



EUROPEAN CENTRAL BANK
EUROSYSTEM

Information Guide for TARGET participants

Part 1 – Fundamentals

Version [4-0R.2023.NOV](#)

[March November](#) / 2023



Contents

1	Introduction	3
1.1	Purpose of the Information Guide for TARGET participants	3
1.2	Structure of the Fundamentals Infoguide	4
1.3	Relationship with other documentation	5
1.4	TARGET Infoguide change management	6
1.5	TARGET settlement services	6
2	General information	18
2.1	Governance structure	18
2.2	Organisational structure of TARGET operations	19
2.3	Communication flows and tools	23
2.4	Types of participation – euro	24
2.5	Types of connectivity	25
2.6	TARGET calendar – euro	26
2.7	Operational day schedule – euro	27
3	Fundamentals of incident management	30
3.1	Purpose and scope of Incident Management	30
3.2	Incident detection	30
3.3	Actors involved in incident management	31
3.4	Incident scenarios	31
3.5	External communication on TARGET incidents	32
4	Fundamentals of problem management	33
4.1	Purpose and scope of problem management	33
4.2	Actors involved in problem management process	33
4.3	Relationship with incident management and change, release and deployment management	33
5	Access management	35
	– Fehler! Verwenden Sie die Registerkarte 'Start', um TOC Heading dem Text zuzuweisen, der hier angezeigt werden soll.	1

5.1	Purpose and scope of access management	35
5.2	Access management activities by central banks	35
5.3	Access management activities by TARGET participants	36
6	Service request management	37
6.1	Retrieval from the Legal Archive	37
7	Business continuity management	38
8	Testing activities in TARGET	39
8.1	Overview of testing activities for TARGET	39
8.2	Test results and reporting	40
9	Information security management	41
9.1	Gathering and sharing information about the endpoint security of TARGET participants	41
10	Financial management	43
10.1	Accessing and receiving invoices	43
10.2	Payment of invoices	43
11	TARGET compensation scheme - euro	45
11.1	Purpose and scope	45
11.2	Procedural steps	45
12	General Data Protection Regulation	47
12.1	Background	47
12.2	Operational procedure	49
13	Annex	52
13.1	Annex I – Central banks in TARGET	52
13.2	Annex II – Data access request	53
13.3	Annex III – Legal archiving form	55
13.4	Annex IV – Terms of Reference – TARGET Crisis Communication Group	56

– Fehler! Verwenden Sie die Registerkarte 'Start', um TOC Heading dem Text zuzuweisen, der hier angezeigt werden soll.

1 Introduction

1.1 Purpose of the Information Guide for TARGET participants

The Information Guide for TARGET participants (hereinafter referred to as the Infoguide) aims to provide TARGET participants (credit institutions, ancillary systems, other entities settling in TARGET¹) with a comprehensive set of information regarding the functioning and operational procedures of TARGET settlement services during both normal and abnormal situations.

The Infoguide consists of four parts:

1. **Fundamentals**
2. CLM & RTGS
3. TIPS and
4. T2S Cash²

The **Fundamentals** part describes the aspects that apply similarly across TARGET settlement services, the **CLM & RTGS** part describes the specific procedures applicable to the operation of central liquidity management (CLM) and RTGS services, the **TIPS** part describes the specific procedures applicable to the TARGET Instant Payment Settlement (TIPS) service and the **T2S Cash** part describes the specific procedures applicable to T2S dedicated cash accounts (T2S DCAs).

While TARGET was developed to offer multi-currency services, this Infoguide describes all relevant procedures for the euro currency. For other currencies, the central bank making its currency available in TARGET³ is responsible for the relevant operational procedures and they are not covered in this Infoguide.

The TARGET Infoguide describes how the relevant legally binding documents and technical/functional documents translate into operational procedures. Its primary objective is to document procedures for live operations. However, it might also serve as a reference for operational and functional testing activities. [The TARGET Infoguide is publicly available on the ECB's website⁴.](#)

¹ Further information can be found in [Chapter 2.4](#).

² Please note that for TARGET2-Securities, this document only covers procedures for dedicated cash accounts (T2S DCAs) and their interplay with other TARGET settlement services. T2S specific procedures fall within the scope of the dedicated T2S Manual of Operational Procedures.

³ By signing a Currency Participation Agreement (CPA).

⁴ [At the following link: For professional use, section Participation/Registration > Supporting Documents > Information Guide for TARGET participants](#)

While the Infoguide might repeat content of other documentation where appropriate or make references to such documents (e.g. by means of links), functional and technical descriptions of TARGET are out of its scope.

All references throughout this document to "TARGET participants" refer to participants⁵ as well as other entities authorised to access their account. All references throughout this document to "TARGET users" refer to an individual or an application that can log into a settlement service with a login name and password.

The Infoguide is not a legally binding document, and its content confers no legal rights on TARGET users, operations or any person or entity. All times in this document refer to the local time at the seat of the [European Central Bank \(ECB\)CB](#), i.e. Central European Time (CET) / [Central European Summer Time \(CEST\)](#).

1.2 Structure of the Fundamentals Infoguide

The Fundamentals Infoguide is based on ITIL⁶ and starts with an introductory part (**Chapter 1**) to explain to the reader the purpose and structure of the Infoguide. This includes the relationship with other documentation, the change and approval process of the Infoguide and a brief introduction to the various services and components that make up the TARGET settlement services.

Chapters 2 to 4 contain general information on the fundamentals of the governance and operational framework and explain how that framework is applied to incidents and problems management.

Chapter 5 and 6 describe how access to the services and service requests are managed.

Chapter 7 addresses business continuity management.

Chapter 8 described testing activities in TARGET.

Chapter 9 addresses information security management and aspects related to operational risk management.

Chapter 10 describes the overall billing process for participants.

Chapter 11 describes the TARGET compensation scheme.

Chapter 12 describes the implications of the General Data Protection Regulation (GDPR) on TARGET.

⁵ As per the [TARGET Guideline](#), a "participant" means an entity that holds at least one MCA and may additionally hold one or more DCAs in TARGET, or an ancillary system.

⁶ Information Technology Infrastructure Library (ITIL) is a collection of best practices for IT service management with the aim to align IT services with business objectives. It improves IT support and service levels.

1.3 Relationship with other documentation

The Infoguide complements and is based on extracts of the documentation listed below. In the event of any discrepancy or contradiction between the Infoguide and the documents listed below, the most up-to-date version of the following documents will prevail.

Table 1
Relationship of Infoguide with other documentation

Document	Content
Guideline (EU) of the European Central Bank on a new-generation Trans-European Automated Real-time Gross Settlement Express Transfer system (TARGET) and repealing Guideline ECB/2012/27	The legal framework for TARGET, with which the Infoguide must be fully compliant.
Harmonised conditions for participation in TARGET (Annex I of the TARGET Guideline)	These are the conditions for opening and operating a main cash account (MCA) /RTGS DCA/TIPS DCA/T2S DCA AS technical accounts in TARGET. The document describes the mutual rights and obligations of participants in TARGET and their respective central banks. Each central bank adopts arrangements implementing the harmonised conditions. These arrangements exclusively govern the relationship between the relevant central bank and its participants in respect of the processing of central bank operations in CLM and cash transfer orders in the CLM and/or RTGS and/or TIPS and/or T2S.
Connectivity Guide	The Connectivity Guide describes the process of connecting to ESMIG through a network service provider (NSP).
User Detailed Functional Specifications (UDFS)*	The UDFS describe the functioning of the different services and common components from a technical perspective: ESMIG UDFS CRDM UDFS CLM UDFS RTGS UDFS TIPS UDFS ECONS II UDFS BDM UDFS BILL UDFS DWH UDFS T2S UDFS MPL UDFS
User Handbooks (UHBs)	The UHBs describe the functionalities available in user-to-application (U2A) mode via the Graphical User Interfaces (GUIs) of the various services and common components: CRDM Handbook CLM Handbook RTGS Handbook TIPS Handbook ECONS II Handbook BDM Handbook BILL Handbook DWH Handbook T2S UHB
TARGET services registration and onboarding Guide	The TARGET services registration and onboarding Guide is there to help users complete the TARGET registration forms. It also describes the onboarding process that must be followed by participants wishing to connect to TARGET for the first time.
TARGET Services pricing guide	The TARGET Services pricing guide includes the pricing schemes for euro TARGET settlement services and gives a detailed explanation of the pricing and billing principles for TARGET. Non-euro central banks making their currency available in TARGET might apply a different pricing.
T2S operational documentation	Of particular relevance is the T2S Manual of Operational Procedures (T2S MOP).

Note: It should be noted that, even if some functionalities are available from a technical perspective, from a policy perspective there might be some constraints on the usage of those functionalities (as reflected in the TARGET Guideline).

– Fehler! Verwenden Sie die Registerkarte 'Start', um Heading 1 dem Text zuzuweisen, der hier angezeigt werden soll.

1.4 TARGET Infoguide change management

The Infoguide is reviewed and updated once a year (in June) according to the releases of the relevant services. For CLM, RTGS and T2S the main annual release is scheduled for the second weekend of June, while the yearly minor release is scheduled for the third weekend of November. For TIPS, the main annual release takes place in the week following the third weekend of November. An optional release may also be planned if needed, with deployment following the second weekend in June.

More information on the change, release and deployment procedures for each service and the common components can be found in the relevant chapters of the three service-specific parts of the Infoguide (CLM and RTGS, TIPS, and T2S Cash). Ad hoc updates of the Infoguide, if required, will be initiated outside of the annual review, in another timeframe as needed. Proposals for changes to the Infoguide may be initiated by the central banks, the TARGET settlement services-providing central banks, and TARGET participants.

1.5 TARGET settlement services

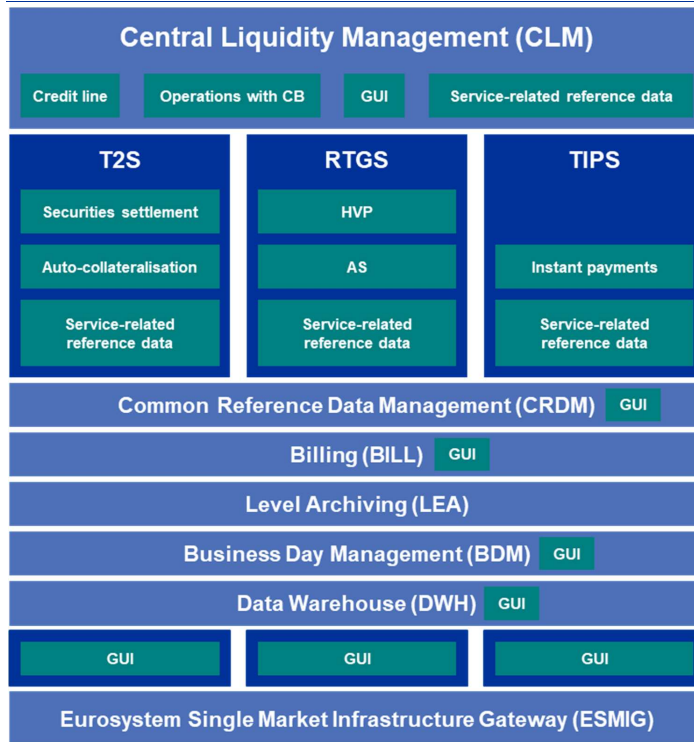
The Eurosystem provides market infrastructures for real-time interbank and customer payments and ancillary system (AS) transactions, as well as for the settlement of securities and instant payments. These infrastructures have been developed and are operated by the 4CB on behalf of the Eurosystem. TARGET settlement services consist of:

1. Central liquidity management (CLM, including central bank services);
2. Real-time gross settlement (RTGS);
3. TARGET2-Securities; and
4. TARGET Instant Payment Settlement (TIPS).

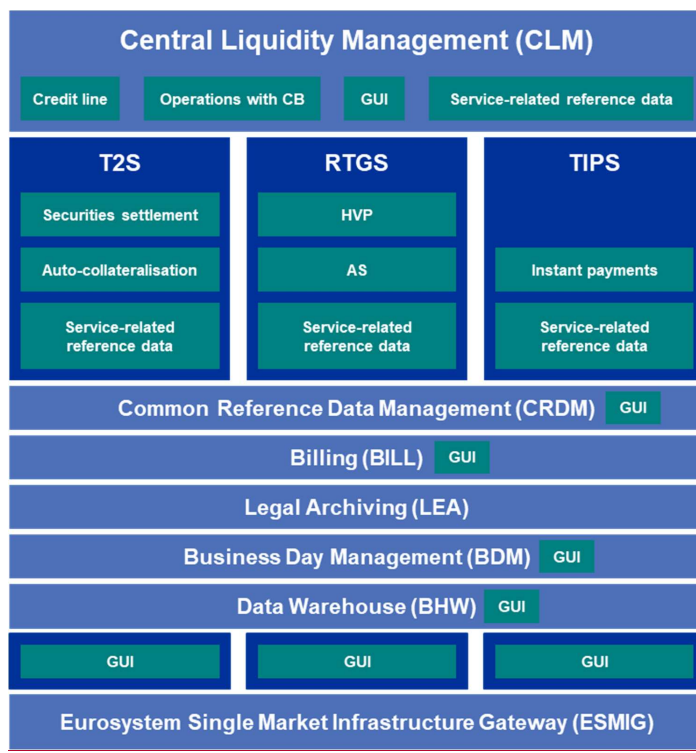
The services mentioned above are supported by common components (see [Figure 1 – High-level functional domains](#)).

Figure 1
High-level functional domains

Kommentiert [A1]: Updated typo : "Level" with "Legal"



– Fehler! Verwenden Sie die Registerkarte 'Start', um Heading 1 dem Text zuzuweisen, der hier angezeigt werden soll.



1.5.1 Central Liquidity Management

Central Liquidity Management (CLM) offers a centralised mechanism for the monitoring and management of liquidity. Central bank operations (CBOs) are managed in CLM. CBOs include the following operations: update of credit line (cash-side); marginal lending and overnight deposits (summarised as standing facilities⁷), cash withdrawals and cash lodgements, monetary policy operations other than standing facilities (e.g. open market operations such as main refinancing operations or longer-term refinancing operations), debiting of the invoiced amount, interest payment orders linked to marginal lending, overnight deposits, minimum reserves, excess reserves and for accounts subject to other purposes of interest calculation, and any other activity that a CB initiates in its capacity as CB of issue. To ensure an adequate provision and clear allocation of liquidity for the different settlement purposes across all TARGET settlement services and accounts, CLM offers a wide range of features such as instruments for liquidity management and information tools

⁷ Setting up and reverse transaction of overnight deposit are activities that can be carried out by the CLM account holder itself.

for liquidity monitoring purposes. MCA holders are responsible for their own liquidity management and for the monitoring of settlement processes on their account(s). They may also authorise another party to perform these tasks on their behalf.

The central source of liquidity in CLM is the main cash account (MCA), upon which CBOs are settled and to which the credit line is provided. If the participant owns multiple MCAs, the credit line is linked to only one MCA – the Primary MCA⁸. The end-of-day balance on MCAs should be zero or positive. However, if the total balance of the MCAs shows a negative balance at EOD, it must be covered with credit lines and liquidity held in DCAs. If the CLM account holder is not authorised for automatic marginal lending, a spillover notification is sent to the responsible CB. It is the responsibility of the CB to ensure that the MCAs have no negative balance before EOD.

The available liquidity can be distributed to cash accounts in RTGS, TIPS and T2S by means of liquidity transfer orders. To calculate fulfilment of minimum reserve requirements and automatic marginal lending, the end-of-day balances on all relevant accounts (MCAs and DCAs) are taken into account.

Connectivity to CLM is possible in user-to-application (U2A) mode via the CLM Graphical User Interface (CLM GUI) and/or in application-to-application (A2A) mode via ISO 20022 compliant XML messages.

The following categories of accounts can be opened in CLM for TARGET participants:

- MCAs;
- overnight deposit accounts; and
- marginal lending accounts.

Cash transfer orders in MCAs:

The following cash transfer orders can be processed in MCAs, either between accounts within CLM (intra-service) or between accounts in CLM and other settlement services (inter-service). Note that participants can instruct only MCA-to-MCA liquidity transfer orders for MCAs belonging to the same MCA liquidity transfer group.

Table 2
Cash transfer orders in MCAs

Cash transfer order type	Message identifier and name	Intra-/Inter-service
Liquidity transfer order	Camt.050 LiquidityCreditTransfer	Both

⁸ Primary MCA is the legal term according to the TARGET Guideline definitions. Note that Primary MCA is also referred to as Default MCA in the Functional Documentation.

1.5.2 Real-time gross settlement

Real-time gross settlement (RTGS) is designed for the real-time gross settlement of interbank and customer payments and ancillary system (AS) settlement. These transactions are settled on dedicated cash accounts (RTGS DCAs) that must always have a zero or positive balance.

RTGS offers a wide range of features to execute real-time payments and AS transfers in an efficient manner (e.g. reservations, priorities and optimisation algorithms). RTGS DCA holders are responsible for their own liquidity management and for the monitoring of settlement processes on their account(s).

RTGS actors can communicate with the RTGS service in:

- A2A, by exchanging single messages and files, using XML messaging based on the ISO 20022 standard; and/or
- U2A, which allows users to access specific functionalities through the dedicated RTGS GUI.

The following categories of accounts can be opened in RTGS for TARGET participants:

- RTGS DCA
- RTGS sub-account
- AS guarantee funds account
- AS technical account

Cash transfer orders in RTGS:

The following cash transfer orders can be processed in RTGS, either between accounts within RTGS (intra-service) or between accounts in RTGS and other settlement services (inter-service). Note that participants can instruct only RTGS DCA to RTGS DCA liquidity transfer orders for RTGS DCAs belonging to the same RTGS liquidity transfer group.

Table 3
Cash transfer orders in RTGS DCAs

Cash transfer order	Cash transfer order type	Message identifier and name	Intra-/Inter-service
Credit transfer order for a payment return	Interbank payment	Pacs.004 PaymentReturn	Intra
Credit transfer order for a customer payment	Customer payment	Pacs.008 CustomerCreditTransfer	Intra
Credit transfer order for an interbank payment	Interbank payment	Pacs.009 FinancialInstitutionCreditTransfer	Intra
Direct debit order for an interbank payment	Interbank payment	Pacs.010 FinancialInstitutionDirectDebit	Intra
AS transfer order	AS transfer order	Pain.998 ASTransferInitiation	Intra
Liquidity transfer order	Interbank payment	Camt.050 LiquidityCreditTransfer	Both

1.5.3 TARGET2-Securities

TARGET2-Securities (T2S) is a single, pan-European platform for securities settlement in central bank money. It provides harmonised and commoditised 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 transactions across all markets in which T2S operates. T2S integrates, in a single technical platform, both securities accounts – held with one or more CSDs – and T2S DCAs held with the respective central banks. Legally, euro denominated T2S DCAs (hereafter referred to as T2S DCAs) fall under the legal and operational perimeter of TARGET. This means that legal issues associated with T2S DCAs are included in the TARGET Guideline and that the operational procedures applying to T2S DCAs are covered by the TARGET operational framework.⁹

The following categories of accounts can be opened in T2S for TARGET participants:

- T2S DCA

Cash transfer orders in T2S-DCAs:

The following cash transfer orders can be processed in T2S-DCAs, either between accounts within T2S (intra-service) or between accounts in T2S and other settlement services (inter-service). Note that participants can instruct only T2S DCA to T2S DCA liquidity transfer orders for T2S DCAs belonging to the same participant or for which the same MCA has been designated.

⁹ However, some operational procedures are applicable at T2S level and therefore relevant procedures for DCA holders can also be found in the T2S MOP.

Table 4

Cash transfer orders in T2S DCAs

Cash transfer order type	Message identifier and name	Intra-/Inter-service
Liquidity transfer order	Camt.050 LiquidityCreditTransfer	Both

1.5.4 TARGET Instant Payment Settlement

TARGET Instant Payment Settlement (TIPS) is a harmonised and standardised pan-European service for settling payments instantly in central bank money, with high capacity and 24/7/365 availability.

While technically hosted by TIPS, legally, euro denominated TIPS DCAs and TIPS AS technical accounts (TIPS ASTAs) fall under the legal and operational perimeter of TARGET. This means that legal issues associated with TIPS euro DCAs/ASTAs are included in the TARGET Guideline and that the operational procedures applying to these are covered by the TARGET operational framework, mainly composed of the Infoguide.

The following categories of accounts can be opened in TIPS for TARGET participants:

- TIPS DCA; and
- TIPS AS technical account.

Cash transfer orders in TIPS:

The following cash transfer orders can be processed in TIPS, either between accounts within TIPS (intra-service) or between accounts in TIPS and other settlement services (inter-service):

Table 5

Cash transfer orders in TIPS DCAs

Cash transfer order type	Message identifier and name	Inter-/Intra-service
Positive recall answer	Pacs.004 PaymentReturn	Intra
Instant payment	Pacs.008 CustomerCreditTransfer	Intra
Liquidity transfer order	Camt.050 LiquidityCreditTransfer	Both

TIPS also offers the Mobile Proxy Lookup (MPL) service. The MPL service in TIPS maps mobile phone number proxies to IBANs. It allows end users (i.e. customers of

TIPS actors) to send payment execution requests to their payment service provider (PSP) by identifying the payee using a proxy¹⁰.

1.5.5 Common components

TARGET settlement services are supported by the following main common components:

1. Eurosystem Single Market Infrastructure Gateway;
2. Common Reference Data Management;
3. Data Warehouse;
4. Billing;
5. Business day management; and
6. Legal archiving.

1.5.5.1 Eurosystem Single Market Infrastructure Gateway

The Eurosystem Single Market Infrastructure Gateway (ESMIG) allows users to connect to TARGET settlement services and common components, as well as the Mobile Proxy Lookup (MPL) service in TIPS. As it is network service provider (NSP) agnostic (i.e. it does not rely on network specific features), ESMIG allows users to connect to all TARGET settlement services, via both A2A and U2A (via GUI), through a single certified NSP.

The communication format for all TARGET settlement services is ISO 20022 compliant messaging. Furthermore, ESMIG protects the TARGET settlement services and common components against intrusion and unauthorised access by means of authentication, authorisation and user management features, thus ensuring that a trusted party transmits the inbound communication through a secure channel.

1.5.5.2 Common Reference Data Management

Common Reference Data Management (CRDM) allows for the creation, maintenance and deletion of common reference data¹¹ relating to parties, cash accounts, rules and parameters across TARGET services.

¹⁰ For the time being no specific arrangements for MPL will be put in place due to the fact that the service is not extensively used at present. The criticality of the service and the need to develop specific operational procedures will be assessed at a later point in time.

¹¹ A common reference data object is a set of logically related, self-consistent information, such as a party or a cash account.

In U2A mode, CRDM allows full maintenance of all reference data objects. In A2A mode, a subset of functions is available, and CBs can also make use of a Data Migration Tool (DMT) for a subset of data objects.

Reference data changes are propagated to the relevant TARGET service(s) on a daily basis; however, the changes become effective on their activation/value date. Specific data changes (e.g. blocking of parties and cash accounts) are propagated with immediate effect to all settlement services when required by specifying the valid from date as immediate. Further information on the propagation of reference data can be found in the relevant chapters of the CLM & RTGS, TIPS and T2S Cash parts.

The scope of data a CRDM user can manage depends on the party the user belongs to and the access rights and privileges granted to the user. The data scope is based on the hierarchical party model, under which:

- (a) Users of the TARGET Service Desk have visibility on all reference data;
- (b) CB users have visibility on reference data of the central bank and its users community; and
- (c) Party users have visibility on reference data linked to the same party and to parties they have been authorised by (e.g. co-managed parties).

1.5.5.3 Data Warehouse

The Data Warehouse (DWH)¹²¹³ stores business information and data derived from CLM, RTGS, T2S and the contingency solution (ECONS II), as well as the CRDM, BILL and BDM.

The DWH allows data consolidation and reporting at different aggregation levels. Users can make use of queries and reports. Depending on their data scope, authorised users have access to a subset of the data available in the DWH. The collected information is available from D+1 and is kept for at least ten years.

1.5.5.4 Billing

The Billing (BILL) component provides functionalities for the aggregation of daily billable items, their enrichment into invoice data and the centralised creation and management of invoices for all TARGET settlement services. Each service and common component identifies the billable items and communicates them to billing on a daily basis. By default, the billing period is set as a calendar month. However, since there is daily gathering and enriching of billable items, it is possible for BILL to also generate invoices on flexible billing periods in exceptional circumstances.

¹² The Data Warehouse does not apply to TIPS.

¹³ ~~Full scope of T2S dData migration to DWH is foreseen in June 20234, is scheduled for DWH as of June 2023--~~

TARGET users can access their billing information via the BILL GUI. More information can be found in [Chapter 10 "Financial management"](#) of this document.

1.5.5.5 Business Day Management

The CRDM for each relevant service or component can be used to define Operating Day Types as default sets of events with specific planned execution times, predecessor dependencies and specific processes to be activated for each event.

At business date-day change, the proper Operating Day Type is loaded from the CRDM to the Business Day Management (BDM) common component, thus allowing for the automatic generation of the current business day schedule (Scheduler List) for each service or component upon start-of-day (SoD).

The BDM manages the Scheduler Lists generated based on CRDM data.

For each service or component, calendar data includes the opening days (with specific Operating Day Types) and closing days that can optionally be defined as currency-based (i.e. different currencies in TARGET can have different opening days as well as business day schedules). The maintenance of Operating Day Type and calendar elements is performed in the CRDM.

Modifications to the Operating Day Type structure are made effective after being loaded in the Scheduler List.

1.5.5.6 Legal Archiving

The Legal Archiving (LEA) component collects all the information subject to legal archiving requirements: i.e. all incoming and outgoing business transactions from and to participants as well as relevant reports such as account statements. The information from TARGET, including common components, will be stored in LEA in its original content and format and can be retrieved by submitting a service request to the relevant TARGET Service Desk within its data retention period of ten years, with the exception of certain TIPS data¹⁴ that have a validity of three months. LEA is not directly accessible to central banks and participants. However, a request may be submitted to the responsible National Service Desk (NSD). Data can be retrieved by the TARGET Service Desk for a period of ten years.¹⁵

¹⁴ For TIPS, instant payment transactions, liquidity transfers, status message data and reference data are archived for a period of exactly ten years. Authentication and security data are archived for a period of exactly three months.

¹⁵ TARGET2 data can still be requested for a period of ten years after the dismantling of TARGET2 in March 2023.

1.5.6 Contingency solution

In the unlikely event that a severe incident occurs, CLM and RTGS services might be affected by a prolonged outage, which could even stretch across a few days. A contingency solution (also known as the Enhanced Contingency Solution, ECONS II) has been developed in order to enable the Eurosystem to manage such extreme situations in an effective way to mitigate systemic risk.

Connection to ECONS II is mandatory for all i) Eurosystem central banks, ii) connected central banks (if they have participants that are required to connect to ECONS II) and iii) **critical** participants and critical ASs, and for those **participants/users** processing very critical payments in CLM and RTGS. In the medium term (i.e. two years after TARGET commenced live operations) connectivity to ECONS II will become mandatory for all TARGET participants.¹⁶

ECONS II is designed to be multi-currency and provide contingency settlement in central bank money (i.e. for the euro and other currencies settling in TARGET).

ECONS II should be activated in the event the specified Recovery Time Objective (RTO \leq 2 hours) of CLM and RTGS cannot be met or if decided by the central banks in TARGET.

The contingency solution aims to address the situation where the CLM and/or the RTGS component are unavailable. Once activated, ECONS II will always substitute both the CLM and the RTGS components for contingency settlement. The settlement of transactions in a contingency session is performed on accounts created in CRDM¹⁷ for contingency settlement, with a starting balance of zero. The liquidity injected by the central banks and used for processing in the contingency solution must be based on already available collateral¹⁸ or newly provided collateral.

The contingency solution offers:

- real-time gross settlement in central bank money for cash transfer orders and AS ancillary system transactions;
- liquidity monitoring functionalities to support the contingency settlement;
- control functions that allow the responsible central bank to monitor and prioritise payments to facilitate the processing of the most critical transactions;
- queries and reporting tools to support monitoring and reconciliation activities;
- a business day change process allowing for contingency sessions spanning over multiple business days should this be necessary; and

¹⁶ As of March 2025, all RTGS DCA holders and AS using RTGS are required to establish a direct connection to ECONS II.

¹⁷ These accounts are daily propagated to ECONS II.

¹⁸ Collateral already used for intra-day credit is not part of the available collateral.

- central banks the possibility to make local reference data changes with immediate effect (i.e. blocking/unblocking of a payment bank's contingency account or contingency technical account).

The contingency solution makes use of the following common components:

- Eurosystem Single Market Infrastructure Gateway (ESMIG);
- Common Reference Data Management (CRDM);
- Legal Archiving (LEA); and
- Data Warehouse (DWH).

ECONS II was designed as a non-similar facility to back up CLM and RTGS.

Note that contingency throughput may be limited due to the following reasons:

- fresh liquidity must be provided;
- application of the Non-Repudiation of Origin (NRO) mechanism;
- ECONS II capacity is about 40,000 transactions per day;
- ancillary system files can be processed using AS settlement procedure A when sent in A2A by the central bank on behalf of the ancillary system.

Note also that while ECONS II does not offer a queuing mechanism, the transactions are prioritised and processed by the central banks according to their criticality.¹⁹ The central banks process the transactions by agreeing/disagreeing in the ECONS II GUI.

¹⁹ Categories of payments subject to contingency processing.

2 General information

2.1 Governance structure

2.1.1 CLM, RTGS and TIPS

The governance structure of CLM, RTGS and TIPS is defined in the [Guideline of the European Central Bank on a new-generation TARGET](#), which sets out the general legal framework. Three levels of governance are established, corresponding to the three levels of responsibility described in the following table.

Table 6
Governance structure of TARGET

Level 1 Governing Council	Level 2 Technical and operational management body	Level 3 Level 3 NCBs
1. General provisions		
Final competence in relation to all TARGET issues, in particular the rules for decision-making in TARGET, and responsible for safeguarding the public function of TARGET	Conducting technical, functional, operational and financial management tasks in relation to TARGET and implementing the rules on governance decided by Level 1	Taking decisions on the daily running of TARGET based on the service levels defined in the agreement referred to in Article 7(6) of the Guideline
2. Pricing policy		
<ul style="list-style-type: none">Deciding on pricing structure/pricing policyDeciding on pricing envelopes	<ul style="list-style-type: none">Conducting regular reviews of pricing structure/pricing policyDrafting and monitoring pricing envelopes	(Not applicable)
3. Financing		
<ul style="list-style-type: none">Deciding on rules for the financial regime of TARGETDeciding on financial envelopes	<ul style="list-style-type: none">Drafting proposals for the main features of the financial regime as decided by Level 1Drafting and monitoring financial envelopesApproving and/or initiating instalments paid by Eurosystem CBs to Level 3 for provision of servicesApproving and/or initiating reimbursement of fees to the Eurosystem CBs	Providing cost figures to Level 2 for the service provision
4. Service level		
Deciding on the level of service	Verifying that the service was delivered in accordance with the agreed service level	Delivering the service in accordance with the agreed service level
5. Operation		
	<ul style="list-style-type: none">Deciding on the rules applicable to incidents and crisis situationsMonitoring business developments	Managing the system based on the agreement referred to in Article 7(6) of the Guideline
6. Change and release management		
Deciding in case of escalation	<ul style="list-style-type: none">Approving change requestsApproving release scopingApproving the release plan and its execution	Assessing change requests Implementing change requests in line with the agreed plan

7. Risk management		
<ul style="list-style-type: none"> Approving the TARGET Risk Management Framework and the risk tolerance for TARGET and accepting remaining risks Assuming ultimate responsibility for the activities of the first and second lines of defence Establishing the organisational structure for roles and responsibilities related to risk and control 	<ul style="list-style-type: none"> Conducting the actual risk management Conducting risk analysis and follow-up Ensuring that all risk management arrangements are maintained and kept up to date Approving and reviewing the business continuity plan as outlined in the relevant operational documentation 	Providing the necessary information for risk analysis according to Level 1/Level 2 requests
8. System rules		
Establishing and ensuring adequate implementation of the European System of Central Banks legal framework for TARGET, including the Harmonised Conditions for participation in TARGET	(Not applicable)	(Not applicable)

2.1.2 T2S

The T2S Governance structure differs from that of CLM, RTGS and TIPS due to the close involvement of central banks and CSDs in the governance framework. The Governance structure of T2S is defined in the Guideline of the European Central Bank on TARGET2-Securities (ECB/2012/13 as well as 2012/473/EU).

Similar to the governance of CLM, RTGS and TIPS, three levels with respective roles and responsibilities can be distinguished for T2S Cash:

Table 7
Governance structure of T2S

Level 1 Governing Council	Level 2 Market Infrastructure Board (MIB)	Level 3 4CB
<i>Responsibility</i>		
Direction, overall management and control of T2S Ultimate decision-making in relation to T2S and allocation of tasks not specifically attributed to Levels 2 or 3	Day-to-day management of T2S Relationships with market stakeholders, the 4CB and the ECB Governing Council	Decision-taking on the daily running of the system Managing T2S

2.2 Organisational structure of TARGET operations

2.2.1 National Service Desks

Each central bank is fully responsible for business relationships with the participants in its own TARGET component system and runs a National Service Desk (NSD) to help them meet their respective obligations. In line with this, each central bank

defines its national support level for its community, during both normal and abnormal situations.

The NSD is the single point of contact for their community participants and is responsible for answering queries, servicing requests and handling incidents.

In normal situations, all NSDs remain reachable and provide support to their community during standard support hours, which run from 07:00 to 18:15 ~~CET~~ during TARGET business days (07:00-18:30 on the last day of the reserve maintenance period for the euro). **Note** that a different calendar might apply to non-euro currencies settling in TARGET.

During standard support hours, the NSDs:

- take all necessary actions within their remit to ensure the smooth operation of TARGET;
- provide support to their community and the other central banks in TARGET for the processing of standard business (e.g. responding to queries, service requests, acting on behalf, communication).

In general, the NSDs are responsible for, among other things:

- providing business support to their participants (e.g. entities holding an MCA and/or DCAs and ancillary systems), including the management of relevant reference data;
- business monitoring (e.g. monitoring of cash transfer order processing with the aim of detecting liquidity problems or participant-related problems);
- operational monitoring to detect functional or operational problems (e.g. real-time monitoring of message flows in national applications, perhaps to detect a halt in processing or slow processing);
- dealing with authorisations for subscription to the Closed Group of Users (CGUs) of NSPs; and
- handling local contingency arrangements and abnormal situations covered by this document.

2.2.2 TARGET Crisis Communication Group

~~The experience gathered from the TARGET-Services incidents in 2020 highlighted the need to change the flow of communication in times of major incidents from one-directional to bi-directional. This is because it is important for TARGET crisis managers to receive feedback from market participants on whether the information latter are receiving is sufficiently clear and to reliably address their most urgent questions.~~

Kommentiert [A2]: For info:
Added as reference and amended

The TARGET Crisis Communication Group (TC2) was set up to strengthen, and make more direct, communication towards market participants, as well as to open an additional channel whereby crisis managers can receive valuable information during a major incident directly from the participants²⁰. The Terms of Reference of the TC2 can be found in [Annex IV](#). It is important to highlight that the **management of the incident itself is not under the scope of this group and remains in the hands of the crisis managers.**

Composition

The **TC2 comprises** all crisis managers (including the [3CB-4CB](#) crisis managers) and representatives from TARGET critical participants ~~to that~~ have expressed their interest in taking part in this group (on a voluntary basis). TC2 calls are **chaired by the ECB crisis manager**. The NSPs may also be involved, depending on the nature of the crisis scenario (i.e. incidents related to or affecting connectivity).

Conference calls of the TC2 group

- A TC2 conference call is triggered only upon the **decision of crisis managers in cases of severe incidents**, either due to the duration of the incident, the uniqueness of the scenario, or the impact the incident could have on the financial markets.
- For example, the TC2 may be **called in the event of**:
 - an intra/inter-region failover;
 - long-lasting incidents;
 - successful cyberattack affecting the integrity of the system;
 - other scenarios identified and agreed by the crisis managers.
- **The time for involving the TC2** as well as the frequency of TC2 calls during an ongoing incident would also be decided by the crisis managers on a case-by-case basis. Note that **the TC2 will not be involved immediately upon the detection of an issue, but at a later stage** when the full picture of the impact and potential workarounds or solutions are clearer.

²⁰ ~~The experience gathered from the TARGET Services incidents in 2020 highlighted the need to change the flow of communication in times of major incidents from one-directional to bi-directional. This is because it is important for TARGET crisis managers to receive feedback from market participants on whether the information latter are receiving is sufficiently clear and to reliably address their most urgent questions.~~

- **During TC2 calls**, market participants will have the opportunity to raise **questions** or to obtain **clarifications** on points that have not been covered, or not sufficiently covered, in communications shared previously. Moreover, the **crisis managers may receive valuable information** directly from market participants relating to the status of their business, which would allow the crisis managers to further enrich the information shared at the next update.
- **TC2 members will have no advantage in terms of communication.** If additional information is disclosed to TC2 members in response to their questions, the same information shall also be shared with the rest of the community in the next communication.
- The TC2 does not replace any existing groups that national central banks may have already put in place to activate in times of crisis with their national community.
- **During TC2 calls:**
 - market participants will have the opportunity to raise questions or to obtain clarifications on points that have not been covered, or not sufficiently covered, in communications shared previously;
 - the crisis managers invite the TC2 members to bring to their attention valuable information relating to the status of their business, which would subsequently allow the crisis managers to further enrich the information shared at the next update.
- **Attendance at TC2 calls is voluntary** for market participants and NCB crisis managers. The **ECB and the 3CB 4CB crisis managers shall always be present** during such calls.
- As TARGET crisis managers are available 24/7, the same principle will apply to the TC2 and as such, the participants could be called at any time.
- Connectivity tests and simulation exercises will be organised by the ECB in order to test the proper functioning of the tool and to simulate the process to be followed in the event of an incident.

2.2.3 TARGET Service Desks

The 4CB run the following three service desks (collectively referred to as TARGET Service Desks), dedicated to all TARGET-related operational, functional, or technical issues:

1. the T2 Service Desk, responsible for CLM and RTGS (as well as ECONS II in the event of contingency);
2. the TIPS Service Desk, responsible for TIPS; and
3. the T2S Service Desk, responsible for T2S.

– Fehler! Verwenden Sie die Registerkarte 'Start', um Heading 1 dem Text zuzuweisen, der hier angezeigt werden soll.

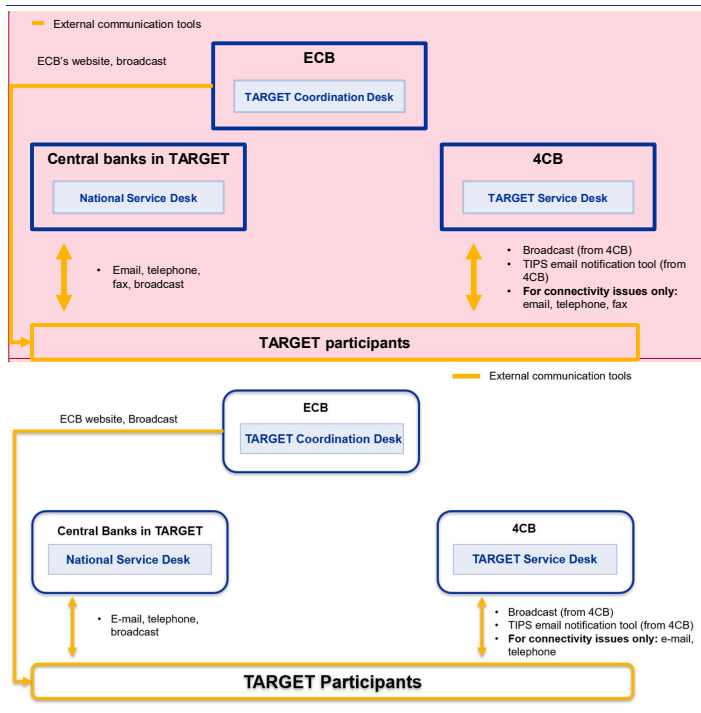
Support for common components is provided by all three Service Desks.

For connectivity-related incidents only, TARGET participants as well as other entities authorised to access their account (e.g. co-managers and TIPS instructing parties) may also contact the relevant TARGET Service Desk directly. Upon request, the contact details can be provided by the responsible NSD. In general, the responsible NSD remains the first contact point.

2.3 Communication flows and tools

The diagram below shows the information flows in normal as well as abnormal situations.

Figure 2
Communication flows and tools



Kommentiert [A3]: Removed fax.

The NSD is the single point of contact for its national user community, with the following exception:

Connectivity issues

– Fehler! Verwenden Sie die Registerkarte 'Start', um Heading 1 dem Text zuzuweisen, der hier angezeigt werden soll.

All TARGET participants are allowed to contact the TARGET Service Desks directly or may be contacted by the TARGET Service Desks in case of connectivity problems. The relevant TARGET Service Desk informs the responsible NCB when opening a ticket for its participant without undue delay. If the participant is unsure whether it qualifies as a connectivity issue, it should contact its responsible NSD first. If a TARGET Service Desk needs to contact a TARGET participant for connectivity-related incidents, the contact details for each participant will be provided by the responsible NCB.

If the TARGET Service Desks are contacted for issues other than connectivity, the request is forwarded to the responsible NSD.

2.3.1 External communication tools

External communication tools are used for communication with the participants and/or the general public. All available tools are described in the following table.

Table 8
External communication tools

Tool	Used for
ECB's website	The ECB's website provides information on the operational status of TARGET services for the attention of participants and the public. Information is reported separately for each service but is visible on the same ECB web page . In case of abnormal situations, the information provided includes the type of failure, its impact as well as the measures envisaged to resolve the problem.
Broadcast	The broadcast functionality is an "alert message" distributed to TARGET participants via the relevant GUI. The broadcast tool is used to share information with TARGET participants via the relevant GUI about specific system events, as well as operations-related and business-related information.
TIPS email notification tool	The TIPS email notification tool is used for communicating TIPS incidents that affect the processing of instant payments and the suspension/extraordinary termination of a TIPS account or TIPS account holder. The TIPS Service Desk communicates via email incidents that affect the availability of TIPS and the settlement of instant payments. Additionally, the TIPS Service Desk supports the NSDs in the absence of the broadcast functionality in TIPS by communicating via email the suspension/extraordinary termination of a TIPS account or TIPS account holder. All central banks and all TIPS DCA holders/TIPS ASTA holders/reachable parties/instructing parties to that have provided their contact details, for this purpose are informed. TARGET participants shall request to their NSD to add on their behalf the contact details directly in CRDM, ensuring that an email address is provided. The submitted contact details should be generic and should not contain any information that, under the General Data Protection Regulation (GDPR), is defined as personal data²¹. The TIPS Service Desk keeps an updated contact list that is used for this purpose.
Communication channels used at national level	Communication between NSDs and their respective national participant community. The most common tools are single hotline numbers, fax numbers and email addresses.

Kommentiert [A4]: FICB: Would it be beneficial to clarify that "The submitted contact details should be generic and should not contain any personal data" similarly to the MOP?

Kommentiert [A5R4]: ECB: Amended accordingly.

2.4 Types of participation – euro

TARGET participants are entities that hold at least one MCA and may additionally hold one or more DCAs in TARGET or ancillary systems.

²¹ See Chapter 15 General Data Protection Regulation

The access criteria that apply for participation are the same across services and are set out in the TARGET Guideline (Annex 1, Part 1, Article 4).

The different types of participation for:

1. CLM and RTGS are described in the CLM & RTGS part;
2. TIPS are described in the TIPS part; and
3. T2S Cash are described in the T2S Cash Part.

2.5 Types of connectivity

TARGET users may connect to TARGET via A2A (application-to-application) and U2A (user-to-application) mode. Both A2A and U2A connections are provided by the network service providers (NSPs) that have been awarded concession contracts by the Eurosystem. TARGET is accessed through the Eurosystem Single Market Infrastructure Gateway (ESMIG). Depending on its business needs, a TARGET user may choose to connect via:

1. both (U2A and A2A); or
2. U2A only (for users with only low volume of payments).

All TARGET participants must establish a technical connection to TARGET services. This obligation can also be fulfilled via a third party (co-manager for MCA, instructing parties for TIPS DCA, etc.).

2.5.1 A2A

A2A connection allows the software of TARGET participants to communicate with TARGET by sending/receiving single messages and files. A2A communication relies on ISO 20022 XML messages.

More information about A2A connection, messages and routing of the messages can be found in the relevant UDFS.

2.5.2 U2A

U2A connection allows TARGET users to access TARGET via the graphical user interfaces (GUIs).

More information about the functionalities available via U2A connectivity can be found in the relevant UDFS and the User Handbooks.

2.5.3 Contingency connection

According to the relevant MIB decision, in order to limit the impact of a prolonged outage affecting one of the two NSPs, all:

1. Eurosystem and connected central banks shall put in place a dual connection to ESMIG (i.e. with both NSPs) at the latest by March 2025.
2. TARGET critical participants shall put in place a dual connection to ESMIG (i.e. with both NSPs) at the latest by March 2026.

It is noted that the **required** second connection shall be a “contingency” U2A connection **at the minimum**, and not **necessarily** a fully-fledged connection to TARGET. Its aims at ensuring the processing of critical transactions in case of an incident impacting the participants’ primary NSP.

Kommentiert [A6]: NEW: Alignment with MOP Fundamentals

2.6 TARGET calendar – euro

CLM, RTGS and T2S Cash are open from Monday to Friday and closed on Saturday and Sunday.

For euro settlement, CLM, RTGS and T2S Cash are closed on the following days:

- 1 January (New Year’s Day)
- Good Friday
- Easter Monday
- 1 May²² (Labour Day)
- 25 December (Christmas Day)
- 26 December (Boxing Day)

While TIPS operates on a 24/7/365 basis, its business days follow CLM business days. For example: instant payments settled on Saturday and Sunday have as a value date the next CLM business day (e.g. Monday).

²² Even though T2S is available on 1 May, there is no settlement in euro; only free-of-payment transactions are possible.

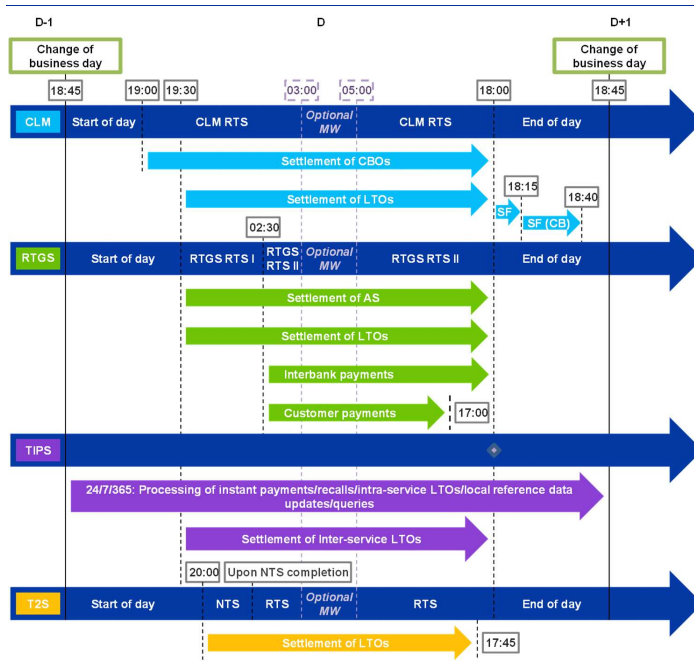
Table 9
TARGET closing days

Closing days	Saturday	Sunday	1 January	Good Friday	Easter Monday	1 May	Christmas- Day 25 December	26 December
CLM & RTGS	Closed							
TIPS	Available for settlement (with the value-date the next CLM business day)							
T2S	Closed					Closed for euro settlement FoP possible	Closed	

2.7 Operational day schedule – euro

The figure below shows the operational day schedules of TARGET settlement services for the euro currency.

Figure 3
Operational day schedules with optional MW – euro




Notes: Operational day schedules with optional MW – euro.

– Fehler! Verwenden Sie die Registerkarte 'Start', um Heading 1 dem Text zuzuweisen, der hier angezeigt werden soll.

CLM

- SF: during this period, participants may request to make use of the standing facilities. The cut-off for SF is 15 minutes later on the last day of the reserve maintenance period.
- SF (CB): during this period, only central banks can input a request to make use of standing facilities. The cut-off for SF (CB) is 15 minutes later on the last day of the reserve maintenance period.

TIPS

- Change of business day: as instant payments are continuously processed, TIPS changes its business day to the next CLM business day following CLM RTS closure. This is indicated in the diagram with .

T2S

- T2S processes: for the purpose of this diagram, only the T2S Cash-relevant processes are reflected, i.e. settlement of LTOs. More information on T2S processes can be found in the T2S MOP.
- NTS: NTS processing is usually completed between 20:00 and 23:30.

MW

- Optional: during weekdays, the maintenance window (MW) is optional and if activated it runs from 03:00 until 05:00. Its activation affects: all CLM/RTGS/T2S/common components processes and settlement of LTOs in TIPS. Its activation does not affect: TIPS processing of instant payments/recalls/local reference data changes/queries and ESMIG availability.
- Non-optional: The non-optional MW takes place weekly from 02:30 Saturday until 02:30 Monday. For TARGET closing days, the non-optional MW is extended to include those days, starting at 02:30 on the closing day (e.g. **Easter Good Friday**) and ending at 02:30 on the next TARGET working day (e.g. the following Tuesday after Easter).

Access to the DWH and the GUIs (with the exception of the TIPS GUI) is available during all periods except for the maintenance window.

Access to the CLM and RTGS GUI is available during all periods except for (i) the MW and (ii) between events "EoD close of service" (CCOS/RCOS) and "Change of business day" (RCOS/RSOD). Access to TIPS GUI is available during all periods.

Common reference data can be captured during all periods except during the maintenance window. However, reference data changes are only propagated to CLM, RTGS, TIPS and T2S at specific times, as described in the relevant service-specific parts of the Infoguide.

Kommentiert [A7]: For info:T2-WG decision 11/07 outcome

Detailed technical descriptions of the business day for each TARGET settlement service can be found in the relevant UDFS chapters.

3 Fundamentals of incident management

3.1 Purpose and scope of Incident Management

An incident is defined as an unplanned interruption or a reduction in the quality of an agreed service. It is not part of standard operations and its effect may be detected immediately or at a later point in time.

The incident management process manages the life cycle of incidents, i.e. it identifies and resolves incidents while providing up-to-date information on their status to CBs and participants involved in the day-to-day operations. This process coordinates the task of restoring the services as quickly as possible and minimising the adverse impact of the incident on business operations.

TARGET Incident Management consists of the following activities:

- detection of the ongoing issue;
- fixing the incident/applying a workaround;
- delayed closing²³;
- business continuity, i.e. the continuation of full processing capacity through the failover to a secondary system/site/region; and
- contingency arrangements to allow for the continued processing of a limited number of payments.

3.2 Incident detection

An incident can be detected:

- by an alarm raised automatically as part of the operational/technical monitoring of the 4CB;
- as the result of regular checks performed by the 4CB;
- by a TARGET stakeholder (e.g. NSDs, TARGET participants, TARGET Coordination Desk) or NSPs when reporting problems observed on their side or not being able to access a specific function or receiving rejection/error messages from TARGET.

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

- failure of a TARGET hardware/software component;

²³ The decision-making for non-euro currency lies with the responsible CB of that currency.

- procedural or operational failure;
- strike or major external event (e.g. natural disasters, large-scale power outages, terrorist attacks, coinciding events, cyberattack).

Note that not every event encountered will result in an incident. In fact, some alarms are purely for information and do not require any direct follow-up or do not have any implications on the system's availability. Additionally, where a participant raises a complaint, the origin of the problem may be solely within the participant's area of responsibility and may not be dependent on a malfunction of, for example, the CLM, RTGS, T2S, TIPS or a national infrastructure component.

3.3 Actors involved in incident management

The TARGET actors involved in incident management are:

- TARGET participants
- National Service Desks (NSDs) of central banks in TARGET
- TARGET Service Desks (4CB)
- TARGET Coordination Desk (ECB)
- T2S Coordination Function (ECB) – may be involved in TARGET incidents related to T2S. During such cases, the two ECB coordination bodies (TARGET Coordination Desk and T2S Coordination Function) cooperate closely.
- Network service providers (NSPs) – may be involved in TARGET incidents related to connectivity.

Formatiert: Aufzählungszeichen

3.4 Incident scenarios

There are five pre-defined incident scenarios, depending on the level at which the incident occurs.

Scenario 1: incident affecting all TARGET services;

Scenario 2: incident affecting one or more TARGET settlement services or the common components;

Scenario 3: incident affecting one or more central banks in TARGET;

Scenario 4: incident affecting TARGET participants;

Scenario 5: incident affecting NSPs.

The flow of activities, information and decisions differs at certain points, depending on the scenario.

– Fehler! Verwenden Sie die Registerkarte 'Start', um Heading 1 dem Text zuzuweisen, der hier angezeigt werden soll.

3.5 External communication on TARGET incidents

Information shared with TARGET participants is collectively agreed by the central banks in TARGET.

Information is communicated globally in the form of a broadcast message²⁴ via the CLM/RTGS GUI or the T2S GUI (if applicable) and on the ECB website, as listed in the [Chapter 2.3.1 "External communication tools"](#).

When communicating to their participants via communication channels used at national level, all information regarding TARGET incidents released by the NSDs is aligned with the information published on the ECB website.

Information related to an incident affecting TARGET participants may be shared ex-post with them via the ECB's website and the NSDs where the incident was resolved very soon after its detection.

²⁴ The broadcast functionality for TIPS is subject to the approval and deployment of Change Request CR-0014.

4 Fundamentals of problem management

4.1 Purpose and scope of problem management

A problem is defined as an abnormal state or condition at a component, equipment, or sub-system level, which may lead to a failure in TARGET revealing a discrepancy between the relevant specifications and the actual behaviour of TARGET. A problem can result in a change request.

The purpose of problem management is to identify and eliminate the root causes of incidents and “known errors” with the aim of minimising any adverse impact on the service. While problems are being resolved, problem management may produce temporary ‘workarounds²⁵’ until permanent solutions are found.

Problem management manages the life cycle of all problems from first identification, through to further investigation, documentation and eventual resolution. It includes the activities required to diagnose the root causes of incidents and to determine the resolution to problems. Through problem management, information about problems and the appropriate workarounds and resolutions are also maintained, enabling a reduction in the number and impact of incidents over time.

4.2 Actors involved in problem management process

The TARGET actors involved in the problem management process are the same as those involved in the incident management process (for more information, see [Chapter 3.3 “Actors involved in incident management”](#)).

4.3 Relationship with incident management and change, release and deployment management

Problem management differs from incident management in its main objective, which is to detect the underlying causes of an incident and their subsequent resolution and prevention, whereas the objective of incident management is to restore any affected services as quickly as possible, often through a workaround, rather than through the implementation of a permanent resolution.

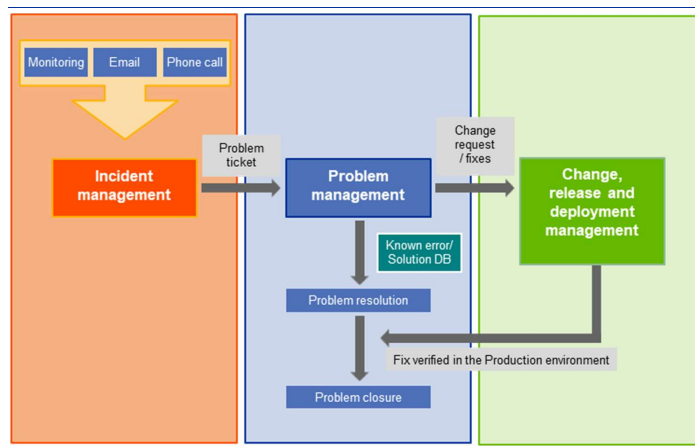
As problem management leads to a permanent resolution, it may sometimes require that a change request be raised. The procedure to be followed is described in [the chapter on change, release and deployment management Chapter 6](#) of each of the three service-specific parts of the Infoguide (CLM and RTGS, TIPS, T2S Cash). If

²⁵ A workaround is a solution that aims to reduce or eliminate the impact and/or likelihood of known errors (and thus problems) for which a full resolution is not yet available. A workaround can be permanent or temporary that once established, is logged as a temporary workaround or known error in TMS or treated as a permanent solution.

the change request is not accepted for implementation, the problem ticket is updated accordingly and closed with the workaround provided.

Once problem solutions are successfully tested in the internal 4CB environments, they are deployed to the test environments for testing by central banks and TARGET participants as needed (as defined in the Infoguide parts of the respective settlement services in the chapter on change, release and deployment management). Problem management also provides key information for identifying and implementing appropriate mitigation measures related to security threats as well as other operational risks. Therefore, it can also interact with other processes such as operational risk and information security management.

Figure 4
 Problem management and its relationship with incident management and change, release and deployment management



5 Access management

5.1 Purpose and scope of access management

The purpose of access management is to grant authorised TARGET users the right to use TARGET settlement services and to prevent access to non-authorised users. Accessing TARGET settlement services requires a three-step approach, as follows:

1. Connectivity to ESMIG (further details can be found in the Connectivity Guide).
2. Reference data **c**Configuration (by **CB**central banks), including the granting of relevant roles and privileges (further details for the euro can be found in the TARGET services registration and onboarding Guide).
3. Granting of roles and privileges (by TARGET user) (further details for the euro can be found in the TARGET services registration and onboarding Guide).

Via access management, each user is granted a set of access rights, which can also be changed or removed.

Roles and privileges are granted in a decentralised way, by each party administrator, in accordance with the TARGET hierarchical party model.

According to best practices on information security risk management, central banks and TARGET participants are required to perform regular reconciliation activities.

5.2 Access management activities by central banks

The central bank:

- creates new roles by including available privileges within its data scope;
- approves the NSP connection of TARGET participants (e.g. e-ordering for SWIFT, Domain-join for **SIA**Nexi-Colt), conditional on the successful certification of the users;
- configures the reference data relevant for its participants and ancillary systems and creates for them the relevant administrator users;
- assigns the relevant set of roles and privileges to their participants and ancillary systems and their administrator users.

5.3 Access management activities by TARGET participants

While most of the activities for managing end-to-end access falls on the shoulders of the 4CB and the central banks and also the licensed NSPs, the access management activities described below are relevant for TARGET participants.

To gain access to TARGET, participants must:

1. establish their connection to TARGET via the NSP (e.g. e-ordering for SWIFT, Domain-join for [SIANexi-Colt](#));
2. ask their responsible central bank to grant U2A/A2A access rights, change existing rights, or remove existing rights;
3. create users within their organisation;
4. create, manage and assign roles and privileges to their users;
5. monitor access to TARGET (within the remit) via regular reconciliation exercises;

The responsible central bank will create the Administrator User(s) for their participants in CRDM, which is/are responsible for:

- managing the users within their institution;
- assigning available roles and privileges to those users.

6 Service request management

6.1 Retrieval from the Legal Archive

Description

TARGET provides a dedicated Legal Archiving common component (LEA) used to store and retrieve, upon request, data needed for audit and/or regulatory purposes.

At the end of each business day, all data relevant for legal purposes produced by the TARGET settlement services are sent to the LEA component. ~~The~~ LEA retains production-related data mainly concerning settlement-related messages and messages changing reference data or transactional data (inbound and outbound messages in their final status [(settled, cancelled, etc.)], but not queries). ~~The~~ LEA's retention period is ten years for all TARGET settlement services.

Retrieval procedure

While LEA is not directly accessible to participants, a request may be submitted to the responsible NSD using the form in [Annex III](#). Data can be retrieved for a period of ten years.²⁶

The requested data can be retrieved upon request. The procedure for retrieving archived data is transparent and reproducible. Generally, the information is retrieved and exported as a flat file which is transmitted via a secure channel.

Once the requested data have been retrieved from LEA, the information is delivered via the channel (e.g. ESCB email, ~~fax~~) defined in the Service Request.

The information to be delivered consists of:

- a copy/extract of the file(s) containing the requested or relevant information; and
- a copy of the extraction log to prove the origin of the requested information.

²⁶ TARGET2 data can still be requested for a period of ten years after the dismantling of TARGET2 in March 2023.

7 Business continuity management

Business continuity management (BCM) identifies risks that may lead to an interruption in the business process, regardless of the root cause, and aims to mitigate those risks. It also includes the analysis and prevention of such risks. Some risks may be IT-related, including disaster-level incidents, while others may be outside the realm of IT, such as natural disasters or facility fires. With regard to TARGET, **service continuity management (SCM) and contingency arrangements** are there to support BCM.

BCM requires the creation of:

1. a business continuity plan that includes plans for prevention and recovery from disaster-level incidents; and
2. business impact analyses that identify the potential business impacts of a disaster.

Service continuity management (SCM) focuses on planning for major incidents (e.g. a fundamental disruption to the operations of TARGET settlement services), along with prevention, prediction and management. It aims to maintain service availability and performance at the highest possible levels before, during and after a disaster-level incident. Effective, standardised processes need to be in place and must be followed when such incidents occur to minimise the resulting downtime, costs and business impact. The aim of the process is to ensure that services are restored within the timelines defined in the relevant service level agreement (SLA) following a major service disruption.

SCM falls under the primary responsibility of the service-providing central banks (4CB). Therefore, the relevant chapters in each service-specific part of the Infoguide do not include 4CB internal processes and focus on describing the interaction with the TARGET participants.

Contingency arrangements are there to support the continuation of normal operations and to minimise interruptions and impacts on participants, central banks and the TARGET operator during an incident. These contingency arrangements consist of interim measures until the service is resumed or restored and require the manual intervention/involvement of central banks.

A business continuity management model is in place for each settlement service. More information on each of these models can be found in the dedicated "Business continuity management ~~model~~" chapter in each of the three service-specific parts of the Infoguide (CLM and RTGS, TIPS, and T2S Cash).

8 Testing activities in TARGET

The regular testing of the business continuity management (BCM) measures aims to ensure that the existing procedures and infrastructure are still sufficient and ready to handle potential disaster scenarios. Additionally, it offers an opportunity for the teams involved to practise the tasks that they would need to perform in a disaster scenario.

Note: A distinction is made between the terms trialling and testing. Trialling refers to exercises performed in the production environment, while testing refers to exercises performed in the test environment.

Service continuity testing for the participants is coordinated by the respective central banks. The NSDs contribute to the organisation and planning of service continuity testing and are expected to follow tests/trials involving their community participants (e.g. critical participant testing) and support their community accordingly.

8.1 Overview of testing activities for TARGET

The following table provides an overview of the tests to be performed. Further details per service, including the requirements for participation, can be found in the relevant Infoguide book.

Table 10
Overview of TARGET testing activities for TARGET

Test name	Environment	Frequency	Applicable to
BCM testing			
Service continuity			
Inter-region failover	PROD	Once per year	CLM&RTGS, T2S DCA
Intra-region failover	PROD	Once per year	CLM&RTGS, T2S DCA
Contingency arrangements			
ECONS II regular testing	UTEST	Once every six months	CLM&RTGS
ECONS II live trial	PROD	Once per year	CLM&RTGS
ECONS II two-day test involving T2S	UTEST	Once per year	CLM&RTGS, T2S DCA
Exceptional payment functionality	PROD/alternatively UTEST	Once every six months	CLM&RTGS
NCB acting on behalf of their participants	PROD/alternatively UTEST	Once every six months	CLM&RTGS
Business continuity at the level of participants			
For critical participants (secondary site test)	PROD	Once per year	CLM&RTGS
Other operational procedures tested			
TC2 connectivity test and simulation exercise (xMatters)	n/a	Once per year	CLM&RTGS, TIPS
TC2 connectivity test and simulation exercise (CISCO)	n/a	Once per year	CLM&RTGS, TIPS
TIPS email notification tool	PROD	Once per year	TIPS

8.2 Test results and reporting

Test results are to be reported by the participants involved in the test to their respective central bank as either being successful or unsuccessful. If the test objectives are not met, the test result should be regarded as unsuccessful.

All central banks in TARGET, as well as the 4CB, report the test results for all tests performed to the ECB in order to ensure the readiness of all central banks and participants in TARGET, identifying any lessons learned during the process. If a test result is deemed partially successful or unsuccessful, an assessment of the test in question is performed on a case-by-case basis to decide whether a retake is necessary, and if so, when.

9 Information security management

9.1 Gathering and sharing information about the endpoint security of TARGET participants

9.1.1 Purpose

The CPSS/IOSCO principles for financial market infrastructures (PFMI)²⁷ prescribe several responsibilities for financial market infrastructures (FMIs). In particular, Principle 17 addresses the security and operational reliability of FMIs and states that an "FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations". Furthermore, the principle 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." This is to ensure the security and operational reliability of TARGET and its participants.

The management of TARGET is a collective responsibility assumed by all central banks in TARGET even if the business relationships are the responsibility of the central bank with which the TARGET participant has a legal relationship. Therefore, the Eurosystem has established processes to gather and share information about the security of TARGET participants.

The objective is to increase the level of awareness of the central banks about any potential threats: (i) to the smooth functioning of TARGET; or (ii) that adversely affect the TARGET participants. This information is to be consistently shared across the TARGET central banks in order to ensure that they can effectively assume their system operator responsibilities. Furthermore, insights gained from this type of information sharing about the security of TARGET participants may be used as input for considerations about how particular risk situations can be addressed/rectified.

Due care must be taken to ensure the confidentiality of information related to any TARGET participant. Security information arising in the context of the overall framework should be made available exclusively to the responsible representatives of the TARGET central banks. This is in accordance with the TARGET Guideline, Annex I, Part 1, Article 20.

This chapter outlines how information is shared among central banks (this is distinct from the dissemination of information to the TARGET community which is outside the scope of this chapter). For the purpose of endpoint security only, "central banks" refers to Eurosystem and connected central banks. In particular, this chapter outlines how information sharing takes place with regard to TARGET participants that adhere

²⁷ See <https://www.bis.org/cpmi/publ/d101a.pdf>.

to the NSP security requirements and how any non-compliance with this information sharing policy is addressed.

9.1.2 Legal basis

According to the TARGET Guideline, Annex I, Part I, Article 28, a central bank shall keep sensitive or secret information confidential, including when such information relates to payment, technical or organisational information belonging to the participant, participants from the same group or the participant's customers, unless the participant or its customer has given its written consent to disclose it, or such disclosure is permitted or required under the specific country's law. However, by derogation of this principle, the responsible central bank may disclose payment, technical or organisational information about the participant or the participant's customers to other central banks or third parties (4CB) that are involved in TARGET operations if this is necessary for the efficient functioning of the system.

Given that none of the TARGET central banks have indicated that the above conflicts with applicable national legislation, the gathering and sharing of information about participants forms an integral and mandatory part of the overall framework for ensuring the security and operational reliability of participants. When central banks share information between themselves that contain personal data, those central banks will need to ensure compliance with the GDPR, as further outlined in [Chapter 12—General Data Protection Regulation](#)[Chapter 12 "General Data Protection Regulation"](#).

Feldfunktion geändert

9.1.3 Requirements for participants – NSP attestations of adherence

Irrespective of the settlement service, all TARGET participants with an NSP connection to ESMIG must provide their central banks with permanent access to their attestation of adherence with the chosen NSP endpoint security requirements (if a participant makes use of two NSPs to connect to ESMIG, it must provide the attestations of adherence of both NSPs).

The compliance implementation measures outlined in the CLM and RTGS Infoguide, Chapter 9.3.1.2. "NSP endpoint security requirements" are to apply to participants based on the NSP attestation of adherence only to the extent that the participant does not share its attestation with its central bank.

10 Financial management

The NSDs are responsible for invoicing activities related to the invoicing of the relevant central bank and their participants, as well as any enquiries stemming from them.

10.1 Accessing and receiving invoices

The duly authorised central bank user and the duly authorised participant users (of those central banks that use BILL to send invoices) may receive/access the system entity and participant invoices in BILL, respectively, depending on their data scope. The following two ways of accessing/receiving invoices are available via BILL (subject to central bank discretion as to how the invoices are shared/sent locally to their participants):

- via push mode via A2A using the BillingReport (camt.077) message to the party technical address if the relevant invoice configuration has been set up by the central bank; or
- via U2A, in order to view and/or download the generated invoice in PDF format.

Central bank users may access their own invoices and those of their participants, while participants may access their own invoices. BILL, by default, sends one invoice (in .xml format) per participant and per service.

Central banks that do not use BILL to create invoices will send the invoices via proprietary applications.

10.2 Payment of invoices

All participant invoices are to be settled via direct debit, whether or not a central bank makes use of BILL for invoicing purposes. Participants must indicate, via the reference data forms, the MCA to be debited for their invoice. This MCA may be under the scope of a central bank other than the one debiting the account.

For those central banks that use BILL for invoicing purposes, an automatic direct debit order is created on the invoice due date (11th business day of the month) and submitted to CLM. The order triggers the debiting of the pre-defined MCA of the participant and credits the pre-defined central bank CLM account (as configured in CRDM). The invoice number is referenced in the payload of the direct debit order to help participants identify the transactions related to billing in their records. If the MCA to be debited does not have enough liquidity, the direct debit order will be queued. Should the debited MCA still have insufficient liquidity at EoD, the direct debit order will be rejected and BILL will not reattempt further direct debiting. Instead, the

respective responsible central bank shall follow up with the participant bilaterally in order to settle the invoice.

Figure 5
Invoicing sequence for RTGS and TIPS

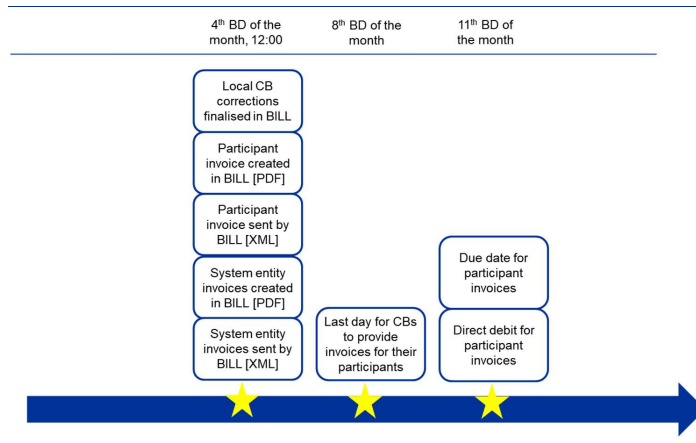
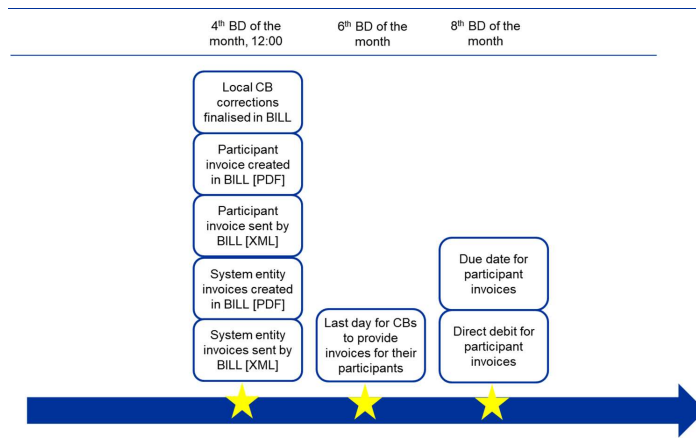


Figure 6
Invoicing sequence for T2S cash-side



– Fehler! Verwenden Sie die Registerkarte 'Start', um Heading 1 dem Text zuzuweisen, der hier angezeigt werden soll.

11 TARGET compensation scheme - euro

11.1 Purpose and scope

If a cash transfer order cannot be settled on the same business day on which it was accepted (warehoused payments are considered to have been accepted by TARGET on the settlement day) due to a technical malfunction of TARGET, central banks shall offer to compensate the participants concerned in accordance with the procedure laid down in Appendix II of the TARGET Guideline.

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

Compensation under the TARGET compensation scheme is the only compensation procedure that the Eurosystem offers in the event of a technical malfunction. Participants may, however, pursue other legal avenues to claim for losses.

A participant's acceptance of a compensation offer under the TARGET compensation scheme constitutes the participant's irrevocable agreement that it thereby waives all claims against any central bank in relation to the payment orders for which it accepts compensation (including any claims for consequential loss). The participant's receipt of the corresponding compensation payment constitutes a 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 TARGET compensation scheme, in respect of any further claims that may be raised by any other participants or any other third party in relation to the cash transfer order or cash transfer 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 TARGET.

11.2 Procedural steps

The following steps apply for a participant submitting a compensation claim under the TARGET compensation scheme:

- **Within four weeks of the technical malfunction:** participants shall submit their claim forms to their home central bank.

A participant shall submit a claim for compensation in English by completing the claim form available on the website of the central bank concerned. 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. Only one claim may be submitted per cash transfer order.

- **Two weeks to provide additional information:** should the respective central bank request any additional information/evidence from the participant that submitted the claim request, that participant has two weeks to respond to such a request.
- **Within nine weeks** of the technical malfunction, the respective central bank shall:
 - prepare a preliminary assessment report containing the central bank's assessment of the claims received; and
 - submit the preliminary assessment report to the relevant Eurosystem groups in order to share the claims with all central banks.
- **Within five weeks following receipt of the preliminary assessment report,** the Governing Council shall carry out the final assessment of all claims and shall decide on the compensation offers to be made to the participants concerned.
- **Within five business days following completion of the final assessment,** the outcome of the final assessment will be communicated to the relevant central banks. The central banks shall, in turn and without delay, inform their participants of the outcome of the final assessment.
- **Within four weeks,** the participants shall either accept or reject the compensation offer in respect of each cash transfer 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 a 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 the **compensation payments on receipt of a participant's letter of acceptance of compensation.** No interest shall be payable on any compensation payment.

12

General Data Protection Regulation

Kommentiert [A8]: For info:

Chapter updated to align with MOP and simplify to avoid duplication of information

12.1

Background

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, known as the General Data Protection Regulation (GDPR or Regulation 2016/679), applicable to national central banks, took effect on 25 May 2018. The GDPR is "mirrored" by Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 (the EU General Data Protection Regulation or EUDPR), which is applicable to the ECB and took effect in December 2018. For ease of reading, the term GDPR is used throughout this Infoguide to refer to both instruments.

Implications of GDPR on TARGET settlement services²⁸

The Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data²⁹ in CLM, RTGS and TIPS.

~~The GDPR defines the concept of personal data as follows: personal data means any information relating to an identified or identifiable natural person (known as a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that data subject.~~

~~The GDPR identifies the following key roles:~~

- ~~• Data subject: a natural person who can be identified, directly or indirectly, in particular by reference to an identifier (personal data).~~
- ~~• Controller: a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Joint controllers take data protection related decisions.~~

²⁸ The implications of GDPR and the relevant procedure for T2S are described in the T2S MOP, Chapter 5.2.22.

²⁹ The GDPR defines the concept of personal data as follows: personal data means any information relating to an identified or identifiable natural person (known as a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that data subject.

12.2 Implications of GDPR on TARGET settlement services

CLM, RTGS and TIPS process ~~the and store~~ reference data ~~that is set-up and maintained in the system, as well as and~~ transactional data received for settlement purposes. Parts of the ~~information transmitted for settlement or~~ reference data set-up for CLM, RTGS and TIPS participants ~~or information transmitted for settlement~~ may contain personal data, either in the fields of an A2A message or ~~via~~ a screen of the CLM, RTGS or TIPS GUI. Therefore, CLM, RTGS and TIPS fall under the scope of the GDPR. ~~The implications of the GDPR and the relevant procedure for T2S are described in the T2S MOP.~~³⁰

Joint controllership description

~~For the purpose of processing personal data in CLM, RTGS and TIPS, the ECB, the euroEurosystem central banks, connected central banks and non-euro-central banks that participate in making their currency available in TARGET with their own-currency³¹ are deemed to be joint controllers (JCs) in the meaning of Article 28 of the EUDPR and Article 26 of the GDPR/EUDPR. Information on personal data and data subjects exercising their rights should only be shared within the respective joint controllership. In line with Art. 28 EUDPR and Art. 26 GDPR/EUDPR the JCs determine their respective responsibilities in an arrangement between them (joint controllership arrangement).~~

~~The comprehensive list of legally binding obligations of the responsible JC - pertaining to:~~

- ~~• Data subject requests can be found in Art. 14 to 24 EUDPR or Art. 12 to Art. 22 GDPR, and~~
- ~~• Breaches can be found in Art. 34 and 35 EUDPR or 33 and 34 GDPR. In compliance with the relevant GDPR rules, the following GDPR roles have been identified within the CLM, RTGS and TIPS governance structures:³²~~
- ~~• **Joint controllers:** the central banks in TARGET and the ECB. A joint controller (JC) determines jointly with others the purposes and means of the processing of personal data, as well as the respective responsibilities vis-à-vis the data subject's rights. The other processing operations, performed in their legacy systems, are performed separately under the sole control of the same controller. Personal data of a data subject might be included in the joint part, or in the legacy part. For the data held in the legacy systems, each central bank has a separate, individual role as controller for all personal data held in their own systems and their part in CLM, RTGS and TIPS.~~

³⁰ Chapter 3.4.29 of the T2S MOP v5.0 describes the implications and the procedure in detail for T2S.

³¹ See the T2 Currency Participation Agreement (T2 CPA) signatory central banks and TIPS CPA signatory central banks.

³² The previously discussed segregation into joint controllers and processors was superseded following the Eurosystem's decision to allocate one role per institution.

Formatiert: Mit Gliederung + Ebene: 1 + Nummerierungsformatvorlage: Aufzählungszeichen + Ausgerichtet an: 0 cm + Tabstopp nach: 0,75 cm + Einzug bei: 0,75 cm

- ~~Joint controllers offering the service: the CLM, RTS and TIPS providing central banks, known as the 4C. With regard to personal data potentially processed in CLM, RTGS and TIPS, JCs stand ready to support and inform the data subject in the following two scenarios.~~

Request of personal data from the data subject:

- ~~data subjects have the right to obtain confirmation from the JC within one³³ calendar month following receipt of the request as to whether or not personal data concerning them are being processed/stored. If so, they have the right of access to this personal data free of charge, as well as information including the purpose, the type, the recipients and archiving time. Furthermore, the data subject may also request an amendment or deletion of this data.~~

Address personal data breaches in CLM, RTGS and TIPS:

- ~~a JC shall inform the other JCs, without undue delay, upon becoming aware of a personal data breach. JCs shall notify the relevant supervisory authorities if the personal data breach is likely to result in a risk to the rights and freedom of the natural persons concerned.~~
- ~~the JC shall communicate the personal data breach to the data subject without undue delay, unless any of the following conditions are met: (i) the JCs have implemented appropriate technical and organisational protection measures that render the personal data unintelligible to any person who is not authorised to access it; (ii) the JCs have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; (iii) it would involve disproportionate efforts.~~

12.312.2 Operational procedure

The Eurosystem has established the following operational procedures to address any enquiries from a data subject about his/her personal data that have been processed by CLM, RTGS or TIPS, or in the event of a personal data breach in CLM, RTGS or TIPS.

- [Data subjects exercising their rights](#)
- [Personal data breaches in CLM, RTGS or TIPS](#)

[As per data protection regulation, each data subject has the right of access, the right to rectification, the right to erasure, or the right to restrict processing.](#)

³³ That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

- ~~Request from a data subject to ascertain whether any personal data have been processed and/or stored by the CLM, RTGS or TIPS settlement services;~~
- ~~Addressing personal data breaches in CLM, RTGS or TIPS.~~

~~12.3.1~~ ~~12.2.1~~ Data subject exercising their rights ~~Request from a data subject to ascertain whether any personal data have been processed and/or retained by CLM/RTGS/TIPS~~

As per data protection regulation, each data subject has the right of access, the right to rectification, the right to erasure, or the right to restrict processing.

Note: With regard to Eurosystem FMIs, the Eurosystem retains information for audit trail purposes, including personal data, for a retention period of ten years.³⁴ During this retention period, a data subject may ask whether his/her personal data were processed by the CLM, RTGS or TIPS settlement services.

If the Data Protection Office (DPO) at the level of a JC receives a GDPR data request from a data subject, the procedure foresees that:

1. Once the request has been received (a template form for data subjects to inquire about their personal data from Joint Controllers can be found in [Annex II](#)) and its scope clarified, ~~the JC requests the TARGET Service Desk to verify whether any personal data of the requesting data subject were processed³⁵ the DPO conducts an assessment to determine whether the request is unfounded or excessive and to estimate the overall processing time needed.~~

3-2. The JC shall provide status update/ feedback to the data subject within one calendar month of receiving the request. Information should be shared via the same channel used by the data subject, unless otherwise indicated. That period can be extended up to a total of three months, where necessary, depending on the complexity and number of requests received for personal data. In such a case, the data subject must be informed of the delay and the reason for it within one calendar month following receipt of the initial request.

4-3. If it is found that the request is clearly unfounded or excessive (in terms of effort to comply), it may be declined. In such a case, the data subject is informed within one calendar month following receipt of the request. This notification must include the reasons for not taking action and delivering the requested information to the data subject and must likewise explain why the request is considered to be unfounded or excessive (e.g. if the data subject has refused or

³⁴ TARGET2 data may still be requested for a period of ten years following the dismantling of TARGET2 in March 2023.

³⁵ ~~The identity of the data subject sending the inquiry shall be verified based on the laws and regulations applicable in the country of the JC receiving the request. Information on the identity document should be used only to verify the data subject's identity and should not be stored longer than needed for that purpose.~~

failed to provide all of the aforementioned information items). ~~Note: a data subject may also submit a request to his/her commercial bank to ask whether any personal data were processed by the CLM, RTGS or TIPS settlement services. Upon receiving the response, the data subject can decide whether to direct the request to the next level, i.e. the responsible central bank in its role as JG.~~

12.3.212.2.2 Addressing personal data breaches in CLM, RTGS and TIPS

A personal data breach means any breach of information security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the controllers. If a breach of the CLM, RTGS or TIPS secure storage occurs, in which the static and/or transactional data of CLM, RTGS or TIPS are recorded, and if this breach has resulted in a personal data breach putting at risk the rights and freedoms of individuals, the JCs shall follow the rules set out in the GDPR. In certain cases, when the breach is likely to result in a personal data breach putting at risk the rights and freedoms of individuals, the concerned data subject(s) might need to be informed by the responsible DPO(s).

~~It is the responsibility of the relevant central bank(s) to inform their participants without undue delay, all potentially affected data subjects of the data breach, and describe the potential impact and measures taken in order to mitigate any potential adverse effects. The nature of the data breach, the potential data loss, or the improper dissemination of data, and the impact that this might have (known as an impact assessment) must also be communicated to the impacted data subject.~~

Disclaimer: Specific activities at the level of the DPO and beyond, such as interaction between the DPO of the JC and data subject, are outside of the scope of the Infoguide.

~~in order to identify and contact any data subject(s) whose data may have been improperly disclosed. However, given the huge number of transactions that may have been affected and the considerable number of potential data subjects involved, a clear delineation of all the affected data subjects may involve a disproportionate effort by the JCs. In such a scenario, a joint decision-making process will be initiated and an assessment of the specific case will be performed, taking into account the severity of the breach. If necessary, a public communication may be made to inform all data subjects possibly affected in an effective and consistent manner.~~

13 Annex

13.1 Annex I – Central banks in TARGET

	Eurosystem central banks	Connected central banks	Central banks making their currency available in TARGET
1	European Central Bank (ECB)	BG – Bulgaria Българска народна банка (Bulgarian National Bank)	DK – Denmark Danmarks Nationalbank (for T2S only)
2	AT – Austria Oesterreichische Nationalbank	DK – Denmark Danmarks Nationalbank	SE – Sweden Sveriges Riksbank (for TIPS only)
3	BE – Belgium Nationale Bank van België/ Banque Nationale de Belgique	PL – Poland Narodowy Bank Polski	
4	CY – Cyprus Central Bank of Cyprus	RO – Romania Banca Națională a României	
5	DE – Germany Deutsche Bundesbank		
6	EE – Estonia Eesti Pank		
7	ES – Spain Banco de España		
8	FI – Finland Suomen Pankki – Finlands Bank		
9	FR – France Banque de France		
10	GR – Greece Bank of Greece		
11	HR – Croatia Croatian National Bank		
12	IE – Ireland Central Bank of Ireland		
13	IT – Italy Banca d'Italia		
14	LT – Lithuania Lietuvos bankas		
15	LU – Luxembourg Banque centrale du Luxembourg		
16	LV – Latvia Latvijas Banka		
17	MT – Malta Central Bank of Malta		
18	NL – Netherlands De Nederlandsche Bank		
19	PT – Portugal Banco de Portugal		
20	SK – Slovakia Národná banka Slovenska		
21	SI – Slovenia Banka Slovenije		

– Fehler! Verwenden Sie die Registerkarte 'Start', um Heading 1 dem Text zuzuweisen, der hier angezeigt werden soll.

13.2 Annex II – Data access request

Data access request (according to Article 17 of Regulation (EU) 2018/1725 and Article 15 of Regulation (EU) 2016/679).

Please provide the necessary information requested below to identify any personal data that may be held within a Eurosystem-operated Financial Market Infrastructure (CLM, RTGS, T2S and TIPS).

1. General questions

Please confirm that you are contacting the Eurosystem:

- (a) As an individual (asking for yourself)
- (b) Or on behalf of an individual (asking for somebody else). If so, you will need to provide proof that you have a power of attorney

If the request is not about your own personal data, please confirm the owner of the personal data in section 2 below.

Please note that prior to any effort undertaken, or any answer/data being provided, you will need to provide proof of your identity or of power of attorney, should you act on behalf of somebody else. Your identity will be verified based on the laws and regulations applicable in the country where the processing took place (i.e. the country of the Partial Joint Controller receiving the request).

2. Required basic identification and delineation information

You are kindly invited to provide the following information (A-a to C-c), which serves as delineation/identification criteria to allow for a timely and efficient search of your personal data in the Eurosystem FMIs databases.

Please note that we are allowed to reject your request, and to not act on it in case your request is deemed to be manifestly unfounded or excessive. Lack of required information to delineate your request (aA to cC) may result in excessive effort and lead to a rejection of your request.

(a) Names

Exact spelling of your first name(s), as you remembered it being used for the instance you wish to inquire about:

Exact spelling of your surname(s), as you remembered it being used for the instance you wish to inquire about:

(b) Reference period

– Fehler! Verwenden Sie die Registerkarte 'Start', um Heading 1 dem Text zuzuweisen, der hier angezeigt werden soll.

Specify one calendar year during which the transaction was initiated (if known, please provide a more narrowed timeframe). If you are enquiring about more than one transaction, please provide the reference period for all transactions you are enquiring about:

(c) Please select the type(s) of transaction(s) applicable to your case

- (i) Security settlement (T2S)
- (ii) Cash transfer (CLM & RTGS)
- (iii) Instant payment (TIPS)

(d) Optional information

To further facilitate the identification of your personal data, please provide the following information, if available (e.g. via your commercial bank):

T2S/CLM/RTGS/TIPS reference:

T2S/CLM/RTGS/TIPS account number:

Transaction amount:

ISIN (security settlement):

IBAN and/or BIC of the originating and of the receiving commercial banks or depository institution (if you are enquiring about more than one transaction, please provide the relevant IBANs/BICs for all transactions you are enquiring about):

Originating: _____

Receiving: _____

13.3 Annex III – Legal archiving form

Purpose <i>(if "Else" chosen, please specify it in few words)³⁶</i>	Choose an item.	
Date of request	Enter date	
Requestor's CB	Choose an item.	
Requestor's name		
Media of retrieval	Choose an item.	
Mandated representative (optional)		
Date of retrieval <i>(if the requestor has mandated a representative)</i>	Enter date	
NSP and type of message requested		
<i>Choose type of data</i>		
Detailed Request		
Type of Data to be retrieved		
Instruction date	From: Enter date	To: Enter date
Settlement date <i>(*applicable for settlement instructions)</i>	From: Enter date	To: Enter date
Business message ID <i>(Actor reference)</i>		
System entity		
Party ID		
Message identifier		
Party Sender		
Party receiver		
Message Type		
Possible amount		
Additional information		

³⁶ Request to access Legal Archiving information must come only after a specific request from a Legal Authority and to support investigations in relation with legal actions.

Annex IV – Terms of Reference – TARGET Crisis Communication Group

These Terms of Reference (ToR) set out the working arrangements for the TARGET Crisis Communication Group (TC2). They contain important information about the group, such as its key principles, purpose, membership, call setup, nomination process and level of administrative support. While they are not for publication, their content should be the basis for any external communication by the Eurosystem on the matter.

1. Role/purpose

The role of the TC2 is to establish a more direct link between the crisis managers and the TARGET key stakeholders, focusing primarily on communication in response to major incidents. In particular, the group contributes to two-way communication in times of crisis, ensuring that the Eurosystem receives feedback from market participants on whether the most recent communication about the incident has been sufficiently clear and to adequately address their most urgent questions. Moreover, the crisis managers may receive valuable information directly from market participants relating to the status of their business, which would allow the crisis managers to further enrich the information shared at the next update. The main objective of the group is to improve communication in case of major incidents in TARGET.

2. Term

This ToR is effective from 20 March 2023³⁷.

3. Composition

The TC2 comprises the crisis managers and representatives from the market participants. The selection criteria for the group membership of the market participants is based on the list of TARGET critical participants. Each TARGET critical participant may nominate one member.

Network service providers may also be involved, depending on the nature of the crisis scenario (i.e. incidents related to or affecting connectivity) or if their involvement is considered beneficial.

The Chairperson shall be the ECB crisis manager.

The list of participants is available only to all TC2 members (on a confidential basis) and will be updated every year to reflect any changes in the list of TARGET critical participants.

4. Roles and responsibilities

³⁷ Replacing the ToR version from 31 March 2022.

The TC2 group is a communication forum and has no responsibility in the management of the crisis, which remains entirely under the control of the crisis managers.

Participation is on a voluntary basis. However, as crisis managers are available on-call 24/7/365, the same principle will apply to the Crisis Communication Group, which may be called upon at any time.

5. General principles

Calls are triggered upon the decision of crisis managers alone in the event of a severe incident, whether due to its duration or nature, or the impact it could have on the financial markets (e.g. long-lasting incidents, successful cyberattack affecting the integrity of the system).

The time for involving the TC2 as well as the frequency of TC2 calls during an ongoing incident would be decided by the crisis managers on a case-by-case basis. In general, the TC2 will not be involved immediately upon detection of an issue, but once the full picture on the impact and the potential workarounds or solutions become sufficiently clear.

During TC2 calls, market participants will have the opportunity to raise questions or to obtain clarifications on points that have not been covered, or not sufficiently covered, in communications shared previously. Moreover, the crisis managers may receive valuable information directly from market participants relating to the status of their business, which would allow the crisis managers to further enrich the information shared at the next update.

6. Conference calls rules and practicalities

During the TC2 call, the ECB and the 3CB 4CB crisis managers will brief the TC2 on the status of the incident, confirm whether the communication shared was clear and sufficient and invite them to raise questions and share any important or relevant aspects they believe should be brought to the attention of the crisis managers.

Important questions/points raised during the TC2 call should be addressed and reflected in the next communication to be published on the ECB's website.

The tools used are xMatters and CISCO meeting manager (back-up). The ECB is responsible for setting up and configuring the tools.

On the side of the TC2 members, there is no requirement for any software installation as both tools used provide dial-in and dial-out options and email notifications; xMatters also provides SMS notifications. Guides on how to join the calls will be prepared by the ECB and distributed via the national central banks.

Connectivity tests and simulation exercises will be organised by the ECB at least once a year in order to test the proper functioning of the tool and ensure that all contact details are correct. Further exercises may also be organised to simulate the process to be followed in case of an incident.

To ensure a clear discussion and flow of information during TC2 conference calls, group members should enter with their phones in 'mute' mode and remain muted at all times unless speaking. They shall also keep their intervention to the strict necessary in order to keep the call as short as possible.

7. Nomination of group members

TARGET critical participants may nominate one group member for their institution by submitting a request to their respective national central bank. TARGET critical participants shall provide the following contact details to their respective national central bank:

- Name
- Name of institution
- Landline or mobile number
- Email address

The ECB³⁸ maintains the list of contact persons of the critical institutions. However, it is the responsibility of the national central banks to provide the ECB with up-to-date information on any changes to the members and their contact details.

³⁸ This is the responsibility of the TARGET Coordination Desk.

© European Central Bank, 2023

Postal address 60640 Frankfurt am Main, Germany

Telephone +49 69 1344 0

Website www.ecb.europa.eu

All rights reserved. Reproduction for educational and non-commercial purposes is permitted provided that the source is acknowledged.

For specific terminology please refer to the [ECB glossary](#) (available in English only).