BANCO DE ESPAÑA
Eurosistema

Dirección General de Operaciones, Mercado y Sistemas de Pago
Departamento de Sistemas de Pago

Aplicación Técnica nº 6/2017

TARGET2-Banco de España – Especificaciones técnicas del procesamiento de órdenes de pago para el acceso basado en internet

---

Con motivo de la adopción por parte del Banco Central Europeo de la Orientación BCE/2017/28 de 22 de septiembre, por la que se modifica la Orientación BCE/2012/27 sobre el sistema automatizado transeuropeo de transferencia urgente para la liquidación bruta en tiempo real (TARGET2), es necesario aprobar una nueva aplicación técnica de especificaciones técnicas del procesamiento de órdenes de pago para el acceso basado en internet para recoger los cambios introducidos por ella.

Además de por lo dispuesto en el Título XII de las Cláusulas Generales relativas a las Condiciones Uniformes de Participación en TARGET2-Banco de España, el procesamiento de órdenes de pago utilizando el acceso basado en internet se regirá por las normas siguientes:

1. Requisitos técnicos de la participación en TARGET2-Banco de España por lo que a infraestructura, red y formatos se refiere

1. Todo participante que utilice el acceso basado en internet debe conectarse al ICM de TARGET2 utilizando un cliente local, un sistema operativo y un navegador de internet conforme a lo especificado en el anexo de las especificaciones funcionales detalladas para los usuarios (UDFS) titulado “Internet-based participation - System requirements for Internet access”, con los ajustes en él definidos. La cuenta del módulo de pagos de cada participante se identificará mediante un BIC de ocho u once dígitos. Además, cada participante pasará una serie de pruebas que demuestren su capacidad técnica y operativa antes de poder participar en TARGET2-Banco de España.

2. Para cursar órdenes de pago e intercambiar mensajes de pago en el módulo de pagos se utilizará como remitente/receptor del mensaje la plataforma BIC de TARGET2, TRGTXEPMLVP. Las órdenes de pago cursadas a un participante que utilice el acceso basado en internet deben identificar a este participante receptor en el campo de la institución beneficiaria. Las órdenes de pago cursadas por un participante que utilice el acceso basado en internet identificarán a este participante como la institución ordenante.

3. Los participantes que utilicen el acceso basado en internet utilizarán los servicios de infraestructura de clave pública especificados en el “User Manual: Internet Access for the public-key certification service”.

2. Tipos de mensajes de pago

1. Los participantes que utilicen el acceso basado en internet podrán hacer los siguientes tipos de pagos:

a) pagos de clientes, es decir, transferencias en las que el cliente ordenante y/o beneficiario no son instituciones financieras;

b) pagos de clientes STP (procesamiento automatizado de principio a fin), es decir, transferencias en las que el cliente ordenante y/o beneficiario no son instituciones financieras y que se procesan de modo STP;

c) transferencias interbancarias para solicitar el movimiento de fondos entre instituciones financieras;

d) pagos de cobertura para solicitar el movimiento de fondos entre instituciones financieras relacionado con una transferencia de cliente subyacente.

Además, los participantes que utilicen el acceso a una cuenta del módulo de pagos basado en internet podrán recibir órdenes de adeudo directo.

2. Los participantes respetarán las especificaciones sobre los campos de los mensajes establecidas en el libro 1 del capítulo 9.1.2.2 de las especificaciones funcionales detalladas para los usuarios (UDFS).

3. El contenido de los campos de los mensajes se validará a nivel de TARGET2-Banco de España de acuerdo con los requisitos de las UDFS. Los participantes podrán concertar entre sí reglas específicas sobre el contenido de los campos de los mensajes. Sin embargo, TARGET2-Banco de España no hará comprobaciones específicas sobre si los participantes cumplen esas reglas.

4. Los participantes que utilicen el acceso basado en internet podrán realizar por medio de TARGET2 pagos de cobertura, es decir, pagos efectuados por los bancos corresponsales para liquidar (cubrir) los mensajes de las transferencias que se presenten al banco de un cliente por otro medio más directo. Los datos sobre el cliente contenidos en esos pagos de cobertura no se mostrarán en el ICM.

3. Comprobación contra dobles entradas

1. Toda orden de pago será objeto de una comprobación contra entradas duplicadas, cuyo fin es rechazar las órdenes de pago que se hayan cursado más de una vez por error.

2. Se comprobarán los siguientes campos de los tipos de mensajes:

Detalles	Parte del mensaje	Campo
Emisor	Cabecera básica	Dirección BIC
Tipo de mensaje	Cabecera de aplicación	Tipo de mensaje
Receptor	Cabecera de aplicación	Dirección de destino

Número de referencia de la operación (TRN)	Bloque del texto	:20
Referencia conexa	Bloque del texto	:21
Fecha valor	Bloque del texto	:32
Importe	Bloque del texto	:32

3. Se devolverá una nueva orden de pago si todos los campos descritos en el punto 2 a ella referidos coinciden con los referidos a una orden de pago validada anteriormente.

4. Códigos de error

Si se rechaza una orden de pago, se facilitará por el ICM una notificación de interrupción en la que se indicará el motivo del rechazo por medio de códigos de error. Los códigos de error se establecen en el capítulo 9.4.2 de las UDFS.

5. Momentos de liquidación predeterminados

1. Para órdenes de pago con indicador del momento inicial de adeudo, se utilizará la palabra clave "/FROTIME/".

2. Para órdenes de pago con indicador del momento límite de adeudo, se dispondrá de la opción siguiente:

a) palabra clave "/REJTIME/": la orden de pago se devolverá si no puede liquidarse a más tardar en el momento predeterminado de adeudo.

b) palabra clave "/TILTIME/": la orden de pago no se devolverá, sino que se mantendrá en espera en la cola pertinente, si no puede liquidarse a más tardar en el momento predeterminado de adeudo.

En ambos casos, si una orden de pago con indicador del momento límite de adeudo no se ha liquidado 15 minutos antes del momento predeterminado, se enviará automáticamente una notificación por medio del ICM.

3. Si se utiliza la palabra clave "/CLSTIME/", la orden de pago se tratará igual que la orden de pago a que se refiere la letra b) del punto 2.

6. Liquidación de órdenes de pago disponibles para la liquidación

1. A fin de facilitar una liquidación bruta rápida que ahorre liquidez, las órdenes de pago disponibles para la liquidación se someterán a procedimientos de compensación y, en su caso, procedimientos de compensación ampliados (términos que se definen en los puntos 2 y 3.

2. El procedimiento de compensación determinará si las órdenes de pago del beneficiario situadas al principio de la cola de las órdenes muy urgentes o, en su caso, urgentes, pueden compensarse con la orden de pago del pagador (en adelante, "órdenes de pago compensables"). Si una orden de pago compensable no ofrece fondos suficientes para la orden de pago del pagador respectivo disponible para la liquidación, se determinará si hay suficiente liquidez disponible en la cuenta del módulo de pagos del pagador.

3. Si el procedimiento de compensación da resultado negativo, el Banco de España podrá aplicar un procedimiento de compensación ampliado. El procedimiento de compensación ampliado determina si hay órdenes de pago compensables en cualquiera de las colas de espera del beneficiario, con independencia del momento en que se hayan colocado en espera. Sin embargo, si en la cola de espera del beneficiario hay órdenes de pago de mayor prioridad dirigidas a otros participantes en TARGET2, el principio FIFO sólo podrá contravenirse si la liquidación de la orden de pago compensable supone un incremento de liquidez para el beneficiario.

7. Liquidación de órdenes de pago en espera

1. El tratamiento de las órdenes de pago en espera dependerá de la calificación de prioridad que el participante ordenante les haya asignado.

2. Las órdenes de pago en espera urgentes y muy urgentes se liquidarán aplicando los procedimientos de compensación descritos en el apartado 6, comenzando por la orden de pago situada al principio de la cola en los casos en que haya un incremento de liquidez o una intervención en la cola (cambio de posición en la cola, momento de liquidación o prioridad, o revocación de la orden de pago).

3. Las órdenes de pago en espera normales se liquidarán de forma continua sin perjuicio de todas las órdenes de pago urgentes y muy urgentes que aún no se hayan liquidado. Se utilizan diversos mecanismos de optimización (algoritmos). Si un algoritmo da resultado, las órdenes de pago en él incluidas se liquidarán; si falla, las órdenes se mantendrán en espera. Se aplicarán tres algoritmos (1 a 3) para compensar los flujos de pagos. Conforme al algoritmo 4, se dispondrá del procedimiento de liquidación 5 (definido en el capítulo 2.8.1 de las UDFS) para la liquidación de las instrucciones de pago de los sistemas vinculados. Para optimizar la liquidación de las operaciones muy urgentes de los sistemas vinculados en las subcuentas de los participantes se utilizará un algoritmo especial (el algoritmo 5).

a) Conforme al algoritmo 1 ("todo o nada"), el Banco de España hará lo siguiente, tanto para cada relación respecto de la cual se haya establecido un límite bilateral como para la suma total de las relaciones respecto de las cuales se haya establecido un límite multilateral:

i. calculará la posición de liquidez general de la cuenta del módulo de pagos de cada participante en TARGET2, determinando si el total de las órdenes de pago en espera salientes y entrantes es negativo o positivo, y, si es negativo, comprobará si excede de la liquidez disponible del participante (la posición de liquidez general constituirá la "posición de liquidez total"), y

ii. comprobará si se respetan los límites y reservas establecidos por cada participante en TARGET2 respecto de cada cuenta del módulo de pagos pertinente.

Si el resultado de estos cálculos y comprobaciones es positivo para cada cuenta del módulo de pagos pertinente, el Banco de España y otros BC interesados liquidarán simultáneamente todos los pagos en las cuentas del módulo de pagos de los participantes en TARGET2 correspondientes.

b) Conforme al algoritmo 2 ("parcial"), el Banco de España:

i. calculará y comprobará las posiciones, límites y reservas de liquidez de cada cuenta del módulo de pagos pertinente igual que conforme al algoritmo 1, y

ii. si la posición de liquidez total de una o varias cuentas del módulo de pagos pertinentes es negativa, extraerá órdenes de pago individuales hasta que la posición de liquidez total de cada cuenta del módulo de pagos pertinente sea positiva.

A continuación, y siempre que haya fondos suficientes, el Banco de España y los demás bancos centrales interesados liquidarán simultáneamente todas las órdenes de pago restantes (salvo las extraídas) en las cuentas del módulo de pagos de los participantes en TARGET2 correspondientes.

Al extraer órdenes de pago, el Banco de España comenzará por la cuenta del módulo de pagos del participante en TARGET2 con la mayor posición de liquidez total negativa y por la orden de pago situada al final en la cola de espera de menor prioridad. El proceso de selección se aplicará sólo por un corto espacio de tiempo que el Banco de España fijará discrecionalmente.

c) Conforme al algoritmo 3 ("múltiple"), el Banco de España:

i. comparará parejas de cuentas del módulo de pagos de participantes en TARGET2 para determinar si las órdenes de pago en espera pueden liquidarse respetando tanto la liquidez disponible de las cuentas del módulo de pagos de los dos participantes en TARGET2 como los límites por ellos establecidos (comenzando por la pareja de cuentas del módulo de pagos con la menor diferencia entre las órdenes de pago recíprocas). En este caso el BC o los BC interesados asentarán los pagos simultáneamente en las cuentas del módulo de pagos de los dos participantes en TARGET2;

ii. extraerá órdenes de pago individuales hasta que haya liquidez suficiente si, respecto de una pareja de cuentas del módulo de pagos como la descrita en el inciso i), la liquidez es insuficiente para cubrir la posición bilateral. En este caso el BC o los BC interesados liquidarán simultáneamente las órdenes de pago restantes, salvo las extraídas, en las cuentas del módulo de pagos de los dos participantes en TARGET2.

Tras cumplir lo dispuesto en los incisos i) y ii), el Banco de España comprobará las posiciones de liquidación multilaterales (entre la cuenta del módulo de pagos de un participante y las cuentas del módulo de pagos de otros participantes en TARGET2 respecto de los cuales se haya establecido un

límite multilateral). Para ello aplicará mutatis mutandis el procedimiento que se describe en los incisos i) a ii).

d) Conforme al algoritmo 4 ("liquidación parcial y del sistema vinculado"), el Banco de España aplicará el procedimiento del algoritmo 2, pero sin extraer órdenes de pago respecto de la liquidación de un sistema vinculado (que liquida simultánea y multilateralmente).

e) Conforme al algoritmo 5 ("liquidación del sistema vinculado por medio de subcuentas"), el Banco de España aplicará el procedimiento del algoritmo 1, con la diferencia de que iniciará el algoritmo 5 por medio de la Interfaz para Sistemas Vinculados y sólo comprobará si hay fondos suficientes en las subcuentas de los participantes. Además, no tendrá en cuenta límites ni reservas. El algoritmo 5 se aplicará también durante la liquidación nocturna.

4. Las órdenes de pago disponibles para la liquidación después de iniciarse uno de los algoritmos 1 a 4 podrán no obstante liquidarse inmediatamente si las posiciones y límites de las cuentas del módulo de pagos de los participantes en TARGET2 implicados son compatibles tanto con la liquidación de esas órdenes de pago como con la liquidación de las órdenes de pago incluidas en el procedimiento de optimización en uso. Sin embargo, no se aplicarán simultáneamente dos algoritmos.

5. En la fase de procesamiento diurno los algoritmos se aplicarán sucesivamente. Mientras no esté pendiente la liquidación multilateral simultánea de un sistema vinculado, la secuencia será la siguiente:

a) algoritmo 1,

b) si falla el algoritmo 1, algoritmo 2,

c) si falla el algoritmo 2, algoritmo 3; si da resultado el algoritmo 2, nuevamente algoritmo 1.

Si está pendiente la liquidación multilateral simultánea ("procedimiento 5") respecto de un sistema vinculado, se aplicará el algoritmo 4.

6. Los algoritmos se aplicarán de modo flexible mediante la fijación de un desfase temporal predefinido en su aplicación sucesiva que asegure un intervalo mínimo entre el uso de dos algoritmos. La secuencia temporal se controlará automáticamente, pero será posible la intervención manual.

7. Mientras estén incluidas en un algoritmo en uso, las órdenes de pago no se reordenarán (no cambiarán de posición en la cola) ni revocarán. Las solicitudes de reordenación o revocación de esas órdenes de pago se colocarán en espera hasta que concluya el algoritmo. Si esas órdenes de pago se liquidan mientras el algoritmo está en uso, se rechazarán las solicitudes de reordenación o revocación; si no se liquidan, las solicitudes de los participantes se tendrán en cuenta inmediatamente.

8. Utilización del ICM

1. El ICM podrá utilizarse para introducir órdenes de pago.

2. El ICM podrá utilizarse para obtener información y gestionar la liquidez.

3. Salvo por lo que respecta a las órdenes de pago almacenadas y a los datos estáticos, sólo podrán consultarse por medio del ICM datos relativos al día hábil en curso. Las pantallas estarán exclusivamente en inglés.

4. La información se facilitará en la modalidad "pull" ("a requerimiento"), es decir, cada participante tendrá que solicitar que se le facilite la información. Los participantes comprobarán el ICM periódicamente durante el día hábil por si hubiera mensajes importantes.

5. Para los participantes que utilicen el acceso basado en internet sólo estará disponible la modalidad usuario-aplicación (U2A). La modalidad U2A permite la comunicación directa entre un participante y el ICM. La información se muestra en un navegador basado en un sistema de PC. Pueden consultarse más detalles en el manual del usuario del ICM.

6. Todo participante dispondrá de al menos un lugar de trabajo con acceso a internet para acceder al ICM por el modo U2A.

7. Los derechos de acceso al ICM se concederán mediante certificados, la utilización de los cuales se describe en detalle en los apartados 10 a 13.

8. Los participantes también podrán utilizar el ICM para traspasar liquidez

   a. entre la cuenta del módulo de pagos y las subcuentas del participante.
   b. de la cuenta del módulo de pagos a la cuenta técnica gestionada por un sistema vinculado utilizando el procedimiento de liquidación 6 en tiempo real.

9. Las UDFS, el manual del usuario del ICM y el "User Manual: Internet Access for the Public Key Certification Service"

Pueden consultarse más detalles y ejemplos de las normas que anteceden en las versiones de las UDFS y del manual del usuario del ICM que se publican en la dirección del Banco de España en internet y en la dirección de TARGET2 en internet en inglés, así como en el "User Manual: Internet Access for the Public Key Certification Service".

10. Expedición, suspensión, reactivación, revocación y renovación de los certificados

1. El participante solicitará del Banco de España la expedición de certificados que le den acceso a TARGET2 -Banco de España utilizando el acceso basado en internet.

2. El participante solicitará del Banco de España la suspensión y reactivación de los certificados, así como su revocación y renovación, cuando su titular ya no desee tener acceso a TARGET2 o si el participante cesa su actividad en TARGET2-Banco de España (p. ej. como resultado de una fusión o adquisición).

3. El participante tomará todas las precauciones y medidas organizativas que aseguren que los certificados sólo se utilizan de conformidad con las Condiciones uniformes.

4. El participante notificará sin demora al Banco de España todo cambio sustantivo en cualquiera de los datos contenidos en los formularios presentados al Banco de España en relación con la expedición de los certificados.

5. El participante podrá tener un máximo de cinco certificados activos por cada cuenta del módulo de pagos. Previa solicitud, el Banco de España podrá discrecionalmente solicitar de las autoridades certificadoras la expedición de más certificados.

11. Tratamiento de los certificados por el participante

1. El participante velará por la custodia de todos los certificados y adoptará estrictas medidas organizativas y técnicas para evitar perjuicios a terceros y velar por que cada certificado lo utilice exclusivamente el titular para quien fue expedido.

2. El participante facilitará sin demora toda la información que solicite el Banco de España y garantizará su veracidad. Los participantes responderán plenamente y en todo momento de que se mantenga la exactitud de toda la información facilitada a el Banco de España en relación con la expedición de los certificados.

3. El participante responderá plenamente de garantizar que todos sus titulares de certificados mantengan los certificados que les hayan sido asignados separados de sus códigos secretos PIN y PUK.

4. El participante responderá plenamente de garantizar que todos sus titulares de certificados no utilicen los certificados para funciones o finalidades distintas de aquellas para las que se expidieron.

5. El participante informará inmediatamente al Banco de España de toda solicitud de suspensión, reactivación, revocación o renovación de los certificados, así como de sus motivos.

6. El participante solicitará inmediatamente del Banco de España la suspensión de todo certificado, o de las claves que contenga, que esté defectuoso o ya no esté en poder de su titular.

7. El participante notificará inmediatamente al Banco de España toda pérdida o sustracción de los certificados.

12. Requisitos de seguridad

1. El sistema informático que el participante utilice para acceder a TARGET2 por medio del acceso basado en internet se encontrará en un local del cual el participante sea propietario o arrendatario. El acceso a TARGET2-Banco de España sólo se permitirá desde ese local; es decir, no se permitirá el acceso remoto.

2. El participante utilizará todos los programas informáticos en sistemas informáticos instalados y adaptados con arreglo a las normas internacionales vigentes de seguridad de la tecnología de la información, que comprenderán al menos los requisitos que se detallan en los puntos 3 del apartado 12 y 4 del apartado 13. El participante adoptará medidas apropiadas, como son, en particular, la protección contra virus y malware, las medidas anti-phishing, y los procedimientos de hardening y de gestión de parches. El participante actualizará periódicamente todas estas medidas y procedimientos.

3. El participante establecerá un enlace cifrado de comunicación con TARGET2-Banco de España para el acceso mediante internet.

4. Las cuentas de usuario de los lugares de trabajo del participante no tendrán privilegios administrativos. Los privilegios se asignarán conforme al principio del menor privilegio.

5. Los participantes protegerán en todo momento como se indica a continuación los sistemas informáticos utilizados para acceder mediante internet a TARGET2-Banco de España:

a) Protegerán en todo momento los sistemas informáticos y los lugares de trabajo frente al acceso físico y a la red no autorizado, utilizando un cortafuegos que proteja a los sistemas informáticos y a los lugares de trabajo del tráfico de ingreso de internet, y que proteja a los lugares del trabajo del acceso no autorizado por la red interna. Utilizarán un cortafuegos que proteja del tráfico de ingreso, así como un cortafuegos en los lugares de trabajo que asegure que solo se comunican con el exterior programas autorizados.

b) Los participantes sólo podrán instalar en sus lugares de trabajo los programas informáticos que sean necesarios para acceder a TARGET2 y estén autorizados conforme a las normas internas de seguridad del participante.

c) Los participantes velarán en todo momento por que todas las aplicaciones informáticas que se utilicen en los lugares de trabajo se actualicen y parcheen con la última versión periódicamente. Esto se aplica en particular al sistema operativo, al navegador de internet, y a los complementos.

d) Los participantes restringirán en todo momento el tráfico de salida de los lugares de trabajo a los sitios críticos para el negocio, así como a los sitios requeridos para actualizaciones informáticas legítimas y razonables.

e) Los participantes velarán por que todos los flujos críticos internos hacia los lugares de trabajo o desde ellos estén protegidos contra su divulgación y su alteración intencionada, sobre todo si los ficheros se transfieren por medio de una red.

6. El participante velará por que sus titulares de certificados sigan en todo momento prácticas de navegación seguras, como son:

a) reservar ciertos lugares de trabajo para acceder a sitios del mismo nivel crítico, y acceder a esos sitios sólo desde esos lugares de trabajo;

b) siempre reiniciar la sesión de navegación antes y después de acceder a TARGET2-Banco de España por internet;

c) verificar la autenticidad de todo certificado SSL del servidor en cada conexión al acceso a TARGET2-Banco de España por internet;

d) sospechar de correos electrónicos que parezcan proceder de TARGET2-Banco de España, y nunca facilitar la contraseña del certificado si se solicita, pues TARGET2-Banco de España jamás pedirá la contraseña de un certificado ni por correo electrónico ni por otra vía.

7. El participante mantendrá en todo momento los siguientes principios de gestión a fin de mitigar los riesgos para su sistema:

a) establecer prácticas de gestión de usuarios que garanticen que solo usuarios autorizados se crean y mantienen en el sistema, y llevar una lista precisa y actualizada de los usuarios autorizados;

b) conciliar el tráfico de pago diario para detectar desajustes entre el tráfico de pago diario autorizado y el efectivo, tanto enviado como recibido;

c) velar por que un titular de certificado no navegue simultáneamente por otro sitio de internet al mismo tiempo que accede a TARGET2-Banco de España.

13. Otros requisitos de seguridad

1. El participante velará en todo momento, por medios organizativos o técnicos apropiados, porque las identidades de los usuarios reveladas con el fin de controlar los derechos de acceso (revisión de los derechos de acceso) no se utilicen indebidamente, y, en particular, porque no se conozcan por personas no autorizadas.

2. El participante dispondrá de un proceso de administración de usuarios que garantice la supresión inmediata y permanente de la identidad del usuario pertinente en caso de que un empleado u otro usuario de un sistema del local de un participante deje el organismo del participante.

3. El participante dispondrá de un proceso de administración de usuarios y bloqueará inmediata y permanentemente las identidades de usuarios que estén en situación comprometida, como en los casos de certificados perdidos o sustraídos o de contraseñas objeto de phishing.

4. Si por tres veces un participante no es capaz de eliminar un fallo relacionado con la seguridad o un error de configuración (p. ej. causado por sistemas infectados por malware), los BC proveedores de la plataforma compartida única podrán bloquear permanentemente todas las identidades de usuarios del participante.

14. Norma derogatoria

La Aplicación Técnica 8/2010, queda derogada con efectos a partir del 13 de noviembre de 2017.
Toda referencia a la Aplicación Técnica 8/2010, en cualesquiera instrumentos jurídicos u otros documentos se entenderá efectuada a la Aplicación Técnica 6/2017.

15. Entrada en vigor

Esta Aplicación Técnica entrará en vigor el 13 de noviembre de 2017. Para cualquier consulta, pueden dirigirse a la dirección de correo electrónico target2@bde.es o a los teléfonos 91 338 5582 ó 91 338 7044

Juan Ayuso Huertas

Director General de Operaciones,
Mercados y Sistemas de Pago