemically important ancillary systems). Taking this into account, a distinction can be made between *critical participants* and *normal participants*.[21]

A basic set of instruments will be used for both critical participants and normal participants. However, in recognition of the vital importance that critical participants have for the smooth functioning of the TARGET2 system, such TARGET2 users will have to implement some additional measures.

In the following, TARGET2 users are subdivided into credit institutions, ancillary systems and service bureaus/concentrators. For each group, it is explained which participants are classified as critical participants and which ones are considered normal participants.

3.6.2.1. Credit institutions

General considerations and rationale

The guiding principle applied when establishing criteria to determine whether a credit institution is a critical participant was that organisations with a sufficient market share in terms of value are eligible, as well as those where *"the inability of one of the [system] participants to meet its obligations […] could result in the inability of other system participants or of financial institutions in other parts of the financial system to meet their obligations as they become due".*[22] In other words, an operational disruption[23] could result in the accumulation of liquidity on a TARGET2 user's account, which in turn could prevent other TARGET2 users from making payments and thus potentially create systemic risk.

Criteria

The definition of criteria to distinguish critical credit institutions from non-critical ones should logically depend on the statistical distribution profile of the credit institution's turnover figures in terms of value.

While there might be different ways to determine the criticality of credit institutions, the Eurosystem has currently defined three criteria that should be applied:

1. As a general guideline, the Eurosystem considers a credit institution as a critical participant in TARGET2 if it consistently settles at least 2% in terms of value of the TARGET2 turnover

21 This is also in line with the document "Business continuity oversight expectations for systemically important payment systems" approved by the Governing Council of the ECB on 31 May 2006. In this document, it is stated that critical participants "… are identified as such by SIPS operators …".

22 Core Principles for Systemically Important Payment Systems, Bank for International Settlements, January 2001.

23 As opposed to balance sheet problems.

(including liquidity transfers[24]) on a daily average.

2. The accumulated market share of those credit institutions settling at least 2% of the value of transactions should reach at least 25% of the overall TARGET2 turnover in terms of value. If this threshold is not reached by adding the individual figures of those credit institutions fulfilling the 2% criterion, banks with a lower market share will be added to the list of critical participants.

3. There should be a noticeable difference (e.g. 0.1%) between the market share settled by the credit institution last-ranked as a critical participant and the top-ranked credit institution in the normal participant.

These criteria will be reviewed at regular intervals. The review clause described in Section 3.6.8 is the mechanism that will be used to ensure that the criteria are brought into line with business practices in the light of experience gained during TARGET2 operations.

It is possible that two or more credit institutions share the technical infrastructure used for participating in the TARGET2 system. If the overall value of the transactions settled by these credit institutions in the shared environment is equal to or greater than 2% in terms of value, the organisation (for instance a transaction bank) operating the infrastructure in the legal sense is classified as a critical participant. It is noteworthy that in addition to these criteria which are commonly agreed by the Eurosystem, central banks may take into account the specific national features when classifying credit institutions with which they maintain a business relationship. As a consequence, central banks can propose to classify direct participants as critical participants even if none of the criteria are met. The relevant central bank has to inform the ECB about this reclassification and to explain the rationale behind it. The ECB will then form an opinion on whether the reclassification is reasonable. This opinion will be submitted to the relevant Eurosystem committee[25] for further consideration and this committee might decide that the criteria used by the reclassifying central bank should be commonly used. Finally, it should be noted that if a direct participant falls within the scope of the three above-listed criteria, central banks are not able to categorise this participant as a normal participant.

[24] Due to the central banks' choice, in some central banks end-of-day/start-of-day liquidity transfers to/from the proprietary home account (PHA) take place, in which participants are not actively involved given that the former are automatically executed by the SSP and the latter are triggered by the central bank. In such cases the liquidity transfers should be deducted from the overall turnover. Whether this can be done in an automated way or requires manual calculations will have to be investigated in the context of the first review exercise (see section "Review clause").

[25] The relevant committee is the Payment and Settlement Systems Committee (PSSC) which assists the decision-making bodies of the Eurosystem in the fulfilment of the ESCB's basic tasks, more specifically to promote the smooth operation of payment systems.

3.6.2.2. Ancillary systems

The group of ancillary systems is composed of organisations in the field of securities clearing and settlement, retail payment systems (systemically important retail payment systems (SIRPS), prominently important retail payment systems (PIRPS) and other retail payment systems), and other large-value payment systems (e.g. CLS and EURO1).

As with credit institutions, for ancillary systems there is no empirical evidence on what exactly could cause systemic risk. Therefore, criteria for determining the criticality of ancillary systems were defined based on the results of a consultation of the relevant Eurosystem entities and available documentation.

Retail and large-value payment systems

Large-value payment systems are by definition classified as systemically important. Considering that a failure to settle payments for these large-value payment systems in TARGET2 could transmit shocks across the financial system (and in case of CLS even globally), these systems are classified as critical participants.

Following the same logic, SIRPS settling via TARGET2 are also assigned to the category of critical participants.

As regards PIRPS and other retail payment systems, it was felt that a failure to clear the net balances in central bank money would not have systemic implications for the TARGET2 system or its participants. Therefore, these systems are classified as normal participants.

Organisations in the field of securities clearing and settlement

Organisations in the field of securities clearing and settlement are CSDs (central securities depositories), ICSDs (international central securities depositories) and CCPs (central counterparties).

In the opinion of the Eurosystem, all these systems are of systemic importance and the failure of an (I)CSD/CCP would have knock-on effects on the smooth functioning of TARGET2. Consequently, all organisations in the field of securities clearing and settlement are considered critical participants.

In order to avoid over-regulation, the relevant central bank may have to examine on a case-by-case basis whether a particular organisation in the field of securities clearing and settlement should indeed be classified as a critical participant. If the outcome of this examination were to demonstrate that the failure of such an organisation would not have systemic implications for the TARGET2 system or its

participants, the relevant central bank could classify it as a normal participant. The relevant central bank has to inform the ECB about this reclassification and to explain the rationale behind it. The ECB will then form an opinion on whether the reclassification is reasonable. This opinion will be submitted to the relevant Eurosystem committee for further consideration and this committee might decide that the criteria used by the reclassifying central bank should be commonly used.

3.6.2.3. Service bureaus and member/concentrators

Apart from sharing the connection to SWIFTNet of another SWIFT customer, there are two other ways for a TARGET2 user to connect indirectly[26] to SWIFTNet. These are:

- outsourcing the day-to-day operation to a third party, called a service bureau[27]; and
- in addition to the technical connectivity (see previous bullet point), using a member/concentrator which provides supplementary business services, e.g. taking care of the SWIFT administration and invoicing on behalf of the TARGET2 user.

Credit institutions and potentially also ancillary systems could decide to use one of these connectivity models. Considering that these organisations obtain a BIC8 for addressing through SWIFT and take responsibility for their messages, they are direct participants, although they are only indirectly connected. Since the payments traffic of multiple TARGET2 users would be routed via an indirect connection, an operational failure of the service bureaus' or member/concentrators' technical infrastructure might have systemic implications.

Although the Eurosystem has provisionally concluded that service bureaus are not as such considered critical participants at this stage, it seems advisable that, if the total payments traffic routed via such an organisation exceeds the 2% criterion applicable to credit institutions, it is treated like a critical participant.

Since service bureaus and member/concentrators do not have a legal relationship with the Eurosystem, the legal basis for such organisations to fulfil the requirements laid down in this Infoguide can only be created via the direct participants.

[26] An indirect connection to SWIFTNet is typically used by smaller institutions which are looking for a cost-effective SWIFTNet connectivity solution.

[27] A service bureau is defined as a *"non-SWIFT organisation entitled under the SWIFT Service Bureau Policy to provide facilities management and/or data processing services to one or more SWIFT Users, including operation of a SWIFT interface for prime connection to the network and/or for disaster recovery. A Service Bureau may not send or receive messages through the SWIFT network for its own account and accordingly is not entitled to a SWIFT address"* (SWIFT Glossary, March 2005 edition).

3.6.3. Measures to ensure the security and operational reliability of TARGET2 users

The guiding policy principle is that measures applied to ensure the security and operational reliability of TARGET2 users should be commensurate with their criticality. In the previous sections criteria for determining critical participants were outlined. Section 3.6.3.1 describes the measures that should be used for both critical participants and normal participants. Section 3.6.3.2 outlines the procedures that should be applied for critical participants only.

3.6.3.1. Measures applied for critical participants and normal participants

Measures applied for critical participants and normal participants

One measure to address security issues from a general perspective is the insertion of a clause in the legal arrangements between the central banks and the TARGET2 users.

In particular, Article 28 (1) of the Harmonised Conditions for participation in TARGET2 clearly states that it is under the full responsibility of the TARGET2 user to ensure that the confidentiality, integrity and availability of its system are adequately protected.

Moreover, Article 31 (4) of these conditions states, *inter alia*, that central banks will not be liable if a loss is caused by the TARGET2 user. It implies that if the smooth functioning of TARGET2 is affected because of an incident caused by the malfunction of the TARGET2 user's system, the TARGET2 system operator will not accept any liabilities towards this TARGET2 user. However, the TARGET2 user which caused the problem would have to reimburse the central bank (subject to the conditions set out in the Harmonised Conditions and under the applicable law) if the latter had to compensate other TARGET2 users because of this incident.

Monitoring and incident reporting

A TARGET2 user's capability to prevent liquidity accumulation on its account is of crucial importance for the smooth functioning of the TARGET2 system. Therefore, monitoring the performance in terms of availability of a TARGET2 user's component and incident reporting are two means that can – in the longer run – contribute to the stability and robustness of the TARGET2 system.

Once a TARGET2 user is live in the TARGET2 system, its performance is closely monitored[28] by the respective central bank.

In the event that a TARGET2 user is affected by an operational disruption, staff responsible are requested to inform, upon their own initiative, the relevant central bank immediately. Once the TARGET2 user has resumed operations, the central bank may send an incident report form (Annex II) to the TARGET2 user for completion. This report requires the TARGET2 user to describe the root cause of the problem, the impact, the steps taken to resolve the issue and mitigating action that should prevent the incident from reoccurring.

A minor operational disruption, although it might cause inconvenience when making some payments, is not considered critical as long as the duration[29] does not exceed 30 minutes for critical participants. As long as the duration of an incident is below this limit, an incident report would not be required. For normal participants, it is up to the relevant central bank to decide whether an incident report is required. The decisive factor is whether the incident had an impact on the smooth functioning of TARGET2 or other TARGET2 users. In this context, it is worth mentioning that an incident report is not required when a TARGET2 user makes a conscious decision to suspend payment processing activities for a certain period of time, although it is not facing any technical problems. In order to avoid confusion, the TARGET2 user is invited to inform its respective central bank about the suspension as soon as possible.

As stated above, a formal incident report is not required if the operational disruption is less than 30 minutes or based on a conscious decision to suspend payment processing activities. However, if a central bank observes repetitive short service interruptions, it will contact its TARGET2 user and ask for clarification which could ultimately result in the need for a formal response.

TARGET2 users must return the incident report to the relevant central bank within two business days of the occurrence of the incident. The character of this report could be twofold:

- If the incident has already been evaluated at that time, this first incident report is considered as the final evaluation report.
- If the incident is still under investigation, the initial information that can already be provided should be considered as an interim report. The final evaluation report**,** which complements the information given in the interim report, should then be sent to the central bank no later than one month after the incident occurred.

28 CP VII (7.7.4): System operator activities should also involve *"monitoring the security and operational reliability of the participants, for example the availability of their components during normal business hours"*.

29 Calculated from the moment the downtime was detected until the moment the system was operational again.

Once the incident report is marked final, it is reviewed, analysed and recorded in a service incident log. If a TARGET2 user's performance was posing risks to the smooth functioning of TARGET2 or other TARGET2 users, adequate measures will have to be taken, e.g. it should be drawn to the attention of senior officials of the TARGET2 user.

Incidents affecting the TARGET2 user's availability are probably the only ones that could be identified by the system operator itself by comparing actual payment processing with normal patterns. When a central bank notices a deviation from the normal pattern and suspects that the TARGET2 user may be experiencing potentially serious availability problems it has not been informed about, the TARGET2 user will be contacted and an explanation will be requested.

In addition, TARGET2 users are requested, upon their initiative, to report security problems concerning confidentiality and integrity. If information about such problems is made publicly available, this could have a negative effect on the reputation of the TARGET2 system as a whole. Only if the system operator is informed about such incidents can it be ensured that an appropriate communication strategy is in place to reassure financial markets and the public.

3.6.3.2. Measures to be used for critical participants only

System security in accordance with standards

Core Principle VII identifies different standards as being appropriate to the payment and banking industry. According to section 7.7.5 of the Core Principles, compliance with such national or international standards will help to ensure a high degree of security and operational reliability.

Taking this into account, critical participants are asked to self-certify that security within their organisation is addressed in line with internationally recognised standards such as ISO/IEC 27002:2005[30], which is explicitly listed in the Core Principles[31]. Compliance with other standards focusing on information security might also be acceptable.

For this purpose, senior management responsible for the business area (i.e. board level) of the critical participant shall file with the relevant central bank a self-certification statement[32] indicating the process by which compliance with one of these standards is envisaged and the actual extent of compliance with the standard. Given the heavy reliance on information technology (IT), the self-

30 This standard was formerly known as ISO/IEC 17799:2005 but its content remained unchanged.

31 The Core Principles *(published in 2001)* make a reference to the British Standard BS 7799:1999. This national standard has in the meantime become an international one and its latest version is known as ISO/IEC 17799:2005 *(published in June 2005)*.

32 The self-certification statement is attached in annex III.

certificate must, in addition, be signed by a senior official from the IT area (board level) of the critical participant's organisation. If one senior official of the critical participant is responsible for both, the business and the IT area, one signature is sufficient.

Central banks will send the self-certification form to their critical participants, which have three months to respond. Central banks monitor whether the signed form is returned by the indicated deadline and, if not, contact the critical participant to clarify the situation.

In case of any non-compliance with the (self-imposed) standard, the self-certificate should be complemented with a description of the major risks[33] associated with this situation. Furthermore, an action plan for rectifying the situation and the planned dates for implementing the particular measures should be included. This information is evaluated and the implementation of mitigation measures monitored by the central bank responsible.

Business continuity

On 31 May 2006 the Governing Council of the ECB approved the "Business continuity oversight expectations for systemically important payment systems (SIPS)" (in the following referred to as "oversight expectations"). This report lays down new oversight expectations with regard to business continuity for systemically important payment systems processing the euro.

The oversight expectations include a section dedicated to system's participants because *"the technical failure of critical participants in the system may induce systemic risk"*. According to this document, participants which are identified as critical by the system operator have to meet certain minimum requirements to ensure that business can be continued in the event of an operational disruption. The oversight expectations allocate the responsibility for verifying whether these requirements have been fulfilled to the system operator.

In particular, critical participants are requested to confirm that:

- business continuity plans are produced and procedures for maintaining them are in place;
- there is an alternate site in place; and
- the risk profile of the alternate site is different from the one of the primary site. Having a different risk profile shall mean that the alternate site must be a significant distance away from, and does not depend on the same physical infrastructure components[34] as the primary business location.

33 Major risks could be: insufficient measures against denial of service attacks; uninterruptible power supply not in place; the four-eyes control is not effective.

34 It should be noted that there is no obligation to use different hardware brands and/or software components, e.g. to install MS

This minimises the risk that both could be affected by the same event. For example, the alternate site should be on a different power grid and central telecommunication circuit from the primary business location.[35]

In this context, it is acknowledged that critical participants can only be responsible for what is within their immediate sphere of control. There is an element of reliance on suppliers and critical participants cannot be held liable if the resilience of a service provided by a third party is less robust than expected. However, the critical participants should make efforts to ensure that an appropriate level of resilience is stipulated in the contract with the suppliers. For example, a telecom provider should commit on multiple routing facilities and this should be laid down in the contractual arrangements.

- in the event of a major operational disruption rendering the primary site inaccessible and/or rendering critical staff unavailable, the critical participant is able to resume normal operations from the alternate site where the business day can be properly closed and reopened the following business day;
- in order to bridge the time needed for moving business from the primary to the alternate site, procedures are in place to ensure that the most critical business transactions can be performed; and
- the ability to cope with operational disruptions is tested at least once a year and critical staff are adequately trained.

Critical participants should confirm their level of compliance with the oversight expectations in the context of the self-certification process. Central banks will then check whether the oversight expectations are being met. A testing programme will verify whether the provisions for business continuity are effective (see the section on "Testing").

Testing

In order to verify that business continuity arrangements are effective, they have to be tested at regular intervals.

Core Principle VII stipulates that testing of the clearly documented business continuity arrangements should also involve the system's participants.

Windows infrastructure in the primary site and UNIX systems in the alternate location. The statement "*…should not depend on the same physical infrastructure…*" emphasizes that alternate sites should not rely on the same infrastructure components (e.g. transportation, telecommunications, water and electricity supply) as those used by the primary site.

35 Derived from the "High-level principles for business continuity" prepared by the 'The Joint Forum', Bank for International Settlements, August 2006.

Testing activities can, in principle, be subdivided into two different scenarios. The first scenario comprises bilateral testing of contingency arrangements between critical participants and a central bank. These activities are already an integral part of the TARGET2 user testing programme that TARGET2 users have to perform prior to joining TARGET2.

For critical participants, it is mandatory to take part in the testing activities. The successful completion of the tests will be monitored by the relevant central banks.

Annual self-recertification

Systems processing information like payment transactions are operating in a changing environment. New threats, new business requirements or newly identified vulnerabilities might change the security situation of a particular system considerably.

For this reason, the TARGET2 system operator needs to be reassured that the security of critical participants' components continues to meet the requirements specified by the Eurosystem. Therefore, on a yearly basis critical participants will be asked to recertify that compliance with the Eurosystem's requirements is still being observed.

In this context, it is noteworthy that the annual self-recertification should not be confused with the technical testing activities each TARGET2 user has to successfully complete before a connection to TARGET2 will be permitted.

3.6.4. Implementation

3.6.4.1. Legal enforceability

The Harmonised Conditions for participation in TARGET2, more specifically Article 28, outline at a high level the security measures, thus setting the framework for the legal enforceability of the detailed measures specified in this Infoguide. However, the practical and legal implementation which makes the individual measures binding for TARGET2 users is a national responsibility of each central bank. Consequently, it is up to the central banks to decide how to integrate the security measures for TARGET2 users into the legal arrangements with their TARGET2 users (e.g. annex to the contract, publication on the website with a reference in the contract, letter from the central bank, etc.). As the legislation varies from country to country, to ensure that the measures are legally enforced in a similar way and in accordance with the provisions of the Harmonised Conditions for participation in TARGET2 in all countries participating in TARGET2, central banks are invited to report through which means this has been achieved.

3.6.4.2. Interim period

The measures for critical participants define access criteria which would ideally have to be met prior to joining the TARGET2 system. Critical participants would have to self-certify that information security is addressed in accordance with internationally recognised standards and that the business continuity requirements specified in the section "Business continuity" are being met. Moreover, business continuity arrangements would have to be successfully tested in accordance with the defined testing programme (see the section on "Testing").

The Eurosystem is aware that a common concept similar to the one described in this Infoguide did not exist for the first TARGET generation and that the requirements are new to the market in the context of TARGET2. It is furthermore acknowledged that some preparatory work might need to be done in order to meet the requirements. The Eurosystem concluded that a transition period is needed allowing critical participants to make the necessary arrangements in order to meet the criteria.

The exercise aiming at identifying TARGET2 critical participants is still under refinement. Critical participants will have 18 months to comply with specific requirements applying to their security and operational reliability[36]. This period will start from the time of their designation as critical participants.

3.6.4.3. Constructive approach

It should be stressed that the objective of the framework is not to prevent institutions from participating in TARGET2. Rather, the specified measures aim at strengthening the resilience and robustness of the TARGET2 system as a whole, thus contributing to the stability of financial markets.

If a critical participant fails to meet one of the requirements, the central bank responsible will raise awareness about the risks arising from the identified weaknesses. In close cooperation with the critical participant in question, the central bank responsible will develop a programme to gradually improve the situation. In case a persistent situation of unwillingness and bad faith impedes such a gradual improvement, the critical participant should normally not be allowed to participate in the TARGET2 system anymore. However, a final decision will only be made following a careful evaluation of the situation at Eurosystem level.

Finally, once the critical participants have been identified, the relevant central banks should contact them and ask them to indicate their level of preparedness considering the above-mentioned deadline

[36] It is expected that most critical participants already comply with the security requirements.

for implementation. If significant gaps between the requirements outlined in this guide and the actual situation are identified, a work plan should be established. This plan should be monitored by the relevant central bank to ensure that the required measures are implemented by the above-mentioned deadline.

3.6.5. Communication and coordination

A sound organisational structure is essential for the communication and coordination of security issues between central banks and their TARGET2 users to be managed in an effective and trustworthy manner. Each central bank and its TARGET2 users have the responsibility to ensure that the necessary activities within the respective organisations are organised in a proper and efficient way. When sensitive information is exchanged between the parties involved, it must be ensured that this information is properly labelled and receives an appropriate level of protection.

3.6.6. Confidentiality

All information provided by the TARGET2 users will be treated as confidential by the Eurosystem. It will only be used to assess whether TARGET2 users are in compliance with the measures required by the Eurosystem in order to fulfil its system operator responsibilities as requested through the Core Principles.

In the event that TARGET2 users receive sensitive information in the context of the overall framework, it goes without saying that they must treat this information as confidential.

3.6.7. Reporting

The central banks are responsible for collecting the required information and monitoring any follow-up activities. For example, if a TARGET2 user's provisions for business continuity were considered to be ineffective, it would need to be discussed how the identified shortcomings could be resolved and by when the mitigating measures would be implemented.

Given the fact that the Eurosystem, as a whole, assumes payment system operator responsibilities, the information about incidents which could have an impact on the smooth functioning of TARGET2 gathered by the central banks will have to be made available to the responsible committee at Eurosystem level. Given the sensitivity of this information, it is of utmost importance that it is treated in strict confidentiality. It might even be considered to present the information in an anonymous form.

The committee will have to review the information and consider on a case-by-case basis which measures should be taken in order to ensure that a particular TARGET2 user does not pose any risk to

the smooth functioning of TARGET2 and the other TARGET2 users.

The reporting format and the detailed procedures for submitting information to the responsible committee are defined at Eurosystem level. These Eurosystem internal procedures should ensure that central banks not actively involved in the data collection process get access to these data and that information is shared in an effective and consistent manner.

3.6.8. Review clause

Regular reviews of the overall framework are necessary to deliver assurance that it remains appropriate.

For example, the criteria used to determine critical participants are not set in stone. The Eurosystem has the responsibility to adapt the criteria in the light of experience gained during TARGET2 business operations or when new research results on systemic risk become available.

Another example could be that the payments traffic generated by individual credit institutions is subject to changes. If following a merger a credit institution is suddenly processing more than 2% of the value of transactions in TARGET2, this credit institution would need to be classified as a critical participant and would have to meet the requirements specified for that type of organisation.

Therefore, the criteria for determining critical participants and the classification of critical participants are reviewed at least on an annual basis. In addition to that, TARGET2 users are obliged to inform their central banks well in advance of significant changes in their business practices.

3.7. Termination or suspension of a TARGET2 user

According to the TARGET2 Guideline, central banks shall immediately terminate without prior notice or suspend a TARGET2 user in the relevant TARGET2 component system if:

(a) insolvency proceedings are opened in relation to the TARGET2 user; and/or

(b) the TARGET2 user no longer meets the access criteria for the participation in the relevant TARGET2 component system.

The central banks may terminate without prior notice or suspend the participant's participation in a TARGET2 component if:

a. one or more events of default (other than those referred to above) occur;

b. the participant is in material breach of the Harmonised Conditions for participation in TARGET2;

c. the participant fails to carry out any material obligation to the central bank;

d. the participant is excluded from, or otherwise ceases to be a member of, a TARGET2 CUG;

e. any other participant-related event occurs which, in the central bank's assessment, would threaten the overall stability, soundness and safety of its TARGET2 component or of any other TARGET2 component system, or which would jeopardise the central bank's performance of its tasks as described in the respective national law and the Statute of the European System of Central Banks and of the European Central Bank; and/or

f. an NCB suspends or terminates the participant's access to intraday credit pursuant to paragraph 12 of Annex III of the TARGET2 Guideline.

If a central bank suspends or terminates a TARGET2 user's participation it shall immediately notify all other Eurosystem central banks thereof. Each central bank shall, if so requested by another Eurosystem central bank exchange information in relation to such TARGET2 user, including – in the event of termination – information in relation to payments addressed to it. The central bank initiates the termination or suspension via the ICM. A suspension becomes immediately effective in all modules at the same time and a termination becomes effective with the start of the new business day.

From a technical point of view the termination or suspension of a TARGET2 user is possible at any time the SSP is running. As next step the central bank informs the TARGET2 coordinator which in turn initiates a teleconference to inform all settlement managers about the termination or suspension. Additionally an ICM broadcast will be sent to all TARGET2 users.

Effects of the suspension of a PM participant

- RTGS account and sub-accounts are **earmarked immediately.**
- No payments can be settled automatically on these accounts any more.
- Payments involved in a **running settlement process** are not affected by the suspension.
- The central bank has to confirm **pending payments** in the queue via ICM before they will be settled on the RTGS account.
- Payments **sent by** the suspended PM participant after suspension are stored for confirmation

by the central bank via ICM.

- Payments **sent to** the suspended PM participant after suspension are stored for confirmation by the central bank via ICM.
- It depends on the national rules on which basis the central bank gives the confirmation on payments

The effect of the termination of a PM participant is that the participant is deleted from the system in all modules at the same time.

As concerns liquidity pooling arrangements, the central banks that are party in an aggregated liquidity (AL) agreement and act as the counterparty for the direct participants that entered into an AL agreement and participate in its TARGET2 component shall exchange all information that is necessary for the performance of their duties and obligations under an AL agreement. These central banks shall immediately notify the managing central bank of any enforcement event of which they become aware relating to the AL group or any AL group member, including the head office and branches thereof.

When suspending a participant the central bank can choose whether or not the suspended participant should still be published in the TARGET2 directory. The TARGET2 directory does not show whether a participant is suspended. However, the detailed record in the TARGET2 static data, visible via the ICM, is marked accordingly.

If the terminated or suspended PM participant is a group of accounts (GoA) manager, it will not be able to act as a GoA manager from the time the termination or suspension becomes effective.

If the terminated or suspended PM participant is an AS Settlement Bank, it will be treated according to the rules valid for direct PM participants. The central bank of the AS Settlement Bank has to confirm the transactions.

If an Ancillary System is terminated or suspended from the PM it will be treated according to the rules valid for direct PM participants. The central bank of the AS has to confirm the transactions.

Effects of the suspension of a HAM participant

- The suspension becomes effective immediately.
- Payments can no longer be settled automatically on the participant’s HAM accounts.
- Payments sent by the suspended participant are stored for confirmation by the central bank.
- Payments sent to the suspended participant are stored for confirmation by the central bank.

- As regards the co-management function, if the suspended HAM participant is a co-manager for HAM accounts it will not be possible for it anymore to act as co-manager from the time the suspension becomes effective. It is up to the co-managed account holders in HAM to nominate a new co-manager. In the meantime the related central bank can act for them on request. When it is the co-managed HAM participant that is excluded, the relation between the co-managed account holder in HAM and the co-manager will remain. Transactions to be debited or credited on the HAM account of the co-managed entity have to be executed by the central bank.

3.8. TARGET2 billing

The invoice for all the TARGET2 services during a given month is sent to the direct participants and ancillary systems by the relevant central bank at the beginning of the next month (no later than on the fifth business day) and it has to be paid at the latest on the tenth business day of that month. The fees will be paid via direct debit (MT204) imitated by the relevant central bank. In case of ancillary systems without PM account, the ancillary system has to initiate a credit transfer to the account specified by the relevant central bank.

The billing period is monthly for the fees that should be paid by the users of TARGET2 services (i.e. core services, ancillary systems, liquidity pooling services), except for the one-off fee.

3.8.1. Transactions initiated by direct participants

Under the TARGET2 core pricing scheme, every transaction received by the PM from a direct participant[37] (e.g. normal payments, liquidity transfers initiated in the PM) incurs a transaction fee. The following types of transactions are excluded:

- transactions crediting the account of an ancillary system used for the settlement of transactions/balances of such a system[38];
- transactions related to reversal payments in the context of ASI procedure 4;

[37] Including the entities authorised to debit the direct participant's account for sending payments to the system, i.e. multi-addressee access.

[38] An ancillary system may hold an account in the PM of the SSP for other purposes than settlement of balances/transactions, e.g. for the payment of expenses, fees, penalties, and interest related to the participation by members of such a system. In this case, the transactions sent by the participants crediting the account of the ancillary system are subject to the core pricing scheme.

- liquidity transfers from an RTGS account to a sub-account or vice versa in the context of ASI procedure 6; and
- transactions for levelling out a group of accounts.

The transactions rejected for reasons other than technical reasons (i.e. a payment rejected at the end of the day because of a lack of liquidity, or a payment cancelled by its sender while queued) will be charged the same way as if they had been settled.

The direct participants are invoiced for all the fees of the core pricing scheme. The invoice is created per RTGS account. A legal entity with several accounts (direct participants) would receive several invoices.

The fee is to be paid by the direct participant whose account is debited (i.e. the sender of the payment messages for credit transfers and the payer for direct debits).

Other kinds of participants (indirect participants, multi-addressee access entities, addressable BICs) are not subject to the billing and do not receive any invoice. Their fees (i.e. one-off, monthly and transaction fees) are charged to the direct participants who have the business relationship with these entities. The transactions of these kinds of participants are included in those of their direct participant and therefore are implicitly charged.

The other types of participants which do not have an RTGS account in the PM (e.g. central bank customers, participants with a HAM account only) are not concerned by the fees as defined for the TARGET2 core service pricing scheme considering that the fees are determined by their relevant central bank.

The account of the direct participant is charged with the amount invoiced by the relevant central bank. In the case of a legal entity with several accounts, the several invoices received would be paid by the direct participant from the account announced to its central bank.

3.8.2. Transactions on accounts included in a group

The group pricing allows for the aggregation of the transactions of all direct participants belonging to a group of accounts. These transactions are charged according to the normal core pricing scheme, but the degressive fee structure is applied to the sum of all transactions on the accounts of the group. In case a group is included in another larger group of accounts (typically, an aggregated liquidity (AL) group and some direct participants from a consolidated account information (CAI) group), the largest group is always the basis for the invoicing.

The direct participant which holds the main account of the group, i.e. the group of accounts manager, will be invoiced for all the fees related to all accounts in the group:

- TARGET2 core service fees (fixed fee, transaction fees and specific fees related to unpublished BICs, multi-addressee access, indirect participation and addressable BICs);
- fees for the liquidity pooling service.

In case the CAI group manager is different from the AL group manager, the direct participant that holds the main account of the CAI group will be invoiced for the total fees of the group of accounts, according to the degressive scheme applied to all payments of its group.

The account of the group manager (i.e. AL group or CAI group) is debited for all the fees applicable to the entities participating in the group of accounts.

3.8.3. Ancillary system transactions

Any transaction sent or received by an ancillary system is considered an ancillary system-related transaction. All the transactions involving accounts belonging to the ancillary systems are invoiced as ancillary system transactions, irrespective of whether they are performed through the ASI or not. Also, the transactions involving the guarantee account are subject to ancillary system transaction pricing. Therefore, in order to avoid charging a system twice, TARGET2 will not charge banks when they send a payment to an ancillary system. The ancillary system would then charge its participants in accordance with its own pricing scheme outside of TARGET2.

With respect to the definition of billable transactions settled via the ASI, the charging modalities for ancillary system transactions are as follows:

- for the ancillary systems settling bilateral transactions under ASI settlement procedures 4, 5 and 6 (i.e. the “double-charging” case): to charge only half of the number of debits and credits on the RTGS accounts/sub-accounts (i.e. the sum of the number of debits and credits on the RTGS accounts/sub-accounts divided by two);
- for the ancillary systems settling bilateral transactions without involving a technical account in the settlement process: to charge for every transaction (i.e. debit) on an RTGS account, similar to a normal TARGET2 payment; and
- for the ancillary systems settling multilateral transactions (necessarily via a technical account): to charge for each debit on the RTGS account/sub-account (to the technical

account) and for each credit to an RTGS account/sub-account (from the technical account).

As regards the charging of the liquidity transfers under the ASI settlement procedures, the Eurosystem decided the following:

- not to charge for the liquidity transfers from the RTGS accounts to sub-accounts and vice versa (i.e. in settlement procedure 6 (interfaced)); and
- to charge for the liquidity transfers between the RTGS accounts and mirror accounts for every debit and credit on the RTGS accounts (i.e. in settlement procedures 1, 3 and 6).

As far as the transactions related to auto-collateralisation are concerned, the Eurosystem decided not to charge for these transactions following the same principle as for liquidity transfers from the RTGS accounts to sub-accounts.

The following types of entities will be invoiced according to the ancillary system pricing scheme:

- ancillary system entities: all the transactions involving accounts belonging to these entities are invoiced as ancillary system transactions, irrespective of whether they are performed through the ASI or not;
- central banks: a central bank operating an ancillary system is subject to the ancillary system pricing scheme just like any private ancillary system; and
- entities (e.g. ancillary systems, central banks) holding a guarantee account: transactions involving this account are subject to ancillary system transaction pricing. The core service fixed fee is not invoiced for this account (it is deemed to be covered by the ancillary system fixed fee for the respective ancillary system).

As a matter of principle, the account of the ancillary system which is used for the settlement of balances/transactions of its participants is never used to pay the TARGET2 invoices. If the ancillary system holds an account on which non-AS-related transactions can be made, this account is charged for all the fees as defined in the ancillary system pricing scheme.

Alternatively, if the ancillary system holds an account with a commercial bank, the invoice could be paid via a direct debit message on the PM account of this bank, or via a credit transfer initiated by the ancillary system via this bank.

3.8.4. Minimum set of information included in the invoice

Given the fact that not all the central banks are using the optional billing services (i.e. CRISP) provided by the SSP (CRSS), a harmonisation with respect to the billing information of the invoices that are sent to the TARGET2 users is needed.

The minimum set of information to be included in the invoice presented to the TARGET2 users is listed below:

- information on the billing period;
- information on the number of priceable items used by the TARGET2 user during the billing period;
- information on the participation type of the TARGET2 user;
- information on the type of settlement and procedure used (in the case of an ancillary system);
- information on the VAT (if needed); and
- information on the option of the TARGET2 core service.

Further information on the billing and pricing scheme for TARGET2 is available in the “TARGET2 pricing guide for users”.

4. TARGET2 business day in normal situations

Each national banking community will be serviced by a national service desk at the relevant central bank. The national service desk will cater for all the TARGET2 users' needs as far as the usage of the services offered within the SSP and local infrastructures are concerned, as well as for general monitoring of business during the day.

The national service desks will give particular attention to payments which are classified as (very) critical or which, according to local experience, deserve a special focus, and in addition to individual TARGET2 users which may have systemic significance (both banks and ancillary systems). Finally, they should carefully look at country-wide/systemic patterns.

In the following sections, the procedures during a normal business day are described according to the phases of the business day. It should be kept in mind that the business day starts already in the evening of the previous working day.

4.1. Start of the business day (18:45 – 19:00)

The new business day in TARGET2 begins after the end-of-previous-day procedures and the start-of-current-day procedures have been successfully completed. This is normally confirmed between 18:45 and 19:00 with a broadcast message which is sent to all TARGET2 users. The time can also be taken from the ICM screen information on the "SSP Operating Day".

The ICM broadcast has the following text:

"End-of-day procedures for dd-mm-yy have been completed. The dd-mm-yy business day is now open."

4.2. Liquidity provision (19:00 – 19:30)

Between 19:00 and 19:30 liquidity is provided for the day-time settlement and night-time settlement if applicable. The following liquidity movements can take place:

- from the SF to the PM;
- from the SF to the HAM;
- from the HAM to the PM; or

- from the PHA to the PM (optional).

These 30 minutes could also be used to update credit lines or to settle repos before opening.

4.3. Night-time settlement (NTS) procedures (19:30 – 07:00)

Liquidity for NTS (setting aside to sub-/mirror accounts)

After all liquidity is again in the PM, sub-accounts and mirror accounts are credited to allow ancillary systems to start the night-time settlement.

The night-time window will be available from 19:30 to 07:00, with a technical SSP maintenance period between 22:00 and 01:00. Hence, the night-time settlement of the different ancillary systems in central bank money is facilitated. There are adequate technical/operational tools available in TARGET2 in order to run the night-time settlement smoothly.

Support for credit institutions or ancillary systems taking part in the night-time settlement will be subject to agreement with their respective central bank.

During the night-time settlement window, liquidity transfers via the ICM to and from the RTGS account are possible.

Liquidity provisioning for NTS ("non-concordant orders")

Concerning the processes of settlement procedure 6, see the diagram below.

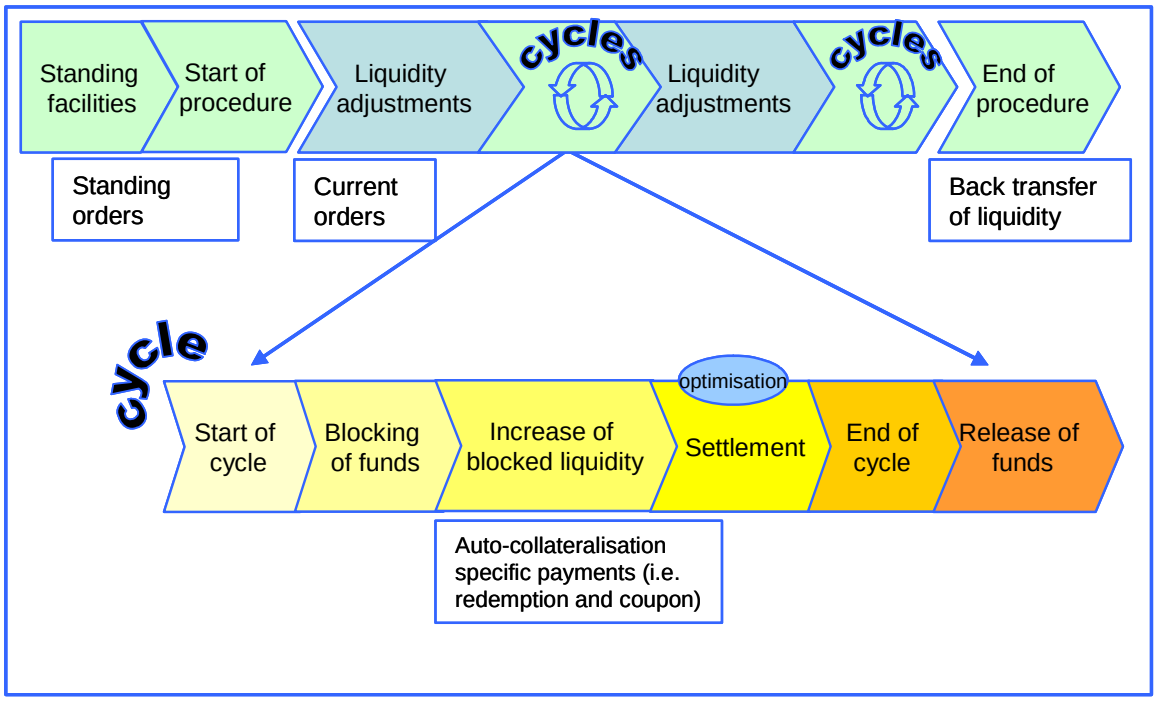


Diagram 7: Settlement procedures 6

A distinction can be made between standing orders and current orders by the direct participant and the ancillary system:

Standing order

The stored amount will be used continuously until the next change. Different orders are possible for day- and night-time business. Standing orders have to be inserted by the direct participant via the ICM by 18:00 at the latest (effective from the forthcoming night-time settlement).

They are executed immediately after the start-of-procedure message is released. A partial execution might apply in case of insufficient liquidity. The remaining part will not be settled.

Current order by the settlement bank

A current order is inserted by the settlement bank via the ICM after the start-of-procedure message is sent (but before the end-of-procedure message is sent). The current order gets immediately executed if received prior to the first cycle or between two cycles (in the liquidity adjustment phase). If received during a cycle, the current order will be stored.

In case of insufficient liquidity, a current order will be rejected.

Current order by the ancillary system

A current order by an ancillary system is based on internal rules. A pre-agreement between the ancillary system and the settlement bank is necessary. A sending of current orders is possible after the start-of-procedure message has been sent. The current order gets immediately executed if it is received prior to the first cycle or between two cycles (in the liquidity adjustment phase). It is stored if it is received during a cycle. A partial execution applies in case of insufficient liquidity. The remaining part will not be settled.

Concordance of orders

A parallel execution of standing orders and current orders cannot happen, because standing orders are already executed before current orders can be sent.

Incoming current orders – independent of whether they are from a settlement bank or an ancillary system – will be executed immediately when they are received.

Stored current orders (due to the running of a cycle) will be executed on a FIFO basis.

For night-time settlement, a common start-of-procedure message is automatically released for all participating ancillary systems. Therefore, all standing orders for a single settlement bank belonging to several ancillary systems will be executed at the same time. If there is insufficient liquidity to cover the sum of standing orders, all standing orders will be reduced following a pro-rata rule. The pro-rata rule functions as follows:

Calculation of a reduction factor: existing liquidity/sum of standing orders

Reduction of standing orders: standing order x reduction factor

4.4. Business window (06:45 – 07:00)

The business window is used by the Eurosystem to prepare for the day trade phase.

4.5. Day trade phase (07:00 – 18:00)

At 07:00 TARGET2 is open for payment processing; this is shown on the respective ICM screen. The normal start-up is confirmed by a message in the T2IS confirming the start of the day trade phase.

During the day trade phase, certain payment flows should be monitored particularly closely due to their systemic importance. It is expected that direct participants give these payments priority internally.

- **07:00 – 12:00: CLS-related payments**

The CLS (Continuous Linked Settlement) scheme provides global multi-currency settlement services for the forex contracts using a payment versus payment (PvP) mechanism. In order to allow this, CLS has access to central bank money in each of the eligible currencies. For the settlement of the euro, CLS holds an account with the ECB and receives and sends euro payments via TARGET2. A pay-in schedule (PIS) is issued daily and specifies the funds the settlement members must transfer to CLS at five hourly deadlines (08:00, 09:00, 10:00, 11:00 and 12:00). Settlement members are free to fund all obligations in "one shot". A delay in the euro funding could affect the multi-currency settlement of CLS and eventually other currency areas, in particular the Asia-Pacific region which, due to the time difference, are close to its end of day.

- **Payments related to margin calls of CCPs (initial and variation margin)**

A central counterparty (CCP) is situated between counterparties to financial contracts traded in one or more markets, becoming the buyer to every seller and the seller to every buyer.

A CCP has the potential to reduce significantly risks to market participants by imposing more robust risk controls on all participants and, in many cases, by achieving multilateral netting of trades. It also tends to enhance the liquidity of the markets it serves, because it tends to reduce risks to participants and, in many cases, because it facilitates anonymous trading.

A CCP margin call is a demand by the clearing house to a clearing member for additional funds or collateral to offset position losses in a margin account. If no initial margins were to be received, it would postpone the start of trading in the respective market or, if some margins were not paid, the positions of the concerned member might be closed out and the member might eventually be excluded.

- **16:08 – 16:45: EURO1 settlement**

EURO1 is a large-value payment system for cross-border and domestic transactions in euro between banks operating in the EU. The system settles at the end of the day via the ASI using settlement procedure 4. The file is sent to the ASI for settlement at around 16:08 CET, with a settlement period until 16:45 CET. In the event that a settlement bank fails to meet its obligation in EURO1 end-of-day settlement because of liquidity problems a guarantee account mechanism is used.

- **Settlement of ancillary systems**

The interdependencies between TARGET2 and the settlement of ancillary systems other than the above and their criticality vary and are at national discretion. Hence, each central bank addresses the extent to which the settlement of ancillary systems is monitored.

- **Processing problems**

In case of problems in the processing of the above-mentioned categories of transactions, problem management procedures should be activated immediately. The relevant TARGET2 users together with the national service desks are expected to do this proactively.

- **17:00: customer cut-off time**

17:00 is the cut-off time for customer payments. As debit and credit booking happens simultaneously, the cut-off is at 17:00 sharp; hence, payments will be rejected immediately afterwards. A rejection of payments occurs after the running of algorithm 3. The timestamp of the SSP is binding; more precisely, the time when the module receives the message prevails. PHAs have to ensure their compliance, e.g. by setting earlier cut-off times.

- **18:00: interbank cut-off time**

18:00 is the cut-off time for interbank payments and also the cut-off time for processing payments. As debit and credit booking happens simultaneously, the cut-off is at 18:00 sharp; hence, interbank payments will be rejected immediately afterwards. A rejection of payments occurs after the running of algorithm 3.[39] The timestamp of the SSP is binding; more precisely, the time when the module receives the message prevails. PHAs have to ensure their compliance, e.g. by setting earlier cut-off times.

4.6. End-of-day processing (18:00 – 18:45)

TARGET2 closes at 18:00. The closing will be confirmed by a message in the ICM and the T2IS. Between 18:00 and 18:15, the following events will take place:

- transfer back of liquidity from sub-accounts to main accounts (emergency procedure);
- rejection of pending payments at 18:00 (immediately after the running of algorithm 3);
- automatic emergency procedure if a group of accounts manager was not able to balance the accounts in time and there is one uncovered overdraft on one account belonging to a group of accounts;
- automatic transfer of liquidity to the PHA (optional);
- use of the standing facilities until 18:15 (18:30 on the last day of the minimum reserve period);

39 See footnote 37.

- transfer of liquidity to the SF accounts, booking of overnight credit to SF accounts, automatic transfer of overnight credit from the SF to the RTGS account in case of use of intraday credit at the end of the day (optional);
- automatic transfer of liquidity to the HAM account (optional);
- levelling out of group of accounts (emergency procedure);
- sending of balance information to the RM module; and
- sending of account statements MT940/950 (optional).

After 18:30 the internal central bank accounting takes place.

5. Fundamentals of procedures in abnormal situations

5.1. Incident definition

Incidents are situations preventing TARGET2 from functioning normally. These can be due to problems in the SSP, PHAs, domestic applications, ancillary systems, direct participants and in the SWIFT services.

More specifically, an incident can be defined as an event which is not part of the standard operation and which causes, or may cause, an interruption to, or a reduction in, the quality of services that TARGET2 offers. The effect might be immediately visible, or only detected at a later stage. Each incident must be documented and a solution must be found and implemented as soon as possible.

Incidents may result from one or more of the following events:

i) a failure of any relevant component or software on the system's technical platform;

ii) a procedural, operational or business failure; and/or

iii) a strike or major external event (e.g. natural disasters, large-scale power outages, terrorist attacks, coinciding events).

The diagram below shows the actors within the scope of TARGET2 abnormal situations.

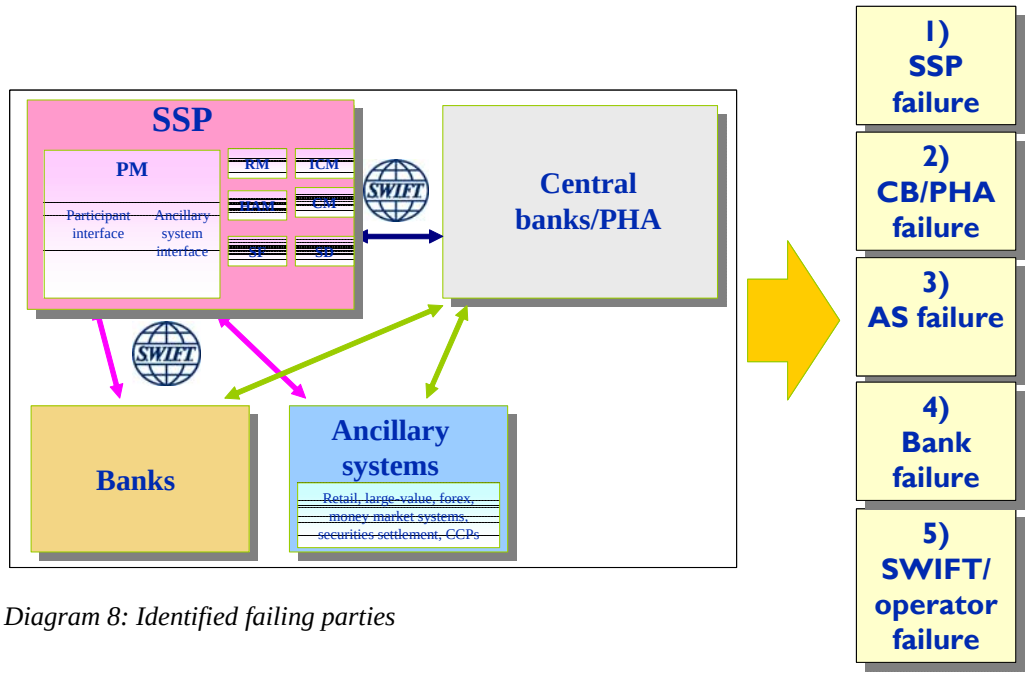


Diagram 8: Identified failing parties

5.2. Incident handling procedures

Incident handling starts with problem detection. Problem detection is the main purpose of monitoring the different actors involved. Once an abnormality has been recognised and confirmed to be a problem, the incident communication and incident handling procedures will be activated. In the case of TARGET2, a problem might be spotted by TARGET2 users or by the central banks.

In general terms, the TARGET2 incident management measures revolve around:

- fixing the problem/ finding a workaround;
- business continuity, i.e. the continuation of full processing capacity by failing over to a secondary system/site/region;
- contingency measures that allow the continued processing of a limited number of payments; and
- delayed closing, i.e. the extension of the day trade phase.

In the event of a failure which only concerns FIN message traffic, the InterAct and FileAct processing could continue, thus allowing the processing of (very) critical payments.

5.3. Incident communication

In an abnormal situation, the flow of information is crucial. During an incident, TARGET2 users keep in touch with their usual contacts for the operational management at their respective central bank via national communication means.

Incidents with a potential systemic impact will be the subject of a coordinated management by the central banks. Moreover, there is an internal decision-making structure at the central banks for TARGET2 incidents that comes on top of the normal organisational structure.

Providing information on a failure

When the central banks become aware of any SSP failure or other failures which might have an impact on TARGET2 transaction flows, the central banks will activate their internal incident communication via established teleconference facilities. Upon agreement on the way forward, information will be disseminated simultaneously among TARGET2 users using the following channels:

- if the SSP is still functioning, information will be disseminated via ICM broadcasts;

- the national service desks will inform their TARGET2 users accordingly using the relevant national communication means; and
- the T2IS will be updated, both for the news agencies and on the ECB website.

To ensure a timely communication, the information will refer to pre-agreed and standardised terms and carry, as far as available, the following information:

- description of the error;
- anticipated delay (if possible);
- information about measures taken; and
- advice to users.

If at the time an incident is identified some of the details indicated above are not available, a relatively general announcement of the incident will first be made, to be subsequently supplemented with more detailed information, typically within 30 minutes after the initial communication.

If in the course of an incident further information relevant for users becomes available, this will be provided using the communication channels listed above. These channels will also be used to inform users once an incident has been resolved.

6. Procedures for handling an SSP failure

6.1. Start-of-day incident procedures (18:45 – 19:00)

The completion of the start-of-day procedure is confirmed with a broadcast to all TARGET2 users. If, for whatever reason, the start-of-day procedure is delayed, this will be communicated by the respective national service desk using national communication means, via the T2IS and, if applicable, via the ICM.

6.2. Night-time settlement incident procedures[40] (19:00 – 22:00 & 01:00 – 07:00)

If an SSP incident occurs during the NTS, it could have an impact on liquidity provision, the NTS and possibly also the day trade phase. The counterpart for TARGET2 users involved in the NTS would still be the respective national service desk.

Depending on the SSP failure, it might be possible to fix the problem or there might be a need to initiate a failover. It is very important that full information about any events and measures taken during the night that could have an impact on the start of the day trade phase at 07:00 is disseminated. Hence, the national service desk will inform its TARGET2 users via national communication means before the regular start time of the day trade phase at 07:00 and via the T2IS and, if applicable, via the ICM.

6.3. Business window (06:45 – 07:00)

The business window is used by the Eurosystem to prepare the daylight operations. In case of incidents, the incident management procedures of the day trade phase will apply.

6.4. Day trade phase incident procedures (07:00 – 18:00)

6.4.1. Business continuity

If an SSP problem cannot be fixed, the main aim is to recover full processing capacity. The decision whether to perform a failover depends on the type of failure, its expected duration, point in time, etc. However, there is no sequential order for intra-region and inter-region failover. In case of a problem at SSP level, the decision is about whether to conduct either an intra-region or an inter-region failover. The latter will only be activated in very rare circumstances.

[40] No procedures during the technical window (22:00 – 01:00).

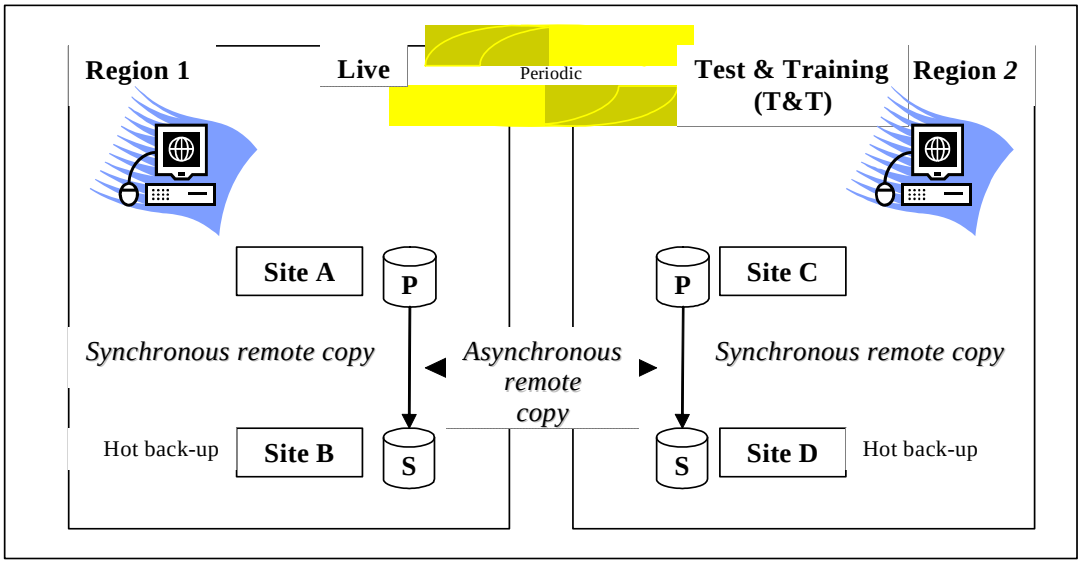


Diagram 9: Two regions, four sites

6.4.1.1. Intra-region failover

- While smaller failures are covered by backups of the main critical elements within the same site, major failures or disasters (e.g. disruption of major hardware caused by fire, flood, terrorist attacks, or by telecommunications faults) require the activation of the second site in the same region (intra-region failover).
- An intra-region failover means the failing over from site A to site B within a region. As a synchronous mode is applied, the databases at both sites are exactly the same and no reconciliation is required after the failover.
- An intra-region failover ensures the continuation of normal business within a maximum of one hour after the central banks' decision-making process.
- Payment processing is interrupted during the failover, but TARGET2 users are encouraged to keep on sending FIN payments to the SSP that will be queued at SWIFT level and to send FileAct messages (in store and forward mode).

6.4.1.2. Inter-region failover

- A wide-scale regional disruption (e.g. severe interruption of transportation, telecommunication, power or other critical infrastructure across a metropolitan or a geographical area) requires the failing over to the second region (inter-region failover).
- An inter-region failover means failing over from Region 1 to Region 2. Usually the inter-

region failover allows the closure of the site in Region 1 normally and hence the resumption of operations in Region 2 without any loss of data and within two hours of a decision-making process. The TARGET2 users will be informed when TARGET2 will be fully available again.

- Due to the asynchronous mode, a loss of data after an inter-region failover could only occur in the extremely rare event of both sites within Region 1 becoming suddenly unavailable at the same time. In such a situation, there is no alternative but to fail over to Region 2 and to reconcile the missing traffic and rebuild the database. Still the resumption of business in Region 2 should be enabled within two hours of the decision-making process and including the retrieval and reconciliation of SWIFT FIN messages[41]. The process of rebuilding requires the active participation of the TARGET2 users. The procedure for inter-region failover with loss of data is described in Annex I and a detailed presentation is available on the TARGET2 website.
- Payment processing is interrupted during an inter-region failover, but TARGET2 users may keep on sending FIN payments to the SSP; these will be queued at SWIFT level and processed upon the recovery of the SSP. TARGET2 users should not send XML traffic until further notice (most XML traffic would be rejected).
- In the event that a rebuilding process is required, please refer to the annexed description of the rebuilding process.

Handling of payments with execution time

➢ Inter-region failover (without loss of data)

In the event of an inter-region failover without loss of data and if the time indicated after the code word has expired, the SSP will follow the "normal" procedures. This means:

/FROTIME/ ⇨ payments will be included in the settlement
/TILTIME/ ⇨ **a** warning broadcast will be shown in the ICM
/REJTIME/ ⇨ payments will be rejected

➢ Inter-region failover (with loss of data)

In the event of an inter-region failover with loss of data and if the time indicated after the codeword has expired, the SSP will follow a special procedure: payments with the codeword /REJTIME/ will not

[41] The retrieval is a service offered by SWIFT, which applies its standard SWIFT pricing scheme to the TARGET2 users.

be rejected immediately since the time will be changed to a future point in time.

Handling of ancillary system transactions with optional mechanisms

settlement procedure	optional mechanism	effect in case of time expired
1, 2	scheduled time ("from")	settlement
	settlement period ("till")	rejection
3	information period	settlement attempt
	settlement period ("till")	rejection
4, 5	information period	settlement attempt
	settlement period ("till") - without guarantee mechanism	rejection
	- with guarantee mechanism	activation of guarantee mechanism

Table 7: Handling of ancillary system transactions

In the event of an inter-region failover with loss of data, in order not to reject payments after the reopening of the SSP, the 3CB will change the information period to 15 minutes before the customer cut-off and will change the end-of-settlement period to the customer cut-off.

6.4.2. Contingency processing using the contingency module[42]

Contingency processing is a temporary means that aims at processing limited business only to avoid the creation of systemic risk. Thus, the contingency module (CM) is used in events where business continuity is impossible or systemically important payments need to be processed during the failover process.[43]

The concept of (very) critical payments in TARGET2 defines which payments are considered systemically important and thus eligible for contingency processing. Contingency processing via the CM is only possible for some specific interbank credit transfers. The processing of other payments will be delayed until after SSP recovery. **Box 1**, entitled "Concept of (very) critical payments in TARGET2", explains which payments must (very critical) or can (critical) be processed. To give guidance to the crisis managers in their decisions on the processing of critical payments, **Box 2**,

[42] Contingency processing using the contingency network is described in Chapter 7.4., "SWIFT/network operator failure".

[43] The use of the CM does not prevent ancillary systems from making use of their own alternative contingency means (e.g. accepting additional collateral or other currencies).

entitled “Aspects to be taken into consideration when selecting critical payments”, is included at the end of this chapter.

Contingency processing involves the manual processing of payments during a failure of the SSP. The failure of the SSP implies that the banks’ payment capacity would be blocked in the SSP.

Due to the following limitations, the contingency throughput is very limited:

- fresh liquidity has to be provided;
- the CM capacity limitation is about 1,000 payments per hour;
- no ancillary system files can be processed.

The CM is always running in the non-active region. In case the settlement managers confirm that very critical payments need to be processed the CM will be used immediately. If there are no very critical payments but only critical payments to be processed, the crisis managers will first have to confirm that these should be processed using the CM.

The value date of the CM is always the same value date as the SSP when the failure occurred. The CM provides only limited functionality; hence, it is not to be compared with a “mini-RTGS” (there are no algorithms to settle payments and there is no support of special functions for ancillary system settlement).

6.4.2.1. Activation procedure for the contingency module

The decision to activate and use the CM for very critical payments is made by the settlement managers in their teleconference. In the event that contingency processing is initiated, the users are informed via all the communication means described in detail in Sections 2.6.1 and 5.3 of this document.

The CM starts with a zero balance, i.e. the payment capacity of the SSP is not available for contingency processing via the CM. In other words, the processing of contingency payments in the CM requires the provision of fresh liquidity by the TARGET2 users.

The CM is operated and accessed solely by the central banks. The TARGET2 users transmit orders to process contingency payments to their respective national service desks using nationally agreed communication means and templates. Information regarding turnover and account balances in the CM is provided to the TARGET2 users by the respective national service desk using the agreed national communication means.

While the processing of very critical payments is mandatory, a request for the processing of critical payments requires the involvement of the crisis managers by means of a teleconference.

While the CM is being used, no SWIFTNet FIN messages are sent to the account holders in the CM.

6.4.2.2. Payment processing in the contingency module

1. TARGET2 users wishing to make contingency payments have to provide fresh liquidity in the form of additional collateral/account balances or via incoming payments and payments (re)distributing liquidity in the euro area (e.g. pay-outs of ancillary systems, liquidity transfers between financial institutions or monetary policy transactions) made in the CM. The procedures for the provision of additional collateral depend on the respective national arrangements.
2. Once fresh liquidity has been booked by the NCB in the CM for a TARGET2 user, contingency processing can start for that user.
3. The sender instructs its central bank to make a contingency payment using the respective national communication means and nationally agreed templates. A request to process critical payments requires a prior decision of the crisis managers.
4. The sending central bank books the payment in the CM (simultaneous debit and credit).
5. After booking, the sending central bank informs the receiving central bank and the latter, after checking the booking, informs the beneficiary of the incoming payment via the respective national communication means.

6.4.2.3. More on the use of the contingency module

- Requests for information on account balances and debits and credits can only be made by the central banks, so TARGET2 users have to request this information from their central bank.
- Only credit transfers are possible in the CM; hence, all CM transactions have to be initiated by the sending bank. This is of particular relevance for some ancillary systems.
- In order to reduce the number of contingency payments, TARGET2 users are encouraged to make use of bulking.
- If a TARGET2 user has transmitted a payment to the SSP that has been queued and it processes this payment again via the CM, a “double processing” of the payment (once in the CM and afterwards upon restart of the SSP in the PM) cannot be prevented.

- After the recovery of the SSP, normal payment processing will be continued on the SSP. After confirmation by the central banks that the use of the CM has been completed, the CM will be closed and the CM balances will be transferred to the RTGS accounts in the PM (no transfer of the individual underlying payments). After the end of the business day the account holders can be informed of the bookings by MT940/950 (optional). When the CM is closed, all accounts within the CM will have a zero balance.
- It is possible to restart the CM should a further SSP incident occur on the same day.
- In general, the detailed procedures for action between the TARGET2 users and their respective central bank are defined at national level.

Box 1 Concept of (very) critical payments in TARGET2

Prevailing principles:

- TARGET2 contingency processing should be limited to payments that need to be processed to avoid systemic risk during the day.
- Owing to strict technical and operational volume limitations related to TARGET2 contingency, the overall number of contingency payments should be minimised.
- Primarily outgoing TARGET2 payments should be considered. Outgoing payments are payments that would be required by other systems.
- Incoming CM payments (e.g. pay-outs of ancillary systems, liquidity transfers between financial institutions, monetary policy transactions) could be considered as critical payments under specific circumstances, i.e. if evidence is provided that they are indispensable for covering (very) critical outgoing payments, the crisis managers might agree on their processing. In any event, the number of these payments should remain very limited.

The following individual categories of payments are considered as very critical or critical, and consequently as eligible for contingency processing:

Very-critical payments must be processed in contingency (order: CLS, FIFO)

- payments related to settlement payments from TARGET2 to CLS (pay-ins);
- payments related to settlement payments from TARGET2 to EURO1 for the end-of-day settlement (pay-ins); and
- payments related to margin payments from TARGET2 to CCPs (pay-ins).

Critical payments can be processed in a contingency but require prior agreement of the crisis managers

- settlement payments to interfaced securities settlement systems for the real-time settlement;
- additional outgoing payments if required to avoid the creation of systemic risk; and
- incoming CM payments if evidence is provided that they are indispensable for covering (very) critical outgoing payments.

Box 2 Aspects to be taken into consideration when selecting critical payments

In addition to the three basic principles avoidance of systemic risk, the limitation of processing volumes and the focus on outgoing payments, the following aspects might support the crisis managers in their decision-making:

- The failure situation, in particular the time of occurrence. Besides the beginning of the day and the end of the day, critical times will also be provided by the overview of settlement times of ancillary systems. The possible spillover, the source of the failure and its duration and the expected recovery time are also important aspects.
- The business day – it could be of relevance whether an incident occurs at the end of the maintenance period, on a public holiday or on a day where particularly high volumes are expected.
- The communicated needs of banks, ancillary systems and other central bank business areas (e.g. for monetary policy operations).
- The liquidity limitations – contingency processing would require additional collateral, i.e. the more payments that would be processed in a contingency, the more additional collateral would have to be provided by a bank, and depending on the time of occurrence the provision of additional collateral might be difficult.
- The principle of prioritisation – very critical payments should generally be processed before critical payments (as long as the critical payments are not required to release a "business gridlock" of very critical payments).
- The incident handling measures might alleviate the need for processing contingency payments; for instance, major ancillary systems might delay their settlement by the same amount of time as the delay in TARGET2's closing and queued payments would be processed at the moment of SSP recovery. Another example is that ancillary systems might try to settle even in the case of a delayed closing of TARGET2.
- The market's contingency means – possible alternative contingency means at the disposal of an individual ancillary system and banks (e.g. pay-ins in a different currency) could ease the need to process critical payments in a contingency.

6.4.3. Delayed closing

The decision to delay the closing in the event of an SSP failure, i.e. to prolong the day trade phase, is always made by the crisis managers. The announced new closing time is the new cut-off time for interbank payments. The aim is to inform TARGET2 users early about how long the delay might be, rather than their receiving hourly or half-hourly updates of the situation, in particular if the reason is a prolonged outage of the SSP. A delayed closing will also delay the customer cut-off time to the same extent, supposing that the delayed closing is granted at least fifteen minutes before the actual customer cut-off time (i.e. before 16:45 at the latest).

It is not possible to delay the customer cut-off time only.

Apart from the following two situations revolving around an SSP failure, which could lead to a delayed closing, there might be situations where a delayed closing is implemented for the management of a banking crisis.

6.4.3.1. Delayed closing due to an earlier SSP failure

In order to give the market additional operational time, the day trade phase can be extended if an SSP failure occurs during the day but is solved before 18:00. Such a delay should not exceed two hours and should be announced early to provide the TARGET2 users with clarity and certainty. If such a delay is granted before 16:45, the minimum period of one hour between the customer cut-off time and the interbank cut-off time should remain. A delayed closing might also be granted in order to facilitate the management of a banking crisis.

Once a delayed closing is granted, it must not be withdrawn even if this might be technically possible.

6.4.3.2. Delayed closing due to an ongoing SSP failure

A delayed closing will be granted in the event that an SSP failure occurs before 18:00 and is not solved by 18:00. In such situations, there is no alternative but to wait for the recovery of the SSP.

Immediately after the crisis managers agree in their teleconference to grant a delayed closing, this information is disseminated to the TARGET2 users via the relevant national communication means, the ICM (if available) and the T2IS. The TARGET2 users are requested to change their internal parameters to reflect the delayed closing.

During a delayed closing, TARGET2 users should keep on sending FIN payments to the SSP. These will be queued and processed once the SSP recovers. The underlying principle is that TARGET2 will process all queued payments with same-day value to close the SSP in a clean and final manner.

Steps after the recovery of the SSP

The below assumes a SSP outage during the day trade phase. If the failure occurs at a later stage, e.g. during the start of day, only the remaining actions apply (shown as boxes).

On the day of the incident

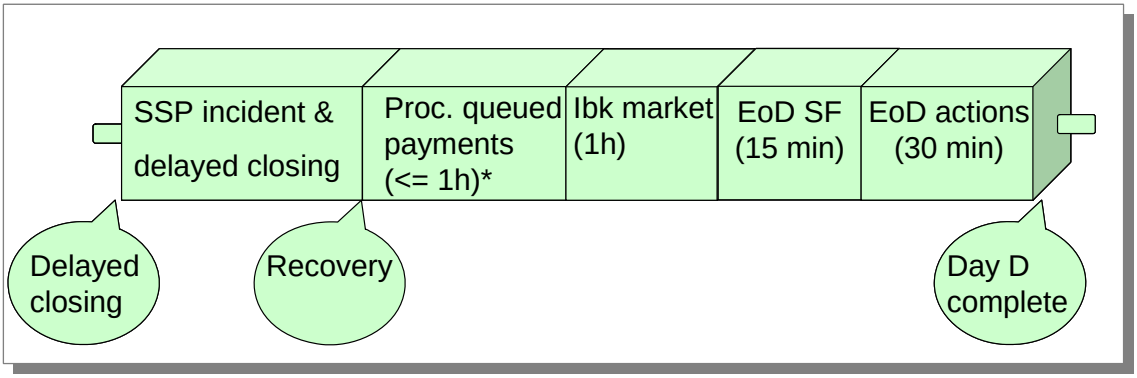


Diagram 10: Processes on the day of the incident

The SSP recovery means that the SSP is ready again to process messages. Upon the recovery and presupposed the SSP outage occurred during the day trade phase, the following steps will take place:

- Processing of all queued payments (one hour); this time is reduced to 30 minutes if the SSP failure occurs within the 30 minutes before the interbank cut-off time. In this period also new messages can be sent by the TARGET2 users.
- Squaring of banks' balances between banks (one hour); this time is reduced to 30 minutes if the SSP failure occurs within the 30 minutes before the interbank cut-off time.
- At the cut-off time for interbank payments, the end-of-day processing (45 minutes or one hour at the end of the maintenance period), including the recourse to the standing facilities, takes place.

The total duration of these steps is 2 hours 45 minutes.

Steps after the delayed closing of Day D

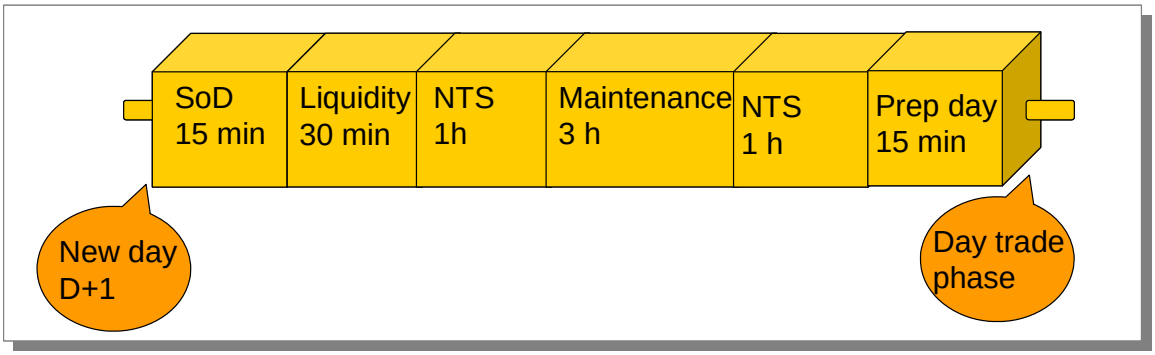


Diagram 11: Processes on the day following the day of the incident

Apart from the above-mentioned mandatory steps on the day of the incident, there are several mandatory steps to be performed after the closing of the current business day. These comprise:

- start of day (15 minutes);
- liquidity provision (30 minutes);
- night-time settlement (liquidity adjustments, 1 hour);
- maintenance period (3 hours);
- night-time settlement (1 hour);
- preparation of day trade phase (15 minutes).

These steps last for six hours. The diagram below shows the overall sequence:

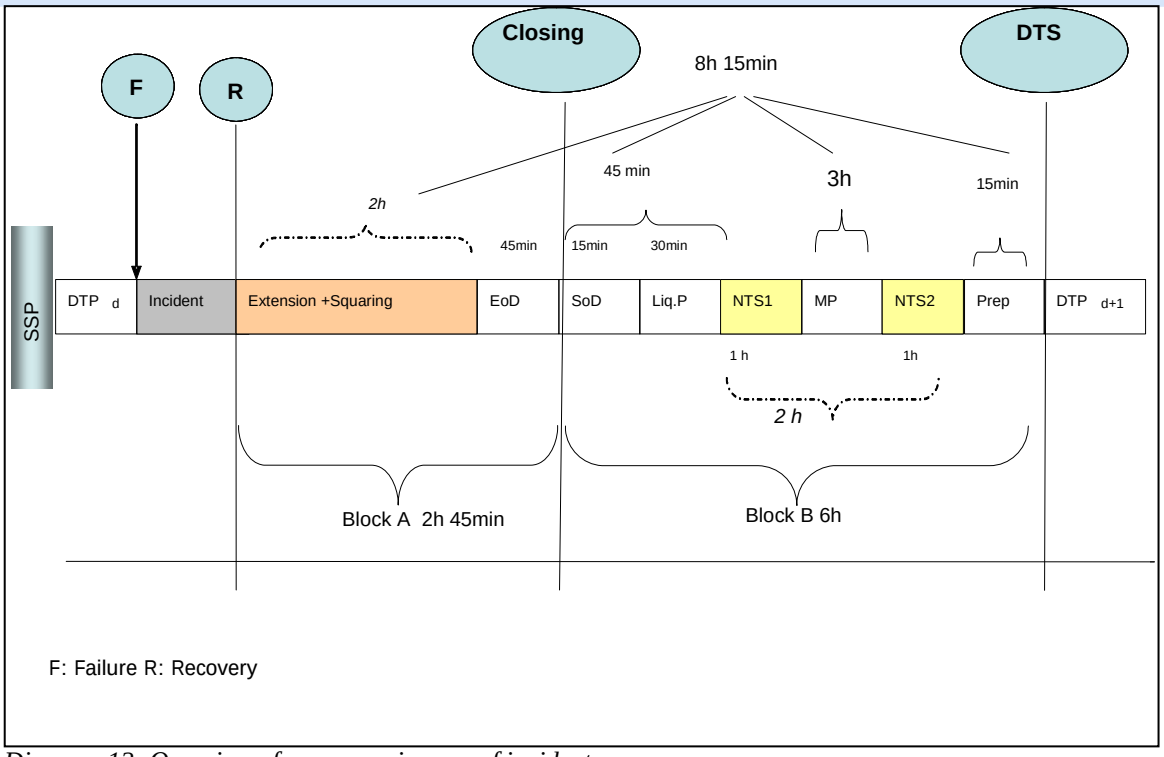


Diagram 12: Overview of processes in case of incident

Prolonged SSP outage

Given the above steps, a SSP outage that occurs during the day trade phase with a recovery of the SSP by 22:15 would still allow a start of the day trade phase at 07:00. An outage going beyond 22:15 (prolonged outage) may prevent a start of the day trade phase at 07:00.

In order to save time and to start the day trade phase as close to 07:00 as possible, the steps "NTS2" and the preparation of the day trade phase might run in parallel immediately after the maintenance period. However, even this procedure might still not allow the day trade phase to start at 07:00.

The ancillary systems needing to receive euro liquidity early in the morning should have established means to cope with such an event.

6.5. End-of-day incident procedures (18:00 – 18:45)

An SSP failure during this period would affect the end-of-day processing, and thus possibly also the recourse to standing facilities, the availability of final account balances and the starting time of the new business day. The delayed closing logic applies here to the same extent as above. However, after the SSP recovery the next step would be the continuation of the end-of-day processing.

7. Other failures

In this chapter, the failure of a central bank/proprietary home account (PHA), an ancillary system, a bank and SWIFT is elaborated upon. While an SSP failure concerns all central banks equally and requires common procedures, the procedures for the failures covered in this chapter are largely at the sole discretion of the respective central bank, the ancillary system or the bank.

In general, the detailed procedures between the TARGET2 users and their respective central bank are defined at national level.

Technical suspension

A technical suspension is a temporary means to protect the SSP from massive and uncontrolled message inflows (e.g. denial of service messages, usually in the non-SWIFT FIN sphere). Such a situation requires immediate action to forestall a disturbance of the smooth functioning of the SSP. It is a purely technical measure. It is envisaged when a central bank, a bank or an ancillary system sends such an extraordinarily high number of messages to the SSP that it could endanger the SSP's functioning.

If the Eurosystem becomes aware of such exceptional and massive message inflows that endanger the smooth functioning of the SSP, it can as a precaution technically suspend the sender. The reasons will be immediately investigated with the sender and, upon resolution of the unintentional sending, the Eurosystem will lift the technical suspension. Depending on the circumstances and as a precaution, a delayed closing could be considered by the crisis managers.

7.1. Central bank/proprietary home account failure

In TARGET2, payments are processed on the SSP. This means that a partial or complete failure of a central bank will not prevent access to the TARGET2 system for an entire national banking community. However, each central bank has its role and responsibilities in TARGET2. Even if the effects of a central bank failure may be limited in TARGET2, adequate measures have to be in place to cope with any malfunctioning in order to properly serve the banking community and to avoid any risk of spillover of a central bank problem to the SSP. Moreover, the impact of a failure of a central bank will differ depending on whether the central bank has fully migrated its business to the SSP or is still running a proprietary home account (PHA). Therefore, a distinction is made between a central bank failure and a PHA failure.

As a general rule, each problem in a central bank/PHA that may have an impact on the SSP or the banking community will be discussed within the central banks as soon as possible. Depending on the

national rules and procedures, a national service desk might inform the national banking community directly about national problems. TARGET2 users will be informed about the problem via the T2IS, the ICM and national communication means, especially if the failure has an effect on TARGET2 users in the other countries (e.g. shortage of liquidity).

7.1.1. Central bank failure

The general principle is to avoid the spillover of a problem by containing it. This means that each central bank will at first rely on its own error handling measures. Should this not be possible or efficient, it might request support from the SSP service desk.

For TARGET2 users, the relevant contact point remains the national service desk. If this is not available, the TARGET2 users should follow the national crisis communication procedures.

7.1.1.1. Start-of-day incident procedures (18:45 – 19:00)

For all the incidents which could occur during this phase, the relevant central bank will have appropriate backup measures.

7.1.1.2. Night-time settlement (19:00 – 07:00)

After the liquidity has been provided, problems at the level of a central bank would not have an impact on the processing of the SSP.

7.1.1.3. Business window (06:45 – 07:00)

The business window is used by the Eurosystem to prepare the daylight operations. In case of incidents, the incident management procedures of the day trade phase will apply.

7.1.1.4. Day trade phase incident procedures (07:00 – 18:00)

A failure during the day trade settlement phase will have an impact on the automated updates of credit lines and execution of repo transactions will not be possible.

For all these actions, the relevant central bank will have appropriate backup measures.

7.1.1.5. End-of-day incident procedures (18:00 – 18:45)

A failure during the end-of-day procedures will, in principle, not have an impact on the SSP or the

banking community.

7.1.2. Proprietary home account failure

Besides the problems described for a central bank failure, the failure of a proprietary home account (PHA) can lead to the following problems:

1) liquidity supply at the start of the business day is impossible;
2) intraday transfers of liquidity between the PHA and the PM cannot be executed;
3) reserve and standing facility management are unavailable; and
4) the settlement of ancillary systems cannot be executed.

It should be noted that a problem at the level of a PHA is entirely under the national responsibility and is addressed individually by the respective central bank. It is most important that the central bank takes all precautions and measures to limit the impact of a PHA problem on the payment processing on the SSP.

7.1.2.1. Start-of-day and provision of liquidity incident procedures (18:45 – 19:30)

A failure at the start of the business day will prevent an automated transfer of liquidity from a PHA to a PM account.

If no data on the PHA are available, no transactions can be executed. It may be possible to execute transactions (e.g. standing orders) based on the closing balance of the RTGS accounts of the participants concerned. In any case, liquidity can be provided against new collateral.

Special attention should be given to those TARGET2 users that participate in night-time settlement. For these TARGET2 users liquidity needs to be shifted before 19:30. If the liquidity is not transferred before 19:30, the crisis managers may decide to postpone the next stage, i.e. agree on a delayed start.

It is at the discretion of the national service desk whether to communicate PHA problems to the national user community. In the event of TARGET2-wide effects, information will also be provided via the T2IS and the ICM.

7.1.2.2. Night-time settlement (19:30 – 07:00)

After the liquidity has been provided, problems at the level of a central bank would not have an impact on the processing of the SSP.

7.1.2.3. Business window (06:45 – 07:00)

The business window is used by the Eurosystem to prepare the daylight operations. In case of incidents, the incident management procedures of the day trade phase will apply.

7.1.2.4. Day trade phase incident procedures (07:00 – 18:00)

A failure in the day trade phase means the PHA is unable to create transactions/operations. Automated updates of credit lines, execution of repo transactions, monetary policy operations and intraday transfers of liquidity between the PHA and the PM will not be possible. Special attention will be given to the settlement of ancillary systems.

PHA data still available

If a PHA failure occurs but the data are still available, the central bank will have appropriate measures to perform these transactions.

PHA data unavailable

If no data on the PHA are available, no transactions can be executed. Liquidity can only be provided against new collateral.

Delayed closing

In the event of a PHA failure, the crisis managers might exceptionally grant a delayed closing for TARGET2 if there is the possibility of systemic risk. This possibility is, of course, closely related to the number and value of payments concerned. The delay should give the central bank concerned more time to solve the problem and alleviate its impact. If a delay is granted, it implies that all central banks have to be available and the SSP must stay open to send and receive payments.

A request for a delayed closing can be made by the central bank concerned until 17:30 and only in exceptional circumstances to avoid a systemic impact. A delay should not exceed two hours (i.e. the system should close no later than 20:00). If a delayed closing is requested and agreed by the crisis managers at 16:50 or earlier, this will result in a delay of the customer cut-off time for the same duration.

A granted delayed closing will never be shortened, although this may be technically feasible. The communication on a delay will follow the general procedures.

Enforced closing

One of the fundamental principles of TARGET2 is that each business day must end with a final and irrevocable position before the start of the next business day.

In the event that a requested delay is not granted by the crisis managers or a central bank with a PHA is still facing problems and unable to participate in the end-of-day procedures before 20:00, an enforced closing procedure will be activated after agreement of the crisis managers. In other words, a delayed closing due to a PHA failure is granted until 20:00 at the latest. In this case, the account balances given by the SSP are considered to be correct.

7.1.2.5. End-of-day incident procedures (18:00 – 18:45)

A PHA problem at the end of the day may have an impact on the retransfer of balances and the shift of liquidity at the start of the day. The NCBs will have appropriate national procedures to address such scenarios.

7.2. Operational or technical bank failure

In the event that a bank has a problem that prevents it from settling payments in TARGET2, it should inform its central bank and it is encouraged to use its own means during the problem to the maximum extent possible. The tools available to each bank are:

- in-house solutions;
- ICM functionality, i.e. payments to redistribute liquidity ("backup lump-sum payments") and backup contingency payments (CLS, EURO1, STEP2 pre-fund); and
- ICM functionality via a stand-alone ICM.

- The ICM can be used in A2A mode, but it is only allowed to be used for the processing of the above-mentioned categories of payments.
- The use of the ICM functionality for making backup contingency payments and payments to redistribute liquidity is completely at the discretion of the bank requiring it. However, before a bank can use the backup functionality it has to request its activation from the respective central bank, which will activate it with immediate effect.
- A bank using the functionality may ask its central bank to send a broadcast to inform other

TARGET2 users about the bank's use of payments to redistribute liquidity.

- If a participant that has faced a technical problem intends to send the original individual payments on the next business day, bearing the original value date, then this needs to be communicated to the respective central bank on the day of the technical failure, i.e. prior to the day on which the individual payments will be sent. The central bank will coordinate the activation of the backup functionality with the modification of the backup parameter to "1" day. This means that the value date check for this sender will be switched off for the following business day, allowing the transmission of the original individual payments bearing the original value date.
- Once it has finished all related business (including the possible receipt of returned backup lump-sum payments), the requesting bank must inform its central bank.
- Payments to redistribute liquidity are an optional feature and based on a bilateral (prior) agreement between the sender and receiver. TARGET2 does not verify whether the original individual payments that have been submitted or returned payments of redistributed liquidity are related to payments submitted on preceding days. Moreover, no check for double submission on preceding days is carried out.
- If these means are exhausted or their use is not efficient, the bank may ask for the support of its national service desk. The detailed contingency means are subject to the bilateral relationship between a bank and its central bank. A bank failure should be reported by the national service desk to the other central banks if it might have an impact on the settlement of ancillary systems or create systemic risk, especially with a potential cross-border impact. Any announcement to the market which is deemed necessary will be coordinated between all central banks.
- A bank failure should never lead to a delayed closing.

7.3. Ancillary system failure

If an ancillary system is facing a problem, it is encouraged to use as much as possible its own contingency means for the duration of the problem. The main aim should be to process all messages to the SSP via normal means, i.e. via the ASI or, if applicable, via the standard payments interface. It should be noted that the use of the payments interface, as well as the support provided by a central bank, require a pre-agreement and pre-communication between the ancillary system and its central bank.

- Among the tools that are at the sole discretion of the ancillary system are backup sites, and multi-access points to multi-network partners. The use of a possible standard payments interface to the SSP to make "clean" payments could also be included here.
- If necessary, the respective central bank might support the ancillary system, for example by processing XML files or making clean payments on its behalf. It depends on the individual central bank whether the ancillary system contingency tool is offered or not.
- In very exceptional circumstances when there may be a Eurosystem-wide risk, the relevant central bank of the ancillary system may request a delayed closing of TARGET2 to give the system more time to resolve the failure or alleviate its impact. The crisis managers will decide whether a delayed closing should be granted or not.

It is at the discretion of each central bank what level of support it wants to provide to its ancillary systems, especially during the night-time settlement. Whatever the contingency arrangements, they presuppose prearrangements and communication with the ancillary system and its central bank. In events at night time, the ancillary system should in general inform its central bank and both need to agree on the contingency processing and the national communication means. Moreover, the ancillary system needs to inform its settlement members separately about the envisaged procedure.

An ancillary system should report a failure to its national service desk. At the discretion of the national service desk, the problem might be communicated to the central banks, in particular in cases with a cross-border impact. Any announcement to the market which is deemed necessary will be coordinated between all central banks.

7.3.1. Ancillary systems using the ancillary systems interface

Pay-ins (from TARGET2 to the ancillary system) could be processed using one of the following methods:

- the relevant central bank sends, on behalf of the ancillary system, an XML file to the SSP using the AS contingency tool[44];
- the ancillary system sends an MT204 message if it is able to use the payments interface, i.e. if its SWIFTNet connection is down but its SWIFT FIN connection is still up and running, or the relevant central bank sends an MT204 message on behalf of the ancillary system (in this case,

[44] In this case, pay-ins and pay-outs can be sent together as in normal settlement with the ASI, if procedures 3, 4, 5 or 6 are used.

all relevant authorisations must have been granted);

- the settlement bank could be requested to make clean PM payments in favour of the ancillary system; or
- the central bank of the settlement bank makes mandated payments[45] on behalf of the settlement bank and on the basis of information provided by the ancillary system, or the central bank of the ancillary system makes these mandated payments on behalf of the settlement bank.

Pay-outs (from the ancillary system to TARGET2) could be processed using one of the following methods:

- the relevant central bank sends, on behalf of the ancillary system, an XML file to the SSP using the AS contingency tool; or
- the ancillary system makes clean payments using the payments interface.

If the central bank does not process XML files on behalf of the ancillary system using the AS contingency tool, the order of settlement becomes important for settlement procedures 4 and 5:

- Procedure 4: the central bank checks in coordination with the ancillary system that all pay-ins are settled before opening the pay-out phase. If all pay-ins cannot be settled, the central bank reverses them by issuing an opposite payment from the AS account to the bank's account (if the pay-in was settled) or by revoking the payment (if it is still pending).
- Procedure 5: procedure 5 is processed like procedure 4, except that there is no reversal of payments because the "all or nothing" approach applies.
- For ancillary systems with a guarantee mechanism, procedure 4 applies, except that, if necessary, the central bank debits the guarantee account[46] in coordination with the ancillary system, rather than making a pay-in.

In settlement procedure 6, the control of the settlement phases becomes vital:

- the relevant central bank can, on behalf of the ancillary system, open procedures and cycles using the AS contingency tool;
- the relevant central bank can, on behalf of the ancillary system, close procedures and cycles

[45] Mandated payments to technical accounts are not possible.

[46] Specific procedures will have to be set up in case ancillary system is calling the guarantees.

using the AS contingency tool or directly through the ICM (using the "stop procedure/cycle" function).

Simulation of the receipt of a technical XML notification message

A problem in the delivery or processing of a technical XML notification message[47] may result in a blockage of the current and subsequent settlement processes on the ancillary system side. Accordingly, it is strongly recommended that ancillary systems are able to simulate the receipt of such messages. This should be done on the ancillary system's own initiative (following a check in the ICM) or on the basis of a confirmation of the settlement result received from the national service desk via secure means (details to be agreed bilaterally). Ultimately, the ancillary system can choose the most appropriate solution in agreement with its national service desk, i.e. opt for the simulation of receipt or deal with non-receipt via an alternative solution.

7.3.2. Ancillary systems using the payments interface

Pay-ins (from TARGET2 to the ancillary system) are still normally processed, but the central bank might have to inform the ancillary system via national communication means about incoming payments.

Pay-outs (from the ancillary system to TARGET2) are processed by the ancillary system using one of the following methods:

i. The ancillary system may make clean payments using the payments interface if it still has access to it, or using backup lump-sum payments via the ICM.

ii. The central bank sends a mandated payment (a payment by the central bank, debiting the ancillary system and crediting the settlement bank). The central bank might have to inform the ancillary system via national communication means about the processed payments.

7.4. SWIFT/network operator failure

Please be aware that the functionality of the Contingency network referred to in this chapter will not be activated together with the release 5.0 on 21 November 2011, but at a later stage following further testing and set-up activities. This will be announced to the users in advance.

[47] For example: ASTransferNotice, ASInitiationStatus, ReceiptAS(I), ReturnAccountAS)

The contingency network considerably improves the resilience of TARGET2 and overall systemic stability in the event of a regional or global SWIFT outage. Central banks can enter (very) critical backup contingency payments, and send ancillary system files to the SSP, on behalf of their customers via a contingency network. They are also able to monitor the accounts of their participants via the ICM. However, it does not fully replace the SWIFT network, as the connection between the participants and their national central bank is not covered and still relies on the means currently available such as e-mail, fax, etc.

In the event of a global SWIFT outage, the daily volume of payments to be processed is around 3,000, consisting of 2,300 (very) critical payments and 700 ancillary system files. A distinction is made between very critical payments, which have to be processed, and critical payments, where approval by the crisis manager in charge is needed before processing. Chapter 6.4.2., “Contingency processing using the contingency module”, explains the concept of (very) critical payments in TARGET2.

The contingency network can be activated for one country, for several countries or for all TARGET2-connected countries. The contingency network will not be activated for only one participant.

The activation of the contingency network automatically activates the backup lump-sum and contingency functionality for all participants connected via the affected central banks.

7.4.1. Processing of payments

TARGET2 users inform their central bank of payments to be processed in contingency mode. The payment instructions are sent to the national service desk using contingency procedures agreed beforehand at local level.

The national service desk, having access to the ICM screens, processes the payment instructions using the four-eye principle. The settlement of the backup payments is monitored. The instructing parties receive feedback from the national service desk using the local procedures.

The following should be taken into consideration:

- Participants having access to the SWIFT network and internet-based participants can continue to send payments, but must as far as possible limit their activities to the sending of (very) critical payments to avoid placing an additional workload on the receiving side.
- As the transaction reference number for payments processed via the backup functionality is generated by the system, no double entry check can be performed to avoid duplicate submission once the connection with the SWIFT network is restored. Every participant

requesting the processing of contingency payments should carefully check its payments flow after the SWIFT outage.

- For payments processed via the contingency network the general format for backup payments is applicable. The payments are provided to the receiver in MT202 format via SWIFTNet FIN (no Y-copy), with field 72 containing the codeword /BUP/. The sender of the payment is the common PM BIC TRGTXEPMXXX. As for any other backup payments, the customer will receive, if requested, a debit notification (MT 900) after the recovery of the SWIFT connection.
- Non-repudiation for the messages transferred via the contingency network is ensured.

7.4.2. Processing of ancillary system files

Ancillary systems unable to access the SSP must create the XML message files and transmit them via contingency means agreed at the national level (private network, e-mail, fax or other) to the respective central bank.

The central bank connects via the contingency network to the ICM and uploads the file on behalf of the ancillary system.

The following specificities are worth mentioning in this context.

- For models 4 and 5 it is possible to confirm or reject the use of the guarantee mechanism.
- For model 6 the ICM screen allows, in addition to the closing of an ancillary system cycle, the opening of a cycle or procedure.
- Duplicate files sent via the different networks are recognised by the SSP and rejected, as long as they use the same reference and are from the same initiating party.
- For files uploaded via the ICM there is no notification (ASTransferNotice, ReturnAccount, MT900/910) sent to he user. The central bank can verify the status of the sent files via the ICM and inform the ancillary system involved.

8. Contingency and business continuity testing

8.1. Scope

TARGET2 includes the Single Shared Platform (SSP), Proprietary Home Accounts (PHAs) and other applications used by NCBs, ancillary systems (AS) and banks to connect to and operate with the SSP.

All these entities fall under the scope of the "Information security policy for TARGET2" approved by the ECB Governing Council and thus have the responsibility to ensure that their infrastructures are operated in a secure and reliable manner. This includes that they have adequate contingency and business continuity measures in place for all business functions considered as critical, which are tested in regular intervals.

A SWIFT failure does not fall within the scope of the testing neither since the ECB Governing Council accepted the residual risk of such an outage.

8.2. Objective of testing

Contingency and business continuity measures have the objective to ensure that failures of TARGET2 components at any level does not cause any disruption to the overall functioning of TARGET2.

Each TARGET2 user should at first rely on its own backup measures. The SSP offers contingency arrangements to overcome short interruptions on the side of the critical participants, NCBs and the SSP, which aim at processing a limited number of (very) critical payments. Additionally NCBs may offer their TARGET2 users other arrangements such as an AS contingency tool and mandated payments.

8.3. Roles and responsibilities

Mandatory and optional contingency and business continuity tests for the SSP and CB environments are organised under the common responsibility of the Level 2 and coordinated by the ECB.

The national service desks organise mandatory tests with their critical participants as well as optional tests with critical and normal participants. This includes the preparation of a test schedule, practical support in performing the tests and the collection of test reports.

The TARGET2 coordination desk contributes to the organisation at the inter-member-state level, whenever needed.

8.4. Test environment

For the tests to be effective, they should either be performed in the production environment or, where this is not considered appropriate due to the additional operational risk, in a test environment as similar as possible to the production environment.

For tests with TARGET2 users (NCBs, banks, ancillary systems), the user test environment of the SSP (CUST) is considered as close to the production environment as a test environment can be.

Occasionally, when new SSP releases are tested, the CUST environment may not use the same version as the PROD environment. With regard to the PHA environments, each NCB providing a PHA is expected to provide a test environment that is as similar as possible to the production environment.

8.5. Frequency and planning

The testing of the contingency arrangements should be performed by all critical participants at least once every six months. The business continuity testing should be performed by all critical participants at least once a year.

By default, the CUST environment of the SSP is open every weekday from 06:30 until 19:00, except on Fridays when it closes at 17:00. The cut-off time for interbank payments is set at 14:30. Exceptions are communicated in advance.

8.6. Test results and reporting

Test results should be classified as either successful or unsuccessful. When the test objectives are not met, the test result should be seen as unsuccessful. For unsuccessful tests a repetition of the test is expected within 3 months.

AS and banks shall report the result of tests in line with the instructions provided by the national service desk.

The national service desks will provide summary reports at regular intervals to the TARGET2 coordination desk at the ECB allowing for the overall monitoring and assessment on a system wide level, which will then form part of the annual reporting on TARGET2 and lead to follow-up actions whenever required.

8.7. Testing contingency arrangements

8.7.1. For direct participants

Direct participants may use two different types of backup payments to initiate payment orders via the ICM in a situation where their normal payment processing ability is interrupted.

- Backup contingency payments are used to fulfil obligations arising from CLS, EURO1 or STEP2 payments on time. They replace the original payment.
- Payments to redistribute liquidity (backup lump-sum payments) allow the direct participant to redistribute liquidity accumulating on its account and avoid the possible build-up of excess liquidity which could impair TARGET2's efficiency and potentially create systemic risk. The reference to backup payments functionality in the UDFS, book 1, section 2.4.5 is subject to review.

Each critical participant intending to use the backup payments feature or an additional arrangement offered by its NCB (e.g. AS contingency tool or mandated payments) should perform one of the following five test scenarios at least twice a year following pre-agreement of the date with the respective NCB:

- Requesting the activation of the backup functionality in live operations via its NCB and the sending of the respective backup payments as low value payments (less than 10€, but different amounts) to pre-agreed accounts. NCBs may offer their accounts to be used as addressee for payments, when no other test counterparty is available.
- NCBs are expected to be able to execute the critical payments on behalf of their critical participants using the backup functionality and test this together with them.
- Alternatively, if the risk of tests in the live environment is considered to be too high, the same type of test can be performed in the CUST environment. Then no limits apply to the amount.
- NCBs offering their ASs the AS contingency tool are expected to test its operational functionality.
- NCBs offering their critical participants mandated payments are expected to test its operational functionality.

NCBs may decide – in cooperation with their TARGET2 users - to limit the number of days and time when such tests are possible or may keep this as a permanent option accessible on each day when the respective environment is operating. When limiting the number of days or the time, NCBs shall ensure

that sufficient opportunities are provided allowing each critical participant to schedule respective tests at least every three months.

Non-critical participants are invited to arrange at regular intervals for similar testing events with their respective national service desk.

8.7.2. For SSP

The Contingency Module (CM) is the common mandatory tool to manage an emergency situation where the normal PM functionality is not available, but still (very) critical payments need to be processed. Only NCBs have access to the CM and can perform payments on behalf of their TARGET2 users. In this respect each TARGET2 user and each NCB should identify and keep up-to-date information about the maximum number of (very) critical payments to be processed per hour and the respective channels that may be used to submit these payments in contingency. NCBs should take into account their own processing requirements plus those of the TARGET2 user with the highest possible hourly number of such payments.

Although only CBs have direct access to the CM, also all TARGET2 users involved in the processing of (very) critical payments shall be involved in this test. The scenario consists of the delivery of the hourly maximum of (very) critical payments by the TARGET2 users to the NCB and the respective processing in the CM by the NCB. TARGET2 users are expected to exchange their hourly maximum number of critical payments. NCBs are expected to confirm the processed payments using a secure channel.

TARGET2 users are expected to find counterparts with whom they can exchange payments. Where inter-member-state payments are part of the scenario and the counterparty is not available for testing, the respective NCB shall replace the external counterpart with one of its own accounts.

For the tests to be most effective and living up to what is expected in a real disaster situation the provision of the fresh liquidity to the CM is part of the test between CBs and their TARGET2 users.

The SSP service desk will test the same scenario acting on behalf of an NCB performing the highest hourly volume of (very) critical payments foreseen for any NCB.

For testing purposes, the SSP service desk activates the CM in CUST on Wednesdays from 10:00 to 12:00. Testing outside this time window needs to be requested to the SSP service desk via the respective national service desk.

8.7.3. For PHAs

PHAs with payments functionalities are expected to execute the identified (very) critical payments on behalf of their own user community. Therefore contingency tests should be carried out to verify that contingency measures are technically and operationally effective, even without involvement and/or exposure to external parties.

The following scenarios for those NCBs shifting liquidity between PM and PHA should be tested:

- Failure at the start of the day trade phase, requiring transferring of liquidity for critical participants to the PM.
- Failure at the end of the day requiring the manual processing in the reserve management module (RM) and/or PHA accounts.

Other scenario's can be elaborated by NCBs using a PHA.

NCBs may decide – where applicable and in cooperation with their TARGET2 users - to limit the number of days and time when such tests are possible or may keep this as a permanent option accessible on each day when the respective environment is operating. When limiting the number of days or the time, NCBs shall ensure that sufficient opportunities are provided allowing each critical participant to schedule respective tests at least every three months.

8.8. Testing business continuity

8.8.1. For critical participants

Each TARGET2 user classified by the Eurosystem as being critical for the smooth functioning of TARGET2 must have a business continuity strategy in place comprising the following elements:

- Business continuity plans have been developed and procedures for maintaining them are in place.
- An alternate operational site must be available.
- The risk profile of the alternate site must be different from that of the primary site (significant distance between the sites, different power grid, different central telecommunications, etc.).
- In the event of a major operational disruption rendering the primary site inaccessible and/or critical staff unavailable, the critical participant must be able to resume normal operations from the alternate site, where it must be possible to properly close the

business day, and must be in a position to open the following business day(s) from the alternate site.

- Procedures must be in place to ensure that the most critical business transactions can be performed while business is being moved from the primary to the alternate site.
- The ability to cope with operational disruptions must be tested at least once a year and all critical staff must be suitably trained. The maximum period between tests should not exceed one year.

Taking into account the above, the business continuity testing requirements can be summarised as follows:

- The critical participants must test their business continuity procedures, perform their critical business transactions and close the business day from the secondary site at least once a year (see Chapter 8.4., "Test environment").
- The critical participants should inform the respective national service desk of the business continuity test in advance and report afterwards on the outcome of the test.

8.8.2. For SSP

Business continuity comprises the procedures and infrastructures in place for the SSP, which allow in case of a failure or disaster, to failover to the backup site within the same region or to the second region. NCBs providing a PHA and critical participants are expected to have similar procedures and infrastructures in place. Furthermore the business continuity oversight expectations for systemically important payments systems are taken into account.

The two available scenarios are tested in regular intervals:

- intra-regional failover
- inter-regional failover

Such tests are by default performed in the PROD environment during week-ends and do not require mandatory user involvement. Users may be invited to take part in such testing activities via the national service desks. Exceptionally, similar tests may be performed in the CUST environment.

8.8.3. For PHAs

PHAs with payments functionalities are expected to also maintain a secondary site. Therefore, business continuity tests should be carried out to verify that business continuity measures are technically and operationally effective, even without involvement and/or exposure to external parties.

9. Change and release management

This chapter describes both the yearly release management process as well as the change process for emergency changes and hot fixes.

9.1. Yearly release

The Eurosystem endeavours to keep the TARGET2 system in line with the various business changes in the field of large-value payments. This continuous interest in the system's evolution is seen as a necessity to further increase its level of service and the satisfaction of its users. For this reason, it is of great importance that all TARGET2 users be involved in the release management process in a proper and timely manner.

In general, TARGET2 releases take place annually and coincide with the annual SWIFT Standard Releases in November. In exceptional circumstances, however, it is possible for an intermediary release to be scheduled (i.e. two releases in the same year) or no release to be issued in a given year.

The annual TARGET2 release is a long process, which takes place over a 21-month period in order to give all parties enough time for discussion, prioritisation, implementation and testing. Furthermore, information is made available to the TARGET2 users early enough to allow for proper planning and budgeting of all changes.

9.1.4. Main applicable deadlines

All dates provided in this section are indicative and are confirmed by the Eurosystem for each annual release in the course of February of year Y-1. While an effort will be made to keep to these dates as much as possible, limited deviations may be allowed, if and when needed, and after consultation with the user community.

Year Y-1	mid February	**Confirmation of final dates**
	early March - mid April	**First user consultation**
	mid September – mid October	**Second user consultation**
	mid November	**Communication on the release content**
Year Y	early March	**Delivery of the UDFS**
	mid April	**Delivery of the test plans and scenarios**

	end August	**Start of user testing**
	mid November	**Go-live**

Table 8: Annual release time-line

9.1.5. User involvement

Two consultations with the user community are organised as part of the discussions regarding the content of the annual TARGET2 release. In order to involve all TARGET2 users in the definition of the release content, the national central banks of countries connected to TARGET2 will contact their respective national user groups (NUGs) and, in parallel, the ECB will approach the TARGET Working Group (TWG) of the European Credit Sector Associations (ECSAs).

- The first consultation aims to collect proposals for functional changes from all TARGET2 users. These changes are expected to be sufficiently detailed and to be beneficial for a large number of TARGET2 users. To facilitate this consultation, a list of functional changes proposed in the framework of earlier releases is provided as a background document, together with a number of changes suggested by central banks on an indicative basis, both marked with unique reference numbers. Proposals should describe the business case and the expected functional changes in a precise manner. A template is provided by the Eurosystem for the submission process. At the end of the first consultation, all proposals made by the NUGs and the TWG are carefully considered by the Eurosystem in order to identify a subset of changes on which a further cost/benefit assessment will be carried out.
- The second consultation aims to collect TARGET2 users' feedback on changes short-listed by the central banks as a result of the first user consultation. No new proposals for changes are possible during this phase. "Ballpark" cost indications for the envisaged features are also provided. The feedback must be provided on the basis of standard rating criteria defined in advance. At the end of the second consultation, the Eurosystem considers all feedback received from TARGET2 users and forms a final view on the content of the annual TARGET2 release, which is communicated shortly thereafter[48].

In order to facilitate the users in the process of defining their change requests, a Change Request (CR) template is available. (Annex IV).

All change requests submitted by the users should use this template. Any other form will be discarded

[48] It should be noted that the Eurosystem may announce changes relating to SWIFT at a later stage, when the final content of the SWIFT FIN and CAMT Standard Release is known. In addition, if the release contains the correction of bugs, those amendments will be communicated at a later stage as well.

and returned.

9.1.6. Prioritisation and decision-making

When prioritising the various proposals received from TARGET2 users, or when making a final decision on the release content, central banks give due consideration to the following criteria:

- For each individual change, a thorough cost/benefit analysis is carried out. This mainly looks at the feedback received from the user community during the consultation rounds, the benefits for the industry as a whole in terms of service brought about by the change, the expected usage of the feature, the investment and operational cost at stake, the sustainability of the new service from a cost recovery perspective, the complexity of the developments, and the possible risk of introducing regression bugs. Lastly, whenever it is relevant, central banks also consider the compliance of the change with the Eurosystem's policy or strategic stances on TARGET2.
- For the release as a whole, the central banks aim to ensure that the release content is well balanced in terms of the benefits for the different types of TARGET2 users and that it complies with the workload and budget limits fixed for the annual release.

As a matter of transparency, after each consultation step, TARGET2 users will be provided with the necessary information as to why a change was selected or discarded.

9.2. Emergency changes and hot fixes

The intention of this section is to describe those elements of the SSP change and release management process, which are strongly linked to the daily operation of TARGET2 and are as such not covered as part of the regular yearly release management process.

The following categories of changes may lead to changes to the SSP in between the yearly major releases:

1. Emergency changes
2. Minor changes considered serious enough to be implemented as "hot fix"

Any other changes will be considered within the normal change and release management procedures applicable for the annual releases.

9.2.1. Emergency changes

Emergency changes occur in the event of system difficulties that require an immediate change to continue the SSP service or to avoid a substantial reduction in the quality of service. Such changes are

strongly linked to the incident management as described in chapter 5 of this document, “Procedures in abnormal situations in TARGET2”, and may be installed within the TARGET2 business day. If the emergency change impacts functionalities used by TARGET2 users, they will be informed by an ICM broadcast.

9.2.2. Hot fixes

Hot fixes are only justified if not solving the issue before the next regular release could lead to substantial operational problems, requires heavy workarounds to be performed and/or leads to any other clear increase in the operational risk level. Such fixes will be always be installed first in the CUST environment and – to the extent possible – tested there. Where necessary due to the impact on the TARGET2 users, an ICM broadcast will be sent to all TARGET2 users before the hot fix is implemented.

10. TARGET2 compensation scheme

If there is a technical malfunction of TARGET2, TARGET2 users can submit claims for compensation in accordance with the TARGET2 compensation scheme laid down in appendix II of the Harmonised Conditions.

Unless otherwise decided by the ECB Governing Council, the TARGET2 compensation scheme shall not apply if the technical malfunction of TARGET2 arises as a result of external events beyond the reasonable control of the central banks concerned or of acts or omissions by third parties.

Compensation under the TARGET2 compensation scheme shall be the only compensation procedure offered in the event of a technical malfunction of TARGET2. TARGET2 users may, however, use other legal means to claim for losses. If a TARGET2 user accepts a compensation offer under the TARGET2 compensation scheme, this shall constitute its irrevocable agreement that it thereby waives all claims in relation to the payment orders concerning which it accepts compensation (including any claims for consequential loss) it may have against any central bank, and that the receipt by it of the corresponding compensation payment constitutes full and final settlement of all such claims. The TARGET2 user shall indemnify the central banks concerned, up to a maximum of the amount received under the TARGET2 compensation scheme, in respect of any further claims which are made by any other TARGET2 user or any other third party in relation to the payment order or payment concerned.

The making of a compensation offer shall not constitute an admission of liability by the respective central bank or any other central bank in respect of a technical malfunction of TARGET2.

Further information is available in appendix II of the Harmonised Conditions.

Procedure to be followed:

- A claim for compensation shall be submitted on the claim form available on the website of the respective central bank in English. Payers shall submit a separate claim form in respect of each payee and payees shall submit a separate claim form in respect of each payer. Sufficient additional information and documents shall be provided to support the information indicated on the claim form. Only one claim may be submitted in relation to a specific payment or payment order.
- Within four weeks of a technical malfunction of TARGET2, TARGET2 users shall submit their claim form(s) to the respective central bank. Any additional information and evidence requested by the respective central bank shall be supplied within two weeks of such request

being made.

- The respective central bank shall review the claims and forward them to the ECB. Unless otherwise decided by the ECB Governing Council and communicated to the TARGET2 users, all received claims shall be assessed no later than 14 weeks after the technical malfunction of TARGET2 occurs.
- The respective central bank shall communicate the result of the assessment to the relevant TARGET2 users. If the assessment entails a compensation offer, the TARGET2 users concerned shall, within four weeks of the communication of such offer, either accept or reject it, in respect of each payment or payment order comprised within each claim, by signing a standard letter of acceptance (in the form available on the website of the respective central bank). If such letter has not been received by the respective central bank within four weeks, the TARGET2 users concerned shall be deemed to have rejected the compensation offer.
- The respective central bank shall make compensation payments on receipt of a TARGET2 user's letter of acceptance of compensation. No interest shall be payable on any compensation payment.

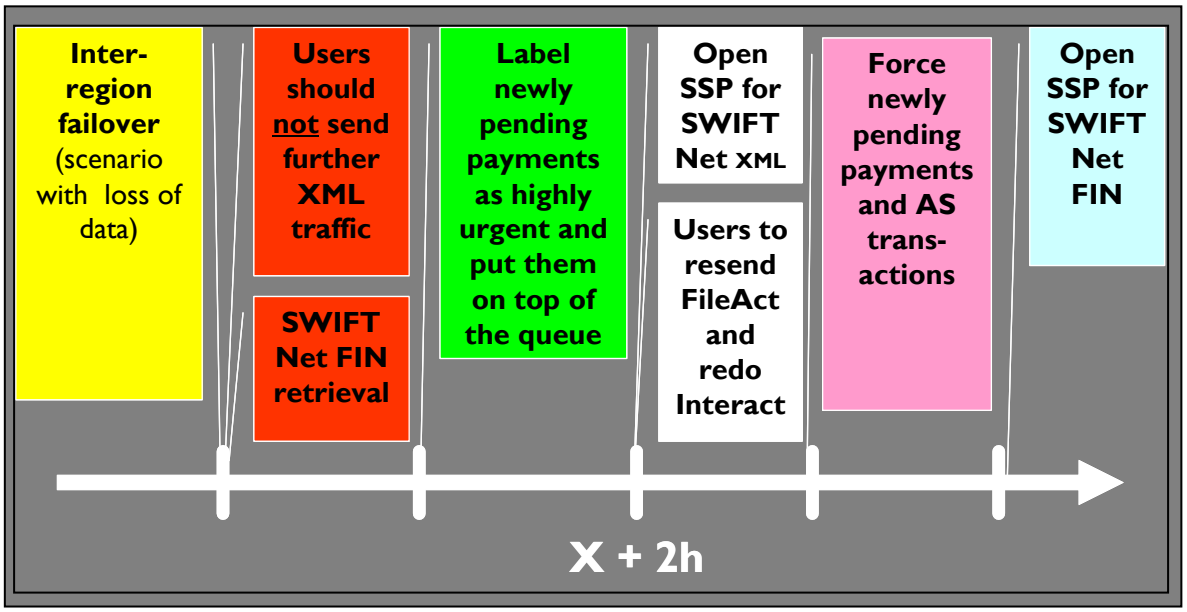
Annex I Inter-region failover with loss of data

Rebuilding process

- According to the 3CB, a rebuilding process in Region 2 is only required in the event that both sites in Region 1 become unavailable at the same time and there is a consequential loss of data:
  - The aim of the rebuilding is to ensure that all messages processed in Region 1 are also shown in Region 2. In order to achieve this, all messages processed in Region 1 in the two minutes preceding the incident are retrieved and reconciled against what is shown in Region 2 to identify possible missing messages.
  - The missing messages could include: (i) SWIFT FIN messages; (ii) FileAct messages (sent by an ancillary system via the ASI); and (iii) InterAct messages (from banks, ancillary systems and central banks).
  - SWIFT FIN messages can be retrieved and the FIN traffic reconciled (this would make up about 80% of the missing traffic).
  - During the outage and the failover, the users might continue to send FIN payments (which would be queued at SWIFT level) but should not send new XML traffic until further notice (InterAct and FileAct messages).
  - Upon the FIN retrieval, all coupled FIN messages (matching messages MT096 and MT097) will be booked in Region 2, while all non-coupled messages will be queued in Region 2. Coupled FIN messages that were final in Region 1 but, due to missing coverage, could not be booked in Region 2 would be shown as “newly pending payments”. The SSP service desk would label all pending payments as “highly urgent” and place them at the front of the queue of highly urgent payments. This should all be achieved within two hours of the decision to fail over.
  - The SSP service desk will inform the TARGET2 coordination desk, which will hold a settlement manager teleconference to initiate the resending of XML traffic (InterAct and FileAct messages, which represent about 20% of the missing traffic). This means the SSP service desk will open the SSP for SWIFTNet services, i.e. FileAct and InterAct. Ancillary systems will be required to resend any FileAct messages with the same references that they had sent in the ten minutes preceding the incident in Region 1 or those files that the ancillary system identified as missing. Moreover, ancillary systems, banks and central banks will also

be required to redo the InterAct traffic they did in the two minutes preceding the incident. However, new XML traffic should not be sent. With the opening of the SSP for SWIFTNet, the users would also get access to the ICM to check the processing status.

- The processing of the missing XML traffic should further reduce the "newly pending payments". Any still remaining "newly pending payments" should be "forced" by the central banks, by this acknowledging that they were final in Region 1 and should remain final in Region 2. Any resulting remaining risk would hence remain with the Eurosystem. Similarly, any remaining "newly pending AS transactions" that were final in Region 1 should remain final in Region 2 and hence be "forced". In order to become aware of "newly pending AS transactions", the ancillary system would have to provide evidence to the respective central bank that these transactions were final in Region 1 (e.g. by means of a copy of the received notification).
- After the SSP service desk confirms to the TARGET2 coordination desk that all newly pending payments have been processed, a teleconference of the crisis managers will be held, in order to get their approval that the SSP should be opened for SWIFT FIN traffic. Any queued FIN payments will be processed. Also, new FileAct and InterAct messages can be sent by the users. In case the CM was used, the transfer of balances from the CM to the PM will take place after the opening of the SSP for SWIFT FIN traffic.



Annex II Incident report for TARGET2 user

Confidentiality

The information included in this document will only be used by the Eurosystem to further strengthen the resilience of the TARGET2 system as a whole. Within the Eurosystem, access to this information is only granted to those with a business-related need to know.

Name of the central bank responsible	

Point of contact (POC) information	
Name of the TARGET2 user	
Name of the contact person	
Title/function	
Telephone number	
E-mail address	

General incident information	
Incident ID (to be assigned by the central bank responsible)	**CC/YYYYMMDD/no**

Status	☐ Interim	☐ Final[49]
Type of failing component	☐ Hardware ☐ Network[51] ☐ Human error	☐ Software[50] ☐ Infrastructure[52]
Date and time the incident started (CET)	ddmmyyyy / hh.mm	
Date and time the incident ended (CET)	ddmmyyyy / hh.mm	
Duration	hh.mm	

Description of the incident (the summary should be a high-level description suitable for senior management and avoiding technical language to the extent possible. The summary should include for instance the following elements: • basic description of the events and their impact; • services/systems affected by the incident; and • external effects (e.g. other TARGET2 users affected)).

Details of the cause of the incident (specifically, the root cause of the incident (who, what, where, when, how?))

Remedial action (this section should include for instance the following elements: • action taken to resolve the incident; and • measures taken to prevent the incident from reoccurring/implementation scheduled for)

49 An incident report is considered "final" when the implementation date of the remedial measure is indicated.

50 Software comprises system software (including DB systems) and application software.

51 Network comprises only the internal network. External network failures should be listed under infrastructure.

52 Infrastructure comprises premises, supporting services (e.g. air conditioning, power supply, telecommunication (including SWIFT)).

_____

Date and signature

Name of the signatory (Print):

Title:

This form should be returned to the central bank mentioned above:

Address	
Contact person	

Annex III Self-certification statement

Introduction

The Core Principles for Systemically Important Payment Systems set out certain responsibilities that must be fulfilled by the operators of a payment system. More specifically, Core Principle VII (CP VII) relates to issues concerning the security and operational reliability of a systemically important payment system.

CP VII states that the *"…operators of a payment system … need to concern themselves not just with the security and operational reliability of the components of the central system, but also with the components of the system's participants…."*

In light of this, the Eurosystem, in its capacity as TARGET2 system operator, developed a set of requirements regarding information security management and business continuity management with which the critical participants in TARGET2 must comply. Critical participants can certify their level of compliance with these requirements in the appendix to this statement. The Governing Council of the ECB approved this concept on 25 October 2007.

Requirements regarding information security management and business continuity management

1 Information security management

Critical participants must assess the security of their initial TARGET2 interface components and of those components which are beyond their initial interface but are of crucial importance for the smooth flow of payments. The set of requirements collects at a high level the principles that are to be implemented by the critical participants with regard to information security management. These principles were derived from the internationally agreed standard ISO/IEC 27002:2005.

Requirement 1.1: Information security policy

Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy applicable across the organisation.

Requirement 1.2: Internal organisation

A management framework should be established to initiate and monitor the implementation of an information security policy within the organisation. Management should approve the information security policy, assign security roles and coordinate and review the implementation of the policy across the organisation.

Requirement 1.3: External parties

The security of the organisation's information and information processing facilities should not be reduced by the introduction of external party products. Any access to the organisation's information processing facilities by external parties should be controlled. When access by external parties or products/services from external parties is/are required, a risk assessment should be carried out to determine the security implications and control requirements. Controls should be agreed and defined in an agreement with the external party.

Requirement 1.4: Asset management

All organisational assets should be accounted for and have a nominated owner. The responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls can be delegated by the owner as appropriate, but the owner remains responsible for the proper protection of the assets.

Requirement 1.5: Information classification

Information should be classified to indicate the need, priorities and degree of protection required when handling it. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.

Requirement 1.6: Human resources security

Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs. Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities. An adequate level of awareness should be ensured among all employees, contractors and third party users, and education and training in security procedures and the correct use of information processing facilities should be provided to them, to minimise

possible security risks. A formal disciplinary process for handling security breaches should be established. Responsibilities should be in place to ensure an employee's, contractor's or third party user's exit from or transfer within the organisation is managed, and that the return of all equipment and the removal of all access rights are completed.

Requirement 1.7: Physical and environmental security

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage and interference.

Equipment should be protected from physical and environmental threats. Protection of equipment (including that used off-site) and the removal of property is necessary to reduce the risk of unauthorised access to information and to guard against loss or damage. Special measures may be required to protect against physical threats and to safeguard supporting facilities such as the electrical supply and cabling infrastructure.

Requirement 1.8: Communications and operations management

Responsibilities and procedures should be established for the management and operation of all information processing facilities. As regards operating procedures, segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

The organisation should, in relation to third party service providers, 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.

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 should be made, to reduce the risk of system overload. The operational requirements of new systems should be established, documented and tested prior to their acceptance and use.

Precautions must be taken 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, and users should be made aware of its dangers. Managers should, where appropriate, introduce controls to prevent, detect and remove malicious code and control mobile

code.

Routine procedures should be established to implement the agreed backup policy and strategy for taking backup copies of data and rehearsing their timely restoration.

The secure management of networks, which may span organisation boundaries, requires careful consideration to be given to dataflow, legal implications, monitoring and protection. Additional controls may also be required to protect sensitive information passing over public networks.

Data storage media should be controlled and physically protected. Appropriate operating procedures should be established to protect documents, computer media, input/output data and system documentation from unauthorised disclosure, modification, removal and destruction.

Exchanges of information and software between organisations should be based on a formal exchange policy and carried out in line with exchange agreements, and should be compliant with any relevant legislation. Procedures and standards should be established to protect information and physical media containing information in transit.

Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure that information system problems are identified. System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

Requirement 1.9: Access control

Access to information, information processing facilities and business processes should be controlled on the basis of business and security requirements. Access control rules should take account of policies for information dissemination and authorisation. Formal procedures should be in place to contro the allocation of access rights to information systems and services. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final deregistration of users that no longer require access. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights which allow users to override system controls

Users should be made aware of their responsibility for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment. A clear desk and clear screen policy should be implemented to reduce the risk of unauthorised access or damage to

papers, media and information processing facilities.

Access to both internal and external networked services should be controlled. User access to networks and network services should not compromise the security of the network services, i.e. it should be ensured that appropriate interfaces are in place between the organisation's network and networks owned by other organisations and public networks, appropriate authentication mechanisms are applied for users and equipment, and controls of user access to information services are enforced.

Security facilities should be used to restrict access to operating systems to authorised access. The facilities should be capable of authenticating authorised users, recording successful and failed system authentication attempts, recording the use of special system privileges, issuing alarms when system security policies are breached, providing appropriate means for authentication and, where appropriate, restricting users' connection times. Logical access to application software and information should be restricted to authorised users.

When mobile computing is used, the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of teleworking the organisation should apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

Requirement 1.10: Information systems acquisition, development and maintenance

Information systems include operating systems, infrastructures, business applications, off-the-shelf products, services and user-developed applications. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.

Appropriate controls should be built into applications, including user-developed applications, to ensure correct processing. These controls should include the validation of input data, internal processing and output data. Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls should be determined on the basis of security requirements and risk assessment.

A policy should be developed on the use of cryptographic controls to protect the confidentiality, authenticity and integrity of information. Key management should be in place to support the use of cryptographic controls.

Access to system files and program source code should be controlled and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments. Project and support environments should be strictly controlled.

Technical vulnerability management should be implemented in an effective, systematic and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems and any other applications in use.

Requirement 1.11: Information security incident management

Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organisational assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact. Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating and overall management of information security incidents.

Requirement 1.12: Compliance

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 the organisation's legal advisers or suitably qualified legal practitioners.

The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies, and the technical platforms and information systems should be audited for compliance with applicable security implementation standards and documented security controls. There should 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.

2. Business continuity management

Each TARGET2 user classified by the Eurosystem as being critical for the smooth functioning of the TARGET2 system must have a business continuity strategy in place comprising the following

elements.

Requirement 2.1: Business continuity plans have been developed and procedures for maintaining them are in place.

Requirement 2.2: An alternate operational site must be available.

Requirement 2.3: The risk profile of the alternate site must be different from that of the primary site, meaning that the alternate site must (i) be a significant distance away from and (ii) not depend on the same physical infrastructure components[53] as the primary business location.[54] This minimises the risk of both sites being affected by the same event. For example, the alternate site should be on a different power grid and central telecommunication circuit from those of the primary business location.[55]

Requirement 2.4: In the event of a major operational disruption rendering the primary site inaccessible and/or critical staff unavailable, the critical participant must be able to resume normal operations from the alternate site, where it must be possible to properly close the business day and open the following business day(s).

Requirement 2.5: Procedures must be in place to ensure that the most critical business transactions can be performed while business is being moved from the primary to the alternate site.

Requirement 2.6: The ability to cope with operational disruptions must be tested at least once a year and critical staff must be suitably trained. The maximum period between tests should not exceed one year.

[53] It should be noted that there is no obligation to use different hardware brands and/or software components for tasks such as installing an MS Windows infrastructure in the primary site and UNIX systems in the alternate location. The statement "*...should not depend on the same physical infrastructure..."* emphasises that alternate sites should not rely on the same infrastructure components (e.g. transportation, telecommunications, water supply and electric power) used by the primary site.

[54] It is acknowledged that TARGET2 users can only be responsible for what is within their immediate sphere of control. There is an element of reliance on suppliers and participants cannot be held liable if the resilience of a service provided by a third party is less robust than expected. However, TARGET2 users should make efforts to ensure that an appropriate level of resilience is stipulated in the contract with the suppliers. For example, a telecoms provider should commit on multiple routing facilities and this should be laid down in the contractual arrangements.

[55] Derived from the "High-level principles for business continuity" prepared by the The Joint Forum, Bank for International Settlements, August 2006.

Compliance identification

For each of the requirements listed in the previous sections the critical participant must report its level of compliance in the appendix to this self-certification statement.

In the event of non-compliance at level 2 or level 3 with the above-mentioned requirements, a description of the major risks[56] should be included in the appendix. Furthermore, an action plan for rectifying the situation and the planned dates for implementing each particular measure should be included. This information must be evaluated and the implementation of risk-mitigating measures monitored by the central bank responsible.

Contact details

In the following table should be given the name and contact details of a person to be contacted in case further information is required.

Name of the critical participant	
Address	
Contact person (name) (print)	
Contact person (telephone)	
Contact person (e-mail)	

Signatory

The self-certification statement should be signed by a senior official (i.e. at board level) responsible for the relevant business area within the critical participant. Given the heavy reliance on information technology (IT), the self-certification statement should, in addition, be signed by a senior official (also at board level) responsible for the IT department within the critical participant. If a senior official from the critical participant is responsible for both the business area and the IT department, one signature is sufficient.

[56] A major risk could be, for instance, insufficient measures against denial of service attacks, uninterruptible power supply not in place, etc.

Certification

The signatories confirm that they have read and understood the requirements outlined in this self-certification statement. The statement (including the annex) is valid for one year and is due for renewal one year after the date of the first signature.

The signatories certify that the information contained in the annex represents a true and accurate picture of the current situation. They further certify that the annex has been prepared under their direction and supervision and that qualified personnel properly gathered and evaluated the information provided. The submitted information is, to the best of the signatories' knowledge and belief, true, accurate and complete. The signatories are aware that submitting false, inaccurate or misleading information constitutes a breach of the legal provisions, which is one of the grounds for termination of an institution's participation in TARGET2.

Finally, the signatories confirm that their organisation has a mechanism in place to ensure that it will remain in compliance over the coming year or, if compliance has not yet been achieved, that appropriate measures will be taken to make satisfactory progress on the work items listed in the action plan.

First signature

Name of official from the business area (print)	
Title	
Date	
Signature	

Second signature

Name of official from the IT department (print)	
Title	
Date	
Signature	

This form (including the annex) should be returned to

(to be filled in by the central bank responsible):

Name of central bank	
Address	
Contact person	

Annex to the self-certification statement

Name of the critical participant …….

1. Level of compliance

Critical participants are required to indicate their level of compliance with the requirements regarding information security management and business continuity management specified by the Eurosystem in its capacity as TARGET2 system operator.

The critical participant should indicate its level of compliance by ticking the appropriate box.

- Full compliance: the critical participant complies with requirements as described in the self-certification statement.
- Levels of non-compliance
    - **Level 1:** no significant areas of non-compliance; reasonable assurance can be given that this does not have the potential to harm the smooth functioning of TARGET2 and/or adversely affect other system participants.
    - **Level 2:** significant areas of non-compliance; reasonable assurance cannot be given, and an exploitation of the vulnerabilities identified could harm the smooth functioning of TARGET2 and/or adversely affect other system participants.
    - **Level 3:** non-compliance; reasonable assurance cannot be given, and an exploitation of the vulnerabilities identified would significantly harm the smooth functioning of TARGET2 and/or adversely affect other system participants

Requirements	**Full compliance**	**Non-compliance**		
		Level 1	**Level 2**	**Level 3**
1. Information security management				

Requirement 1.1	☐	☐	☐	☐
Requirement 1.2	☐	☐	☐	☐
Requirement 1.3	☐	☐	☐	☐
Requirement 1.4	☐	☐	☐	☐
Requirement 1.5	☐	☐	☐	☐
Requirement 1.6	☐	☐	☐	☐
Requirement 1.7	☐	☐	☐	☐
Requirement 1.8	☐	☐	☐	☐
Requirement 1.9	☐	☐	☐	☐
Requirement 1.10	☐	☐	☐	☐
Requirement 1.11	☐	☐	☐	☐
Requirement 1.12	☐	☐	☐	☐
Which information security standard is mainly used for security controls?				
2. Business continuity management				
Requirement 2.1	☐	☐	☐	☐
Requirement 2.2	☐	☐	☐	☐
Requirement 2.3	☐	☐	☐	☐
Requirement 2.4	☐	☐	☐	☐
Requirement 2.5	☐	☐	☐	☐
Requirement 2.6	☐	☐	☐	☐

2. Towards compliance

If any areas of non-compliance at level 2 or level 3 have been identified, the following section must be completed.

Have any risks resulting from non-compliance at level 2 or level 3 with requirements 1.1 to 1.12 and 2.1 to 2.6 been identified? **Comments:**
What steps will be taken to achieve full compliance or reduce non-compliance to level 1? **Comments:**
By when will full compliance or non-compliance at level 1 be achieved? **Comments:**

Annex IV Change Request template

Header of the change	
Title of the change	*A short statement*
Users understanding for the priority	*Possible options: High; Medium; Low*
Affected modules	*If known. Possible options: PM, ICM, SD, HAM; SFM, RMM, ASI; (multiple selection possible)*
Description of the change	
Current behaviour of the system	• *Indication if CR relates to the existing service or to a new one;* • *Description of the relevant current service (provide references to the UDFS and/or ICB User Handbooks);*
Requested changes - functional description	• *Functional description of a new/improved service* • *Indication if the proposed change is optional or mandatory for using (if it is relevant);*
Business case and expected result with the change implementation	*Free text for describing the business case behind the CR as well as the benefits if the CR is implemented.*
Supporting documents	
1 document	*Any further documents as attachments: screen prints, flowcharts etc.*
2 document	*Meaningful examples*

Notes: For the field " Requested change " – the functional description to be precise as much as possible with clear rules which leave no room for interpretation

SSP Change Request Memo	
Originator: _____	**Originators' NCB: _____**
Date: _____	

Some examples of the use of the Change Request Template

Example 1.doc

Example 2.doc

Annex V Glossary

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

-A- *glossary*

Accredited Certification Authority

One or more central banks designated by the Governing Council to act on behalf of the Eurosystem to issue, manage, revoke and renew electronic certificates for the purpose of internet-based access.

Algorithm

An algorithm is a mathematical method to provide a smooth, fast and liquidity saving resolution of the payment queue, for example by taking offsetting payment flows into account.

Ancillary system (AS)

Organisations providing clearing or settlement services that are established in the EEA and are subject to supervision and/or oversight by a competent authority and complies with the oversight requirements for the location of infrastructures offering services in euro, as amended from time to time and published on the ECB website, in which payments or financial instruments are exchanged and/or cleared while the resulting monetary obligations are settled in TARGET2 in accordance with the Guideline on TARGET2 and a bilateral arrangement between such organisation and the relevant Eurosystem central bank.

Ancillary systems can be:

- retail payment systems (RPS)
- large value payment systems (LVPS)
- foreign exchange (FX) systems
- money market systems
- clearing houses
- securities settlement systems (SSS)

Ancillary System Interface

The ancillary system interface (ASI) is a standardised interface to the payments module (PM) which can be used by ancillary systems (ASs) to perform the cash clearing of their business.

AS Technical Account

Account offered in TARGET2 for specific use of ancillary systems.

Auto collateralisation

The auto collateralisation is a specific mechanism used to provide additional liquidity to the SSS settlement process. This technique is based on the automatic interaction between the collateral manager, the SSS and the SSP to perform collateralisation functions (e.g. eligibility checks, valuation of collateral) and the related increase of liquidity.

The auto collateralisation is activated during the SSS settlement process to cope with liquidity shortage of a participant: the collateral to be transferred is automatically selected by the SSS on behalf of the participant based on a specific pre-authorisation.

Two distinct auto collateralisation techniques are currently used by the SSSs:

- firm collateralisation (collateralisation on stock: participants single out the eligible securities that could be used)
- auto collateralisation (collateralisation on flows: with securities deriving from the settlement process itself)

Available liquidity

Credit balance on the account plus collateralised credit line for overdraft (if available).

-B- *glossary*

Backup payments

Owing to a breakdown a direct PM participant's system may be unavailable for the rest of the business day. In order to avoid liquidity concentration on his account or rather to enable him to fulfil his payment obligations against CLS, EURO1 or STEP2, the respective direct PM participant has the possibility to make backup payments. Backup payments are initiated via ICM. Two kinds of backup payments are available:

- Backup lump-sum payments are used to redistribute the liquidity that has accumulated on the defaulting direct participant's account. As soon as the defaulting direct PM participant is once again able to do so, the original single payments belonging to the backup lump-sum payments previously made are submitted to the PM and the recipients of such backup lump-sum payments have to return the backup lump-sum payments.
- Backup contingency payments are used to fulfil obligations against CLS, EURO1 or STEP2 arising from settlement or pre-fund payments on time. The backup contingency payment replaces the original payment.

Batch

A batch is a group of orders (payment orders and/or securities transfer orders) to be processed as a set.

BIC

Business Identifier Code

BIC-1

A non-SWIFT BIC which is identified by a "1" in the 8th position. A BIC-1 cannot be used in the header of a SWIFT message.

BIC-8

The first 8 characters of the BIC, when used for addressing purposes, are called destination.

BIC-11

In addition to the first 8 characters of the BIC, an optional branch code of 3 characters is used to identify any branch or reference of an institution.

BIC directory

Directory published by SWIFT. It contains the Business Identifier Codes (BIC) of the credit institutions.

Broadcast

A broadcast is an information message simultaneously available in the ICM to all or a selected group of SSP participants.

Business continuity

Payment system's arrangements which aim to ensure that it meets agreed service levels even if one or more components of the system fail or if it is affected by an abnormal external event. Include both preventative measures and arrangements to deal with contingencies.

-C- *glossary*

CB

Central bank

CBT

SWIFT Computer Based Terminal

Correspondent Central Banking Model (CCBM)

A mechanism established by the European System of Central Banks (ESCB) with the aim of enabling counterparties to obtain credit from the central bank of the country in which they are based using collateral held in another country. In the CCBM, a CB acts as custodian for the other CBs with regard to the securities held in its domestic securities settlement system.

Central Counter Party (CCP)

An entity that interposes itself between the counterparties to the contracts traded in one or more financial markets, becoming buyer to every seller and the seller to every buyer.

Central securities depository (CSD)

A CSD is an organisation holding securities either in certificated or uncertificated form, to enable book entry transfer of securities. In addition to safekeeping and administration of securities, a central securities depository may incorporate clearing and settlement and assets servicing functions.

Clearing

Clearing is the process of calculating the mutual obligations of market participants for the exchange of securities and money. It may include the process of transmitting, reconciling and, in some cases, confirming payment or securities orders.

Clearing house

An entity hosting a clearing system, which consists of a set of rules and procedures, whereby financial institutions present and exchange data and/or documents relating to funds or securities transfers to other financial institutions at a single location. The procedures often also include a mechanism for the calculation of participants' mutual positions, possibly on a net basis, with a view to facilitating the settlement of their obligations in the settlement system.

Closed User Group (CUG)

A subset of customers grouped for the purpose of their use of the relevant SWIFT services and products when accessing the Payments Module.

Continuous Linked Settlement (CLS)

CLS is a global settlement system for foreign exchange transactions, providing participants with simultaneous processing of both sides of the transaction and thereby eliminating the settlement risk.

Collateral

Collateral is an asset or a third party commitment that is accepted by the collateral taker to secure an obligation to the collateral provider vis-à-vis the collateral taker. Collateral arrangements may take different legal forms; collateral may be obtained using the method of title transfer or pledge.

Collateral pool

Assets owned by members of a transfer system that are collectively available to the systems collateral to enable it to obtain funds in circumstances specified in its rules.

Contingency

Contingency refers to running limited business operations in a failure situation. Systemically important payments will be processed in contingency.

Contingency Module (CM)

Is a common mandatory tool for the CBs for the management of the emergency situations in order to process critical and very critical payments.

Country Code (CC)

Two letter code to identify the country where the respective entity is located; e.g. a country code is used in the SWIFT BIC (digits 5 and 6) of the 8-digit or 11-digit BIC.

Credit institution (CI)

It is the definition given to a "bank" in the European Union. The First EC Banking Directive defines it as an undertaking whose business is to receive deposits or other repayable funds from the public and to grant credits for its own account.

Credit line

Maximum collateralised overdraft position of the balance on an RTGS account in PM or on the PHA. The respective direct participants can get information about changes regarding their credit lines via the ICM. Changes of credit lines will be executed immediately. In case of a reduction of a credit line this change has a "pending" status if the reduction would lead to an uncovered overdraft position. The change will be executed when the overdraft position is covered by the reduced credit line.

Credit transfer

A transfer of funds made on the basis of a payment order or sometimes a sequence of payment orders made for the purpose of placing funds at the disposal of the payee. The payment order may be processed via several intermediaries and/or via one or more funds transfer system.

Crisis manager

Each central bank has a crisis manager who is responsible for managing abnormal events.

CRISP

SSP block of services dedicated to NCBs and to be used on an optional basis by them which provides billing services.

CROSS

SSP service dedicated to CBs and to be used on a mandatory basis by them which comprises archiving and storage services, files for billing calculation, files for statistics on intraday credit and profiling information. The CROSS is offered on the CRSS platform.

Customer Related Services Systems (CRSS)

The CRSS is one of the two technical configurations of the SSP (the other is the PAPSS). On this technical configuration the core and optional services reserved to central banks only are totally or partly implemented.

Customer Relationship and Knowledge of System (CRAKS)

It gathers all services needed to support customer relationship and knowledge of payment systems by the central banks.

Customer Relationship Management (CRM)

Term referring to the management by NCBs of customer-oriented information related to participants and customers (CIs, AS, other customers e.g. NCB customers in HAM).

-D- *glossary*

Day Trade Phase

Is the period of time in TARGET2 between 7.00 a.m. and 6.00 p.m..

Dedicated account

Account in the PM on which dedicated liquidity for ancillary system settlement is held. This can be either a sub-account (interfaced model) or a mirror account (integrated model).

Dedicated liquidity

Liquidity held on a PM sub-account or mirror account to allow the settlement of an ancillary system.

Delayed closing

A delayed closing is the prolongation of the day trade phase.

Delivery versus payment (DVP)

A link between securities transfers and funds transfers system that ensures that delivery occurs if, and only if, payment occurs.

Deposit facility

A standing facility of the Eurosystem which counterparties may use to make overnight deposits at a national central bank, which are remunerated at a pre-specified interest rate.

Depository

An agent with the primary role of recording securities either physically or electronically and may keep records of the ownership of these securities.

Direct debit

Is an authorised debit on the payer's bank account initiated by the payee.

Direct participant

Is a participant in a system that directly carries out transactions with other participants in the system. He can perform all activities allowed in the system without intermediary. In some systems direct participants also carry out transactions on behalf of indirect participants.

-E- *glossary*

EBA Clearing (EBA)

Is an association which, on behalf of its members, maintains the EURO 1 and STEP2 clearing systems.

ECB

European Central Bank

EEA

European Economic Area

Encryption

Is the use of cryptographic algorithms to encode clear text data (plaintext) into cipher text to prevent unauthorised observation.

ESCB

European System of Central Banks

EU

European Union

-F- *glossary*

Failover

A failover is the capability to switch over technically from one site to a second site. Within the configuration of the SSP there are two failover situations:

- intra-region failover: from one site to the second site within the same region
- inter-region failover: from one region to the other region.

FIFO

First In, First Out: processing sequence in which the payment orders are treated in the same sequence as they arrived (i.e. the first payment arrived is treated first, the latest one is treated at the end). The relevant timestamp of each payment is arrival in the SWIFT interface of SSP.

FIFO by-passing

The system tries to process the first transfer in the queue, but if that cannot be executed owing to lack of funds it then tries to settle the next transfer instead; also called Bypass FIFO.

Final settlement

The final settlement is the discharge of an obligation by a transfer of funds and a transfer of securities that have become irrevocable, irreversible, or not annullable.

-G- *glossary*

General Ledger

The General Ledger sometimes known as nominal ledger, is the main accounting record of a business which uses double-entry bookkeeping.

Gridlock

A situation that can arise in a funds or securities transfer system in which the failure of some transfer orders to be executed (because the necessary funds or securities are unavailable) prevents a substantial number of other orders from other participants from being executed.

Gross settlement system

A gross settlement system is a transfer system in which the settlement of funds or securities transfer orders occurs individually (on an order by order basis).

Group of accounts

See Liquidity pooling functionality

Guarantee fund mechanism

Mechanism to provide the complementary liquidity needed according to pre-defined rules in case an AS cannot settle using the settlement banks liquidity only.

Guarantee funds account

Account held on the SSP for maintaining or collecting funds allocated to the settlement of balances of an ancillary system in case of failure of settlement bank(s).

-H- *glossary*

Home account

Account held by NCBs outside of the Payments Module, e.g.

- for entities that cannot have the status of a direct participant in PM
- for entities allowed to open RTGS accounts that are indirect PM participants (or do not participate in PM neither as direct participant nor as indirect participant)
- for RTGS account holders for the settlement of operations which are not processed in the Payments Module

The home accounts are managed by the HAM or by a proprietary accounting system.

Home Accounting Module (HAM)

The Home Accounting Module is an optional module. In the case, a central bank opts for the use of this module different standardised account services are offered for the central bank and its customers.

-I- *glossary*

Information and Control Module (ICM)

Mandatory and unique functional interface between the direct participants and the Payments Module (PM) and the other optional modules like

- Home Accounting Module (HAM)

- Reserve Management Module (RM)
- Standing Facilities Module (SF)
- Static Data Module (SD)

Integrity

The quality of being protected against accidental or fraudulent alteration of transmission and of storage, or the quality of indicating whether or not alteration has occurred.

Internet-based access

An arrangement under which the participant has a PM or HAM account that can only be accessed via the internet and payment messages and control messages are submitted to TARGET2 via the internet.

Intraday credit

Credit extended and reimbursed within a period of less than one business day; in a credit transfer system with end-of-day final settlement, intraday credit is tacitly extended by a receiving institution if it accepts and acts on a payment order even though it will not receive final funds until the end of the business day. It can take the form of:

- a collateralised overdraft or
- a lending operation against a pledge or in a repurchase agreement

Intraday liquidity

Funds which can be accessed during the business day, usually to enable financial institutions to make payments on an intraday basis.

-L- *glossary*

Legal entity

Credit institution directly participating in the SSP through (also AS when participating as a direct participant) one or more participants/accounts in the PM and/or HAM is called a legal entity. This allows to group general information about this credit institution in the Static Data Module.

Level 1

Governing Council of the ESCB

Level 2

Eurosystem central banks

Level 3

SSP providing central banks

Limit

Amount for normal payments a direct PM participant is willing to pay to another direct participant (bilateral limit) or to the other direct participants (multilateral - limit towards whom no bilateral limit is defined), without having received payments (that are credits) first. For a direct participant it is possible to establish standing orders or current bilateral (respectively multilateral) limits.

A normal payment can only be settled if it does not breach the respective limit. Setting limits is only possible vis-à-vis RTGS account holders (in case of a group of accounts: only possible vis-à-vis the virtual account) in the SSP. It is not possible to use limits vis-à-vis participating CBs. Incoming urgent payments from a direct participant towards whom a bilateral/multilateral limit is defined also affect the bilateral/multilateral position.

Liquidity pooling functionality

A facility based on the idea of allowing direct participants to pool their RTGS accounts in an account group. Such an account group consists of one or more account(s) held by a direct PM participant(s) which has a capital and/or management link. The following two options are offered: virtual accounts (only for euro area participants) and consolidated information (available also to participants from non-euro area countries).

Liquidity transfer

Transfer of funds between accounts of the same direct participant or between two accounts of a group of accounts.

It is also a generic settlement procedure (procedure 1), where liquidity is transferred from/to a mirror account to/from a settlement bank's RTGS account.

There are two kinds of liquidity transfers available:

- current order: transfers executed immediately after entry if sufficient liquidity is available
- standing order: transfers of fixed amounts executed regularly at certain points of time, e.g. liquidity injections from HAM accounts to RTGS accounts at the start of the business day. Changes of standing orders become effective on the following business day.

-M- *glossary*

MAC

Message Authentication Code

Mandated payment

Payment initiated by an entity that is not party to the transaction (typically by an NCB or an AS in connection with ancillary system settlement) on behalf of another entity. An NCB sends a credit transfer (with specific message structure) on behalf of the failed direct participant (only in case of contingency situations).

Marginal lending facility

A standing facility of the Eurosystem which counterparties may use to receive overnight credit from an NCB at a pre-specified interest rate against eligible assets.

In general possible options:

- Marginal lending on request: Use on request of the direct participant in general needed for the fulfilment of reserve requirement.
- Automatic marginal lending: Automatic transformation of intraday credit in overnight credit at the end of the day.

Message type (MT)

A specific type of SWIFT messages as identified by a three-digit number. The first digit defines the message category, indicating the general use of the message, the second digit defines the message group and the third digit defines particular message function.

Mirror account

In fact specific RTGS accounts opened to NCBs for the specific use of AS. Mirror accounts are mirrored by another account opened in the SSS. It is debited or credited in case of liquidity transfer between a direct participant's RTGS account in PM and its account in an ancillary system.

-N- *glossary*

National service desk

The national service desk is the contact point for the banking community and ancillary systems at their home central bank. The national service desk will cater for all the TARGET2 users' needs as far as the usage of the services offered within the SSP and local infrastructures are concerned.

NCB

National Central Bank

Netting

An agreed offsetting of positions or obligations by direct participants in a clearing or settlement system. The netting reduces large number of individual positions or obligations to a smaller number of obligations or positions. Netting may take several forms which have varying degrees of legal enforceability in the event of default of one of the parties.

Night-time processing

Period of time for settlement of AS transactions (settlement procedure 6) between 19:30 and 07:00 (interruption for technical maintenance between 22:00 and 01:00).

-P- *glossary*

PAPSS

Payment and Accounting Processing Services Systems

One of the two technical configurations of the SSP (the other one is the CRSS). The following modules of the SSP are implemented on the PAPSS:

- Contingency Module (CM)
- Home Accounting Module (HAM)
- Information and Control Module (ICM)
- Payments Module (PM, including the interface for ancillary systems)
- Reserve Management Module (RM)
- Standing Facilities Module (SF)
- Static Data Module (SD)

Parts of the following services are also implemented on the PAPSS:

- CRISP
- CRAKS3

Payment

In the SSP two general kinds of payments are possible for direct participants:

- customer payments (MT103, MT103+)
- bank-to-bank payments (MT202, MT202COV, MT204)

Payment message/instruction

An order or message to transfer funds (in the form of a monetary claim on a party) to the order of the beneficiary. In TARGET2 the order may relate either to a credit transfer or a direct debit.

Payments Module (PM)

Mandatory module which allows the settlement of payments in the RTGS account, held by all direct participants. In addition, it offers advanced services for liquidity management, for the communication with direct participants and ancillary systems.

Pledge

A delivery of assets to secure the performance of an obligation owed by one party (debtor) to another (secured party). A pledge creates a security interest (lien) in the assets delivered, while leaving ownership with the debtor.

Priority

In general, payments are settled immediately, if sufficient liquidity is available on the RTGS account of the participant. Considering their urgency, they can be submitted by the sender using priorities:

- highly urgent payments (priority class 0)
- urgent payments (priority class 1)
- normal payments (priority class 2).

Payments which cannot be settled immediately are queued according to their priority (highly urgent queue, urgent queue, normal queue). Priorities can be changed via the ICM.

Profiling information

Information delivered to NCBs on the past behaviour of a direct participant or a group of direct participants, aggregated over a past period, and aimed at being comparable with current business day information.

Proprietary home account (PHA)

Account held by NCBs outside of the SSP e.g.

- for entities that cannot have the status of direct participants in PM
- for entities allowed to open RTGS accounts that are indirect PM participants (or do not participate in PM neither as direct participant nor as indirect participant)

- for RTGS account holders for the settlement of operations which are not processed in the PM

The proprietary home accounts are not implemented in the SSP but within every NCB.

-Q- *glossary*

Queuing

An arrangement whereby transfer orders are held pending by the sending direct participant or by the system until it can be processed according the rules of the system.

-R- *glossary*

Raw data file

The raw data file

- serves as check file for the verification of the positions of the General Ledger
- can be used for archiving purposes of NCBs not using CRAKS1 services
- can be used for own reports of the NCBs

Real-time gross settlement (RTGS)

The continuous (real-time) settlement of funds or securities transfers individually on an order by order basis (without netting).

Real-time gross settlement (RTGS) system

A settlement system in which processing and settlement take place in real-time on a gross basis. An RTGS system may provide centralised queues for orders which cannot be settled at the time of the submission due to insufficient funds or quantitative limits on the funds.

Remote participant

A direct participant in the SSP which does not have any representation in the SSP country via he takes part in the SSP.

Repurchase agreement (Repo)

A contract to sell and subsequently repurchase securities at a specified date and price.

Reservation

With the usage of the reservation facility liquidity can be reserved by RTGS account holders for the execution of special transactions with a certain priority class. HAM account holders can use the reservation facility to reserve liquidity for the execution of cash withdrawals. Reservations can be

effected and adjusted using the ICM.

Reserve holdings

Liquidity intraday and overnight maintained on the RTGS account at the end-of-day.

Reserve Management Module (RM)

Module enabling NCBs to perform some functionality for the reserve requirements management e.g. verify the minimum reserves fulfilment or calculate the interest to be paid to credit institutions for minimum reserves.

Reserve requirement

The obligation of euro area credit institutions to hold minimum reserves on reserve accounts with their home NCBs. The reserve requirement is determined in relation to certain elements of the credit institutions' balance sheet. Institutions' holding of required reserves are remunerated at the rate of the Eurosystem's main refinancing operations.

RM Interest and Penalty Account

Account held by an NCB for performing bookings related to the payment of interest on minimum reserves and to the payment of penalties of a CI which has not fulfilled minimum reserve requirements (optional).

Relationship management application (RMA)

See SWIFT relationship management application (RMA)

RTGS account

Account managed within the PM and maintained by a direct participant to settle all transactions submitted to and processed by the PM (except for transactions of the AS settlement procedure 6 which are settled on sub accounts).

-S- *glossary*

Securities settlement system (SSS)

The full set of institutional arrangements for confirmation, clearing, settlement, custody and registration of securities.

Settlement manager

Each central bank has a settlement manager who is responsible for managing, monitoring and communicating with other settlement managers within the Eurosystem.

Single Shared Platform (SSP)

TARGET2 is based on a single technical platform, known as the Single Shared Platform which includes the PAPSS (Payment and Accounting Processing Services Systems) and the CRSS (Customer Related Services Systems).

Standing Facilities Module (SF)

The Standing Facilities (Module) is an optional module and enables to manage the overnight standing facilities (deposit facility, marginal lending facility).

Standing facility

A central bank facility available to counterparties on their own initiative. The Eurosystem offers two overnight standing facilities:

- the marginal lending facility and
- the deposit facility.

Standing order

Instruction of a direct participant to transfer regularly a fixed amount from his home account to an RTGS account (PM) and also from the RTGS (main) account to the sub-accounts (interfaced model) or to a mirror account (integrated model).

Static Data Module (SD)

This module ensures a proper and reliable management of static data by storing all statistic data actually used. It caters for data consistency between all modules of the SSP. Inter alia the Static Data Module is used to generate the TARGET2 directory.

Sub-account

Specific account, belonging to an RTGS account, holding dedicated liquidity to allow the settlement of an ancillary system.

S.W.I.F.T.

Society for Worldwide Interbank Financial Telecommunication

SWIFT Alliance Access (SAA)

SWIFT Alliance Access is a messaging interface that allows the user to connect in-house applications with SWIFTNet FIN (MT) and MX-based SWIFT solutions.

SWIFT Alliance Gateway (SAG)

SWIFT Alliance Gateway is the single window to all SWIFTNet communications. All SWIFTNet message flows can be concentrated through one interface. This includes applications connected via WebSphere MQ, and also those designed for linking to SWIFTNet Link or based on SWIFTAlliance WebStation.

SWIFT-BIC

A bank identifier code of a financial institution connected to the SWIFT network.

SWIFTNet Browse

SWIFT service based on the "https" internet standard protocol, enabling users to browse remote web servers. In SSP the use of the Browse service provides access to the Information and Control Module (ICM) via the Secure IP Network (SIPN) of SWIFT.

SWIFTNet FileAct

File transfer service provided by SWIFT, typically used to exchange batches of structured financial messages and large reports. In the SSP, e.g. the TARGET2 directory is transferred via the Secure IP Network (SIPN) by SWIFT using the FileAct service.

SWIFTNet InterAct

SWIFT interactive messaging service supporting the exchange of messages between two parties. On the SSP the InterAct service is used for the transfer of XML requests via the Secure IP Network (SIPN) by S.W.I.F.T. to the ICM.

SWIFT payment message

An instruction to transfer funds; the exchange of funds (settlement) subsequently takes place over a payment system or through correspondent banking relationships; used for all payments and the related transactions on the SSP.

SWIFT relationship management application (RMA)

Service provided by S.W.I.F.T. to manage the business relationships between financial institutions. RMA operates by managing which message types are permitted to be exchanged between users of a SWIFT service.

-T- *glossary*

TARGET

Trans-European Automated Real-time Gross settlement Express Transfer

TARGET2

TARGET2 is the second generation of TARGET and replaced the former decentralised infrastructure by a single technical platform.

TARGET2 business day

The TARGET2 business equals the calendar day with the exception of the days when the TARGET2 system is not operated.

TARGET2 directory

Directory used by TARGET2 users to find out where a payment has to be addressed by SWIFTNet Y-Copy mode. On a domestic level, it could be used to find the relation between the national sorting codes and the related BICs.

Technical account

Account used in the context of ancillary systems operations as intermediary account for the collection of debits/credits resulting from the settlement of balances or DVP operations. The balance of such an account is always zero because debits (resp. credits) are always followed by credits (resp. debits) of an overall equal amount.

Transaction Reference Number (TRN)

An alphanumeric reference of up to 16 characters assigned by the sender to messages sent over the SWIFT network.

Transfer

Operationally, the sending (or movement) of funds or securities or of a right relating to funds or securities from one party to another party by

- conveyance of physical instruments/money,
- accounting entries on the books of a financial intermediary or
- accounting entries processed through a funds and/or securities transfer system.

The act of transfer affects the legal rights of the transferor, transferee and possibly third parties in relation to the money balance, security or other financial instrument being transferred.

T2SRC

TARGET2 Security Requirements and Controls

-U- *glossary*

User-to-application (U2A)

The objective is to permit direct communication between a participant's users and the ICM. The information is displayed in a browser running on a PC system. Control activities are performed manually by the user.

-V- *glossary*

Virtual account

Method for aggregating data among accounts within a group of accounts that are held on the books of euro area NCBs. Payments made by holders of an account within a virtual account are checked against the global liquidity of the virtual account, which is the sum of the available liquidity of all accounts composing it.

-W- *glossary*

Warehoused Payment

Payments submitted up to five TARGET2 business days in advance. In this case, the payment message will be warehoused until the day trade phase of SSP with the respective date starts.

-X- *glossary*

XML

Acronym for Extensible Markup Language Subset of Standard Generalized Markup Language (SGML - ISO 8879) designed especially for use on the Web and in Web-based applications.

-Y- *glossary*

Y-Copy

Standard type of transmission of SWIFT messages on the SSP which is used in the context of payments processed via PM.