Information Guide for TARGET2 users

Version 11.0

November 2017

infoguide

Table of Contents

INFORMATION GUIDE FOR TARGET2 USERS

Table of Contents

Table of Contents

Table of Contents

Table of Contents

List of diagrams, tables and boxes

Diagrams

Tables

List of diagrams, tables and boxes

Boxes

1. Introduction

This "*Information guide for TARGET2 users*" (hereafter "Infoguide") aims at providing **TARGET2 users** (credit institutions, ancillary systems and other entities settling in TARGET2[1]) with a standard set of information, in order to give them a better understanding of the overall functioning of TARGET2 and to enable them to make use of it as efficiently as possible. It is intended to cover all operational matters related with the daily use of TARGET2, including the ones concerning the euro cash settlement in TARGET2-Securities (T2S), aiming at ensuring smooth operations.

In addition, the Infoguide gives users a clear understanding of which features are common and which are specific to each Central Bank (CB), i.e. the euro area National Central Banks (NCB), the European Central Bank (ECB) and other NCBs connected to TARGET2. Documentation on CB specific features can be found on the respective websites.

The Infoguide has been drafted specifically with a view to being updated when necessary and as a document to which CBs, the 3CB/4CB[2] and TARGET2 users can contribute. It is intended to serve as a dynamic tool, incorporating updates that may emerge from the national TARGET2 user groups (NUGs), meetings organised for TARGET2 users at the euro area level by the European System of Central Banks (ESCB), operational experience or system releases.

The Infoguide may also be of relevance for other TARGET2 stakeholders and the public and, thus, is available via the TARGET2 website (www.target2.eu).

The content of this document confers 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. 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 TARGET2 and TARGET2-Securities, the TARGET2 governance and technical structure, the organisational structure at central bank level, the communication with the users, the opening days and operational day schedule, the TARGET2 transactions and the settlement of ancillary systems.

1 Additional information may be found in Chapter 3. Participation.

2 The 3CB, the technical providers of the Single Shared Platform (SSP), comprises Banca d'Italia, Banque de France and Deutsche Bundesbank. The 4CB, the technical providers of the T2S Platform comprises Banca d'Italia, Banque de France, Deutsche Bundesbank and Banco de España.

The part on "Participation" in Chapter 3 describes the access criteria, the connection and registration process, in particular as regards the static data collection, the certification testing, the measures to ensure security and operational reliability, the termination or suspension of participants and the billing.

In Chapter 4, the procedures in the different phases of a normal business day are described. Chapter 5, Chapter 6, Chapter 7 and Chapter 8 describe the procedures to be followed in abnormal events . These parts (Chapters 4 to 8) are described in the chronological order of an operational 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, and finishing with the end-of-day procedures.

Chapter 9 describes the testing requirements for contingency arrangements and business continuity. Chapter 10 deals with the change management for the yearly releases as well as for the emergency changes and the so-called hot fixes. Chapter 11 describes the TARGET2 compensation scheme.

Finally, the Annexes provide a detailed description of a TARGET2 inter-regional failover with loss of data (Annex I), an incident report form (Annex II) and the self-certification statement for use by critical participants (Annex III), the template to be used for Change Requests (Annex IV), and a glossary, including abbreviations (Annex V).

Note that all references to times in this document are to the local time at the seat of the ECB, i.e. Central European Time (CET).

1.2. Further relevant documentation

Legal documentation (available on the ECB's website)

- Guideline on TARGET2 (and subsequent amending guidelines)

The Guideline on TARGET2 (ECB/2012/27) is the legal framework for TARGET2, with which the Infoguide must be fully compliant. It includes in its remit the T2S euro denominated dedicated cash accounts, while other T2S related aspects are covered within the T2S Guideline (ECB/2012/13).

The Guideline on TARGET2 addressees Central Banks and is based on the principle of maximum harmonisation despite being enforced in a decentralised manner by each Central Bank. Under its annexes Governance, Harmonised conditions for TARGET2 participants and Intraday Credit/ Auto-collateralisation facilities are covered.

- Harmonised Conditions

Each Central Bank adopts arrangements implementing the Harmonised Conditions for participation in

TARGET2[3] that are laid down in the Guideline on TARGET2. These arrangements shall exclusively govern the relationship between the relevant Central Bank and its TARGET2 users.

The Harmonised Conditions address TARGET2 users and include a description of TARGET2, access criteria, participants' acceptance, management of accounts and processing of payment orders, rights and obligations of the parties, finality and liability. In addition, they also encompass appendices related with the technical specifications for the processing of payments, terms of reference for the country/capacity opinions, fee schedule, operational hours, contingency requirements, arrangements for liquidity pooling, compensation scheme, among others.

Operational documentation (available on the TARGET2 website)

- User guide for collection of static data and Registration Guide for DCA holders

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

- User information guide to the TARGET2 pricing

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

- Settlement times of ancillary systems

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

Specifications (available on the TARGET2 website)

- TARGET2 General Functional Specifications (GFS) and TARGET2 User Detailed Functional Specifications (UDFS)

These documents provide the technical details on the functioning of the Single Shared Platform (SSP).

- ICM User 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 TARGET2. The service is provided by Banca d'Italia on behalf of the Eurosystem.

[3] Harmonised Conditions for the Opening and Operation of a PM (Payment Module) account in TARGET2, as laid down in Annex II; Supplemental and Modified Harmonised Condition for the Opening and Operation of a PM account in TARGET2 using Internet-Based Access, as laid down in Annex V; and the Harmonised Conditions for the Opening and Operation of a Dedicated Cash Account in TARGET2, as laid down in Annex IIa.

- SWIFT documentation

The SWIFT documentation provides details of the different SWIFT standards and it is available at the SWIFT website.

- T2S scope defining set of documents

Of particular relevance are the T2S User Detailed Functional Specifications (UDFS), the T2S User Handbook (UHB) and User Requirement Definitions (URD), available on the T2S website.

In addition to the documents mentioned so far, the CBs provide further information on specific national characteristics and procedures.

2. Fundamentals

2.1. 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 money market.

TARGET2 is technically based on a Single Shared Platform (SSP)[4], offering the same level of service to all users. It has been designed and built to meet the highest standards of robustness and operational reliability and is able to process equally smoothly domestic and cross-border payments denominated in euro. TARGET2 processes only transfers denominated in euro. The aim is to allow payments – especially large-value payments such as those relating to foreign exchange, securities and money market transactions – to be made in euro 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.[5] There is no minimum amount set for a payment made through TARGET2.

In addition, TARGET2 encompasses the **euro denominated Dedicated Cash Accounts (DCAs),** which are technically hosted in the T2S Platform (see additional information below).

2.2. What is TARGET2-Securities

A major infrastructure and interdependency aspect for TARGET2 is TARGET2-Securities (T2S). T2S services are provided by the Eurosystem based on the T2S platform, which has been built and is operated by the 4CB: Deutsche Bundesbank, the Banque de France, the Banca d'Italia and Banco de España.

T2S provides harmonised and commoditized securities settlement to Central Securities Depositories (CSDs) at national level and across national borders. With T2S, a single set of rules, standards and tariffs is applied to all CSDs that use the T2S platform for the settlement of their securities

4 SSP refers to the technical platform via which the TARGET2 related services are provided. TARGET2-Securities (T2S) related services are provided via the T2S Platform.

5 With some exceptions like for example warehoused payments and payments to a suspended participant.

transactions across all markets in which T2S operates. Also the cash leg is settled in central bank money and follows a single set of rules and standards.

T2S integrates in a single technological platform both the market participants' securities accounts, held with either one or multiple CSDs, and Dedicated Cash Accounts (DCAs), held with the respective central banks.

T2S is designed as a multi-currency system. The euro has been the first currency in which securities are settled on the T2S platform. Thus, T2S and TARGET2 are closely inter-related in view of euro liquidity management. The interconnection between TARGET2 and T2S is based on an application-to-application approach and is ensured by the T2S Interface (T2SI).

Note that this Infoguide only addressees transactions and accounts expressed in euro.

Important aspects deriving from T2S:

- Despite being technically hosted by the T2S platform, legally, the euro denominated DCAs (hereafter, referred to just as DCAs) fall under the legal perimeter of TARGET2. This means that legal issues associated with DCAs are included in the TARGET2 Guideline and that the operational procedures applying to DCAs are reflected in the Infoguide.
- SSP and the T2S platform are liquidity-wise interconnected via the so called 'transit accounts', which allow the exchange of liquidity between PM accounts and DCAs and vice versa.
- Any entity that holds at least one PM account and/or one DCA with a Central Bank is a participant in TARGET2.
- The DCA holder, or the main PM account holder acting on its behalf, shall access the DCA via: *(i)* a direct connection to the T2S platform, through a licensed value-added network service provider (VA-NSP) for T2S (directly connected DCA holders); or/and *(ii)* an indirect connection, through the TARGET2 value-added services (VAS) for T2S (indirectly connected DCA holders).
- Subject to the fulfilment of the relevant eligibility criteria, an entity may open a DCA in euro, from the first T2S migration wave onwards, with any Central Bank. This rule applies irrespective of the wave in which the national CSD migrates to T2S. The eligibility criteria for the opening of a DCA are similar to those applicable to the opening of a PM account, as reflected in the TARGET2 Guideline.

- Each DCA has to be linked to one PM account, so-called "Main PM account"[6]. However, several DCAs can be linked to the same (main) PM account. The main PM account can be opened within the books of the same Central Bank as the DCA or not.
- The DCA holder and the main PM account holder may be different entities (i.e., a DCA holder does not need to hold a PM account, even though the DCA has to be linked to a PM account). The contractual arrangement between the DCA holder and the PM account holder are their own responsibility.
- The main PM account holder is responsible for the fees for the T2S services provided to the linked DCAs as well as for the penalty fee in case of collateral relocation.
- DCAs cannot have a negative balance at any point (except for the Central Bank's DCA). In addition, at the end of day, each DCA's balance has to be zero. This is ensured by the automated cash sweep, via which, after the inbound liquidity transfers cut-off (at 17:45), any liquidity remaining in the DCA is automatically transferred to the main PM account. Notwithstanding, DCA holders are recommended to transfer liquidity, which is not required for securities settlement anymore, from DCAs to PM accounts at earlier points in time. In the very unlikely event that due to a technical malfunction, liquidity held in the DCAs cannot be returned to the PM accounts, T2S closes the end-of-day period with liquidity remaining in the DCAs overnight [conditional until the implementation of the T2S CR 562 (scheduled for 9 June 2018) allowing for such a possibility]. On the next business day the T2S DCAs will start with the end-of-day balance of the previous business day.
- DCA holders may benefit from auto-collateralisation, i.e., intraday credit granted by the Central Bank, triggered when the liquidity on the DCA is insufficient to settle securities transactions, whereby such intraday credit is collateralised either with the securities being purchased (collateral on flow), or with securities held by the DCA holder and earmarked for auto-collateralisation (collateral on stock).
- To benefit from Central Bank auto-collateralisation, the DCA holder has to hold a PM account with access to intraday credit within the books of the same central bank as the DCA.
- DCA holders may provide credit to their clients (e.g., securities accounts holders) automatically collateralised by T2S via the client auto-collateralisation functionality. Client auto-collateralisation will be triggered if the client lacks external guarantee headroom to settle a settlement instruction and it might use either the securities being purchased by the client (collateral on flow) or securities held by it and earmarked for auto-collateralisation (collateral

6 External RTGS account linked to the DCA under the GUI screen "*Static Data > Dedicated Cash Account*".

on stock). If a DCA holder provides client auto-collateralisation, it must set-up the list of securities accepted as collateral (list of eligible securities), as well as the respective valuation (i.e., the prices that T2S can use for the valuation of securities positions). Further information is provided in Box 2 under section 4.1.

- Central Banks are solely responsible for the business relationship with their users and should address all incidents, enquiries or problems raised by them. However, for connectivity problems, a DCA holder with a direct connection to T2S may contact the T2S Service Desk directly, and vice versa, as reflected in section 2.4.
- T2S is not an ancillary system and does not have a system status (since T2S comes within the legal perimeter of TARGET2, finality is addressed in the TARGET2 Guideline). Therefore, but also in view of the close interlinks to TARGET2, T2S relevant provisions are differentiated from ancillary system relevant provisions in the Infoguide.

2.2.1. Central banks' roles in view of T2S

The Eurosystem distinguishes four roles for Central Banks in view of T2S[7], namely:

- Role I. **System entity** or **bank of banks**, in particular implying the business relationship with banks for cash related issues and the opening of DCAs;
- Role II. **TARGET2 System owner,** status of the Market Infrastructure Board (MIB), together with the roles of central banks as TARGET2 participating central banks. In terms of Governance, the Governing Council, also known as Level 1 (L1), has the final competence in relation to TARGET2 and the Eurosystem Central Banks, known as Level 2 (L2) and represented by the MIB, collectively have the subsidiary competence in relation to issues that have been delegated by L1.
- Role III. **Collateral manager,** meaning handling the collateralisation of Eurosystem monetary policy operations, intraday credit and auto-collateralisation facilities;
- Role IV. **Settlement Agent,** mainly in terms of settling its own operations, as a CSD participant.

Roles I to II are of particular relevance for the Infoguide and are addressed within this document (see red frames in figure 1). Role III and IV are not covered.

7 The identified roles may show partial overlaps. The role of central banks as operator of a Securities Settlement System/Central Securities Depository (i.e. BE and GR) is not taken into account.

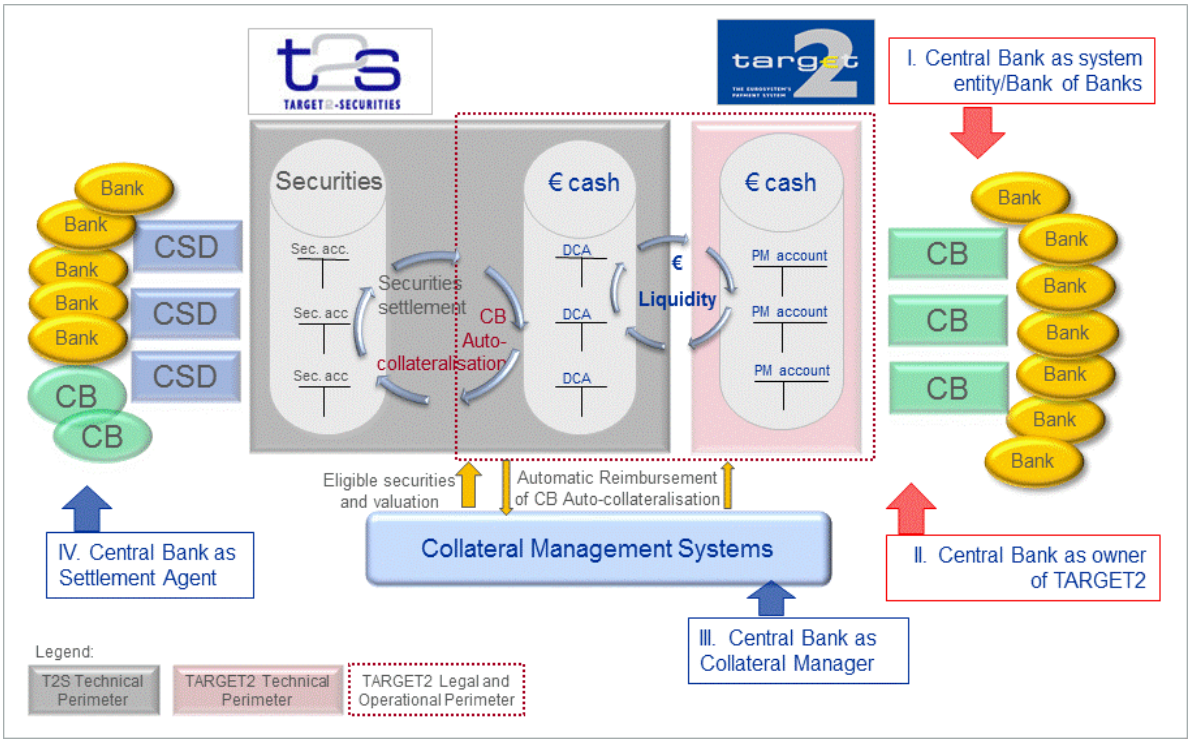

Diagram 1. Four roles for central banks in view of T2S

2.2.2. **Bank's roles in view of T2S**

A bank may have the following roles in view of T2S:

- As DCA holder, i.e. as holder of one or more DCAs;
- As CSD participant, i.e. as holder of securities accounts in one or more CSDs;
- As liquidity provider, i.e. as an entity that allows the settlement of securities transactions of its clients (CSD participants) on its DCA or as an entity that provides liquidity form its PM account to a DCA of a different entity;
- As credit provider, i.e. as an entity that provides intraday credit, via client auto-collateralisation, to its clients (CSD participants).

2.3. TARGET2 structure

2.3.1. **Governance structure**

The management of TARGET2 is based on a three-level governance scheme. The tasks are assigned to the Governing Council of the ECB (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 Market Infrastructure Board (MIB) assists the Governing Council as an advisory body in all matters relating to TARGET2. . In addition to its advisory role, the MIB 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 Technical and operational management body	Level 3 SSP providing central banks
- 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

2.3.2. **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 (CRSS core reporting functions and CRISP);

- the T2S Interface (T2SI) which connects the SSP with the T2S Platform. The system-to-system connection between both is based on the internal 4CB network and uses the same XML message standard as required by the T2S specifications.
- the central banks, with a proprietary home account (PHA), reserve management and intraday credit;
- the credit institutions and other entities (than ancillary systems) settling in TARGET2, connected to the SSP via SWIFT or internet, and/or to the T2S Platform via the licensed Value-added Network service providers (VAN-SP);
- the ancillary systems, connected to the SSP via SWIFT.

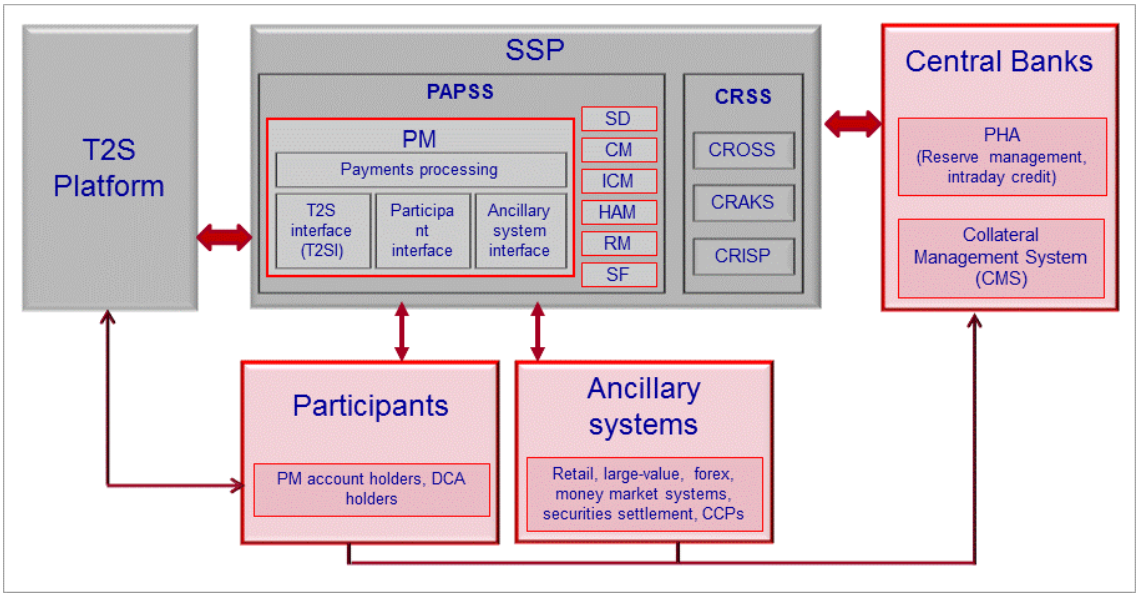

Diagram 2. TARGET2 structure

2.3.3. **Organisational structure at central bank level**

Each CB has a **national service desk** acting as contact point for the respective TARGET2 users. Within the TARGET2 framework, the national service desks are represented by the **settlement managers**, who are responsible for the daily management of operations. All settlement managers are interlinked by means of a pre-set teleconference facility, known as "TARGET2 Settlement Manager Forum". The TARGET2 settlement managers' teleconference comprises the CB's settlement managers, the SSP service managers and the TARGET2 coordinator.

Each Central Bank has also a **crisis manager,** who is informed via the respective settlement manager and involved in the case of problem escalation. The crisis managers are also interlinked via a pre-set teleconference facility. The TARGET2 crisis managers' teleconference comprises the CB's crisis managers, the SSP crisis managers and the ECB crisis manager.

Each Central Bank's Settlement Manager and Crisis Manager will also participate in the respective T2S teleconferences.

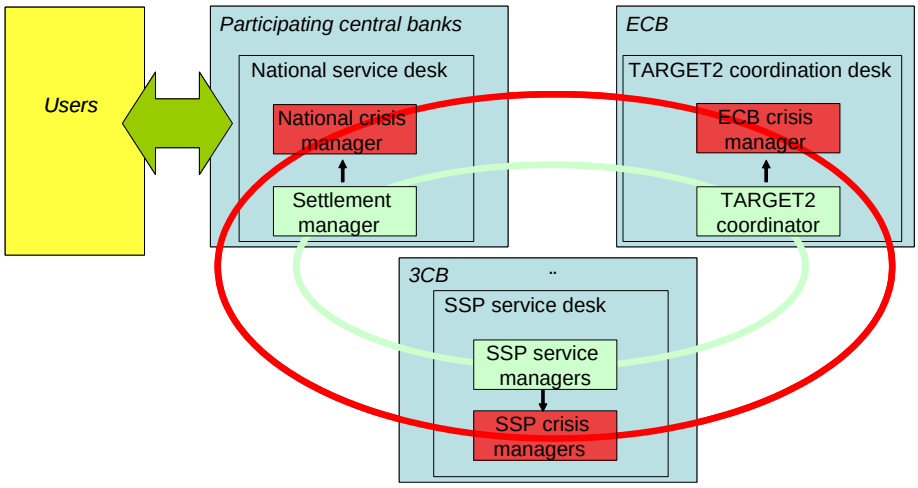

Diagram 3. Overview of TARGET2 actors

2.4. Communication with the users

The contact point for TARGET2 users is the national service desk. However:

(i) for connectivity problems, a DCA holder directly connected to T2S may contact the T2S Service Desk directly. The T2S Service Desk will open a ticket and inform the respective Central Bank. In case of doubt whether it is a connectivity problem or not, the directly connected DCA holder should contact the national service desk. Contacts with the T2S service Desk related with other issues than connectivity should be diverted to the national service desks, and vice versa. The contact details of the T2S Service Desk will be provided to the directly connected DCA holders by the respective Central Bank;

(ii) the T2S Service Desk can also contact directly connected DCA holders directly regarding connectivity issues. The T2S Service Desk will inform the national service desk upon doing this. The contact details of the person/team responsible for issues related to T2S connectivity at each DCA holder that is directly connected will be collected by the respective Central Bank. In case a DCA holder prefers not to be contacted directly by the T2S Service Desk, then the Central Bank's national service desk will be contacted instead (and its contact details will be collected instead).

2.4.1. Communication tools

The following communication tools might be used between the respective Central Bank and its users:

Information and control module (ICM)

The Information and Control Module (ICM) gives PM account holders and ancillary systems 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 (excluding DCA holders). In addition, a ticker at the top of the screen 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 a SWIFTNet connectivity problems or SSP failure.

T2S GUI

The T2S GUI gives directly connected DCA holders access to a wide range of general information (e.g., on account balances or transactions) to monitor and manage their business (e.g. limit management). It also allows the national service desks to broadcast messages to their DCA holders.

Local tools

Local tools refer to national communication means. 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*.

TARGET2 Information System

The TARGET2 information system (T2IS)[8] refers to the information about the operational status of TARGET2 which is made available via the ECB Market Information Dissemination (MID) system[9], to the users of that system (e.g., news agencies), and to the general public via the ECB's website,. Such information refers to normal operations (start of day/close of day) as well as to abnormal situations. In the latter case, information provided includes the type of failure, its impact and the measures envisaged to solve the problem.

T2S Information System

The T2S Information System (T2S-IS) refers to the information about the operational status of the T2S Services which is made available via the ECB MID system[10], to the users of that system (e.g., news agencies), and to the general public via the ECB's website. Such information refers to normal operations (start of day/close of day) as well as to abnormal situations. In the latter case, information provided includes the type of failure, its impact and the measures envisaged to solve the problem.

8 In the same vein as for TARGET2 a T2S-info system is set-up

9 Additional information about the ECB MID is available at the ECB website.

10 Additional information about the ECB MID is available at the ECB website.

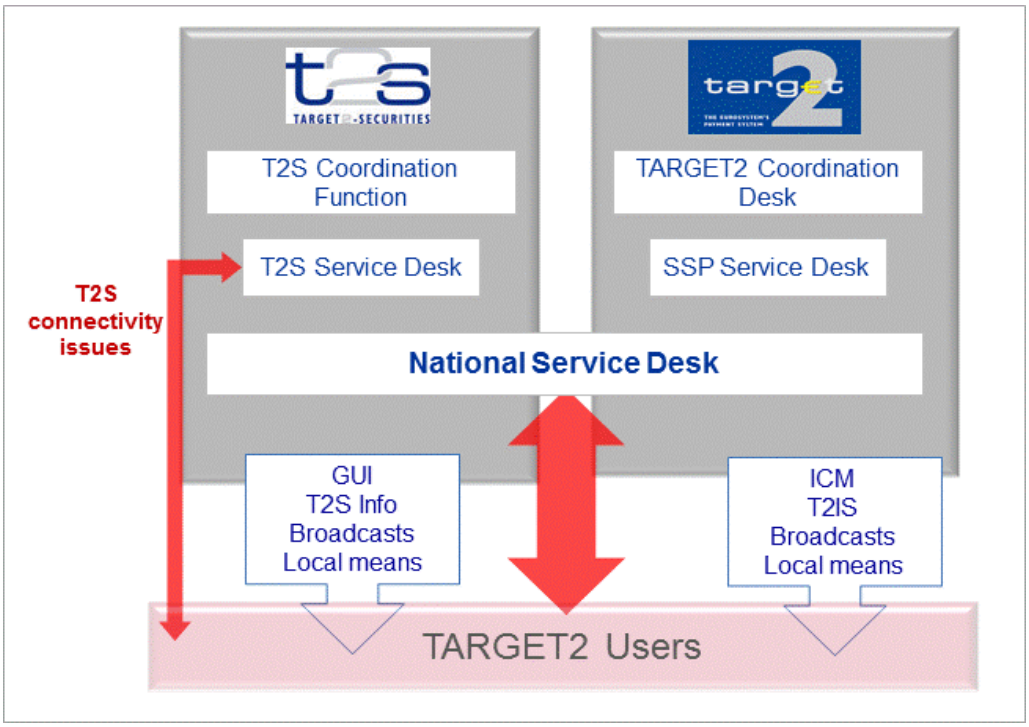

Diagram 4. Information flows

2.5. Opening days

TARGET2 opening days are the de facto settlement days for the financial markets in euro, as well as for foreign exchange transactions involving the euro.

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. The same calendar applies for euro cash settlement in T2S.

Therefore, even if on the first of May, Good Friday and Easter Monday, T2S is available, there is no settlement in euro, i.e., only Free-of-payment transactions are possible. This means that, on these dates, there is a time lag between the moment when standing liquidity transfer orders from PM account to DCAs are processed in the SSP (at 19:30, on the evening before 1st May and Easter period, for the next TARGET2 business day which is day after the 1st of May or Easter period) and on the T2S Platform (at 20:00, on the evening of the 1st of May and Easter period, when T2S opens the business day that is the same value date as of TARGET2). In other words the standing liquidity transfers will not wait for T2S settlement for 30 minutes but for at least 24 hours and 30 min.

Closing days	Saturday	Sunday	New Year's Day	Good Friday	Easter Monday	1st May	Christmas Day	26th December
TARGET2	Closed							
T2S	Closed			Closed for euro settlement (only FoP is possible)			Closed	

Diagram 5. TARGET2 and T2S Closing Days

2.6. Operational day schedule

The table below shows the different phases of the TARGET2 and T2S operational day schedule.

SSP schedule		T2S schedule (applicable to DCAs)	
Time	**Description**	**Time**	**Description**
18:45 – 19:00(1)	Start of day processing (2)	18:45 – 20:00	Start of day: - Change of business date - Deadline for acceptance of CMS data feeds (19:00) - Preparation of the night time settlement
19:00 – 19:30(1)	Night-time settlement: provision of liquidity from SF to HAM and PM; from HAM and PHA to PM.	20:00 – 03:00	Night-time settlement: - First Night-time settlement cycle - Last Night-time settlement cycle (Sequence X includes the partial settlement of unsettled Settlement Instructions eligible for partial settlement and that have failed to settle due to a lack of securities; Sequence Y includes the reimbursement of multiple liquidity providers at the end of cycle)
19:30(1) – 22:00	Night-time settlement (NTS1): - Start-of-procedure message; - Setting aside of liquidity on the basis of standing orders for the night-time processing (ancillary system settlement procedure 6 and T2S)		
22:00 – 01:00	Technical maintenance window(3)	03:00 – 05:00	Technical maintenance window(4)
01:00 – 06:45	Night-time processing (ancillary system settlement procedure 6 and T2S)	05:00 – 18:00	Day trade/Real-time settlement(5): - Real-time settlement preparation(5) - Partial settlement windows at 14:00 and 15:45[11] (for 15 minutes **- 16:00:** DvP cut-off /Cut-off for auto-collateralisation reimbursement by Payment banks **- 16:30:** Automatic auto-collateralisation reimbursement, followed by the optional cash sweep **- 17:40**: Cut-off for Bilaterally agreed treasury management operations (BATM) and central bank operations (CBO) cut-off **- 17:45**: inbound liquidity transfer cut-off Automatic cash sweep after 17:45 **- 18:00:** FOP cut-off
06:45 – 07:00	Business window to prepare daylight operations		
07:00 – 18:00	Day trade phase: **- 17:00**: Cut-off for customer payments **- 17:45**: cut-off for liquidity transfers to DCAs **- 18:00:** Cut-off for interbank payments and incoming liquidity transfers from DCAs		
18:00 –	**- 18:15** (1)**:** Cut-off for the use of standing facilities	18:00 –	- End of T2S settlement processing - Recycling and purging

11 Each partial settlement window last for 15 minutes. The partial settlement applies to unsettled Settlement Instructions eligible for partial settlement and that have failed to settle due to a lack of securities.

18:45	**- 18:30**[1]**:** Central bank accounting End-of-day processing	18:45	- End of day reporting and statements

Table 2. Operational day schedule

(1) Plus 15 minutes on the last day of the reserve maintenance period.

(2) In the Guideline on TARGET2, the start-of-day processing phase is shown until 19:30 (i.e., also covering the subsequent provision of liquidity) as from a business perspective the provision of liquidity (19:00-19:30) is considered to be preparation for payment processing in the strict sense.

(3) Over a weekend or on a holiday, the TARGET2 technical window will last throughout the weekend or the holiday, i.e., from 22:00 on Friday until 1:00 on Monday or, in the case of a holiday, from 22:00 on the last business day until 1:00 on the next business day.

(4) Over a weekend or on a holiday, the T2S technical window will last throughout the weekend or the holiday, i.e., from 03:00 a.m. on Saturday until 05:00 a.m. on Monday or, in the case of a holiday, from 03:00 a.m. on the holiday until 05:00 a.m. on the next business day.

(5) Real-time settlement preparation and real-time settlement may start before the maintenance window if the last night-time settlement cycle ends before 03:00 am.

2.7. TARGET2 transactions

As described in section 3.1 below, PM accounts are only opened for certain eligible participants who must also have successfully completed a series of certification testing activities prior to opening an account (see chapter 3). As long as there are no good reasons for terminating or suspending a TARGET2 participant's participation (see section 3.6), PM accounts are not excluded from settling transactions. Hence, in the interests of a smooth operation of TARGET2, every participant is expected to accept payments from the PM accounts of other participants. A participant is not entitled to "block" the receipt of other participants' payments, neither from a specific PM account nor from all PM accounts.

The following types of transactions are settled in TARGET2:

***(i)* Customer payments**

Customer payments are settled in the PM accounts and are defined as payments in the SWIFT FIN MT103 format (standard or STP). Customer payments can be processed via TARGET2 between 7:00 and 17:00.

***(ii)* Interbank payments**

Interbank payments are settled in the PM accounts and are defined as payment messages in the SWIFTNet FIN MT202 and MT202COV format. This type of message is sent by or on behalf of the

ordering institution to the financial institution of the beneficiary institution, either directly or through a correspondent.

Interbank payments processed via MT202 are payments such as the cash leg of money market, foreign exchange and derivatives transactions, which take place between credit institutions or between central banks and credit institutions. MT202COV are interbank payments that "cover" underlying customer payments and contain fields for the originator and beneficiary of the credit transaction. Interbank payments can be processed via TARGET2 between 7:00 and 18:00.

***(iii)* Direct debits**

Direct debits are settled in the PM accounts and are defined as payment messages in the SWIFTNet FIN MT204 format. Direct debits in TARGET2 are interbank transactions intended for wholesale purposes only. The respective PM account holders have to agree with the parties allowing the debiting of their accounts on the terms and conditions for using this service. The PM account holder authorises another PM account holder to issue a direct debit order and informs its central bank, which is responsible for recording and administrating the pre-agreements. Direct debits can be processed via TARGET2 between 7:00 and 18:00. PM account holders using internet-based access are not able to issue direct debits orders (but may receive them).

***(iv)* Ancillary system transactions**

Payments related to the settlement of ancillary systems: retail payment systems, large value payment systems, foreign exchange systems, money market systems, clearing houses, and securities settlement systems.

***(v)* Liquidity transfers**

Liquidity holdings in central bank money can be held in PM accounts, home accounts or DCAs, with the possibility to transfer liquidity between the different accounts.

Liquidity transfers involving PM accounts (but not DCAs) can be processed via SWIFTNet FIN MT 202, from 7:00 until 18:00, or via ICM (in U2A or A2A mode), based on SWIFTNet InterAct. Liquidity transfers initiated via ICM are executed immediately after transmission during the operating hours of the PM and 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 window used for SSP maintenance.[12]

Information about liquidity transfers from PM accounts to DCAs and vice-versa, as well as about liquidity transfers between DCAs (belonging to the same payment bank or linked to the same main

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

PM account) is available in section 2.8.

(v) **Cash leg of securities transactions,** settled on DCAs, namely:

- Delivery versus Payment (DVP) and Receive versus Payment (RVP) transactions, which define an exchange of securities for cash;

- Delivery with Payment (DWP) transactions, which defines the delivery of securities from one party to another, together with a cash payment;

- Payment Free of Delivery (PFOD) transactions, which define an exchange of cash without the delivery of securities;

- Settlement restrictions, which enable the blocking and reservation of cash in a DCA.

It should be noted that T2S also processes Free of Payment (FOP) transactions, through which securities may be delivered (Delivery Free of Payment - DFOP) or received (Receive Free of Payment - RFOP) without payment. However, by definition, this kind of transactions does not require cash movements and, therefore, is not settled based on DCAs.

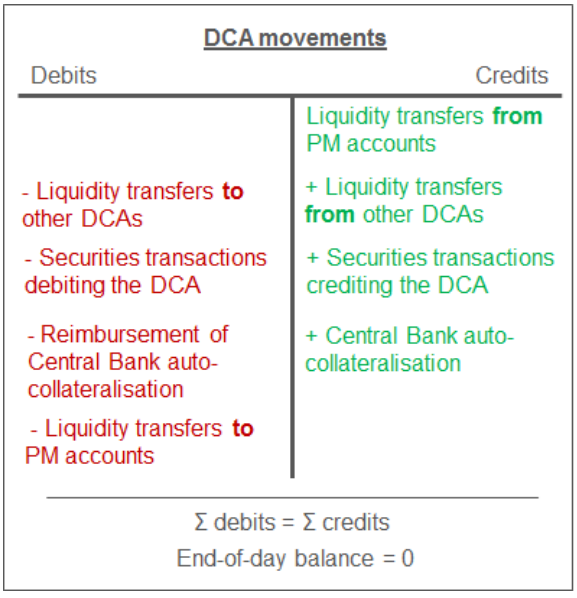

Diagram 6. DCAs movements

2.8. Liquidity flows between PM accounts and DCAs and between DCAs

It is possible to transfer liquidity from PM accounts to DCAs as well as from DCAs to PM accounts. In addition, it is also possible to transfer liquidity between DCAs when the involved DCAs are linked to the same RTGS account or belong to the same DCA holder.

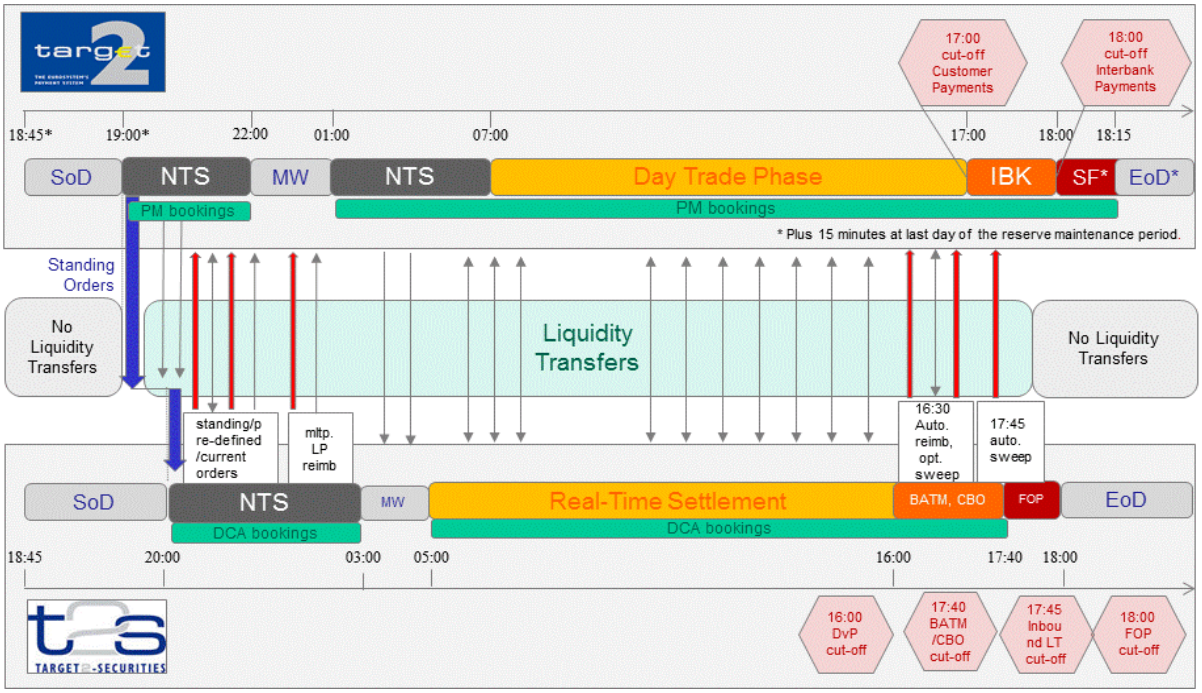

Diagram 7. Liquidity flows between PM accounts and DCAs

Liquidity transfers between DCAs are possible if the DCAs are linked to the same RTGS account or belong to the same DCA holder. These liquidity transfers can be settled in T2S from night-time settlement cycle 1 - sequence 0 onwards (see section 4.4). In case of contingency, it is also possible to execute liquidity transfers between DCAs owned by a Payment Bank and its central bank's cash account. Partial settlement in case of insufficient liquidity on the DCA is only possible if the liquidity transfer is initiated by a third party authorised by the DCA holder.

As regards **liquidity transfers from PM accounts to DCAs,** a distinction can be made between:

(i) **Standing order** initiated by a PM account holder

In the SSP, the stored amount of a standing order is used continuously until the next change. The orders can be inserted until 18:00 at the latest (effective from the forthcoming night-time settlement). They are executed in the SSP immediately after the start-of-procedure message has been automatically released (night-time settlement only) and, in the T2S Platform during the sequence zero of the first night time settlement cycle. In case of lack of liquidity on the PM account, there will be a pro rata execution of all standing orders executed at that time (i.e. together with the ASI standing orders), as described under section 4.3 (Concordance of orders).

(ii) **Current order** initiated by a PM account holder

The order can be entered in push (via the TARGET2 core services) or in pull mode, if the PM participant uses the TARGET2 value added services for T2S. The current orders initiated by a

PM account holder are rejected if liquidity is insufficient (no partial settlement).

Current orders received by T2S platform can be settled from night-time settlement cycle 1, sequence 0 onwards. They are executed immediately, if the night time settlement has started and received between two sequences. If they are received during the processing of a sequence, they are stored for settlement during the next sequence.

(iii) **Current order** by a third party (T2S Actor in TARGET2)[13] acting on behalf of the PM account holder

The deposition of a current order by a third party acting on behalf of the PM account holder is based on internal rules. These orders are executed immediately once sent and once the T2S night-time settlement has started. A partial execution occurs if liquidity is insufficient; the remaining part will not be settled.

Concerning the **liquidity transfers from DCAs to PM accounts**, it is possible to distinguish:

(i) **Immediate liquidity transfer** initiated in the T2S platform

Immediate liquidity transfers initiated in the T2S Platform are executed immediately during the night time settlement from cycle 1, sequence 1 onwards. If they are received during the processing of a sequence, they are stored. Partial settlement in case of insufficient liquidity on the DCA is only possible if the liquidity transfer is initiated by a third party authorised by the DCA Holder. Immediate liquidity transfers initiated by the DCA holder itself are not submitted to partial settlement and are rejected if liquidity is insufficient.

(ii) **Predefined liquidity transfer order** initiated in the T2S Platform

A predefined liquidity order is executed only once and can be triggered by an event or time. It is possible to enter more than one predefined order for different times or events. The order can be generated for a special amount or for all cash of the DCA. In case of insufficient liquidity, predefined liquidity transfer orders are executed partially; there is no further settlement for the part that could not be settled on first attempt.

(iii) **Standing liquidity transfer order** initiated in the T2S Platform

In T2S a standing order can be defined in the static data. It is executed on a repetitive basis until

13 The access as T2S Actor in TARGET2 is a special type of access to TARGET2, via the T2SI and in application-to-application mode only, via which at third party (for example, a CSD) might initiate current liquidity transfers orders to T2S on behalf of a PM account holder.

it is deleted. The order can be triggered by a special event or time. The order can be generated for a special amount or for all cash of the DCA. Different orders are possible during the business day for different times or events. A partial execution occurs in the event of insufficient liquidity.

Type of liquidity transfer		Partial execution	Recurrence	Execution time
From PM accounts to DCAs	Standing order	Yes	Each business day	Start of the business day
	Current order	No	Once	When triggered
	Current order initiated by a third party (T2S actor in TARGET2)	Yes	Once	When triggered
From DCAs to PM accounts	Immediate liquidity transfer	Yes	Once	When triggered
	Predefined liquidity transfer order	Yes	Once	Per defined time/event
	Standing liquidity transfer order	Yes	Each business day	Per defined time/event
Between DCAs	Internal and immediate liquidity transfer	Only if initiated by a third party.	Once	When triggered

Table 3. Liquidity transfers overview

Box 1. Euro transit accounts

There will be two euro transit accounts for settling and monitoring all liquidity transfers between the SSP and the T2S platform, i.e. between the PM accounts and the DCAs. The liquidity flows including transit accounts are depicted in the following diagrams below:

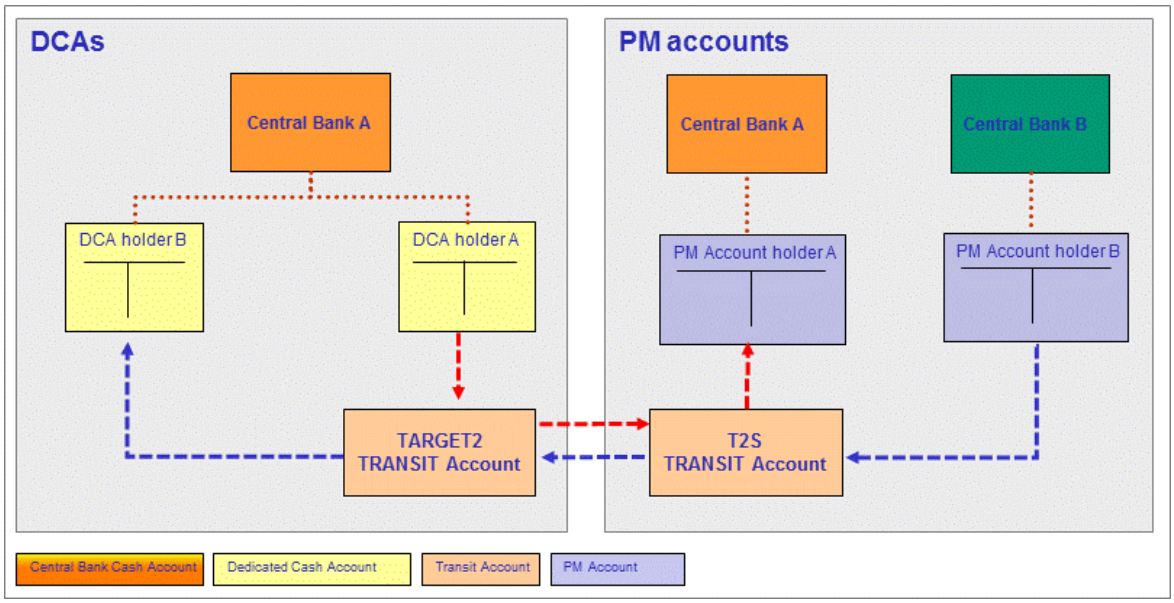

Diagram 8. Euro Transit accounts

As shown above, there is a TARGET2 transit account on the T2S platform, which reflects all movements impacting DCAs, and one T2S transit account on the SSP, which reflects all movements impacting PM accounts. The two transit accounts have mirror balances and the total credits and total debits net-off to zero. At the end of the day, the balances on both accounts are normally reduced to zero (the total debit positions equal the total credit positions). To ensure this, any pending auto-collateralisation will be automatically reimbursed at 16:30 and any remaining balances on DCAs are "swept" to their corresponding main PM accounts via the automated cash sweep, which takes place after the cut-off for inbound liquidity transfers, at 17:45. In case of an abnormal situation balances may remain on DCAs overnight.

2.8.1. Initiation of liquidity transfers

DCA Holders directly connected to T2S can initiate liquidity transfers in T2S, in A2A mode, via ISO20022 messages, or in U2A mode, via the T2S GUI.

DCA Holders indirectly connected to T2S that use the TARGET2 value added services for T2S[14], which enables them to pull liquidity from the DCA in T2S to the PM account using the ICM, MT202 messages or a Liquidity Credit Transfer message without the Business Application Header (BAH), as well as to see the balances on the respective DCAs.

Liquidity transfers from DCAs (triggered directly in T2S or via the TARGET2 VAS for T2S) are processed in the SSP at any time excluding the end-of-day and start-of-day processing (shortly after 18:00 to 19:30) and the technical maintenance window (22:00 to 01:00). As the balance on DCAs has to be zero at the end of business day, all liquidity transfers to PM accounts must be processed before the run of the last algorithm (shortly after 18:00). This is ensured through the T2S automated sweep, by 17:45.

Liquidity transfers from PM accounts to DCAs have to be triggered in the SSP and are executed by the start of the new business day, from 19.30 (interrupted by the maintenance window from 22:00 to 01:00) and till the cut-off for liquidity transfers to T2S (17:45). Any PM account holder with SWIFT-based access may send liquidity transfers to DCAs.

The following table provides an overview about the possibilities h**ow liquidity can be moved between PM accounts and DCAs and within DCAs**, either in U2A mode (via the ICM or the T2S GUI) or in A2A mode:

Liquidity Transfer Type		User-to-Application			Application -to-Application		
		TARGET2 core services (ICM)	**TARGET2 VAS (ICM), includes core services**	**T2S (GUI)**	**TARGET2 core services**	**TARGET2 VAS, includes core services**	**T2S**
From PM accounts to DCAs	Standing order	✔	✔	-	✔	✔	-
	Current order	✔	✔	-	✔ [15]	✔ [16]	-
	Current order initiated by a third party (T2S actor in TARGET2)	-	-	-	✔ [17]	✔ [18]	-
From	Immediate liquidity	-	-	✔	-	-	✔

14 Additional information may be found in the UDFS, Book I.

15 Possible via XML message.

16 Possible via XML message or MT202.

17 Possible via XML message.

18 Possible via XML message or MT202.

DCAs to PM accounts	transfer						
	Predefined liquidity transfer order	-	-	✔	-	-	✔
	Standing liquidity transfer order	-	-	✔	-	-	✔
	Current order	-	✔	-	-	✔ [19]	-
Between DCAs	Immediate liquidity transfer	-	-	✔	-	-	✔

Table 3. Liquidity transfers between DCAs and PM accounts

2.9. Message flows

In TARGET2 there are two general types of message: SWIFT FIN messages (in particular customer and interbank payments as well as direct debits) and XML messages (InterAct and FileAct).

SWIFT FIN messages

The payments module (PM) of the SSP uses the SWIFTNet FIN Y-Copy[20] 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).

SWIFT FIN messages can be submitted up to five TARGET2 business days in advance. In this case, the payment message will be warehoused until the relevant day trade phase of the SSP is reached.

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 3.2. "Internet-based access").

19 Possible via XML message or MT202.

20 In the HAM, V-shape is used.

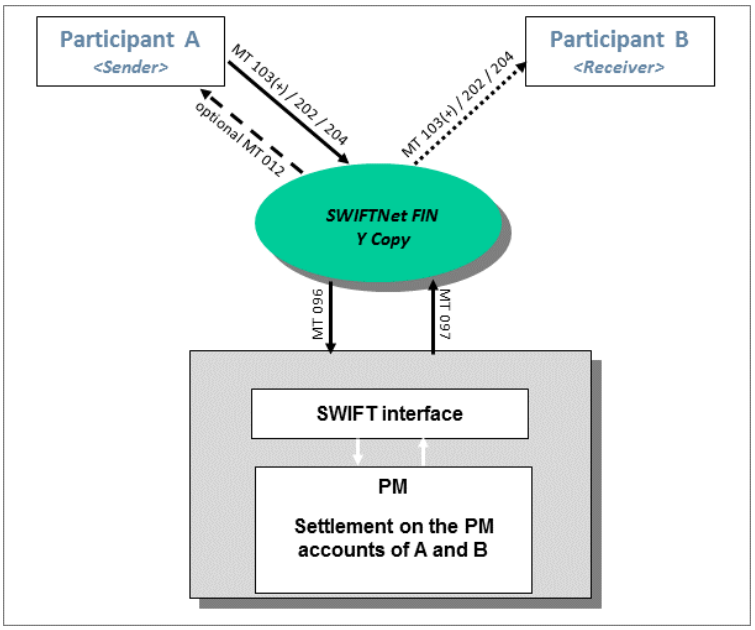

Diagram 9. Y-copy transaction flows

The TARGET 2 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.

XML messages

If a user connects to the ICM in application-to-application mode (A2A), SWIFTNet InterAct and SWIFTNet FileAct are used. The various information and control options are set up as XML messages[21]. SWIFTNet Browse allows the initiation of InterAct or FileAct exchanges via a secure browser link.

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 during the SSP maintenance period; the end-of-day and start-of-day processing and during the provisioning of liquidity.

SWIFTNet InterAct allows the transfer of XML requests via the Secure IP Network (SIPN) by SWIFT to the ICM and the ancillary system interface (ASI). XML messages are used for requests and

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

responses related to the ICM (A2A mode) and for ancillary system business. Concerning ancillary system business, the messages are accepted as explained in TARGET2 UDFS Book I. 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.

The system-to-system connection between TARGET2 and T2S also uses XML messages, which are compliant with the ISO 20022 standard, as required by T2S specifications. XML messages used by the TARGET2 users in the context of the TARGET2 core and value-added services for T2S are also based on the same standard but the Business Application Header is not required. DCA holders directly connected to T2S also need to use the ISO 20022 message standard, as required by T2S specifications.

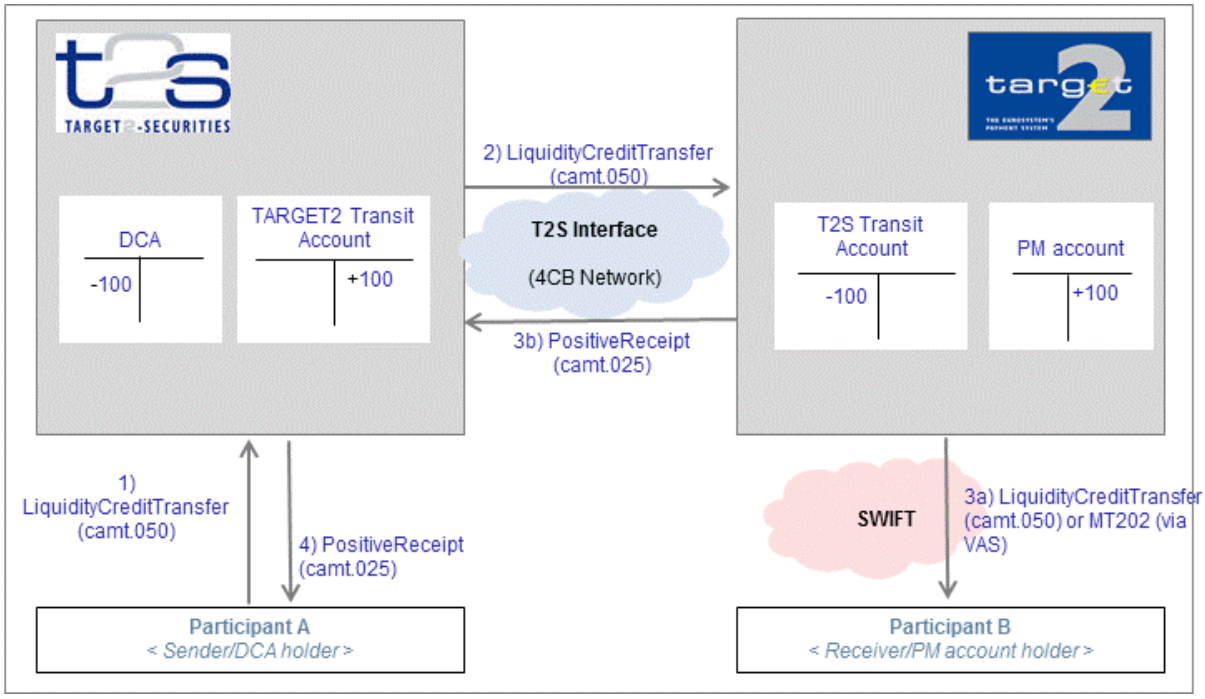

Diagram 10. Liquidity transfer from T2S to TARGET2 (ISO 20022 message flows)

2.10. Settlement of ancillary systems[22]

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

22 For further information, see the UDFS, Section 2.8 (Settlement of ancillary systems).

includes a number of specific features specially designed to facilitate AS settlement, such as 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 PM account holder and open a PM account. Thus, it could be using the ASI for its settlement activities and the PM 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[23]	Description
Procedure 1 Liquidity transfer	Transfer between the cash positions of a participant in the ancillary system and in the PM through a mirror account. Settlement occurs in the ancillary system itself.
Procedure 2 Real-time settlement	Transfer between the accounts of two PM account holders, aimed at finalising a transaction already able to settle in the ancillary system.
Procedure 3 Bilateral settlement	An ancillary system sends simultaneously debits and credits to the PM. The two transactions (the debit and the credit leg) are processed independently of each other.
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	PM account holders dedicate liquidity for the settlement of ancillary system transactions, either on specific sub-accounts or on the mirror account. Settlement occurs either on the sub-accounts or in the ancillary system itself. This settlement procedure can be used especially for night-time business, but also in daylight.

Table 4. Settlement procedures

[23] Integrated model: the final settlement of the cash leg takes place in the securities settlement system itself.
Interfaced model: the final settlement of the cash leg takes place in the PM.

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.

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 BIC holders"[24] 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;

c) NCBs of EU Member States and the ECB.

The relevant Central Bank may, at its discretion, also admit the following entities as direct participants:

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

b) EU Member States' public sector bodies authorised to hold accounts for customers;

c) investment firms established in the EEA;

d) entities managing ancillary systems and acting in that capacity;

e) credit institutions or any of the entities of the types listed under subparagraphs (a) to (d), in both cases where these are established in a country with which the European Union has entered into a monetary agreement allowing access by any of such entities to payment systems in the European Union 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

[24] The BIC (Business Identifier Code) "is the mostly used international identifier of financial institutions. […] SWIFT in its role of ISO registration authority issues BICs to financial and non-financial institutions connected to the SWIFT network as well as to non-connected institutions. The BIC is used in financial transactions, client and counterparty data bases, compliance documents and many others. The ISO 9362 standard defines the BIC structure." (cf. SWIFT website)

Union legislation.

Direct participants are entities that hold at least one PM account in the Payments Module of the SSP (PM account holders) and/or a DCA in the T2S Platform (DCA holders). The PM account holders may access the SSP via SWIFT (SWIFT-based PM account holder) or via Internet (internet-based PM account holder). For the internet-based access, special rules apply, as described in section "3.2 Internet-based access".

The DCA holder, or the main PM account holder acting on its behalf, shall access the DCA via: *(i)* a direct connection to the T2S platform, through a licensed value-added network service provider (VA-NSP) licensed for T2S (directly connected DCA holders); or/and *(ii)* an indirect connection, through the TARGET2 value-added services (VAS) for T2S (indirectly connected DCA holders).

Direct participants are able to*:*

(i) submit/receive payments directly to/from the SSP/T2S Platform;

(ii) settle directly with their central bank;

(iii) open special purpose PM accounts for non-payment activity (e.g., for the maintenance of reserve requirements). These special purpose accounts are identified by a separate BIC11.

In addition, PM account holders are responsible for all payments sent from or received on their accounts by any entity registered through them in TARGET2: indirect participants, multi-addressee access entities and addressable BIC holders, as described below.

Under the terms of the TARGET2 contract with the respective Central Bank, participants are deemed to be aware of, and comply with, all obligations on them relating to legislation on data protection, prevention of money laundering and the financing of terrorism, proliferation-sensitive nuclear activities and the development of nuclear weapons delivery systems. For further information on these responsibilities, participants should refer to the contract signed with the respective Central Bank.

3.1.2. **Indirect participation**

Credit institutions established in the EEA can enter into a contract with (only) one PM account holder , in order to submit payment orders and/or receive payments, and to settle them via the PM account of that entity. Central Banks recognise indirect participants by registering them in the TARGET2 directory.

Where a PM account holder which is a credit institution and an indirect participant belong to the same group, the PM account holder may expressly authorise the indirect participant to use the 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**

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

More precisely, multi-addressee access may be provided as follows:

(a) a credit institution which has been admitted as a PM account holder 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 PM account holder, the other branches of the same legal entity and/or its head office, in both cases provided that they are established in the EEA, may 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. However, the payments are booked on the account of its PM account holder.

3.1.4. **Addressable BIC holders**

TARGET2 addressable BIC holders are not subject to any system rules. Any PM account holder'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 BIC holders, meaning that it is up to the PM account holder to define a marketing strategy for offering such status. It is the responsibility of the PM account holder to forward the relevant information to the respective central bank for inclusion in the TARGET2 directory.

Payment orders to/from addressable BIC holders are always sent and received via a PM account holder. Their payments are settled in the account of the PM account holder in the PM of the SSP.

	Account	Way to submit	Settlement of Payments	Subject to the system	Listed in TARGET2

			/receive payments		rules	directory
Direct participation	**PM account holder**	PM account	Directly	Own account in the PM	Yes	Yes
	DCA holder	DCA account	Directly	Own account in the T2S Platform	Yes	No
Multi- addressee access		No account	Directly	Account of the direct participant	Yes	Yes
Indirect participation		No account	Via direct participant	Account of the direct participant	Yes	Yes
Addressable BIC holder		No account	Via direct participant	Account of the direct participant	No	Yes

Table 5. TARGET2 participation structure

3.1.5. **Group of accounts**

Different categories of entities can receive the "group of accounts" status:

Category 1: credit institutions that consolidate according to the International Accounting Standards (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[25] without requiring a connection to the SWIFT network. Accordingly, participants with internet access do not send and receive messages 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 a PM account via the ICM, including online information on inward and outward (final and pending) transactions and on ancillary system settlement and liquidity positions.
- Initiating credit transfers via specific ICM screens, including MT103/MT103STP, MT202/MT202COV and liquidity transfers to both SWIFT-based and internet-based participants.
- Displaying inward credit transfers from both SWIFT-based and internet-based participants, including MT103/MT103STP, MT202/MT202COV 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.

It should be noted that:

- Internet-based PM account holders can access the ICM in user to Application (U2A) mode only.
- It is not possible to include an internet-based PM account in a group of accounts arrangement or multi-addressee access arrangement, or to have addressable BICs linked to it.
- The TARGET2 value-added services for T2S are not available for an Internet-based PM account holder.
- An Internet-based PM account holder cannot be designated as the Main PM account holder for a DCA.

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

- 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. Connection and registration process

3.3.1. Connection to the SSP

In order to connect to the SSP, PM account holders have to register with SWIFT, in the case of SWIFT-based PM account holders, or with an Accredited Certification Authority, for internet-based PM account holders.

For the Internet-based PM account holders, the 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.

As regards SWIFT-based PM account holders, the SWIFT registration allows them to get the appropriate SWIFT services for TARGET2. It is 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 only becomes effective on one day per month. For the e-ordering process, CBs first validate and approve all registration requests and the SSP service desk makes the second approval. The full process, including validations and implementation by SWIFT can take two to five weeks. In order to ensure the consistency of static data between SWIFT and the SSP, the PM account holder 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 PM account holder uses "myswift.com", a SWIFT customer relationship management website, the change should be made in coordination with the central bank. The CB has to be informed, before the implementation date. Further information on SWIFT registration is available at www.swift.com.

In addition to the registration with SWIFT, SWIFT-based PM account holders need to have an RMA authorisation in place with TRGTXEPM, HAM account holders with TRGTXEHM, the HAM co-manager with TRGTXEPM and TRGTXEHM, and central bank customers with TRGTXECB. This step is compulsory for all PM and HAM account holders as well as for central bank customers.

3.3.2. Connection to the T2S Platform

In order to directly connect to the T2S platform DCA holders (**directly connected DCA holders**) need to choose one[26] of the value added network service providers (VA-NSP) licensed for T2S and

[26] Directly connected DCA holders may use both of the network service providers, for instance, for business continuity reasons.

subscribe to the T2S Connectivity Services via the VA-NSP website. This request will, first, be assessed and approved by the Central bank and, after, by the T2S Service desk. The DCA holder will be informed via e-mail of any change in the status of the request. If the request is rejected, the rejection cause is provided. If it is accepted, a final confirmation is provided once the implementation date is defined. On the implementation date, the VA-NSP will perform the service provisioning activities according to the request form, after which a final confirmation is sent to the DCA holder.

It should be noted that in case a DCA holder is also customer of a CSD or of another Central Bank this step must be performed only once. Upon request, the T2S Service Desk can confirm to a Central Bank if the DCA holder is already registered to the T2S Connectivity Services or not.

In addition to the T2S Connectivity Services, the DCA holder should also request from the VA-NSP the issuance of digital certificates to be used for authentication and signing purposes. These certificates may be provided on USB tokens, for the U2A access of end-users, or on the Hardware Security Module (HSM), for the A2A access of applications.

Further information is available in the VA-NSP documentation and on the T2S Connectivity Licences and Licence Agreement and T2S Connectivity Guide.

As regards **indirectly connected DCA holders**, registration with a VA-NSP is not needed. It is just necessary that the main PM account holder subscribes to the TARGET2 value-added services for T2S, via the SSP registration forms (see section below).

3.3.3. Static data collection

All users must provide static data to the Central Bank via the SSP forms, for the users connecting to the SSP, or via the DCA forms, for the DCA holders. Users can deliver their forms (paper-based) to their national service desk by the means agreed with the respective Central Bank.

Central Banks key in the information from the forms via the ICM, for the users connected to the SSP[27], or via the T2S GUI, for the DCA holders[28].

From a procedural point of view, there are four steps to be followed:

- **Analysis**

The user 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.

[27] Additional information and a detailed description of the forms can be found in the "User guide for collection of static data".

[28] A detailed description of the forms can be found in the DCA registration Guide.

The processing of changes to the static data is mainly driven by the user. The user defines its requirements; often in contact with SWIFT and/or the VA-NSP 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. Users may start with a business description of their future organisation/change. The time required for the analysis depends on the user's organisation.

The user submits to its Central Bank the registration forms and, where applicable:

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

- **Assessment and validation**

In the event of significant changes, the above-mentioned analysis should involve the Central Bank. At the legal and technical levels, the Central Bank checks the forms according to its local rules. Additionally, the Central Bank checks if the SWIFT/VAN-SP 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 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[29] and successfully performed. A 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 and/or T2S GUI. 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 relevant user should check the validity of the new static data entry/modification, using the ICM or

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

T2S GUI.

3.3.3.1. Conflicting registration of addressable BIC holders and indirect participants

The TARGET2 directory allows only one registration per BIC[30] and only a single relationship between an addressable BIC holder/indirect participant and the PM account holder 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 PM account holder before they send a registration form to their Central Bank for the registration of addressable BIC holders.

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

The PM account holder B which is currently the relationship of Bank X, who 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 PM account holder A.

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

In the event that the addressable BIC holder/indirect participant is not in the TARGET2 directory at the time when the PM account holder makes the check, but during the same week another PM account holder requests the registration of the same BIC as an addressable BIC holder/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 PM account holder representing the correspondent.

3.3.3.2. 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 PM account holder during the SSP registration. The TARGET2 directory is the

[30] BIC with eleven digits.

database of BICs used for the routing of payment orders.

Unless otherwise requested by the PM account holder, BICs shall be published in the TARGET2 directory.[31]

The content of the TARGET2 directory is based on the SSP static data, as collected from PM account holders on designated forms. The forms will be used by PM account holders to request the opening of their account(s) and to collect all other information required by the system. In particular, the PM account holder is responsible for the registration of its indirect participants, multi-addressee access entities or addressable BIC holders 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, 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 PM account), institution name, city heading and national sorting code (if available). The following is an example of an entry for a PM account holder in the TARGET2 directory:

Field in the TARGET2 Directory	Example
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 6. TARGET2 directory

The TARGET2 directory is distributed[32] only to PM account holders. Distribution takes place via SWIFTNet FileAct (pull mode only for the full directory; pull mode and push mode for updates). Downloading the full content might mainly be envisaged for the initial loading of the directory or

[31] BICs that are unpublished in the TARGET2 directory are still published in SWIFT's BIC directory.
[32] Internet-based participants can consult the TARGET2 directory online.

where there is a need to rebuild it. Owing to the size of the file, the use of compression is strongly recommended. Furthermore, PM account holders might download the TARGET2 directory at a central point and distribute it internally. PM account holders 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 PM account holders 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.

3.3.3.3. External RTGS accounts list in the T2S Platform

T2S platform will maintain a list of external RTGS accounts, which is required to validate the beneficiary account when processing outbound liquidity transfers (from a DCA to a PM account). If a PM account mentioned as beneficiary is not included in the list of external RTGS accounts, the liquidity transfer will be rejected. It should be noted that the account number included in this list are visible to DCA holders that are directly connected to T2S (however, neither the BIC nor the name of the account holding institution are visible – unless it can be derived as part of the RTGS account number)[33].

In this context, all PM accounts that can possibly receive liquidity transfers from a DCA should be included in the T2S list of external RTGS accounts, i.e., all PM accounts will be included in the list, with the exception of mirror/technical accounts, PM accounts of participants with Internet access and unpublished accounts (unpublished BICs)[34.]

Each Central Bank is responsible for the update of the T2S list of external RTGS accounts whenever a PM account is created, amended or deleted in the SSP (with the exception of a mirror/technical account, Internet-based participant account or an unpublished account).

33 Each DCA holder can just see the RTGS accounts within the data scope of its Central Bank.

34 Unpublished PM accounts and PM accounts of participants with Internet access may be included in the list by the Central Bank, upon request of the participant.

3.3.3.4. Information flows between Central Banks, DCA holders and CSDs

The creation and closure of a DCA is performed by the responsible Central Bank, based on the static data forms received from the DCA holder. Once the DCA is opened the DCA holder may contact its CSD(s) in order to complete the set up and perform the link of the DCA to the securities account(s).

In case a DCA holder intends to close a DCA, it should inform its CB and CSD. Subsequently, it should request its CSD(s) to remove the link(s) between the DCA and the securities account(s) and, once all the link(s) have been removed, it can request the Central Bank to close the DCA. Upon closure, it will not be possible to use the DCA for securities settlements or liquidity transfers anymore.

Therefore, no formal communication is envisaged between the Central Banks and CSDs as regards the registration of DCA holders. It is the DCA holder's responsibility to request the respective CSD(s) to create or remove the link(s) of the DCA to the securities account(s) when requesting the opening or closure of a certain DCA.

In special situations such as the insolvency of a DCA holder, where a Central Bank may decide to suspend a DCA, the Central Bank will inform the CSD(s) via a GUI broadcast.

3.3.3.5. Directly connected DCA holders access rights management

Access rights management in T2S is decentralized and follows the three-level T2S hierarchical party model (see diagram below). According to this hierarchical party model, the T2S operator (4CB) is the party on the top level of the hierarchy. Central Banks and CSDs are on the second level and its participants (DCA holders and CSD participants, respectively) are in the third level.

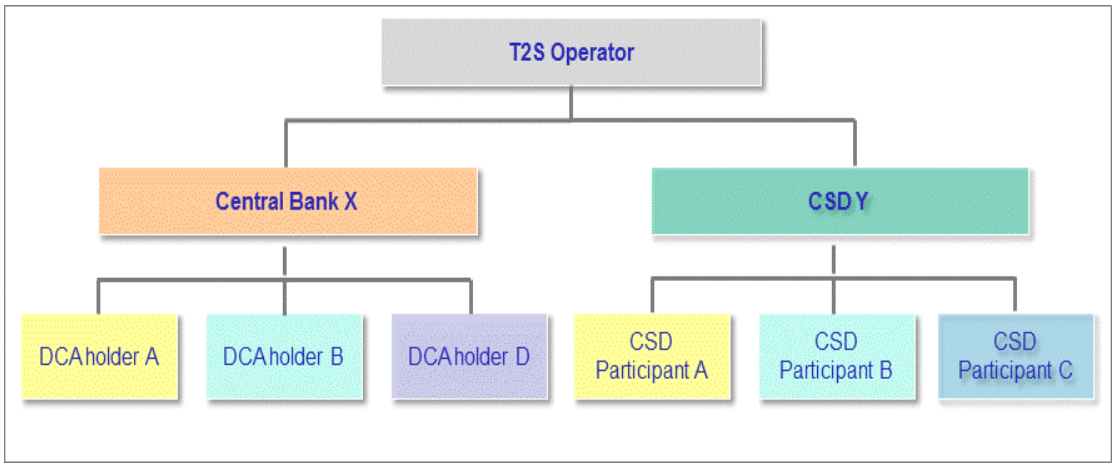

Diagram 11. T2S hierarchical party model

On this basis, via the access rights management, the T2S Operator defines the different T2S functionalities that Central Banks and CSDs are able to use and each Central Bank/CSD defines the different T2S functionalities that their participants are able to use. The data scope (in terms of static

and transactional data) of each entity/party is determined by the hierarchical party model.

Furthermore, access rights management is based on the concepts of privileges and roles as well as the concept of party administrators. A privilege is the capability of triggering a certain T2S function (for example, to perform a given query). Privileges can be grouped into roles. The access rights profile of a given user is determined by the set of roles and privileges granted to it.

Each entity/party must have at least one party administrator, i.e. a user that may grant any roles and privileges previously granted to its entity. A privilege becomes available to a party administrator after this privilege has been granted to this party. From this moment on, the party administrator can grant this privilege. I.e., after the configuration of access rights at party level has been set up for a given party, its party administrator(s) can perform the configuration of access rights at user level, in order to assign the appropriate roles and privileges to all the party users[35].

Roles and privileges are granted in a decentralized way, by each entity party administrators, according with the T2S hierarchical party model, meaning that:

(i) the administrator of a Central Bank: a) creates new roles, including the available privileges; b) manages and assigns the available roles and privileges to its users; c) creates the administrators of its DCA holders; e) assigns the available roles and privileges to its DCA holders;

(ii) the administrator of a DCA holder: a) manages the users of its institution; b) assigns the available roles and privileges to these users.

Note:

- The user's login name and Unique system user reference should be defined according with the following structure: C (to indicate that it is a payment bank user) + Country code of the parent Central Bank (2 characters) + BIC11 of the party + Free text, determined by the DCA holder and up to 21 characters.
- The privileges and roles to be granted to the DCA holders are described in the Registration Guide for DCA Holders, available in the TARGET2 website.

3.4. Certification testing

Each TARGET2 user must undergo a number of certification testing activities depending on the SSP

[35] As described in the Registration Guide for DCA holders, the DCA holders' administrators created by the Central Banks can be made subject to the two-eyes or four-eyes principle. In the case of the four-eyes principle, as a specific procedure needs to be applied, DCA holders shall contact the respective Central Bank.

modules chosen by the respective central bank and the SSP and/or T2S Platform functionalities chosen by the 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 and operational certification:

- Technical certification of PM account holders and ancillary systems consist of the successful individual completion of a number of connectivity and interoperability test cases. Operational certification is assessed based on the participation in country and business day testing;
- Technical certification of directly connected DCA holders consists of the successful individual completion of a number of connectivity, certification and authorisation test cases. Operational certification is assessed based on the participation in community and business day testing;
- Technical certification of indirectly connected DCA holders consists of the successful individual completion of a number of interoperability and authorisation test cases. Operational certification is assessed based on the participation in community and business day testing.

Further information on the test cases to be performed by PM account holders, ancillary systems and DCA holders is available in the Guide to TARGET2 User Testing.

The test environment of the 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 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. A business change means 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 are possible, changes during the business certification should be avoided and changes after a 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 T2S Platform 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 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.

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

3.5.1. Tasks and responsibilities

In order to ensure the security and operational reliability of 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 users;
- compliance check by Central Banks: checking whether the users are in compliance with the measures laid down in the framework;
- provision of information by the 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 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 Central Bank with which the user has a legal relationship. In this context, it must be stressed that the decisive criterion is not whether the user is located inside or outside the euro area. Rather, it has to be considered whether a Central Bank is within the TARGET2 area[36].

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

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

it is responsible for collecting the relevant information from a particular user:

Does the 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)?
    - 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.
    - 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:

Description of the situation	Central Bank responsible
Head office located inside/outside[37] 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	Central bank having the legal relationship with the branch/subsidiary.

37 If the head office is located outside the TARGET2 area, it must be within the EEA.

infrastructure is located).	
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 7. 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 bureau are legally bound by the Harmonised Conditions to provide their central bank with information about a failure of such an organisation.[38] 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[39] 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 users (see the section on "Critical participants and non-critical participants").

When direct participants use a member/concentrator[40], 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 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.

38 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."

39 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.

40 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).

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.

3.5.2. Critical participants and non-critical participants

Notwithstanding the overarching requirement to ensure a level playing-field between 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 processed (e.g. settlement transactions of systemically important ancillary systems). Taking this into account, a distinction can be made between *critical participants* and *non-critical participants*.[41]

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

In the following, 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 are considered non-critical participants.

3.5.2.1. Credit institutions

General considerations and rationale

The guiding principle applied when establishing criteria to determine whether a credit institution is a critical participant is that organisations with a sufficient market share in terms of value are eligible, as well as those where its inability to meet its obligations could result in the inability of other participants or of financial institutions in other parts of the financial system to meet their obligations as they become due.[42] This means, in particular, that an operational disruption[43] could result in the accumulation of liquidity on a user's account, which in turn could prevent other users from making payments and thus potentially create systemic risk.

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

42 *Principles for Financial Market Infrastructures*, Bank for International Settlements, April 2012.

43 As opposed to balance sheet problems.

Criteria

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

As a general guideline, the Eurosystem considers a credit institution as a critical participant in TARGET2 if it consistently settles at least 1% in terms of value of the TARGET2 turnover[44] (excluding transactions submitted by third parties, e.g. ancillary systems, payments processed via MT 204 and transfers between accounts of the same participant) on a daily average in the first quarter of the year. In addition, criticality also depends on the previous year's classification, both for critical and non-critical participants. This implies that, once classified as critical, a participant stays as such for a minimum of two years.

This criterion will be reviewed at regular intervals. The review clause described in Section 3.5.8 is the mechanism that will be used to ensure that the criterion is 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 1% 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 the above stated main criterion, which is 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 the main criterion is not 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.

In order to be able to assess reclassification requests based on measurable criteria simulation techniques are applied[45]. More specifically, a technical failure of a credit institution is simulated and the impact this failure might have on the settlement of payments in TARGET2 is measured. As a

44 The TARGET2 turnover also includes transfers to/from DCAs but not the securities related settlements (e.g. DvP).

45 The tool used for the simulations is the TARGET2 Simulator, developed by the Bank of Finland in collaboration with the 3CB. Further information about the TARGET2 simulator can be obtained from the TARGET Newsletter, Issue number 7, Q4 2013 published on the TARGET2 website (http://www.target2.eu).

general rule, a credit institution could be (re)classified as critical in the event the simulation illustrates that on average 1.5 % of the overall TARGET2 turnover could not be settled because of the outage of the credit institution's technical infrastructure[46].

The opinion formed by the ECB will be submitted to the relevant Eurosystem committee[47] for further consideration.

3.5.2.2. 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 non-critical participants.

Organisations in the field of securities clearing and settlement

Organisations in the field of securities clearing and settlement are CSDs (central securities

46 The participants above the 1,5 % threshold that are not classified as critical will be reclassified, unless the Central Bank of the participant provides a different evidence.

47 The relevant committee is the Market Infrastructure Board (MIB) 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.

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 non-critical 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.

3.5.2.3. Service bureaus and member/concentrators

Apart from sharing the connection to SWIFTNet of another SWIFT customer, there are two other ways for a user to connect indirectly[48] to SWIFTNet. These are:

- outsourcing the day-to-day operation to a third party, called a service bureau[49]; 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 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 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

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

49 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).

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.

3.5.3. Measures to ensure the security and operational reliability of users

The guiding policy principle is that measures applied to ensure the security and operational reliability of users should be commensurate with their criticality. In the previous sections criteria for determining critical participants were outlined. Section 3.5.3.1 describes the measures that should be used for both critical participants and non-critical participants. Section 3.5.3.2 outlines the procedures that should be applied for critical participants only.

3.5.3.1. Measures applied for critical participants and non-critical 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 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 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 participant. It implies that if the smooth functioning of TARGET2 is affected because of an incident caused by the malfunction of the user's system, the TARGET2 system operator will not accept any liabilities towards this user. However, the 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 users because of this incident.

Monitoring and incident reporting

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

Once a user is live, it is closely monitored[50] by the relevant central bank. In the event that a user is affected by an operational disruption, staff responsible is requested to inform, upon their own initiative, the relevant central bank immediately. Once the user has resumed operations, the central bank may send an incident report form (Annex II) to the user for completion. This report requires the 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[51] does not exceed 30 minutes for critical participants. As long as the duration of an incident is below this limit, an incident[52] report would not be required. For non-critical 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 users. In this context, it is worth mentioning that an incident report is not required when a 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 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 user and ask for clarification which could ultimately result in the need for a formal response.

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.

Once the incident report is marked final, it is reviewed, analysed and recorded in a service incident log. If a user's performance was posing risks to the smooth functioning of TARGET2 or other users,

50 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"*.

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

52 Incident reports for AS migrating to T2S apply until the migration date to T2S

adequate measures will have to be taken, e.g. it should be drawn to the attention of senior officials of the user.

Incidents affecting the 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 user may be experiencing potentially serious availability problems it has not been informed about, the user will be contacted and an explanation will be requested.

In addition, 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.

3.5.3.2. Measures to be used for critical participants only

System security in accordance with standards

Principle 17 of the CPSS/IOSCO Principles for Financial Market Infrastructures (in the following referred to as the "PFMI") recalls that "There are many relevant international, national, and industry-level standards, guidelines, or recommendations that an FMI may use in designing its operational risk-management framework." Conformity with such commercial standards can 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 the Code of practice for information security management (ISO/IEC 27002). 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 or equivalent) of the critical participant shall file with the relevant central bank a self-certification statement[53] 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-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.

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

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[54] 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 the "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 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[55] as the primary business location. 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

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

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

the primary business location[56].

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.

Principle 17 of the PFMI stipulates that testing of the clearly documented business continuity arrangements should also involve the system's participants.

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 user testing programme that TARGET2 users have to perform prior to joining TARGET2.

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

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.

3.5.4. Implementation

3.5.4.1. Legal enforceability

The Harmonised Conditions for participation in TARGET2, more specifically Article 28 (Security requirements), 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 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 users into the legal arrangements with their 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 reported through which means this has been achieved.

3.5.4.2. Interim period

The measures for critical participants define access criteria which would ideally have to be met by a new critical participant prior to joining the TARGET2 system. New critical participants 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").

A critical participant will have 18 months to comply with specific requirements applying to its security and operational reliability. This period will start from the time of its designation as critical participant.

Finally, once a critical participant has been identified, the relevant central bank should contact it and ask it to indicate its level of preparedness considering the above-mentioned deadline 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.

3.5.4.3. 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.

3.5.5. Communication and coordination

A sound organisational structure is essential for the communication and coordination of security issues between central banks and their users to be managed in an effective and trustworthy manner. Each central bank and its 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.

3.5.6. Confidentiality

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

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

3.5.7. **Reporting**

The central banks are responsible for collecting the required information and monitoring any follow-up activities. For example, if a 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 user does not pose any risk to the smooth functioning of TARGET2 and the other 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.

3.5.8. **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, for example, following a merger a credit institution is suddenly processing more than 1% of the value of transactions in TARGET2, this credit institution may need to be classified as a critical participant and may have to meet the requirements specified for that type of organisation. Similarly, if the payments' value of a critical participant drastically decreases and remains for a sufficiently long period below the threshold, this participant may be reclassified as a non-critical participant.

Therefore, the criteria for determining critical participants and the classification of critical participants are reviewed at least on an annual basis but, in case of a need, the classification may also be updated on an ad-hoc basis. In addition to that, users are obliged to inform their central banks well in advance of significant changes in their business practices.

3.6. Termination or suspension of a participant

According to the TARGET2 Guideline, a Central Bank **shall immediately terminate or suspend** a participant's participation (PM account or DCA holder) in a TARGET2 component system without prior notice if:

a. insolvency proceedings are opened in relation to the participant; and/or

b. the participant no longer meets the access criteria for participation in that component system.

The Central Bank **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 the Opening and Operation of a PM account or the Harmonised Conditions for the Opening and Operation of a DCA;

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 Closed User Group (CUG) or the T2S Closed Group of Users (CGU), in the case of directly connected DCA holders;

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 poses risks on the grounds of prudence.

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 participant's participation in TARGET2, it must immediately notify all other central banks via an ICM broadcast (see below). Each central bank must,

if so requested by another central bank, exchange information in relation to the participant, including, in the event of termination, information in relation to payments addressed to it.

3.6.1 Effects of the suspension of a PM account holder

- PM 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 PM account.
- Payments sent by the suspended PM account holder after suspension, are stored for confirmation by the central bank via ICM.
- Payments sent to the suspended PM account holder 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 account holder** is that it is deleted from the system.

It should be noted that:
- As concerns liquidity pooling arrangements, the central banks that are party in an aggregated liquidity (AL) agreement and act as the counterparty for the PM account holders 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 PM account holder the central bank can choose whether or not the suspended PM account holder should still be published in the TARGET2 directory. The TARGET2 directory does not show whether a PM account holder is suspended. However, the detailed record in the TARGET2 static data, visible via the ICM, is marked accordingly.

- If the terminated or suspended PM account holder 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 suspended PM account holder is the **co-manager** for HAM accounts, it can no longer act as co-manager after suspension. It is up to the co-managed HAM account holders to nominate a new co-

manager. By default the central bank can co-manage the accounts.

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

3.6.2 Effects of the suspension of a DCA holder

- The Central Bank auto-collateralisation limit will be set to zero and any Central Bank auto-collateralisation previously granted should be reimbursed.

- An intraday restriction will be applied to the DCA in order to block any settlement.

- The Main PM account will be changed to the PM account of the Central Bank, unless the Main PM account belongs to the same legal entity as the DCA and has also been suspended. .

- The privileges necessary to initiate liquidity transfers in T2S will be revoked.

- Predefined and standing liquidity transfers orders will be deleted.

- Remaining liquidity in the DCA on the suspension day will be transferred to the main PM account via the automated cash sweep.

3.6.3 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[57], if the suspended PM 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

[57] A HAM account can be managed by a PM account holder with SWIFT-based access as a co-manager. The aim of the co-management function is to allow small banks to manage directly their reserve requirement but delegate cash flow management to other banks.

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.

3.7. Limitation, suspension or termination of intraday credit and/or auto-collateralisation facilities

A central bank shall suspend or terminate access to intraday credit / auto-collateralisation facilities if one of the following events of default occurs:

(i) the DCA and/or PM account of the entity is suspended or closed;

(ii) the entity concerned ceases to meet any of the requirements laid down in the Annex III of the Harmonised conditions for the opening and operation of a PM account and a DCA, respectively;

(iii) a decision is made by a competent judicial or other authority to implement in relation to the entity a procedure for the winding-up of the entity or the appointment of a liquidator or analogous officer over the entity or any other analogous procedure;

(iv) the entity becomes subject to the freezing of funds and/or other measures imposed by the European Union restricting the entity's ability to use its funds;

(v) the entity's eligibility as a counterparty for Eurosystem monetary policy operations has been suspended or terminated.

A central bank may terminate access to intraday credit and/or auto-collateralisation facilities if the central bank or another central bank suspends or terminates the DCA holder's participation in TARGET2, or if one or more events of default occur.

In addition, if the Eurosystem decides to suspend, limit or exclude counterparties' access to monetary policy instruments on the grounds of prudence or otherwise in accordance with Section 2.4 of Annex I to Guideline ECB/2011/14, the central bank shall implement that decision in respect of access to intraday credit and/or auto-collateralisation facilities pursuant to provisions in the contractual or regulatory arrangements applied by the central bank.

The central bank may decide to suspend, limit or terminate the access to intraday credit and/or auto-collateralisation facilities if the PM account holder/DCA holder is deemed to pose risks on the grounds of prudence. In such cases, the central bank shall immediately notify the ECB and other central banks thereof in writing. Such decision shall not take effect until the ECB has approved. Where appropriate, the Governing Council shall decide upon uniform implementation of the measures taken in all TARGET2 component systems.

Notwithstanding, in urgent circumstances, a central bank may suspend the access to intraday credit

and/or auto-collateralisation facilities with immediate effect. In such cases the central bank shall immediately notify the ECB thereof in writing. The ECB shall have the power to reverse the central bank action. However, if the ECB does not send the central bank notice of such reversal within ten business days of the ECB's receipt of notification, the ECB shall be deemed to have approved the central bank action.

In case of limitation of intraday credit, the intraday credit line should be adjusted, according with the limit defined. **In case of intraday credit**, the intraday credit line should be set to zero.

Similarly**, in case of limitation of auto-collateralisation facilities**, the central bank auto-collateralisation limit should be adjusted, according with the limit defined. **In case of suspension or termination of auto-collateralisation facilities**, the central bank auto-collateralisation limit should be set to zero.

3.8. TARGET2 billing

The monthly invoice for TARGET2 services is sent to the PM account holders and ancillary systems by the relevant central bank at the beginning of the next month (no later than on the ninth business day) and it has to be paid at the latest on the 14th business day of that month.

Additionally, all PM account holders with one or more DCAs linked to its PM account (main PM account) or defined as a party in T2S are invoiced also as regards the cash related T2S service items, in accordance with the T2S pricing policy.

Further information is available in the TARGET2 Pricing Guide for Users.

4. Business day in normal situations

TARGET2 users are responsible for monitoring of their daily activities carried out in the SSP and/or T2S platform. In parallel, each national service desk also caters for the general monitoring of business during the day as well as for the respective community needs.

These activities might be performed via the ICM, as concerns the services offered at SSP level (including the TARGET2 value-added services), or via the GUI, as regards the services offered via the T2S Platform.

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

The new business day in TARGET2 (SSP) begins after the end-of-previous-day procedures and the start-of-current-day procedures have been successfully completed (being the first activity the load of changes in the users' static data). The switch to the new business day is normally confirmed between 18:45 and 19:00 with a broadcast message which is sent to all users. The phases are also visible in the ICM screen "SSP Operating Day", under "Services" – "Administration".

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*."

The start-of-day process in **T2S** is launched at 18:45 too and lasts until 20:00.This is confirmed via a "Status of the T2S Settlement Day Notification" message, via the GUI screen "Daily Schedule" and/or via the "T2S Diary Query". The start-of-day period includes the change of settlement date, the acceptance of data feeds for client auto-collateralisation from DCA holders (received until 19:00 and effective for the current settlement date), the valuation of securities positions for client-collateralisation on stock and the valuation of collateral eligible settlement instructions.

During this period, no cash settlement occurs and it should be used by the participants to prepare for the Night Time Settlement (NTS).

Box 2. Data feeds for Client auto-collateralisation

Each DCA Holder offering client auto-collateralisation in T2S is responsible for the setup and maintenance of the auto-collateralisation feature in T2S, including the configuration of the necessary static data. In particular, the following information (data feeds) should be provided to T2S:

- The list of eligible securities for auto-collateralisation (after the first upload, it should be updated whenever changes occur);
- The daily valuations of the eligible securities;

Collateral data feeds (eligible securities and respective valuations) to be used for the settlement day that starts at 18:45 should be provided throughout the day and, ideally, by 17.45 (even if information sent until 19:00 is still accepted). The valuations should be provided in the form of a flat file, while the list of eligible securities is delivered via an ISO 20022 message or file, as described in the T2S UDFS[58].

In case of a delay in the provision of the valuations of the eligible securities (i.e., in case the information is not provided by 19:00), the previous available collateral values will be used. In case there is no information about the previous day valuation for a given eligible security, a zero price will be applied.

Note that, for the time being, the T2S close links functionality will not be used by the Eurosystem and, therefore, it is not necessary to provide information about the list of close links.

4.2. Liquidity provision

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 or HAM;
- from the HAM or PHA to the PM.

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

4.3. SSP Night-time settlement

Liquidity for night-time settlement (setting aside to sub-/mirror accounts)

At 19:30 sub-accounts and mirror accounts are credited to allow ancillary systems to start the night-

[58] The provision such information requires a direct connection to T2S in application-to-application mode.

time settlement (NTS) procedures.

The night-time window is available from 19:30 to 7:00,[59] with a technical SSP maintenance period between 22:00 and 1:00. Hence, the NTS of the different ancillary systems in central bank money is facilitated. There are adequate technical/operational tools available in TARGET2 in order to run NTS smoothly.

Support for credit institutions or ancillary systems taking part in NTS is subject to agreement with their respective central bank.

During the NTS window, liquidity transfers via the ICM to and from the PM account are possible.

Liquidity provisioning for night-time settlement ("non-concordant orders")

The diagram below shows the processes of settlement procedure 6[60].

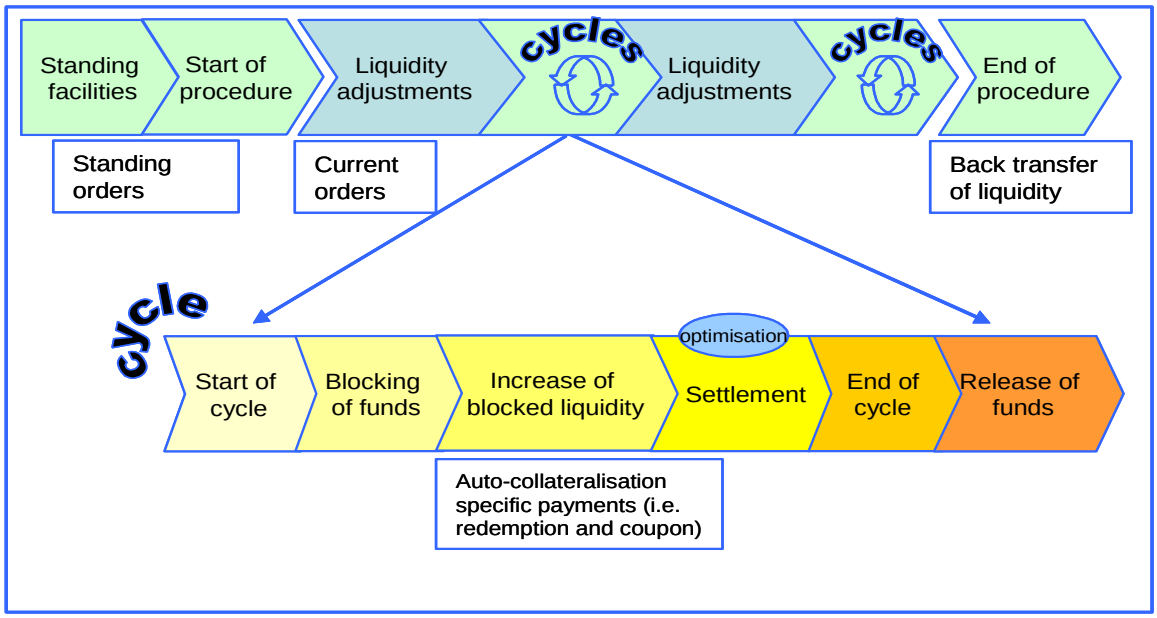

Diagram 12. Settlement procedures 6

In this context, a distinction can be made between standing orders and current orders by the PM account holder/settlement bank and the ancillary system:

(i) Standing order (by the settlement bank only)

59 The time between 6:45 and 7:00 (start of daylight settlement) is used for the preparation of the opening of the day trade phase.

60 During the NTS, just settlement procedure 6 can be used. Notwithstanding, settlement procedure 6 might be used during the NTS as well as during the day trade phase.

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 settlement bank 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.

(ii) 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.

(iii) 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. Cash relevant aspects of T2S night time settlement

During the night time settlement (NTS) of T2S, T2S processes liquidity transfers in two settlement cycles, according to an automatic pre-defined order called "sequence". A settlement cycle consists of more than one sequence.

Liquidity transfers from PM accounts to DCAs and liquidity transfers between DCAs are settled from sequence zero (in the first NTS cycle) onwards, i.e. the first input of liquidity is settled right at the beginning of NTS. It should be noted that standing liquidity transfer orders from PM accounts to DCAs are processed in the SSP at 19:30 and, on the T2S Platform, at 20:00, with the start of sequence zero.

Liquidity transfers from DCAs to PM accounts are settled from sequence 1 (in the first NTS cycle) onwards. Liquidity transfers received while sequences are running are taken into account in the following sequences.

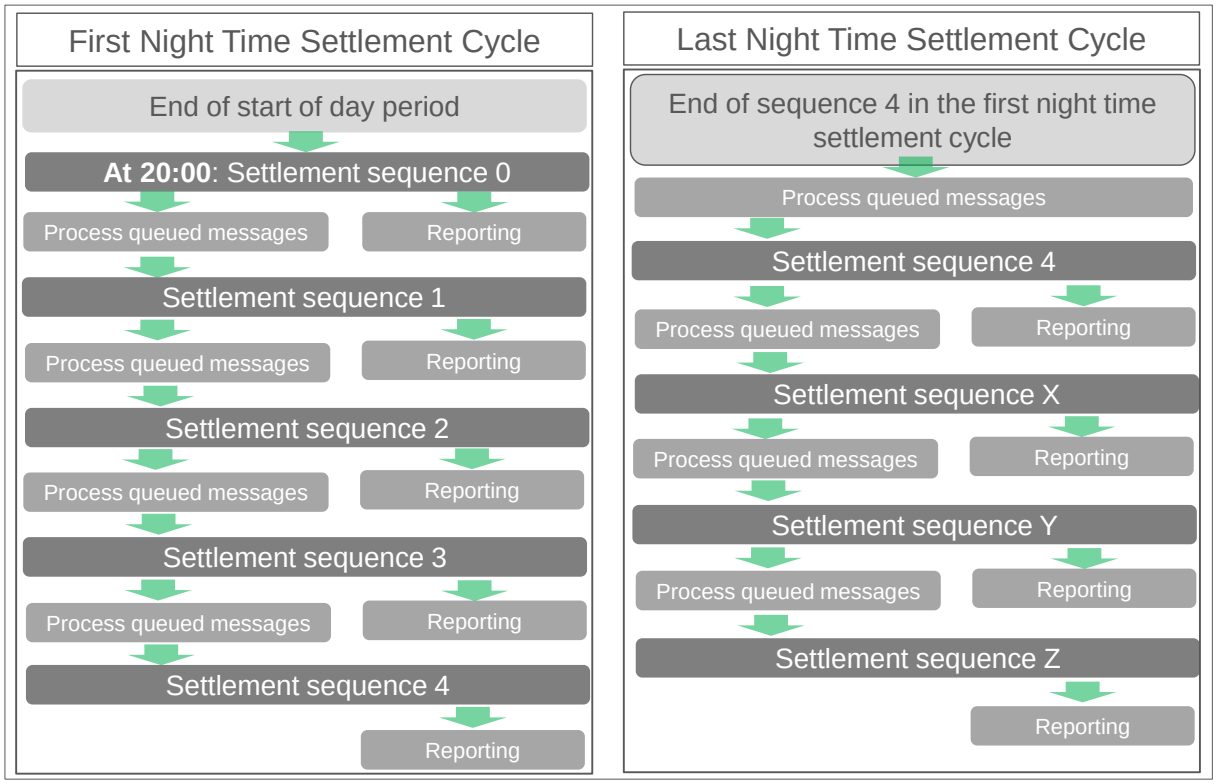

Diagram 13. T2S night time settlement sequences

At the end of each sequence, T2S generates full or delta reports as per report configuration setup of the relevant directly connected DCA holder. Indirectly connected DCA holder will not be offered such reports.

In case the NTS is completed before 03.00, real-time settlement begins before the start of the

Maintenance Window (at 3:00). During the Maintenance Window no settlement takes place in T2S.

Multiple liquidity provider functionality

T2S enables a DCA holder to receive liquidity from different PM accounts, i.e. from different liquidity providers. In case the DCA holder uses the multiple liquidity provider functionality, the liquidity providers can initiate the necessary liquidity transfers to the DCA.

At the end of the night-time settlement –in sequence Y of the last night-time settlement cycle - the remaining liquidity on the DCA is automatically retransferred to the PM accounts of the liquidity providers, according to the standing liquidity transfer orders (to shift the remaining liquidity back to the PM accounts) and the predefined order for the execution of those standing orders defined in the static data.

The Multiple Liquidity Provider functionality is an optional and can only be used during night-time settlement, in sequence Y of the last night-time settlement cycle.

4.5. Business window

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

4.6. SSP Day trade phase

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 ancillary system interface (ASI) using settlement procedure 4. The file is sent to the ASI for settlement at around 16:08, with a settlement period until 16:45. 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. Central Banks holding a PHA should ensure their compliance with this cut-off, 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. The timestamp of the SSP is binding; more precisely, the time when the module receives the message prevails. Central Banks holding PHAs should ensure their compliance with this cut-off, e.g. by setting earlier cut-off times.

4.7. Cash relevant aspects of the T2S Real-time settlement

The start of the T2S real-time settlement (RTS) might be checked via a "Status of the T2S Settlement Day Notification", an entry in the T2S GUI "Daily Schedule" screen or a "T2S Diary Response" query response message.

The RTS includes:

(i) The **real-time settlement preparation**;

(ii) Five **partial settlement windows**, of a duration of 15 minutes, which start at 8:00, 10:00, 12:00, 14:00 and 15:45 (15 minutes before the beginning of the Delivery versus Payment cut-off time). During the partial settlement windows, T2S partially settles new settlement instructions arriving in T2S and eligible for partial settlement, as well as previously unprocessed or partially processed settlement instructions eligible for partial settlement.

(iii) the Real-Time Settlement Closure. The closure of the real-time settlement period is scheduled to start at 16:00 and includes the following processes that are highly relevant for cash settlement:

Time	T2S euro settlement day events/processes
16:00	DVP cut-off (no new auto-collateralisation instructions can be triggered after this cut-off)
	Cash settlement restriction cut-off
	Release of unused cash settlement restriction
16:30	Automatic reimbursement of Central Bank auto-collateralisation
(thereafter)	Optional automated cash sweep (if configured via standing liquidity transfer orders)
17:40	Cut-off for BATM (Bilaterally Agreed Treasury Management) and CBO (Central Bank Operations) settlement instructions

17:45	Cut-off for liquidity transfers from PM accounts to DCAs
(thereafter)	Automated cash sweep to transfer **the** remaining liquidity from DCAs to the respective Main PM account. **NOTE**: DCA holders are recommended to transfer liquidity from the DCAs to the PM accounts at earlier points in time, i.e. before the automated cash sweep, to limit liquidity risks in the event of a problem with this process.
18:00	Securities settlement restriction cut-off and Free-of-Payment cut-off

Table 8. T2S Real-time settlement closure

Directly connected DCA holders may check the mentioned cut-offs via the T2S GUI screen "Daily Schedule" and/or via "T2S Diary Response" query response messages.

Box 3. Automatic Central bank auto-collateralisation reimbursement

During the night-time settlement period, as well as during the day trade phase, DCA holders may benefit from central bank auto-collateralisation. However, it is not possible to have overnight credit in the T2S platform and, therefore, DCA holders are expected to repay the Central Bank auto-collateralisation before 16:30. This should be done via the release (as CSD participant or as DCA holder if the DCA holder has been granted the object privilege over the relevant SAC(s)) of the relevant reverse pending instructions. If this action is not performed until 16:30, the automatic reimbursement will be triggered by the T2S platform. Therefore, DCA holders should either reimburse central bank auto-collateralisation until 16:30 or to provide sufficient liquidity on the DCA, in order to allow the reimbursement of auto-collateralisation via the automatic auto-collateralisation reimbursement (at 16:30).

This process involves the following steps, triggered automatically by the T2S platform:

(i) Release of the reverse auto-collateralisation instructions still "on hold";

(ii) Attempt to settle the pending reverse transactions, based on the liquidity existing on the DCA;

(iii) Attempt to settle the (remaining) pending reverse transactions, based on the liquidity available on other DCAs held by the same DCA holder (identified via the party BIC11) and within the books of the same central bank (i.e. rebalancing);

(iv) Collateral relocation, step via which a new securities transaction is initiated in order to move the securities given as collateral by the DCA holder to the regular collateral account of the respective Central Bank. Upon reception of the information regarding this collateral movement, the central bank will transform the Central Bank auto-collateralisation into an intraday credit in the PM account indicated by the DCA holder as the account for the automatic Central Bank auto-collateralisation reimbursement. This is usually done via a connected payment via which the Central Bank increases the counterparty's credit line and simultaneously debits the relevant account.

A penalty fee of EUR 1,000 will be applied for each business day where one or more recourse to the collateral relocation occurs. This penalty fee will be charged to the holder of the PM account indicated as the one for the automatic Central Bank auto-collateralisation reimbursement according with the national procedures defined by the respective Central Bank.

Note: The credit line registered in the relevant PM account is independent from the Central Bank auto-collateralisation granted during the day to the DCA on the T2S platform. The amount of the credit line

is collateralised by a pool of securities. The Central Bank auto-collateralisation granted during the day is collateralised by securities that have not been included in the pool previously. It is only when the counterparty fails to reimburse the auto-collateralisation by 16:30 that the collateral is moved to the regular pool, resulting in an increase of the credit line in the PM account. To make sure that the credit line increase is used for the reimbursement of Central Bank auto-collateralisation, the cash stemming from the increase of the credit line is debited immediately from the PM account of the participant in favour of the PM account of the central bank. Usually, the use of a Connected Payment ensures this (in certain situations, Central Banks might deviate from this procedure, for example, if a fixed credit line is used).

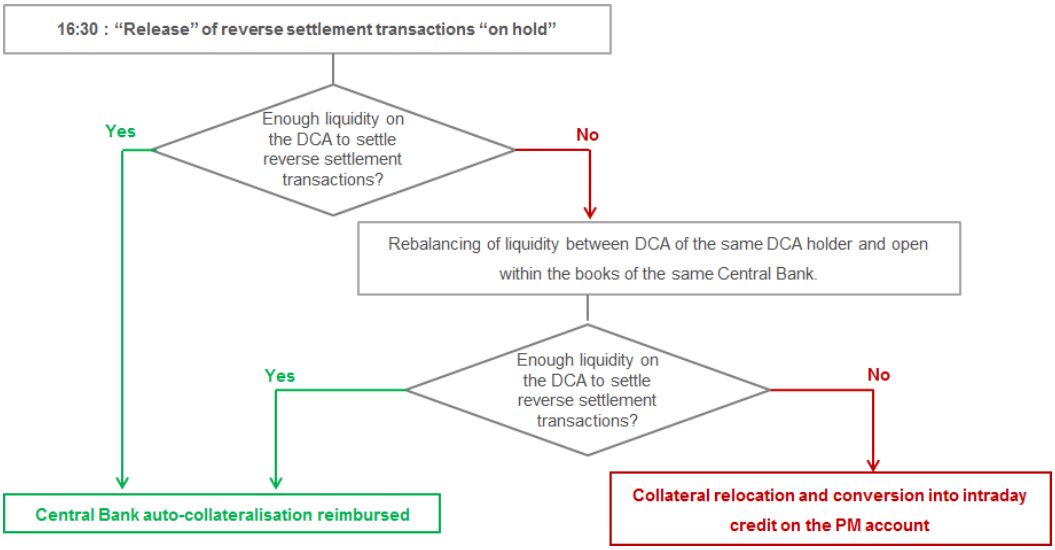

Diagram 14. Automatic Central Bank auto-collateralisation Reimbursement

There is no automatic reimbursement in the case of Client auto-collateralisation.

4.8. End-of-day processing

TARGET2 closes at 18:00. The SSP closing will be confirmed by a message in the ICM and the T2IS. The cut-off time can also be seen in the ICM (under "Services" – "Administration" – "SSP Operating Day"). 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 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 reserve maintenance period);
- 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;
- sending account statements (MT940/950) to PM account holders (optional).

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

As regards the T2S platform, the execution of the EOD process might be confirmed by directly connected DCA holders via a "Status of the T2S Settlement Day Notification", an entry in the GUI screen "Daily Schedule" and/or via a "T2S Diary Query". By this time T2S generates all the end-of-day reports and account statements on DCAs, according with the report configuration setup, and sends them to the directly connected DCA holders. Indirectly connected DCA holders will not receive end-of-day reports from T2S (in particular, will not receive statements of account).

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, T2S Platform, 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 and it may be of technical, operational or financial nature. 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 or operational failure;

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

The diagram below shows which parties could be involved in TARGET2 abnormal situations.

Diagram 15. 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 through failover to a secondary system/site/region;
- contingency measures that allow the continued processing of a limited number of payments;
- delayed closing, i.e. the extension of the day trade phase.

As FIN messages and InterAct and FileAct files go via different SWIFT channels, 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 incident management 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 communication tools means mentioned under section 2.4.1.

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

(i) description of the error;

(ii) anticipated delay (if possible);

(iii) information about measures taken; and

*(iv) a*dvice 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 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.A delay in the start-of-day may lead to a delay in the start of the consecutive phases and thus impact the liquidity provision to ancillary systems and DCAs.

6.2. Night-time settlement incident procedures[61] (19:00 – 22:00 & 01:00 – 07:00)

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

In case standing liquidity transfers orders from PM accounts to DCAs are not executed timely and/or successfully, T2S may continue with the standard schedule, relying on auto-collateralisation only. As regards liquidity transfers from DCAs to PM accounts, these should be queued until the SSP recovery. Depending on the SSP failure, it might be possible to fix the problem or there might be a need to initiate a failover (see below). 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

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

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.

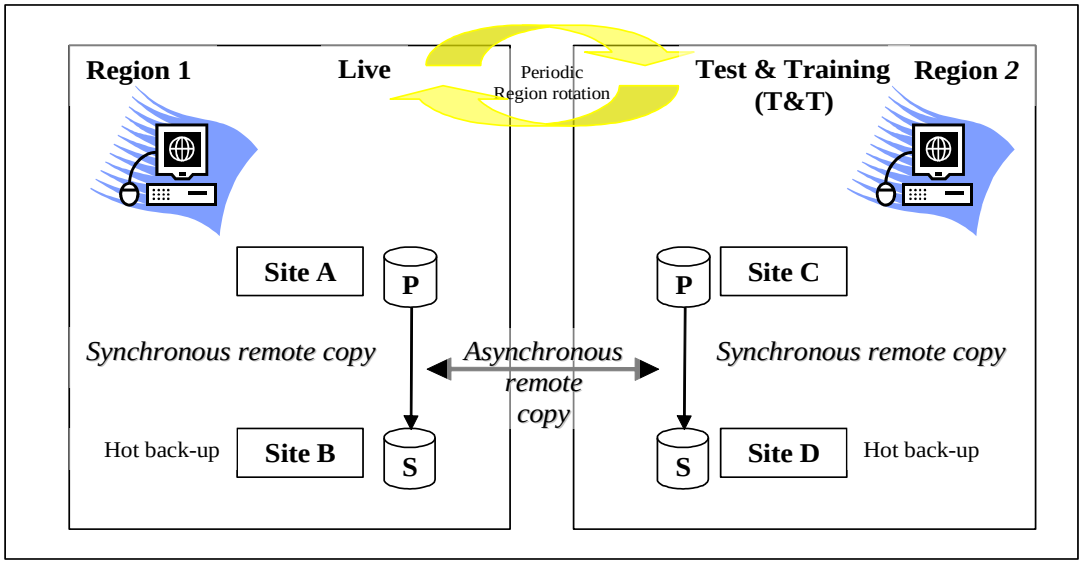

Diagram 16. Two regions, four sites

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 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[62]. The process of rebuilding requires the active participation of the users. The procedure for inter-region failover with loss of data, including the rebuilding process, is described in Annex I.
- Payment processing is interrupted during an inter-region failover. If users keep on sending FIN payments, these will be queued at SWIFT level and processed upon the recovery of the SSP. The same applies to the liquidity transfers to/from DCAs initiated directly via T2S or via the TARGET2 core or value added services for T2S, which will be queued at the T2S Interface or SWIFT level.

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

Handling of ancillary system transactions with optional mechanisms

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

Settlement procedure	Optional mechanism	Effects 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 period	Rejection
	- with guarantee period	Activation of guarantee mechanism

Table 9. 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[63]

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.[64]

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 4. "*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 5. "*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

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

64 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).

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 2.4.1 "Communication Tools" and 5.3 "Incident Communication" 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 incoming payments or 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. While very critical payments can be processed immediately, any processing of 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 CM 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 following the procedures which each central bank has set out for contingency situations.

- 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: it is the sole responsibility of the sender to take the necessary measures to avoid double processing.

- 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 4. 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.

Note that according with this definition, liquidity transfers to/from DCAs would be considered critical payments, thus would be eligible for the processing in contingency. However, the possibility to use auto-collateralisation and existing DCA balances may reduce the impact in T2S and hence liquidity transfers will not be processed via the CM in a contingency situation.

Box 5. 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 TARGET2 crisis managers. The announced new closing time is the new cut-off

time for interbank payments. The Eurosystem will inform the users as early as possible of the possible duration of the delay. As long as this cannot be anticipated, in particular if the reason is a prolonged outage of the SSP, regular updates of the situation will be provided. 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 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.

In principle, TARGET2 and T2S should always operate on the same value date for euro settlement which means that, as long as TARGET2 is still open for euro cash settlement on day D, T2S should not allow euro cash settlement on day D+1. Thus, in case of a TARGET2 delayed closure, a T2S delayed closing, T2S delayed start of the next settlement day or T2S start with non-settlement in euro should be envisaged. An advantage of a T2S delayed closing could be that collateral could be activated through T2S in order to provide liquidity for a settlement in the TARGET2 contingency module (CM).

In a TARGET2 delay situation, the TARGET2 Coordinator will immediately inform the T2S Coordinator so that T2S incident management process might be triggered. Nonetheless, if DCAs have a zero balance, auto-collateralisation positons are closed and no reconciliation actions after a restart after disaster are needed, T2S may not delay.

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 TARGET2 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

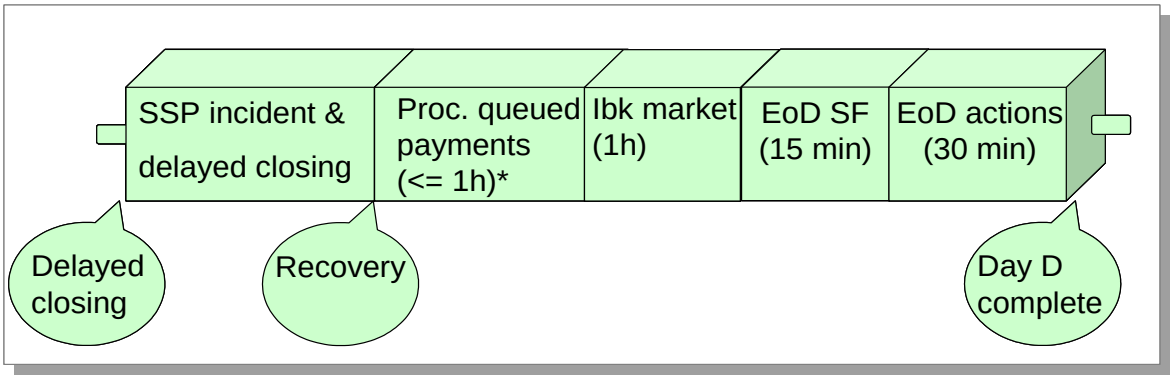

Diagram 17. Processes on the day of the incident

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

- Processing of all queued payments (maximum up to 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, at maximum, up to two hours and 45 minutes.

Steps after the delayed closing of Day D

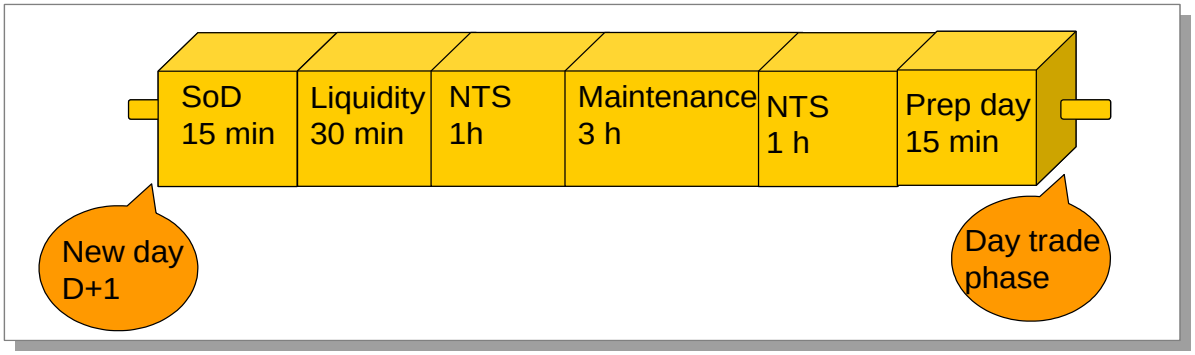

Diagram 18. Processes on the following day

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 - NTS1-, including provision of liquidity for DCAs (minimum one hour);
- maintenance period (maximum three hours);
- night-time settlement - NTS2 (minimum one hour);
- preparation of day trade phase (15 minutes).

These steps add up to for six hours and may be further reduced by reducing the maintenance window and facilitating the non-NTS processes. The diagram below shows the overall sequence:

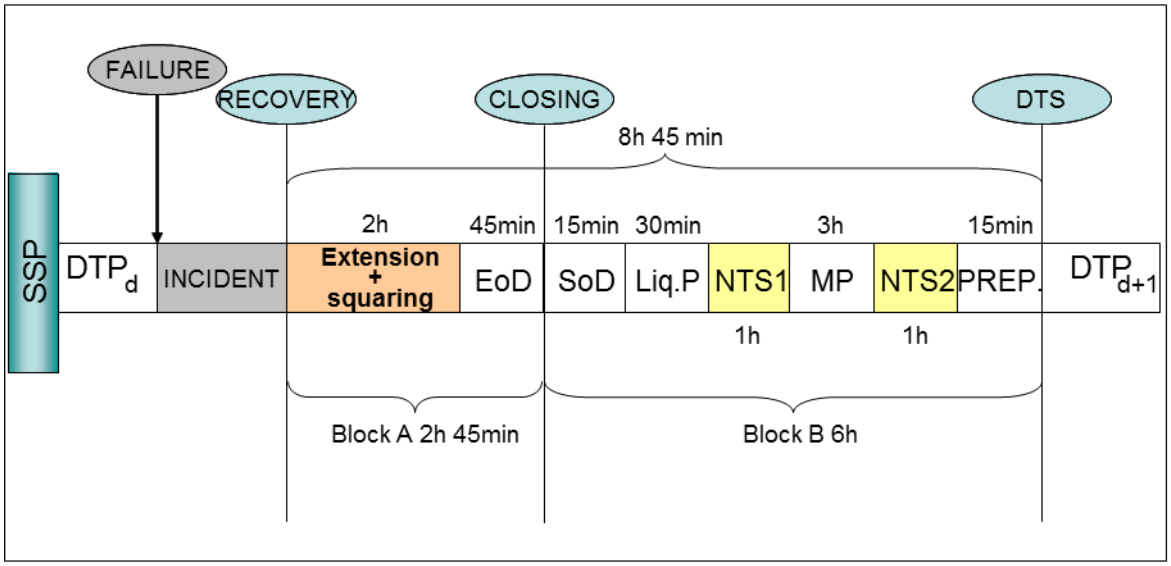

Diagram 19. Overview of processes in case of incident

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 7:00. An outage going beyond 22:15 (prolonged outage) may prevent a start of the day trade phase at 7:00, in case the phases could not be further shortened (in particular the maintenance window).

In order to save time and to start the day trade phase as close to 7:00 as possible, the steps "NTS2" and "preparation of the day trade phase" may be run in parallel immediately after the maintenance period. However, even this procedure might still not allow the day trade phase to start at 7:00. 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 (see section 6.4.3), with all cut-off times being shifted in parallel with the one which is first delayed. After the SSP recovery the next step would be the continuation of the end-of-day processing.

7. Failure at T2S level

7.1. Impact on TARGET2

Depending on the moment in which a T2S failure occur it may impact payment bank's liquidity, collateral provision and/or the reimbursement of intraday credit (including auto-collateralisation), as shown below. All throughout the settlement day, in case of a T2S technical failure, banks may have difficulties to provide fresh collateral in order to increase their credit lines.

Operational day phase	Impact of T2S failure
Start of Day (18:45 to 20:00)	T2S standing liquidity transfer orders scheduled at 20:00 might need to be resent.
Night Time Settlement (20:00 to 3:00)	DCA's liquidity would remain on the T2S Platform. Since no contingency processing is foreseen to sweep liquidity back to TARGET2, this could have an impact on (very) critical payments to be settled in TARGET2 (early) in the day trade phase (CLS, EURO1 bridge, CCPs).
Maintenance Window (3:00 to 5:00)	No impact on TARGET2.
Real Time Settlement (5:00 to 18:00)	Delay in the automatic reimbursement of auto-collateralisation (16:30), could lead to a delay in TARGET2 until the intraday credit can be reimbursed in T2S. The deadline for the reimbursement of intraday credit by connected, non-Eurosystem NCBs may need to be postponed. Liquidity may not be sent/swept to TARGET2 as foreseen/ or monetary policy operations may not be sent onward to TARGET2 and cause liquidity impacts and require a delay in TARGET2[65]. Impact on BATM with repercussions on the money market possible.
End of Day (18:00 to 18:45)	No direct impact on TARGET2.

Table 10. Impact on TARGET2 of a T2S failure

Given the dependencies highlighted in the table above, when a failure of the T2S platform occurs, the

[65] In exceptional cases, due to a technical malfunction in T2S, funds on DCAs at the end of day may remain overnight in T2S without triggering a delay in TARGET2. Under such circumstances the remaining balance (or balances) on the DCA (or DCAs) will be taken into account for the minimum reserve calculation. Moreover, if at the end of the day a participant would have a debit position on its PM account that would be covered by the DCA balance (and hence be forced to access the marginal lending facility) it would be allowed to claim for compensation under the TARGET2 compensation scheme.

T2S Coordinator has to mandatorily inform the TARGET2 Coordinator as soon as possible.

In principle, TARGET2 and T2S should always operate on the same value date for euro settlement which means that, as long as TARGET2 is still open for euro cash settlement on day D, T2S should not open euro settlement on day D+1, and vice-versa. Thus, in case of a T2S delayed closure, a TARGET2 delayed closing or delayed start of the next settlement day could be envisaged. Nonetheless, if DCAs have a zero balance, auto-collateralisation is reimbursed and no reconciliation actions after a restart after disaster are needed, a TARGET2 delay closure may not be necessary.

7.2. T2S failover situation

In case of a T2S platform failure that triggers the failover to another site or region, it is necessary to wait for the platform recovery and to delay the closing/postpone the respective T2S phase, if applicable (as a consequence and dependent on the time in the day, also a TARGET2 delay closing might be needed).

Central Banks shall inform the participants as early as possible about the situation and recommend that no new messages to debit/credit DCAs should be sent to the T2S platform (via the direct connection to T2S or via the TARGET2 core and/or value-added services for T2S). Regular updates of the situation will be provided via the available communication means (as described in section 2.4.1).

In case of an inter-region failover (from Region 1 to Region 2), once the T2S Platform has been recovered in Region 2 the Central Banks will need to ensure the reconciliation and synchronisation of the euro transit accounts in terms of balances and turnover – this is only required in the unlikely event of a restart after disaster with loss of data. In this context, the missing liquidity transfers will be identified and the participants will be informed by the respective Central Bank about the actions that will be performed and the liquidity transfer affected.

As regards the **liquidity transfers from PM accounts to DCAs**, the following actions might be performed:

(i) If the liquidity transfers were booked on the SSP but not yet on the T2S Platform (i.e. no camt.025 – Receipt has been received from T2S), provided that messages sent to T2S are still with status "provided" or "acknowledged", the TARGET2 Coordination Desk (acting as T2S transit account holder) will resend the messages via ICM (screen RTGS > Payments and messages > Select messages > Possible Messages for Repeat Sending).

(ii) If the liquidity transfers were booked on the SSP and also on the T2S Platform (i.e., camt.025 – Receipt has already been received from T2S), from a SSP perspective the business case is closed and, thus, messages cannot be resent via ICM. Therefore, a technical resending will be made (i.e.,

messages will be resent from the middleware). In case there are a high number of liquidity transfers it might be decided to resend all the liquidity transfers processed during the last 10 minutes before the incident (the double input control on T2S side will prevent a double processing in T2S of any liquidity transfer already processed before in Region 2).

In this situation, the DCA holders which have subscribed for T2S credit and/or ceiling notifications should disregard the notifications related with the second booking (on region 2).

Concerning the liquidity transfers from DCAs to PM accounts, the Central Bank responsible for the credited PM account holder will debit the PM account and credit the T2S transit account, upon authorisation of the PM account holder. In this case, if the DCA holder has opted for debit and/or floor notifications, the notifications related with the initial liquidity transfer (made in region 1, before the disaster) should be disregarded. After the recovery, the DCA holder might resend the liquidity transfer to the PM account again.

8. Other failures

In this chapter, the failure at central bank level, at ancillary system and bank level (including the case of uncontrolled message inflows) and at SWIFT level 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, ancillary system or bank.

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

8.1. Failure at Central Bank level

In TARGET2, payments are processed on the SSP and/or T2S Platform. This means that a partial or complete failure of a central bank will not prevent access to TARGET2 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.

As a general rule, each problem in a central bank/PHA that may have an impact on the SSP and/or on the T2S Platform 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.

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

The impact of an incident at Central bank level depends on the phase of the operational day as shown below:

Operational day phase	Impact / Incident procedures
Start-of-day (18:45 – 19:00)	For all the incidents which could occur during this phase, the relevant central bank will have appropriate backup measures

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 or T2S.
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.
Day trade phase (07:00 – 18:00)	A failure during the day trade settlement phase might have an impact on the update of credit lines/repo transactions and on the execution of the Central Bank related operations (monetary policy operations, cash deposits and withdrawals, etc). For all these actions, the relevant central bank will have appropriate backup measures.
End-of-day (18:00 – 18:45)	A failure during the end-of-day procedures will, in principle, not have an impact on the SSP, T2S or on the banking community.

Table 11. Impact of a Central Bank failure

8.1.2. **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;
4) it might not be possible to perform the collateral relocation (in case Central Bank auto-collateralisation n has not been reimbursed in due time).

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.

The impact of a PHA failure might be summarized as below:

Operational day phase	Impact
Start-of-day and provision of liquidity (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 PM accounts of the participants concerned or if liquidity is provided in the PHA against new collateral. - Special attention should be given to those users that participate in night-time settlement. For these 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. - Knock-on effects to the provision of liquidity to DCAs may be induced. 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.
Night-time settlement (19:30 – 07:00)	After the liquidity has been provided to the PM accounts, problems at the level of a central bank would not have an impact on the processing of the SSP.
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.
Day trade phase (07:00 – 18:00)	A failure in the day trade phase means that the PHA is unable to create transactions/operations. Hence, for example, automated updates of credit lines and intraday transfers of liquidity between the PHA and the PM will not be possible. In addition, it might have an impact on the collateral relocation (in case Central Bank auto-collateralisation has not been reimbursed in due time). **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 is available, no transactions can be executed. **Delayed closing:** In the event of a PHA failure, the crisis managers do not grant a delayed closing for TARGET2.
End-of-day	A PHA problem at the end of the day may have an impact on the

(18:00 – 18:45)	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.

Table 12. Impact of a PHA failure

8.2. Operational or technical failure at participant level[66]

In the event that a PM account or DCA holder has a problem that prevents it from settling payments and/or liquidity transfers to/from DCAs in TARGET2[67], it should inform and stay in regular contact with its central bank. It is encouraged to use its own means during the problem to the maximum extent possible.

The tools available to each DCA holder are:

- Liquidity transfers from DCAs to PM accounts via the T2S interface, if the main PM account holder opted for the TARGET2 value added services;
- GUI, for the DCA holders that normally use A2A functionalities.

The tools available to each PM account holder are:

- in-house contingency solutions;
- via normal ICM access, the backup payment functionality, which allows (i) initiation of payments to the CLS account, to the EURO1 collateral account or to the EURO1 prefunding account ("backup contingency payments") and (ii) initiation of payments for redistributing liquidity ("backup liquidity redistribution payments[68]");
- liquidity transfers from PM account to DCA via normal ICM access (in case the PM account holder normally uses the A2A functionalities);
- the same functionalities via a stand-alone ICM connection, if the normal ICM connection is no longer available.

If a participant's own means are exhausted or their use is not efficient, the participant may ask for the support of its national service desk, which in such a situation can perform a limited number of

66 Financial failure is covered under sections 3.6 and 3.7

67 Including a problem with the SWIFT connection to the SSP, and/or with the direct connection to the T2S Platform via one of the licensed Value-added Network Service Providers.

68 Backup liquidity redistribution payments are intended solely to redistribute excess liquidity and avoid it being trapped in the PM account of the participant suffering a technical outage. They are completely separate from the underlying commercial payments. Therefore institutions to which liquidity is redistributed may be different entities from the participants for which the underlying payments are destined. Also, there is no need for the institutions to which liquidity is redistributed to be TARGET2 direct participants provided that the funds are transferred through TARGET2.

payments on behalf of the affected participant. The detailed contingency communication means are subject to the bilateral relationship between a participant and its central bank.

A participant's technical problem 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 among all central banks.

A single participant's system outage should never lead to a delayed closing.

Box 6. Backup Contingency Payments

Backup payments via the ICM (in both U2A and A2A mode) may only be used for the processing of payments to the CLS account, to the EURO1 collateral account or to the EURO1 prefunding account ("backup contingency payments") and of payments for redistributing liquidity ("backup liquidity redistribution payments");

Within these limitations, making backup payments is entirely at the discretion of the bank requiring it, which is fully responsible for the credit risk involved. Both backup contingency payments and backup liquidity redistribution payments are by nature fully-fledged payment orders. That means that there is no need to resend the same or a similar payment after normal operations are resumed.

When the backup functionality is used, the following aspects should be taken into account.

- Before a PM participant can use the backup functionality it has to request its activation from the relevant central bank, which will activate it with immediate effect.
- A PM participant using the functionality may ask its central bank to send a broadcast to inform other TARGET2 users about the participant's use of backup payments to redistribute liquidity.
- If a participant that has faced a technical problem intends to send the delayed original payments with the business date of the problem (the original value date) on the next business day, this needs to be communicated to the relevant central bank on the day of the technical system outage, i.e. prior to the day on which the individual payments will be sent. This request for the value date control to be lifted must reach the relevant central bank at least 30 minutes before the closing time of TARGET2. The central bank will arrange for the value date control for this sender to be switched off for the following business day, allowing the transmission of the original individual payments with the original value date. TARGET2 always settles on the business day on which the payment is sent; if the value date differs from this, any interest adjustment will need to be effected outside the TARGET2 system.
- If the lifting of the value date check is required for another day, this must be requested on the

previous business day at least 30 minutes before the closing time.

- Once it has finished all related business, the participant having requested the lifting of the value date check must inform its central bank, which will reactivate the value date check.
- When creating backup payments it is important to consider not only the balance on the PM account but also possible debits to the PM account not originated by the affected participant, such as those in respect of settlement of ancillary systems.
- Recipients of backup payments should be aware that the sender BIC for backup payments is the BIC of the PM (TRGTXEPMXXX) and that the debtor/ordering party of the payment can only be identified via the BIC in field 52 of the FIN message.

When sending backup payments for liquidity redistribution the affected participant should do so on the basis of an individual bilateral prior agreement. Market practices as defined in the European Interbank Liquidity Management Guidelines must be followed.

8.3. 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. 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.

8.3.1. Ancillary systems using the ancillary system 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[69];
- 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, 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[70] on behalf of the settlement bank and on the basis of information provided by the ancillary system.

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:

69 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.

70 Mandated payments are payments initiated by an entity that is not party to the transaction (typically by an NCB or an ancillary system in connection with ancillary system settlement) on behalf of another entity. In particular, for example, an NCB sends a credit transfer (with a specific message structure) on behalf of a failed direct participant (only in contingency situations). Mandated payments to technical accounts are not possible.

- 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[71] 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 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[72] 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.

8.3.2. 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

71 Specific procedures will have to be set up in case ancillary system is calling the guarantees.
72 For example: ASTransferNotice, ASInitiationStatus, ReceiptAS(I), ReturnAccountAS.

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 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.

8.4. Technical suspension

A technical suspension is a temporary means to protect the SSP and/or the T2S Platform 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 and/or T2S Platform. It is a purely technical measure which is applied when a central bank, a bank or an ancillary system sends such an extraordinarily high number of messages to the SSP and/or the T2S Platform that it could endanger the its functioning.

If the Eurosystem becomes aware of such exceptional and massive message inflows that endanger the smooth functioning of the SSP and /or the T2S Platform, 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, Eurosystem will lift the technical suspension. Depending on the circumstances and as a precaution, a delayed closing could be considered by the crisis managers.

8.5. SWIFT failure

In case of a SWIFT outage, an alternative contingency network is used to provide a payment channel. The contingency network considerably improves the resilience of TARGET2 and overall systemic stability in the event of a regional or global SWIFT outage. Even without SWIFT access, central banks can send (very) critical backup contingency and liquidity redistribution payments and ancillary system files and perform liquidity transfers between PM accounts and DCAs via the contingency network on behalf of their customers. The central banks are also able to monitor the accounts of their participants via the contingency network (including the DCAs linked to the main PM account holders that have opted for the TARGET2 Value-added services for T2S). However, the contingency network does not fully replace the SWIFT network, as the connection between the users and their national central bank is not covered and relies on the national means agreed.

The daily volume of payments that can be processed is around 3.000, consisting of 2.300 (very) critical payments and 700 individual ancillary system transactions. A distinction is made between very critical payments, which have to be processed, and critical payments, where approval by the crisis

managers 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 payment functionality for all participants connected via the affected central banks.

8.5.1. Processing of payments

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

The national service desk, having access to the ICM backup screens via the contingency network, processes the payment instructions using the four-eyes principle. The settlement of the backup payments is monitored. The instructing parties receive feedback from the national service desk using the local contingency communication 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 backup 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.
- Liquidity transfers from PM accounts to DCAs can be processed via the contingency network. Liquidity transfers from DCAs to the main PM accounts can be processed only if the main PM account holder has opted for the TARGET2 value-added services for T2S.

- Non-repudiation for the messages transferred via the contingency network is ensured.

8.5.2. 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. Files for all the six different ancillary system settlement procedures implemented in TARGET2 are also supported by the contingency network. It should be taken into account that the daily volume of payments from ancillary system files that can be processed is 700 transactions. Furthermore, each file has a maximum size limit of 1MB. Files going beyond these limits are rejected.

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 the user. The central bank can verify the status of the sent files via the ICM and inform the ancillary system involved.

8.6. Failure of the T2S interface (T2SI)

In the event the transfer of liquidity from TARGET2 to T2S and/or from T2S to TARGET2, does not function properly, the participant may ask for the support of its national service desk. In such a situation the national service desk can perform a limited number of liquidity transfers between TARGET2 and T2S on behalf of the requesting participant. The detailed communication means are subject to the bilateral relationship between a participant and its central bank.

9. Contingency and business continuity testing

9.1. Scope

TARGET2 includes the Single Shared Platform (SSP), Proprietary Home Accounts (PHAs) and other applications used by Central Banks, ancillary systems (AS) and other entities which connect to and operate with the SSP and/or T2S Platform.

Central banks fall under the scope of the "Information security policy for TARGET2" approved by the Governing Council of the ECB and thus have a 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 critical, which are tested at regular intervals.

A SWIFT failure does not fall within the scope of the testing since the Governing Council accepted the residual risk of such an outage.

9.2. 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 user should at first rely on its own backup measures. The SSP offers contingency arrangements to overcome short interruptions on the side of participants and Central Banks to process (very) critical payments. Additionally Central Banks may offer their users other arrangements such as an Ancillary Systems' contingency tool and mandated payments.

9.3. Roles and responsibilities

Mandatory and optional contingency and business continuity tests for the SSP and central bank 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 non-critical 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.

9.4. 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 users, 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 Central Bank providing a PHA is expected to provide a test environment that is as similar as possible to the production environment.

9.5. 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, and there should be not more than one year between two tests.

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 17:30. The cut-off time for interbank payments is set at 15:30[73]. Exceptions are communicated in advance.

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

9.7. Testing contingency arrangements

9.7.1. For critical participants

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

[73] As of 01 July 2014.

- Backup contingency payments are used to fulfil pay-in obligations to CLS, to the EURO1 collateral account or to the EURO1 prefunding account (TARGET2-EURO1 liquidity-bridge). They replace the original payment.
- Backup liquidity redistribution payments allow the PM account holder 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.

Critical participants intending to use the backup payments feature or an additional arrangement offered by their Central Bank (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 Central Bank:

1) Requesting the activation of the backup functionality in live operations via its Central Bank and the sending of the respective backup payments as low value payments (less than €10, but different amounts) to pre-agreed accounts. Central Banks may offer their accounts to be used as addressee for payments, when no other test counterparty is available.
2) Central Banks 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.
3) 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.
4) Central Banks offering their ASs the AS contingency tool are expected to test its operational functionality.
5) Central Banks offering their critical participants mandated payments are expected to test its operational functionality.

Central Banks may decide – in cooperation with their 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, Central Banks 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.

9.7.2. For the SSP (contingency module testing)

The 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 Central Banks have access to the CM and can perform payments on behalf of their users. In this respect each user and each Central Bank 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. Central Banks should take into account their own processing requirements plus those of the user with the highest possible hourly number of such payments.

Although only Central Banks have direct access to the CM, also all 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 users to the Central Bank and the respective processing in the CM by the Central Bank. Users are expected to exchange their hourly maximum number of critical payments. Central Banks are expected to confirm the processed payments using a secure channel.

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 Central Bank 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 Central Banks and their users.

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

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.

In addition, every six months, the ECB organises live trial sessions for the CM. Each session involves a group of Central Banks; the Central Banks may also decide to involve users. On these days the SSP service desk activates the CM in the PROD environment in parallel with normal operations, with the twofold aim of verifying both the connectivity to the CM and the adequate set-up of users for live CM operations. Volume testing is not carried out.

9.8. Testing business continuity

9.8.1. For critical participants

Each 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 9.4, "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.

9.8.2. **For the 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, i.e., intra-regional failover and inter-regional failover. Such tests are by default performed in the PROD environment during weekends 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.

9.9. Critical participant exercise for AS migrating to T2S during migration phase

CSDs migrating their whole business to T2S are exempted of their testing obligations, as a critical AS participants in T2 as of the semester of their migration to T2S, if they don't use the AS interface anymore.

10. 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 as regards the SSP. For changes on the T2S platform cash related functionalities the Change and release management process described in the T2S Framework Agreement – Schedule 9 should be followed.

10.1. 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.

10.1.1. 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 13. Annual release timeline

10.1.2. 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 contact their respective national user groups.

- The first consultation aims to collect proposals for functional changes from all users. These changes are expected to be sufficiently detailed and to be beneficial for a large number of 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 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 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. When applicable, pricing elements 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 users and forms a final view on the content of the annual TARGET2 release, which is communicated shortly thereafter[74].

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 and returned.

10.1.3. Prioritisation and decision-making

When prioritising the various proposals received from 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

74 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.

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 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, users will be provided with the necessary information as to why a change was selected or discarded.

10.2. 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.

10.2.1. 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, "Fundamentals of procedures in abnormal situations", 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.

10.2.2. 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 always be installed first in the CUST environment and – to the extent possible – tested there. Where necessary due to the impact on the

users, an ICM broadcast will be sent to all users before the hot fix is implemented.

11. TARGET2 compensation scheme

11.1. Fundamentals

If there is a technical malfunction of TARGET2, participants can submit claims for compensation in accordance with the TARGET2 compensation scheme laid down in appendix II of the Harmonised Conditions for the opening and operation of a PM account, as well as on the appendix II of the Harmonised Conditions for the opening and operation of a DCA.

Unless otherwise decided by the Governing Council of the ECB, 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 participants may, however, use other legal means to claim for losses. If a TARGET2 participant 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 participant 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 participant 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 for the opening and operation of a PM account, as well as on the appendix II of the Harmonised Conditions for the opening and operation of a DCA.

11.2. Procedural rules

- 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, participants 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 Governing Council of the ECB and communicated to the participants, 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 participants. If the assessment entails a compensation offer, the participants 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 participants 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 SSP 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 might include: FIN messages (payments and liquidity transfers, including the ones sent to/from DCAs via the T2SI); FileAct messages (sent by an ancillary system via the ASI); InterAct messages (XML messages sent to one of the SSP modules or to the T2SI).

The rebuilding process should be done according with the following steps:

1) FIN messages can be retrieved and the FIN traffic reconciled (this would make up about 80% of the missing traffic).

Upon the FIN retrieval (from which DCAs related traffic will be excluded), 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 will label all pending payments as "highly urgent" and place them at the front of the queue of highly urgent payments.

2) The SSP service desk will inform the TARGET2 coordination desk of the completion of the former step.

3) In order to synchronise the turnover and balances between PM accounts and DCAs, the TARGET2 Coordination Desk will reconcile the positions on both euro transit accounts and will identify the missing payments (settled on the TARGET2 transit account on the T2S platform and missing in the T2S transit account on the SSP).[75]

Once the identification has been performed, the TARGET2 Coordination Desk will inform the Central Banks about the missing liquidity transfers, who, in turn, should inform the concerned participants about the impacted liquidity transfers and actions that will be carried out.

[75] TARGET2 and T2S should not close the business day until the transit accounts are synchronised. Notwithstanding, at the end-of-day, if DCA balances are zero, if auto-collateralisation has been reimbursed and if the TARGET2 transit account is zero, T2S might close the business day even if the SSP is facing a Restart after disaster. However, it should be ensured that all the necessary messages from T2S are resent to the SSP before (messages should be queued and processed by the SSP afterwards).

The following actions might be performed:

- For **liquidity transfers from PM accounts to DCAs** booked on T2S and in the SSP (Region 1) before the disaster but not in the SSP (Region 2) after the disaster, the Central Bank responsible for the debited PM account holder will debit the relevant PM account and credit the T2S transit, upon authorisation of the PM account holder. In case the PM account holder has opted for debit notifications, the notification related with the rebooking performed via the previous step should be disregarded.

- For **liquidity transfers from DCAs to PM accounts** booked on T2S and in the SSP (Region 1) before the disaster but not in the SSP (Region 2) after the disaster, the Central Bank responsible for the debited DCA will identify the outbound messages related with the liquidity transfers and resend them (via the GUI screen Cash > Liquidity > Immediate Liquidity Transfers > Search/List screen > Related Outbound Messages > Resend). In case the PM account holder has opted for credit notifications, the notification related with the rebooking performed via the previous step should be disregarded.

The above steps should all be achieved within two hours of the decision to failover.

4) After the completion of the former steps, a TARGET2 settlement managers' teleconference to agree the initiation of the resending of InterAct and FileAct messages (which represent about 20% of the missing traffic) should be held. This means that the SSP service desk will open the SSP for SWIFTNet services, i.e. FileAct and InterAct.

5) Ancillary systems should 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 (with the exception of the one related with liquidity transfers to/from DCAs). However, new FileAct and InterAct 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.

6) The processing of the missing FileAct and InterAct 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 signal the existence 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).

7) 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 FIN traffic. Any queued FIN payments will be processed. Also new FileAct and InterAct messages can then be sent by the users. If the CM was used, the transfer of balances from the CM to the PM will take place after the closure of the CM and the opening of the SSP for SWIFT FIN traffic.

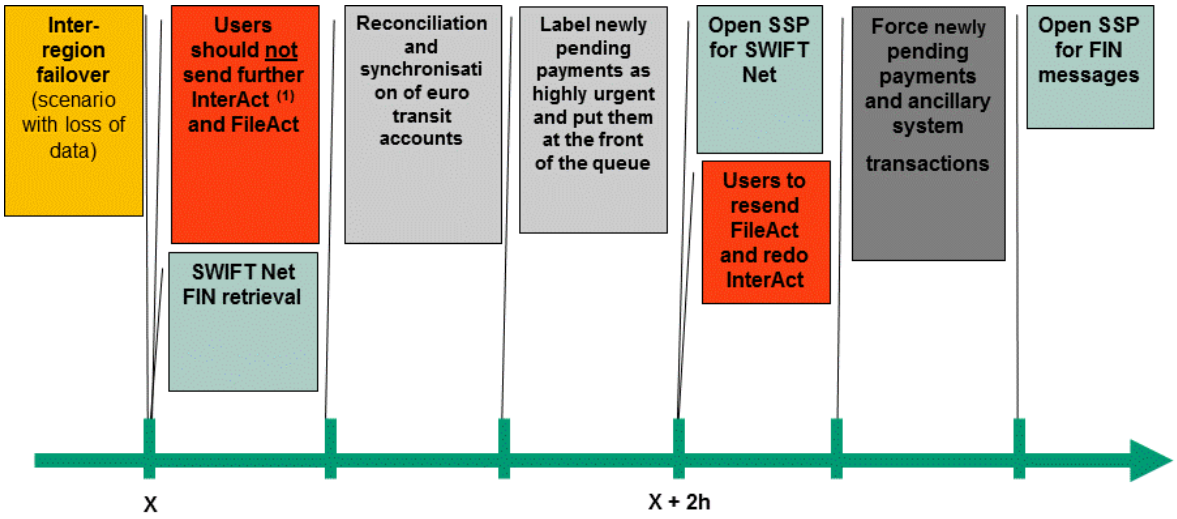

Diagram 23: Processes after inter-region failover with a loss of data

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 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[1]
Type of failing component	☐ Hardware ☐ Network[3] ☐ Human error	☐ Software[2] ☐ Infrastructure[4]
Date and time the incident started	ddmmyyyy / hh.mm	
Date and time the incident ended	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)

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

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

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

4 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 Principles for Financial Market Infrastructures set out certain responsibilities that must be fulfilled by the operators of a payment system. More specifically, Principle 17 relates to issues concerning the security and operational reliability of Financial Market Infrastructures such as systemically important payment systems.

Principle 17 states that "…an FMI should consider establishing minimum operational requirements for its participants. For example, an FMI may want to define operational and business continuity requirements for participants in accordance with the participant's role and importance to the system.""

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 (SEC/GovC/07/041).

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.

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 control 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[5] as the primary business location.[6] 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.[7]

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 aptly trained. The maximum period between tests should not exceed one

5 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.

6 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.

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

year.

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[8] 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 or equivalent) 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 or equivalent) responsible for the IT department within the critical participant. If a senior official is responsible for both, the business area and the IT department, one signature is sufficient.

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

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

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 the submission of this information is a material obligation and that submitting false, inaccurate or misleading information constitutes a breach of Article 34 (2) (c), 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 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

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

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, T2S Interface; (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

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

Some examples of the use of the Change Request Template

Annex V Glossary and Abbreviations

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 of the ECB 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, payment 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's 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)

Application-to-application (A2A)

A connectivity mode that enables the exchange of information between the SSP and T2S platform software application and the software application(s) of the users.

AS contingency tool

The ancillary system contingency tool is an instrument to facilitate the creation and handling

of XML messages. It is available to central banks only.

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

If a PM account holder becomes unavailable, it can fulfil its payment obligations to CLS and EURO1 and avoid liquidity concentration on its PM account by making backup payments via the ICM. Two kinds of backup payment are available:

- backup contingency payments, which are used to fulfil pay-in obligations to CLS, to the EURO1 collateral account or to the EURO1 prefunding account (TARGET2-EURO1 liquidity bridge);
- backup liquidity redistribution payments, which are intended to redistribute excess liquidity

accumulating on the PM account of the affected participant.

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 eight characters of the BIC. When used for addressing purposes, are called destination.

BIC-11

In addition to the first eight characters of the BIC, an optional branch code of three 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.

Book-entry system

A system which enables transfers of securities and other financial assets which do not involve the physical movement of paper documents or certificates (e.g. the electronic transfer of securities).

Broadcast via GUI

A broadcast is an information message simultaneously available in the GUI to a selected group of participants.

Broadcast via ICM

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

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 central bank acts as custodian for the other central banks with regard to the securities held in its domestic securities settlement system.

Central Bank Auto-collateralisation

Secured intraday credit provided by the central bank. Auto-collateralisation with a DCA holder is called client collateralisation.

Central counterparty (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.

Client collateralisation

Credit provided by a DCA holder to its clients in T2S through a collateralisation mechanism.

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.

Closed Group of Users (CGU)

A subset of customers grouped for the purpose of their use of the relevant Value-added Network service provider's services and products when accessing the T2S Platform.

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, following specifically agreed contingency processes and communication procedures.

Contingency module (CM)

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

Contingency network

Alternative network for routing payment traffic in the event of a SWIFT services failure. The contingency network is operated by the Eurosystem.

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 a PM account. The respective PM account holder 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.

Critical payment

See Box 4.

CRISP

SSP block of optional services for Central Banks. Provides billing services.

CRSS core reporting functions

As of November 2012, Core Requirements on Statistics and Storage (CROSS) and Customer Relationship and Knowledge of Systems (CRAKS1) have merged to form the CRSS core reporting functions. These consist of SSP services for central banks, to be used by them on a mandatory basis, for, among other things, archiving and storage activities, billing calculation, the provision of statistics on intraday credit, and profiling information. Support for customer relationships and knowledge of payment systems is provided by CRAKS3, which is also available in the CRSS.

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 management (CRM)

Term referring to the management by Central Banks of customer-oriented information related to the users (participants, Ancillary Systems, other customers e.g. NCB customers in HAM).

CSD participant

A customer of a CSD.

-D- *glossary*

Day trade phase

Is the period of time in TARGET2 between 7.00 and 18.00.

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 cash account (DCA)

A cash account in T2S opened in the books of a central bank.

Dedicated cash account holder (DCA holder)

An entity that has opened in T2S at least one dedicated cash account with a central bank.

Dedicated liquidity

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

Dedicated transit account

A cash account in the RTGS system and in T2S held and used by the responsible system operator to transfer funds between the two. The transit account opened within T2S is referred as RTGS dedicated transit account and the transit account opened within the RTGS system is referred as T2S dedicated transit account.

Delayed closing

A delayed closing is the prolongation of the day trade phase in TARGET2.

Delivery free of payment (DFP or DFOP)

A delivery of securities that is not linked to a corresponding transfer of funds.

Delivery versus payment (DVP)

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

Delivery with payment (DwP)

A type of instruction and settlement mechanism that requires a delivery of securities and a corresponding cash payment.

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 who may keep records on the ownership of these securities.

Direct debit

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

Direct participant

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.

Directly connected DCA holder

A DCA holder that has been authorised by its central bank to access T2S directly when using T2S services, i.e. without the central bank acting as a technical interface (which would in this case be termed an "indirectly connected DCA holder").

-E- *glossary*

Earmarking

The process of specifying that a quantity of a security in a securities account is only eligible for specific types of transactions or processes. For example, a CSD participant can earmark a securities position in a securities account or the complete account for use as eligible collateral.

EBA Clearing (EBA)

The company that maintains on behalf of its members the EURO 1 and STEP2 clearing systems.

ECB

European Central Bank

EEA

European Economic Area

Eligible assets

Asset that can be used as collateral in order to obtain credit.

Encryption

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

Eurosystem

The ECB and the NCBs of the EU Member States whose currency is the euro, as provided for in Article 1 of the Statute of the ESCB and of the ECB.

External guarantee limit

The cap on credit secured outside T2S that the DCA holder sets for its client. The external guarantee limit and the unsecured credit limit are identical from the T2S viewpoint, except for the sequence in which they are triggered. Usage of the external guarantee limit is triggered before client collateralisation.

-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 arrival is 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.

Graphical User Interface (GUI)

The interface that allows a user to interact with the T2S software application through the use of graphical elements (e.g. windows, menus, buttons and icons) on a computer screen, using the keyboard and mouse.

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 bank's 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
- for entities allowed to open PM accounts that are indirect PM participants (or do not participate in PM neither as direct participant nor as indirect participant)
- for PM 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 such as:

- the home accounting module (HAM);
- the reserve management module (RM);
- the standing facilities module (SF);
- the 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 the SSP via the internet.

Internet-based participant (IBP)

A participant with Internet-based access to its PM or HAM account.

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 of a 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.

ISO 20022

The international standard for financial services messaging, maintained by the International

Organization for Standardization (ISO).

-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 ECB

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 PM 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 central banks. 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 PM 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 PM account.

There are two kinds of liquidity transfers available in the SSP:

- 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 PM accounts at the start of the business day. Changes of standing orders become effective on the following business day.

There are three kinds of liquidity transfers available in the T2S platform:

- Immediate liquidity transfer order: An instruction to transfer a specified amount of money from one cash account to another cash account in real-time (i.e.) immediately on receipt of the instruction.
- Predefined liquidity transfer order: An instruction to transfer a specified amount of money from one cash account to another, to be executed only once at a defined time or at the time of a specific event.
- T2S standing liquidity transfer order: An instruction to transfer a specified amount of money from one cash account to another, to be executed on a regular basis at a defined time or at the time of a specific event in the T2S processing cycle until the order is changed.

-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. In particular, for example, an NCB sends a credit transfer (with specific message structure) on behalf of a failed direct participant (only in contingency situations). Mandated payments to technical accounts are not possible.

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 message 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 PM accounts opened to Central Banks 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 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).

NSP

Network Service Provider

NUG

National User Groups

-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 payment 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 PM 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.

PM 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).

Priority

In general, payments are settled immediately, if sufficient liquidity is available on the PM 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.

Privilege

A right, either granted or denied, to execute certain functions within an application, or to access and/or update certain data.

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 some National Central Banks outside of the SSP, for example: for entities that cannot have the status of direct participants in PM; for entities allowed to open PM accounts that are indirect PM participants (or do not participate in PM neither as direct participant nor as indirect participant); for PM 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 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 country where it 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 credit institution which has not fulfilled minimum reserve requirements (optional).

Relationship management application (RMA)

See *SWIFT relationship management application (RMA)*

Role

A group of privileges (see also *Privilege*).

RTGS

Real-time gross settlement system.

-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

An instruction to transfer regularly a given amount from one account to another account.

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

An 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

The “Business Identifier Code” of an institution connected to the SWIFT network (formerly “bank identifier code” for financial institutions).

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 SWIFT to manage the business relationships between financial institutions. RMA sets the message types that 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.

TARGET2-Securities (T2S)

The set of hardware, software and other technical infrastructure components through which the Eurosystem provides the services for CSDs and central banks that allow core, neutral and borderless settlement of securities transactions on a DvP basis in central bank money

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.

T2S actor

Either a contracting/participating CSD, CSD participant (a legal entity or, as the case may be, an individual) having a contractual relationship with the CSD for the processing of its securities settlement-related activities in T2S, a central bank, whose currency is available for settlement-related processing in T2S, or a client of a central bank having a contractual relationship with the central bank for the processing of its settlement-related cash-processing activities in T2S.

T2S operator

The legal and/or organisational entity/entities that operates/operate the T2S Platform. As part of an internal distribution of work within the Eurosystem, the Governing Council entrusted the 4CB with operating T2S on behalf of the Eurosystem.

T2S Party

Any legal entity or organisation interacting with T2S either directly or indirectly (i.e. through a CSD or CB in T2S).

T2SRC

TARGET2 Security Requirements and Controls.

T2S scope-defining set of documents

The set of documents defining the scope of T2S, composed of the URD, the UDFS, the GUI Business Functionality, the GFS Functional Chapter, the Dedicated Link Connectivity Specifications and the Data Migration Tool Specifications and Related Procedures.

T2S Service Desk

Single point of contact for the CSDs, the non-euro area CBs making their currency available to T2S, the Eurosystem CBs, the DCPs and the NSPs for handling al incidents, queries and requests related to T2S operational, functional or technical issues. For all cash-related issues, with the exception of

connectivity issues, the TARGET2 Organisational Framework applies.

T2S settlement currency

A currency for which T2S provides settlement in central bank money on T2S dedicated cash accounts for securities transactions.

T2S system entity

Either the T2S operator or a CSD or NCB for which a segregation of processing capabilities and data are required.

T2S system user

An individual or a technical process/application that can log into T2S with a login name and password. For example, a user may be an individual who has interactive access to T2S online functions or an application programme that requests services from T2S.

-U- *glossary*

Unsecured credit limit

The cap on unsecured credit in T2S that the payment/settlement bank sets for its client. The external guarantee limit and the unsecured credit limit are identical from the T2S viewpoint, except for the sequence in which they are triggered. Usage of the unsecured credit limit is triggered after client collateralisation.

User Handbook (UHB)

The document describing the way in which T2S users can make use of a number of T2S software functions that are available in a user-to-application (screen-based) mode.

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*

VAN-SP

Value-added Network service provider.

Very critical payment

See *Box 4*.

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. The payment message is warehoused until the relevant day trade phase of the SSP.

-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 to the SSP which is used in the context of payments processed via PM.