

USER REQUIREMENTS DOCUMENT

FOR

COMMON COMPONENTS

Version:	R2025.NOV
Status:	Final
Date:	05/08/2025

Contents

1	EUROSYSTEM SINGLE MARKET INFRASTRUCTURE GATEWAY (ESMIG)...	6
1.1	Overview	6
1.1.1	Context Diagram	6
1.1.2	General User Requirements for ESMIG	6
1.2	Eurosystem Single Market Infrastructure Gateway – non-functional Requirements	15
1.2.1	Availability.....	15
1.2.2	Disaster Recovery.....	15
1.2.3	Performance Requirements	16
2	COMMON REFERENCE DATA MANAGEMENT (CRDM).....	17
2.1	Overview	17
2.1.1	Context Diagram.....	17
2.1.2	Business Processes.....	18
2.1.3	General User Requirements for CRDM.....	19
2.2	Create an occurrence of Common Reference Data.....	20
2.2.1	Business Process Model.....	20
2.2.2	Process Overview.....	22
2.2.3	User Requirements	23
2.3	Amend an occurrence of Common Reference Data.....	27
2.3.1	Business Process Model.....	27
2.3.2	Process Overview.....	29
2.3.3	User Requirements	30
2.4	Delete an occurrence of Common Reference Data	34
2.4.1	Business Process Model.....	35
2.4.2	Process Overview.....	36
2.4.3	User Requirements	37
2.5	Propagate Changes	40
2.5.1	Process Overview.....	40
2.5.2	General User Requirements	41
2.6	Block an occurrence of Common Reference Data	42
2.6.1	Business Process Model.....	42
2.6.2	Process Overview.....	44
2.6.3	User Requirements	44
2.7	Unblock an occurrence of Common Reference Data.....	48

User Requirement Common Components

2.7.1	<i>Business Process Model</i>	48
2.7.2	<i>Process Overview</i>	50
2.7.3	<i>User Requirements</i>	51
2.8	Close a Cash Account	53
2.8.1	<i>Business Process Model</i>	53
2.8.2	<i>Process Overview</i>	54
2.8.3	<i>User Requirements</i>	54
2.9	Directory Service	58
2.9.1	<i>Process Overview</i>	58
2.9.2	<i>User Requirements</i>	58
2.10	Common Reference Data Management – non-functional Requirements	61
2.10.1	<i>Availability</i>	61
2.10.2	<i>Disaster Recovery</i>	61
2.10.3	<i>Performance Requirements</i>	61
3	BUSINESS DAY (BD)	63
3.1	Overview	63
3.1.1	<i>Context Diagram</i>	63
3.1.2	<i>Business Processes</i>	63
3.2	Scheduler Process	64
3.2.1	<i>Business Process Model</i>	64
3.2.2	<i>Process Overview</i>	65
3.2.3	<i>User Requirements</i>	65
3.3	End of Day/Start of Day Process	68
3.3.1	<i>Business Process Model</i>	68
3.3.2	<i>Process Overview</i>	69
3.3.3	<i>User Requirements</i>	70
3.4	Availability of services	74
3.4.1	<i>Business day schedule</i>	75
3.4.2	<i>User Requirements</i>	76
4	USER ROLES AND ACCESS (URA)	81
4.1	Overview	81
4.1.1	<i>Business Processes</i>	81
4.1.2	<i>General User Requirements for URA</i>	82
4.2	Two-Eyes Approval	84

4.2.1	User Requirements	84
4.3	Four-Eyes Approval	85
4.3.1	Business Process Model.....	86
4.3.2	User Requirements.....	87
5	INFORMATION AND REPORTING (IR)	90
5.1	Overview	90
5.1.1	Context Diagram.....	90
5.1.2	Business Processes.....	91
5.2	Query.....	92
5.2.1	Business Process Model.....	92
5.2.2	Process overview.....	93
5.2.3	User Requirements.....	94
5.3	Produce Scheduled Report and Send (A2A) / Store for Download (U2A)	97
5.3.1	Business Process Model.....	97
5.3.2	Process overview.....	98
5.3.3	User Requirements.....	98
5.4	Information and Reporting – non-functional Requirements.....	100
5.4.1	Availability.....	100
5.4.2	Disaster Recovery.....	100
5.4.3	Performance Requirements	100
6	DATA WAREHOUSE (DWH).....	102
6.1	Overview	102
6.1.1	Context Diagram.....	102
6.1.2	Business Processes.....	103
6.2	Data Warehouse Information Collection	104
6.2.1	Business Process Model.....	104
6.2.2	Process Overview.....	104
6.2.3	User Requirements.....	104
6.3	Data Warehouse Gather Information	106
6.3.1	Business Process Model.....	106
6.3.2	Process Overview.....	106
6.3.3	User Requirements.....	106
6.4	Non-functional Requirements for Data Warehouse	107
6.4.1	Availability.....	107

6.4.2	Disaster Recovery.....	107
7	GENERAL NON-FUNCTIONAL REQUIREMENTS	109
7.1	General framework.....	109
7.2	Information Security	109
7.3	Cyber Resilience	109
7.4	TARGET Service Desk	110
7.5	General Business Continuity Requirements	110
7.6	Service Management	112
7.7	Clock Synchronisation	112
7.8	Testing Requirements	112
8	USER INTERACTION	113
8.1	General User Requirements for User Interaction	113
8.1.1	Query.....	113
8.1.2	Action.....	113
8.2	User Interaction for Eurosystem Single Market Infrastructure Gateway	115
8.2.1	Query.....	115
8.3	User Interaction for Common Reference Data Management.....	116
8.3.1	Query.....	116
8.3.2	Action.....	120
8.4	User Interaction for Business Day.....	125
8.4.1	Query.....	125
8.5	User Interaction for Data Warehouse (DWH)	125
8.5.1	Report.....	125
9	BUSINESS DATA DEFINITIONS	126
9.1	Entity Relationship Diagrams	127
9.1.1	Party.....	127
9.1.2	Cash Account	131
9.1.3	User.....	132
9.2	Entities and Attributes	133

1 EUROSYSTEM SINGLE MARKET INFRASTRUCTURE GATEWAY (ESMIG)

1.1 OVERVIEW

This section describes the user requirements for the long term solution of ESMIG. ESMIG shall offer a catalogue of features to be used by each of the different services, components and applications (e.g. CLM, RTGS, T2S, TIPS, ECMS). The list of ESMIG features will include "mandatory features" (like connectivity and authentication) and "optional features"¹ which may be configured for use according to the specific business needs of the service, component or application. All requirements of ESMIG described in this URD are mandatory apart from those specifically flagged as optional. All services, components and applications can freely choose from the ESMIG features portfolio according to their needs. The complete set of user requirements are described to provide a comprehensive picture of the future ESMIG, to be taken into account for the entire architecture of ESMIG.

1.1.1 Context Diagram

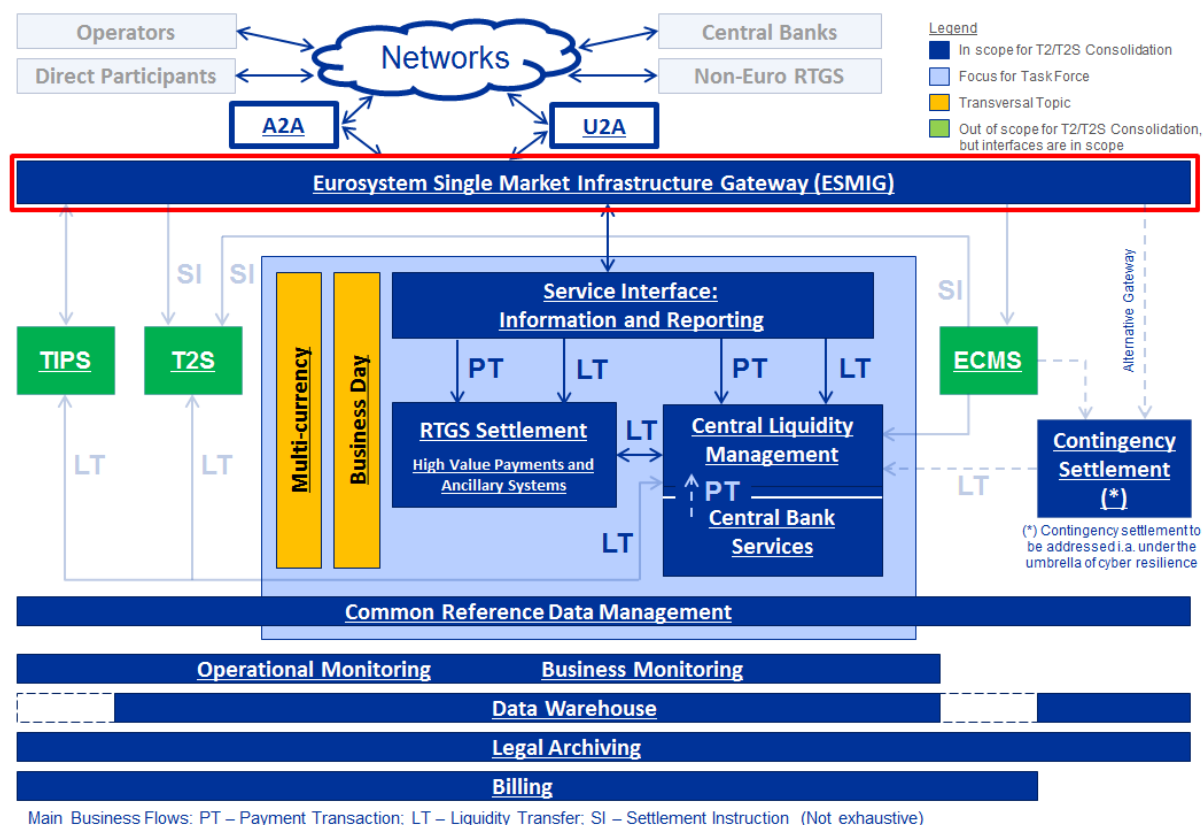


Figure 1: Context diagram for Eurosystem Single Market Infrastructure Gateway

1.1.2 General User Requirements for ESMIG

The user requirements for ESMIG are grouped according to the following topics: network connectivity, security services, operational services and messaging services.

Network connectivity

¹ Among the possible ESMIG optional features there is the XML schema validation.

User Requirement Common Components

Id	SHRD.UR.ESMIG.ALL.000.010
Name	Connectivity through multiple Network Services Providers
Description	ESMIG shall provide connectivity via multiple Network Service Providers (NSPs) in parallel, which means that ESMIG is reachable for the users using one or more NSPs selected from the available multiple Network Service Providers.

Id	SHRD.UR.ESMIG.ALL.000.020
Name	Network agnostic - no proprietary features
Description	ESMIG shall ensure a network agnostic communication with the users, where network agnostic means multiple Network Service Providers are allowed. All Network Service Providers shall fulfil the same communication interface specification towards ESMIG but are free to use their own features internally in terms of network and messaging.

Id	SHRD.UR.ESMIG.ALL.000.030
Name	Single access to all Eurosystem Market Infrastructure Services
Description	ESMIG shall provide the single access point for the external communication to all Eurosystem Market Infrastructure Services. It should be designed following a concept allowing an easy adoption of further services, components and applications to be accessed via ESMIG.

Id	SHRD.UR.ESMIG.ALL.000.040
Name	Support for business continuity
Description	ESMIG shall provide business continuity measures (e.g. multiple sites, path diversification, etc.) based on the different Eurosystem Market Infrastructure Service requirements.

Id	SHRD.UR.ESMIG.ALL.000.050
Name	Support for business continuity - no message loss
Description	An acknowledged message must never be lost - except in a regional disaster scenario (see section 1.2.2. on Disaster Recovery in this User Requirements Document).

Id	SHRD.UR.ESMIG.ALL.000.060
Name	Redundancy against single component failures
Description	ESMIG shall provide redundancy against single component failures by supporting redundant components and automated failover.

User Requirement Common Components

Id	SHRD.UR.ESMIG.ALL.000.070
Name	Restart after Disaster (RAD)
Description	ESMIG shall have defined procedures for handling a set of disaster scenarios. The procedures shall ensure the recovery of any potential data loss encountered (see section 1.2.2. on Disaster Recovery in this User Requirements Document).

Id	SHRD.UR.ESMIG.ALL.000.080
Name	Provision of a cost-effective and easy access solution
Description	ESMIG shall offer a cost-effective access via U2A to the services, components and applications especially for participants with only a low volume of payment orders. Note: The cost effective solution for low volume customers could also be provided as an additional option.

Id	SHRD.UR.ESMIG.ALL.000.090
Name	Authorisation
Description	ESMIG shall offer basic authorisation service to access Eurosystem Market Infrastructure Services in U2A and A2A mode. Note: The basic authorisation should cover a check which services, components or applications a user is allowed to access. In the case of a rejection a message including an error code will be sent to the sender in A2A mode and an error message will be displayed on U2A screen.

Id	SHRD.UR.ESMIG.ALL.000.100
Name	Generalised interface for the Common Reference Data Management to feed the Identity Access Management (IAM) for U2A
Description	ESMIG shall use a standardised interface to CRDM, provided by CRDM, for collecting reference data information of the different services, components and applications to enable the authentication and basic authorisation features.

Id	SHRD.UR.ESMIG.ALL.000.110
Name	Supported protocols to access via A2A
Description	ESMIG shall support communication using multiple protocols as requested by the different services, components and applications served to access via A2A for the external communication of the Eurosystem Market Infrastructure Services.

User Requirement Common Components

Id	SHRD.UR.ESMIG.ALL.000.120
Name	Supported protocols to access via A2A: DEP
Description	ESMIG shall support communication using the Data Exchange Protocol (DEP) to access via A2A.

Security services

Id	SHRD.UR.ESMIG.ALL.000.130
Name	Compliant with Information Security and Cyber Resilience Requirements
Description	ESMIG shall be compliant with the Information Security and Cyber Resilience requirements. Note: For details see the following documents • Market Infrastructure Security Requirements and Controls • Market Infrastructure Cyber Resilience requirements All requirements must be fulfilled in a central integrated way.

Id	SHRD.UR.ESMIG.ALL.000.180
Name	Support of security services – Inbound traffic
Description	ESMIG shall provide authentication of all inbound traffic (U2A and A2A).

Id	SHRD.UR.ESMIG.ALL.000.190
Name	Support of security services – Sender Identification
Description	ESMIG shall provide sender (i.e. external party sending communication) identification.

Id	SHRD.UR.ESMIG.ALL.000.200
Name	Support of security services – Non repudiation
Description	ESMIG shall provide non repudiation features for digital signature management for U2A and A2A communication.

Id	SHRD.UR.ESMIG.ALL.000.210
Name	Support of security services – Security monitoring
Description	ESMIG shall provide security monitoring for the TARGET Service Desk.

User Requirement Common Components

Id	SHRD.UR.ESMIG.ALL.000.230
Name	Support of security services - CUG
Description	ESMIG shall support Closed User Groups.

Id	SHRD.UR.ESMIG.ALL.000.240
Name	Support of security services - PKI
Description	ESMIG shall provide Public Key Infrastructure Services.

Operational services

Id	SHRD.UR.ESMIG.ALL.000.250
Name	Service time of ESMIG
Description	ESMIG shall offer a service time compatible with the availability requirements of the Eurosystem Market Infrastructure Services.

Id	SHRD.UR.ESMIG.ALL.000.260
Name	Response time and throughput of ESMIG
Description	ESMIG shall be subject to the service level agreements of all dependent services, components and applications. The dependent services, components and applications should specify their service levels including the required processing in ESMIG.

Id	SHRD.UR.ESMIG.ALL.000.270
Name	Feature catalogue of ESMIG
Description	ESMIG shall provide a feature catalogue with the features offered to the dependent services, components and applications. The dependent services, components and applications can select the features they require from the ESMIG feature catalogue.

Id	SHRD.UR.ESMIG.ALL.000.280
Name	Scalability
Description	ESMIG shall offer scalability to cope with the different Eurosystem Market Infrastructure Service throughput.

User Requirement Common Components

Id	SHRD.UR.ESMIG.ALL.000.290
Name	Independency of services, components and applications regarding volumes
Description	ESMIG shall take care that the traffic of one service, component or application may not impact the processing time of messages from or to other services, components or applications.

Id	SHRD.UR.ESMIG.ALL.000.300
Name	Archiving of inbound and outbound communications and events
Description	ESMIG shall archive all inbound and outbound communications. The retention period shall be configurable (up to 30 calendar days). After this period the data shall be available via Legal Archiving for a period defined for the legal archive. ESMIG shall offer this feature on an optional basis so that each service, component and application may opt for it or not as applicable. Note: There is no need to store the inbound and outbound communications in the services, components and applications but they will offer functionality to the users to provide information on the communications for a configurable period of time by making use of the data archived by ESMIG.

Id	SHRD.UR.ESMIG.ALL.000.310
Name	Logging of all inbound and outbound communications and events
Description	ESMIG shall log all inbound and outbound communication.

Id	SHRD.UR.ESMIG.ALL.000.320
Name	Provision of operational/monitoring tools
Description	ESMIG shall provide operational/monitoring tools to enable the monitoring of the system's operational performance by the TARGET Service Desk.

Messaging services

Id	SHRD.UR.ESMIG.ALL.000.330
Name	Provision of access via A2A and U2A
Description	ESMIG shall provide access via A2A and U2A.

User Requirement Common Components

Id	SHRD.UR.ESMIG.ALL.000.340
Name	Provision of store-and-forward (S&F) and real time communication (RT) modes
Description	ESMIG shall support store-and-forward and real time communication modes, both in push and pull mode. ESMIG shall provide time out and oversize handling for RT messages if requested i.e. ESMIG shall offer this feature on an optional basis so that each service, component and application can opt for it or not as applicable.

Id	SHRD.UR.ESMIG.ALL.000.350
Name	Provision of retry mechanism for S&F communication modes
Description	ESMIG shall provide a retry mechanism for store-and-forward communications.

Id	SHRD.UR.ESMIG.ALL.000.360
Name	Provision of message and file channel
Description	ESMIG shall handle messages and files via all supported modes (S&F and RT).

Id	SHRD.UR.ESMIG.ALL.000.370
Name	Provision of message and file routing to the different Eurosystem Market Infrastructure Services
Description	ESMIG shall route incoming messages and files to the different Eurosystem Market Infrastructure Services addressed. ESMIG shall identify and select the appropriated service, component or application based on information provided as part of the communication. Additionally, ESMIG shall pass the ID of the sender (as a result of authentication process) and additional parameters to the service.

The identification could for instance be based on a Distinguished Name (DN) for the service, component or application.

Id	SHRD.UR.ESMIG.ALL.000.380
Name	Provision of message and file routing to the external party
Description	ESMIG shall route messages and files to the external party using the Network Service Provider, address used by the NSP to identify the external party, communication mode and protocol provided by the Eurosystem Market Infrastructure Services (i.e. external user address).

User Requirement Common Components

Id	SHRD.UR.ESMIG.ALL.000.390
Name	Provision of decompression/compression mechanism
Description	ESMIG shall provide decompression/compression mechanisms for the communications.

Id	SHRD.UR.ESMIG.ALL.000.400
Name	Provision of inbound message queueing and restart of queued inbound messages
Description	ESMIG shall queue messages in A2A (e.g. in case a service is temporarily unavailable). At the point in time the service, component or application is up and running again ESMIG shall forward the queued inbound message. ESMIG shall offer this feature on an optional basis so that each service, component and application can opt for it or not as applicable.

Id	SHRD.UR.ESMIG.ALL.000.410
Name	Information of Network Service Providers about opening and closure of a service, component or application due to queueing and restart of inbound messages
Description	ESMIG shall inform the Network Service Providers about the closure of each dedicated service, component and application, so that the relevant messages could be queued at NSP level. ESMIG shall inform the Network Service Providers about the opening of each dedicated service, component and application, so that the relevant queued messages could be forwarded to ESMIG. ESMIG shall offer this feature on an optional basis so that each service, component and application can opt for it or not as applicable.

Id	SHRD.UR.ESMIG.ALL.000.420
Name	Provision of outbound message queueing and restart of queued outbound messages
Description	ESMIG shall queue messages (e.g. in case the external connectivity layer is temporarily unavailable). At the point in time the connectivity is up and running again ESMIG shall forward the queued message to the external connectivity layer. ESMIG shall offer this feature on an optional basis so that each service, component and application can opt for it or not as applicable.

User Requirement Common Components

Id	SHRD.UR.ESMIG.ALL.000.430
Name	Validation checks for inbound communication received on the message and file channel
Description	ESMIG shall perform the following validation checks, at transport level, for inbound communication regardless of the channel via which they are received: • The technical sender is allowed to use the addressed service, component or application; • Duplicated inbound communications are rejected; and • XML message is well-formed. ESMIG shall forward only valid messages to the services, applications and components. Where a message does not pass the validation checks, ESMIG will send a rejection message, including the appropriate error code(s), to the sender.

Id	SHRD.UR.ESMIG.ALL.000.440
Name	Resending of messages and files
Description	ESMIG shall provide resending functionality for all inbound and outbound messages and files, either for single messages/files or for massive resends (such resending functionality will be available only to the 4CB Service Desk and will not be performed automatically by the system).

This ESMIG requirement is complementary to the Retrieval capability provided by the Network Service Providers. Actors will be able to request messages and files directly or indirectly from the 4CB Service Desk, according to operational processes to be defined.

Id	SHRD.UR.ESMIG.ALL.000.460
Name	Single sign-on for all Eurosystem Market Infrastructure Services in U2A
Description	ESMIG shall be the access portal for U2A users to all underlying business applications, meaning to all Eurosystem Market Infrastructure Services. After the logon to ESMIG a landing page will be displayed offering all Eurosystem Market Infrastructure Services according to the access rights of the user.

1.2 EUROSYSTEM SINGLE MARKET INFRASTRUCTURE GATEWAY – NON-FUNCTIONAL REQUIREMENTS

1.2.1 Availability

Id	SHRD.UR.ESMIG.NFR.020
Name	Availability
Description	Availability, calculated on a quarterly basis should be at least 99.7% for real time based communication (including U2A).

ESMIG may be subject to incidents or failures, which may cause a temporary and unforeseen interruption of the availability of the component. Regardless of the total number of such unplanned interruptions, the overall amount of unavailability time calculated on a quarterly basis shall not exceed 2.16 hours.

Id	SHRD.UR.ESMIG.NFR.030
Name	Availability for store-and-forward communication
Description	Availability, calculated on a quarterly basis, equivalent to an availability of 99.7% for store-and-forward based communication.

1.2.2 Disaster Recovery

Id	SHRD.UR.ESMIG.NFR.040
Name	Recovery Point Objective
Description	ESMIG shall ensure a recovery point objective (RPO) value of zero minutes in the event of site failures. Where there is a loss of a complete region the RPO shall not exceed two minutes.

The RPO is a point of consistency to which a user wants to recover or restart the service. It is measured as the amount of time between the moment when the point of consistency was created and the moment when the failure occurred.

ESMIG ensures synchronous point of consistency creations and, as a consequence, no data loss in the event of failures, unless the component cannot be restarted in the same region and a failover to the backup-region has to be conducted. In this case a data loss of two minutes will be tolerated.

Id	SHRD.UR.ESMIG.NFR.050
Name	Rebuilding of Lost Data
Description	External parties shall be able to resend messages, should the addressed service, component or application require this. Resending messages shall be possible for all messages sent during at least the previous two minutes.

This requirement covers that in the event of a possible data loss due to a regional disaster, transactions can be rebuilt.

User Requirement Common Components

Id	SHRD.UR.ESMIG.NFR.060
Name	Recovery Time Objective
Description	ESMIG shall have a recovery time objective (RTO) according to the requirements of the connected services, components and applications.

The RTO is the maximum amount of time required for recovery or restart of the service to a specified point of consistency. In the event of a site failure, ESMIG shall ensure maximum time of unavailability of zero minutes for TIPS and one hour for all other services, components and applications starting from the time when the decision to restart the service, component or application is made up to the time it is restored. In the event of a major failure or a regional disaster, ESMIG shall ensure maximum time of unavailability of 15 minutes for TIPS and two hours for all other services, components and applications starting from the time when the decision to restart the service, component or application is made up to the time it is restored.

1.2.3 Performance Requirements

Id	SHRD.UR.ESMIG.NFR.070
Name	Response Time Goals
Description	ESMIG shall be subject to the response time requirements of the connected services, components and applications. The dependent services, components and applications should specify their service levels including the required processing in ESMIG.

ESMIG shall be efficient enough to cope with the service levels of all connected services, components and applications.

Id	SHRD.UR.ESMIG.NFR.080
Name	Upward Scalability
Description	ESMIG shall be scalable to handle higher throughputs in order to cope with e.g. short-term market shocks and foreseeable increases: • a 20% higher workload within 15 minutes; and • a double of the workload (but up to 200 transactions per second) within 365 days.

In the course of the service's lifecycle the number of business transactions to be handled by ESMIG will change. ESMIG must be scalable to handle such changes.

Id	SHRD.UR.ESMIG.NFR.100
Name	Maximum Size of Files and Messages
Description	ESMIG shall be able to handle a maximum file size of 99 MB.

2 COMMON REFERENCE DATA MANAGEMENT (CRDM)

2.1 OVERVIEW

2.1.1 Context Diagram

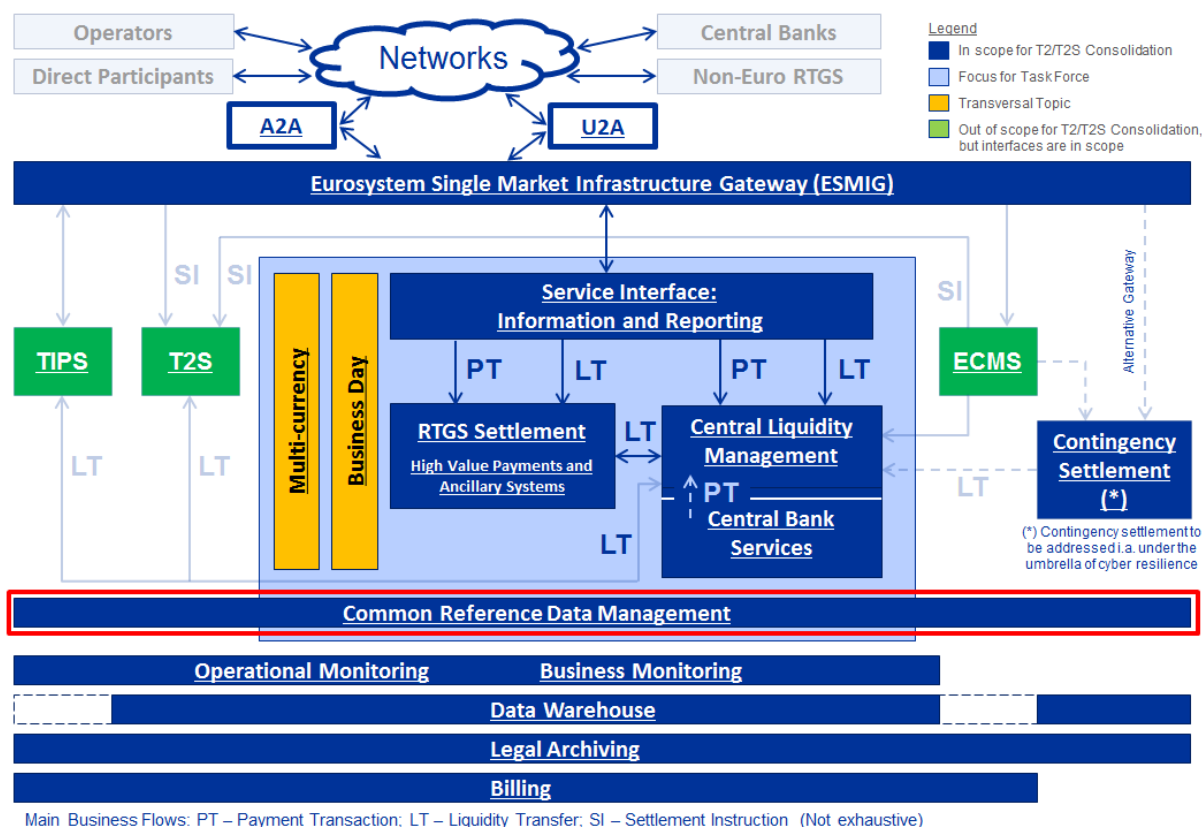


Figure 2: Context Diagram for Common Reference Data Management

This section describes the common processes for the management of reference data required for the configuration and operation of all services, components and applications. This includes the *creation*, *amendment* and *deletion* of all reference data entities as well as the propagation of all changes to all services, components and applications impacted by the change.

The analysis of the data requirements completed so far for TIPS, ECMS and T2-T2S Consolidation indicates that the majority of reference data would need to be shared with at least one other service, component or application and thus would be considered as Common Reference Data.

From the perspective of the processes required to manage the reference data, it is envisaged that all reference data, common or specific for one service, component or application, shall be maintained by the same set of common processes described. The aim is to achieve consistency and integrity of all reference data and the relationships between them across all services, components and applications, and to avoid duplication and redundancy.

As the intention is to not change T2S, it is implied without being stated explicitly that all Common Reference Data required for T2S is included within the scope of this section. The intention is to build a common data model shared across all services, components and applications during the realisation phase of the project.

User Requirement Common Components

Within the context of the User Requirements Document, an 'entity' is a person, organisation, place, thing or concept which helps to define or is of interest to RTGS and CLM, such as Party, Central Bank, Cash Account, Standing Order etc. Each entity is described by a number of 'attributes' which are the individual pieces of information about that entity.

No distinction is made between which processes may be used by which type of Party. Some processes will be available to any account holder whilst others will only be available to Central Banks or Operators. This will be managed through User Roles and Access. Similarly, it is envisaged that all processes could be provided in both U2A and A2A modes.

Although it has not been explicitly stated, all of the business processes include the requirement to record a full audit trail of all changes made to any reference data, including the date and timestamp of the change, which user or system process made the change and the details of the change made.

2.1.2 Business Processes

Business Process	BP Reference	Business Process Description
Create an occurrence of Common Reference Data	SHRD.BP.CRDM.CRERD	Creation of any Common Reference Data entity
Amend an occurrence of Common Reference Data	SHRD.BP.CRDM.AMDRD	Amendment of any Common Reference Data entity
Delete an occurrence of Common Reference Data	SHRD.BP.CRDM.DELRD	Deletion of any Common Reference Data entity
Propagate Changes	SHRD.BP.CRDM.PROP	Propagate changes to Common Reference Data to all services, components and applications that need the information for their processing
Block an occurrence of Common Reference Data	SHRD.BP.CRDM.BLKRD	Blocking of a cash account, an account holder or an Ancillary System
Unblock an occurrence of Common Reference Data	SHRD.BP.CRDM.UNBLKRD	Unblocking of a cash account, an account holder or an Ancillary System
Close a Cash Account	SHRD.BP.CRDM.CLOACC	Closing a cash account
Directory Service	SHRD.BP.CRDM.DIR	Provides the services' directories

Table 1: Business Processes for Common Reference Data Management

2.1.3 General User Requirements for CRDM

The generic processes for the creation, amendment and deletion of an occurrence of reference data (referred to generically as maintain data) can be applied to all Common Reference Data entities.

For revisions and audit trail requirements the modified data at attribute level as well as the user and timestamp will be documented. Additionally, a chronological record of changes will be stored to keep a history.

Id	SHRD.UR.CRDM.ALL.000.010
Name	Audit trail
Description	CRDM shall ensure that for each creation, amendment and deletion of a reference data entity, the modified data at attribute level, the user performing the change and the timestamp of the change are logged.

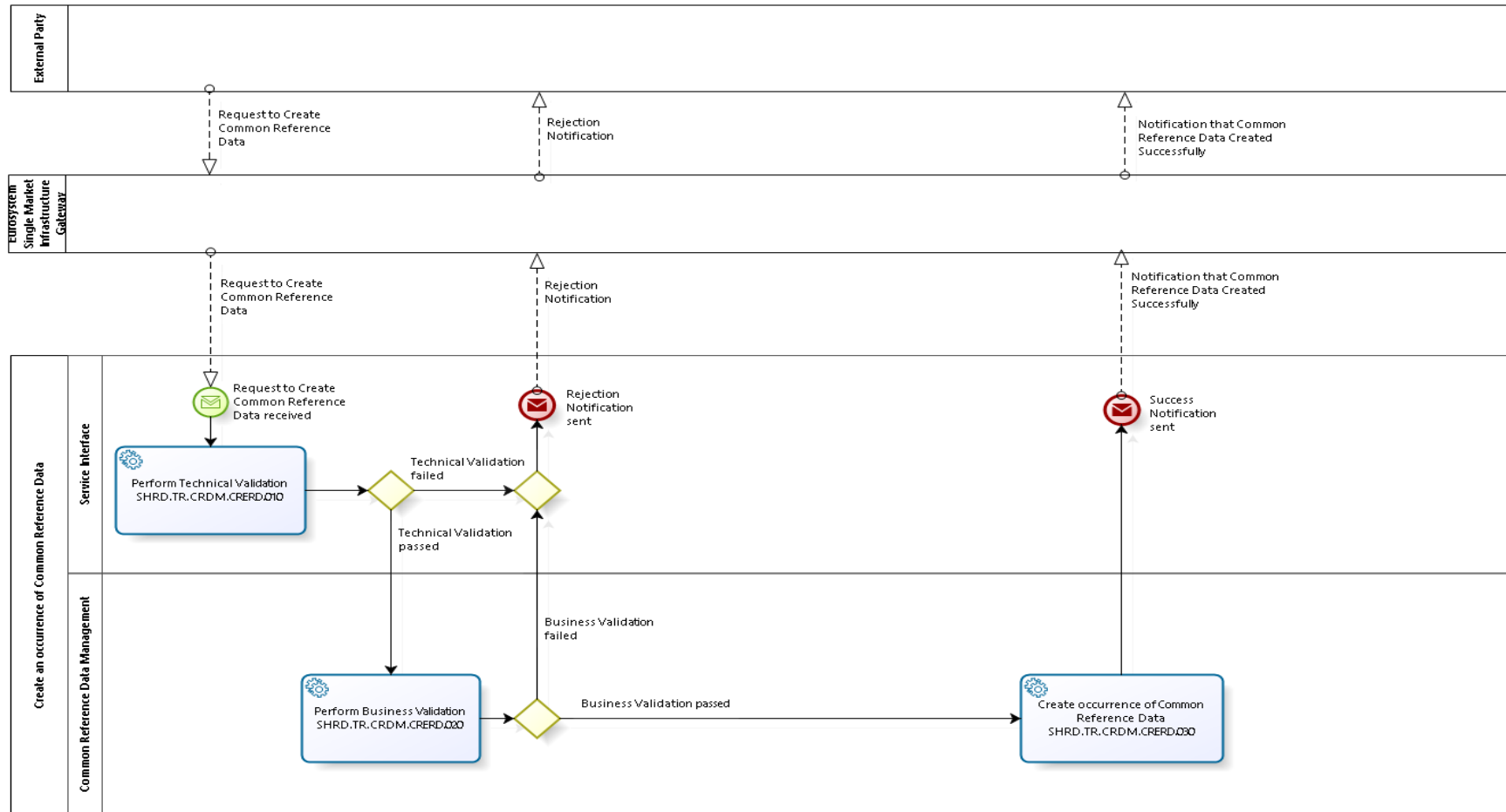
Id	SHRD.UR.CRDM.ALL.000.020
Name	Data history
Description	CRDM shall maintain a chronological record of all changes to the values held for the reference data.

Id	SHRD.UR.CRDM.ALL.000.030
Name	Check user access rights
Description	CRDM shall check that the user has appropriate authorisation, through User Roles and Access Rights, to perform the intended function on the intended reference data entity.

2.2 CREATE AN OCCURRENCE OF COMMON REFERENCE DATA

Business Process Ref: SHRD.BP.CRDM.CRERD

2.2.1 Business Process Model



Business Process Model 1: Create an occurrence of Common Reference Data

2.2.2 Process Overview

Process goal:

This business process describes the creation of an occurrence of reference data. The relevant entities are described in chapter 9 on Business Data Definitions (BDD) in this User Requirements Document.

Where the Common Reference Data entity includes a Valid From Date and a Valid From Event, these shall be used to determine which version of the Common Reference Data entity is valid at the time.

The Valid From Date indicates the business date when it will become valid in the system, which by default will be the next business date. If the Valid From Event is not specified then it will become valid at the start of the business day indicated by the Valid From Date. Otherwise it will become valid in the system when the Valid From Event occurs, such as at the Start of Day, End of Day or the completion of a specified process.

Common Reference Data may also include a Valid To Date and a Valid To Event, indicating the point at which it will no longer be valid in the system and can no longer be used.

The user will select Valid From Event and Valid To Event from a list of possible values, each of which shall be an event recognisable by the system and recorded in the scheduler. In addition, the Event may be specified as 'Immediate'.

When a Common Reference Data entity requires the above described date validity attributes (or any subset of them), this is explicitly specified in the definition of the entity in the Business Data Definitions section in this User Requirements Document.

Process context:

- ▶ The generic process and its descriptions are valid for all reference data entities.

Pre-conditions:

- ▶ None

Time constraints:

- ▶ Maintenance window

Expected results:

- ▶ If the request content is either invalid or fails the reference data checks, it will be rejected and a rejection notification with the appropriate error code(s) will be sent to the sender of the message.
- ▶ If the request content is valid and reference data checks have been passed successfully, the platform will create an occurrence of reference data and the platform will send a success notification to the sender of the message.

Triggers:

- ▶ The process will be initiated by a Party sending a request to the platform to create a new occurrence of reference data.

2.2.3 User Requirements

2.2.3.1 PERFORM TECHNICAL VALIDATION

Task Ref: SHRD.TR.CRDM.CRERD.010

Technical validation shall perform checks such as field level validation (fields have correct data type and size).

If the validation fails, a rejection notification with the appropriate error code(s) shall be sent to the sender of the message.

Id	SHRD.UR.CRDM.CRERD.010.010
Name	Validation of messages received
Description	CRDM shall parse the message received and validate it against the relevant schema to ensure that all attributes are of the correct data type and length. After encountering the first negative validation result, the component interface shall continue to validate as far as possible and report all negative results together in a single message. The component interface shall reject the order only after performing all possible technical validation.

Id	SHRD.UR.CRDM.CRERD.010.020
Name	Check mandatory attributes
Description	CRDM shall ensure that all mandatory attributes are populated

2.2.3.2 PERFORM BUSINESS VALIDATION

Task Ref: SHRD.TR.CRDM.CRERD.020

Where the result of the technical validation is positive, the message is submitted for business validation. The business validation comprises checks on the values of the attributes, cross-field consistency checks (where the value of one field is dependent upon, or has a relationship with, the value of another field, either in the same message or in the data already present in the database) and authorisation checks to ensure that the sender of the creation request has suitable permissions. Additionally, the system will ensure that duplicate entities cannot be created.

If the validation fails, a rejection notification with the appropriate error code(s) shall be sent to the sender of the message.

Id	SHRD.UR.CRDM.CRERD.020.010
Name	Check attribute values
Description	CRDM shall check that the values of all attributes that are populated (mandatory or optional) are valid according to the allowed values or value ranges.

Id	SHRD.UR.CRDM.CRERD.020.020
Name	Check data integrity
Description	CRDM shall check that all cross-field validations (data integrity) are satisfied, either between attributes within the message or between an attribute in the message and one or more items of data held in the system.

Id	SHRD.UR.CRDM.CRERD.020.030
Name	Check Valid From Date
Description	The creation request may include a Valid From Date, although it may not be populated. The value indicates the business date from which the occurrence of Common Reference Data will be valid. If not stated, the next business date shall be used by default. Valid From Date must be a valid date that must be on or after the current business date.

Id	SHRD.UR.CRDM.CRERD.020.040
Name	Check Valid To Date
Description	The creation request may include a Valid To Date, although it may not be populated. The value indicates the business date from which the occurrence of Common Reference Data will no longer be valid. If not stated, no default value will be applied and the occurrence of Common Reference Data will remain valid indefinitely. Valid To Date is optional. If populated, it must be a valid date that must be on or after the current business date, and also on or after the Valid From Date.

Id	SHRD.UR.CRDM.CRERD.020.050
Name	Check Valid From Event
Description	The creation request may include a Valid From Event, although it may not be populated. The value indicates the event that, when it occurs, will be the point from which the occurrence of Common Reference Data will be valid, on the Valid From Date. If the Valid From Event is not populated the occurrence of Common Reference Data will be valid from the Start of Day on the business date indicated by the Valid From Date, or from the Start of Day on the next business date, if the Valid From Date is not populated. The default value for Valid From Event is thus 'Start of Day'. The Valid From Event shall be populated from a list of possible values, each of which shall be an event recognisable by the system and recorded in the scheduler.

Id	SHRD.UR.CRDM.CRERD.020.060
Name	Check Valid To Event
Description	The creation request may include a Valid To Event, although it may not be populated. The value indicates the event that, when it occurs, will be the point from which the occurrence of Common Reference Data will no longer be valid, on the Valid To Date. If the Valid To Event is not populated the occurrence of Common Reference Data will no longer be valid from the Start of Day on the business date indicated by the Valid To Date. The default value for Valid To Event is 'Start of Day'. If the Valid To Event is populated then the Valid To Date must also be populated. The Valid To Event shall be populated from a list of possible values, each of which shall be an event recognisable by the system and recorded in the scheduler.

Id	SHRD.UR.CRDM.CRERD.020.070
Name	Check for duplicate of entity to be created
Description	CRDM shall ensure that an active entity cannot be created a second time.

2.2.3.3 CREATE OCCURRENCE OF COMMON REFERENCE DATA

Task Ref: **SHRD.TR.CRDM.CRERD.030**

After processing all validation successfully the occurrence of Common Reference Data will be created in the system, using the attributes from the request received.

Although the occurrence of Common Reference Data will be present in the system immediately after it has passed the validation, it will not necessarily become valid for use with immediate effect as the

changes in general will be valid from the following business day or may be post-dated through the use of date validity attributes. Only a few reference data will be valid immediately, e.g. blocking, limit.

Processes using the Common Reference Data will need to determine at the time whether the data is valid, by checking the Valid From Date and Valid To Date and the Valid From Event and Valid To Event, or their default values where they were not populated:

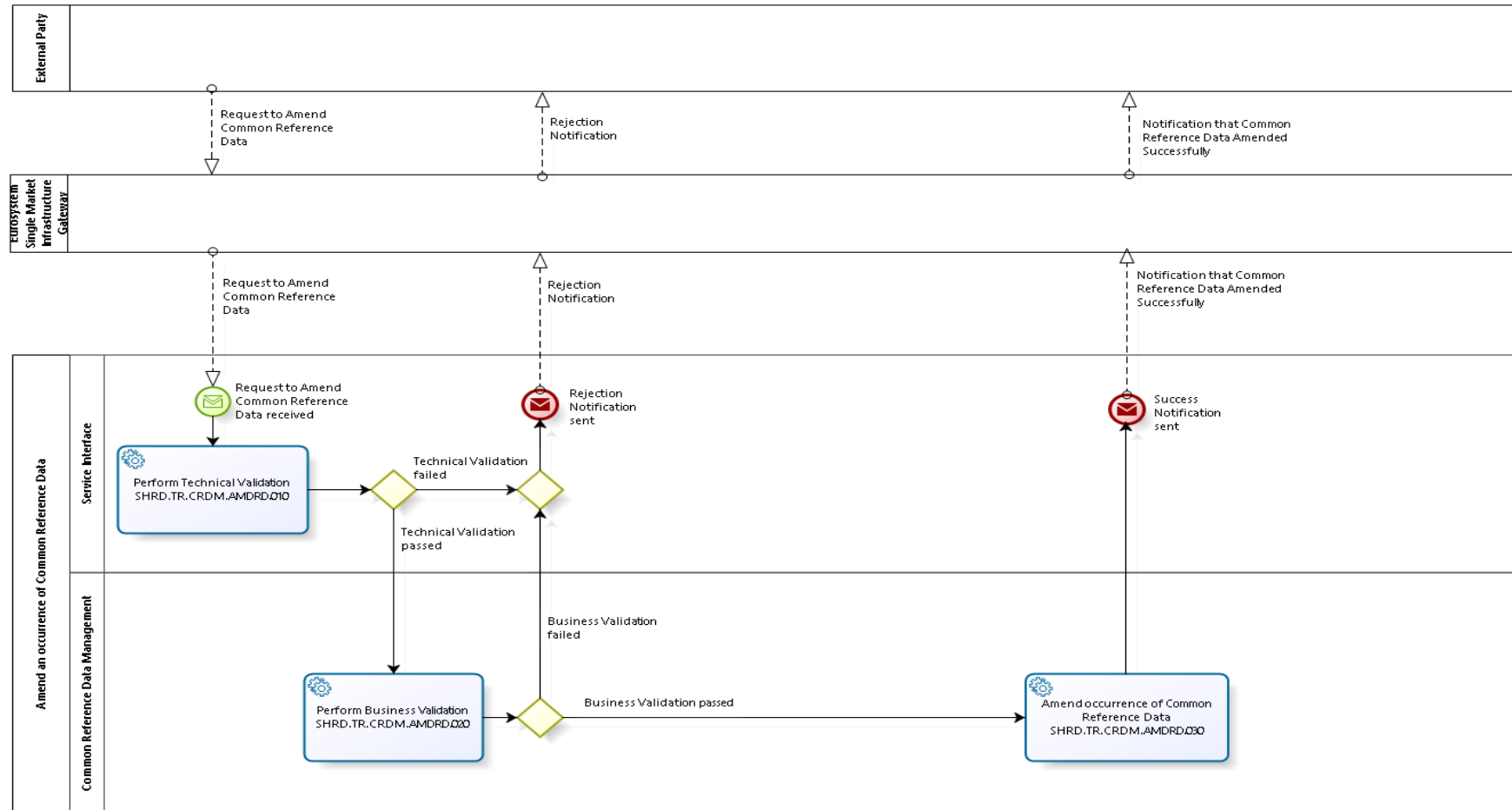
- ▶ If the Valid To Date is not populated and the current business date at that time is after the Valid From Date then the Common Reference Data is valid
- ▶ If the Valid To Date is populated and the current business date at that time is between the Valid From Date and the Valid To Date (i.e. not on either date) then the Common Reference Data is valid
- ▶ If the current business date at that time is the same as either the Valid From Date or the Valid To Date then the process attempting to use the Common Reference Data must check the scheduled processes that have been executed in order to examine whether the Valid From Event or Valid To Event have already occurred or not.

Where the Common Reference Data entity does not include date validity attributes then the new occurrence of the Common Reference Data shall become valid with immediate effect.

2.3 AMEND AN OCCURRENCE OF COMMON REFERENCE DATA

Business Process Ref: SHRD.BP.CRDM.AMDRD

2.3.1 Business Process Model



Business Process Model 2: Amend an occurrence of Common Reference Data

2.3.2 Process Overview

Process goal:

This business process describes the amendment of an occurrence of reference data.

Where the Common Reference Data entity includes a Valid From Date and a Valid From Event, these shall be used to determine which version of the Common Reference Data entity is valid at the time.

The Valid From Date in the amendment request indicates the business date from which the amended version of the reference data will become valid in the system, which by default will be the next business date. If the Valid From Event in the amendment request is not specified then it will become valid at the start of the business day indicated by the Valid From Date. Otherwise it will become valid in the system when the Valid From Event occurs, such as at the Start of Day, End of Day or the completion of a specified process.

The Common Reference Data entity may also include a Valid To Date and a Valid To Event, indicating the point at which it will no longer be valid in the system and can no longer be used. If this has not yet occurred and the occurrence of reference data is currently valid, the Valid To Date and/or Valid To Event can be amended.

When a Common Reference Data entity requires the above described date/event validity attributes (or any subset of them) for specifying the validity of new attribute values, this is explicitly specified in the definition of the entity in section 9 on Business Data Definitions in this User Requirements Document.

Process context:

- ▶ The generic process and its descriptions are valid for all reference data entities.

Pre-conditions:

- ▶ The occurrence of the reference data must already exist.

Time constraints:

- ▶ Maintenance window

Expected results:

- ▶ If the request content is either invalid or fails the reference data checks, it will be rejected and a rejection notification with the appropriate error code(s) will be sent to the sender of the message.
- ▶ If the request content is valid and reference data checks have been passed successfully, the platform will amend the occurrence of reference data and the platform will send a success notification to the sender of the message.

Triggers:

- ▶ The process will be initiated by a Party sending a request to the platform for an amendment to an existing occurrence of reference data.

2.3.3 User Requirements

2.3.3.1 PERFORM TECHNICAL VALIDATION

Task Ref: SHRD.TR.CRDM.AMDRD.010

Technical validation shall perform checks such as field level validation (fields have correct data type and size) for messages received.

If the validation fails, a rejection notification with the appropriate error code(s) shall be sent to the sender of the message.

Id	SHRD.UR.CRDM.AMDRD.010.010
Name	Validation of messages received
Description	CRDM shall parse the message received and validate it against the relevant schema to ensure that all attributes are of the correct data type and length.

Id	SHRD.UR.CRDM.AMDRD.010.020
Name	Check mandatory fields
Description	CRDM shall ensure that all mandatory attributes are populated.

2.3.3.2 PERFORM BUSINESS VALIDATION

Task Ref: SHRD.TR.CRDM.AMDRD.020

Where the result of the technical validation is positive, the message is submitted for business validation. The business validation comprises checks on the values of the attributes, cross-field consistency checks (where the value of one field is dependent upon, or has a relationship with, the value of another field, either in the same message or in the data already present in the database) and authorisation checks to ensure that the sender of the amendment request has suitable permissions.

If the validation fails, a rejection notification with the appropriate error code(s) shall be sent to the sender of the message.

Id	SHRD.UR.CRDM.AMDRD.020.010
Name	Identify occurrence of Common Reference Data entity to be amended
Description	CRDM shall ensure that the occurrence of reference data to be amended has already been created (regardless of whether it is currently valid or not).

Id	SHRD.UR.CRDM.AMDRD.020.020
Name	Check attribute values
Description	CRDM shall check that the values of all attributes that are populated (mandatory or optional) are valid according to the allowed values or value ranges.

Id	SHRD.UR.CRDM.AMDRD.020.030
Name	Check data integrity
Description	CRDM shall check that all cross-field validations (data integrity) are satisfied, either between attributes within the message or between an attribute in the message and one or more items of data held in the system.

Id	SHRD.UR.CRDM.AMDRD.020.040
Name	Check Valid From Date
Description	The amendment request may include a Valid From Date, although it may not be populated. The value indicates the business date from which the amendment to the occurrence of Common Reference Data will be valid. If not stated, the next business date shall be used by default. Valid From Date must be a valid date that must be on or after the current business date.

Id	SHRD.UR.CRDM.AMDRD.020.050
Name	Check Valid To Date
Description	The amendment request may include a Valid To Date, although it may not be populated. The value indicates the business date from which the occurrence of Common Reference Data will no longer be valid. If not stated, no default value will be applied and the occurrence of Common Reference Data will remain valid indefinitely. Valid To Date is optional. If populated, it must be a valid date that must be on or after the current business date, and also on or after the Valid From Date.

Id	SHRD.UR.CRDM.AMDRD.020.060
Name	Check Valid From Event
Description	The amendment request may include a Valid From Event, although it may not be populated. The value indicates the event that, when it occurs, will be the point from which the amendment to the occurrence of Common Reference Data will be valid, on the Valid From Date. If the Valid From Event is not populated the amendment will be valid from the Start of Day on the business date indicated by the Valid From Date, or from the Start of Day on the next business date, if the Valid From Date is not populated. The default value for Valid From Event is thus 'Start of Day'. The Valid From Event shall be populated from a list of possible values, each of which shall be an event recognisable by the system and recorded in the scheduler.

Id	SHRD.UR.CRDM.AMDRD.020.070
Name	Check Valid To Event
Description	The amendment request may include a Valid To Event, although it may not be populated. The value indicates the event that, when it occurs, will be the point from which the occurrence of Common Reference Data will no longer be valid, on the Valid To Date. If the Valid To Event is not populated the occurrence of Common Reference Data will no longer be valid from the Start of Day on the business date indicated by the Valid To Date. The default value for Valid To Event is 'Start of Day'. If the Valid To Event is populated then the Valid To Date must also be populated. The Valid To Event shall be populated from a list of possible values, each of which shall be an event recognisable by the system and recorded in the scheduler.

2.3.3.3 AMEND OCCURRENCE OF COMMON REFERENCE DATA

Task Ref: SHRD.TR.CRDM.AMDRD.030

After processing all validation successfully the attribute(s) of the specified reference data entity shall be amended to the values from the request received.

Although the amended version of the reference data entity will be present in the system immediately after it has passed the validation, it will not necessarily become valid for use with immediate effect as the change may be post-dated through the use of date/event validity attributes.

Processes using the Common Reference Data will need to determine at the time whether the data is valid, by checking the Valid From Date and Valid To Date and the Valid From Event and Valid To Event, or their default values where they were not populated:

- ▶ If the Valid To Date is not populated and the current business date at that time is after the Valid From Date then the Common Reference Data is valid.
- ▶ If the Valid To Date is populated and the current business date at that time is between the Valid From Date and the Valid To Date (i.e. not on either date) then the Common Reference Data is valid.
- ▶ If the current business date at that time is the same as either the Valid From Date or the Valid To Date then the process attempting to use the Common Reference Data must check the scheduled processes that have been executed to check whether the Valid From Event or Valid To Event have already occurred or not.

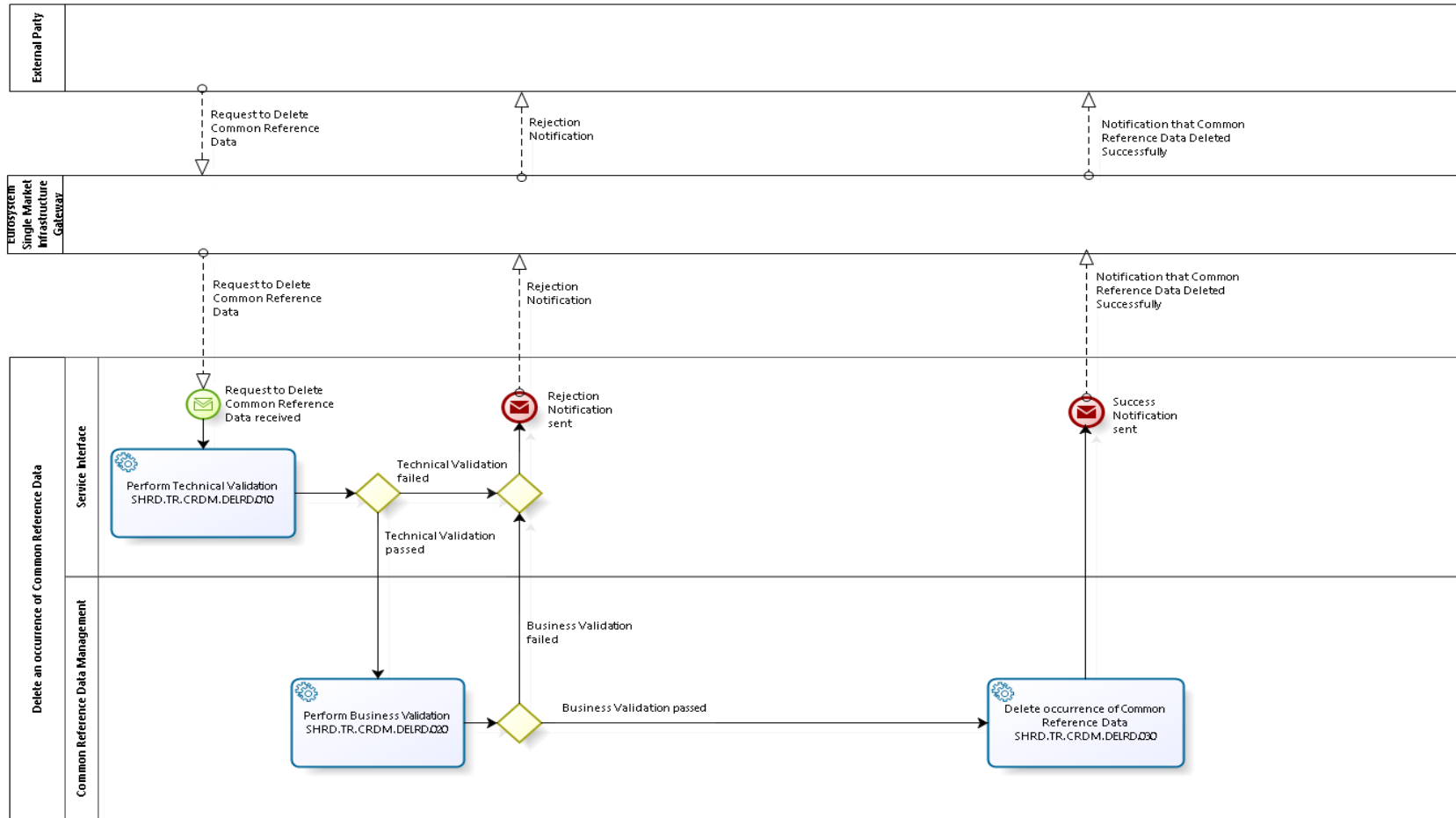
Id	SHRD.UR.CRDM.AMDRD.030.010
Name	Validity of amended reference data
Description	CRDM shall amend the attributes of the entity as requested. Where the entity has date/event validity attributes but these are not stated in the amendment request then, by default, the new values become valid as of the start of the next business day. Alternatively the user may specify a future date and/or event from which the new values become valid by using the Valid From Date and the Valid From Event in the amendment request. Where the entity does not have date/event validity attributes then the amendment shall become valid with immediate effect.

Id	SHRD.UR.CRDM.AMDRD.030.020
Name	Previous version of reference data no longer valid
Description	CRDM shall amend the Valid To Date and Valid To Event for the previous version of the reference data that has been amended, using the values of the Valid From Date and Valid From Event of the new version of the reference data. This will ensure that the end of validity of the previous version and the start of validity of the new version are simultaneous. Where the entity does not have date/event validity attributes then the old values of the amended entity shall become invalid with immediate effect.

2.4 DELETE AN OCCURRENCE OF COMMON REFERENCE DATA

Business Process Ref: SHRD.BP.CRDM.DELRD

2.4.1 Business Process Model



Business Process Model 3: Delete an occurrence of Common Reference Data

2.4.2 Process Overview

Process goal:

This business process describes the logical deletion of an occurrence of reference data, which will be marked as a status update. The subsequent archiving and physical deletion will be handled by a separate process.

Where the Common Reference Data entity includes a Valid From Date and a Valid From Event, these shall be used to determine which version of the Common Reference Data entity is valid at the time.

The Valid From Date in the deletion request indicates the business date on which the logical deletion of the reference data will occur in the system, which by default will be the next business date. If the Valid From Event in the deletion request is not specified then it will occur at the start of the business day indicated by the Valid From Date. Otherwise it will occur in the system when the Valid From Event occurs, such as at the Start of Day, End of Day or the completion of a specified process.

When a Common Reference Data entity requires the above described date/event validity attributes (or any subset of them) for specifying when the entity shall become logically deleted, this is explicitly specified in the definition of the entity in section 9 on Business Data Definitions of this User Requirements Document.

Process context:

- ▶ The generic process and its descriptions are valid for all reference data entities.

Pre-conditions:

- ▶ The occurrence of the reference data must already exist.

Time constraints:

- ▶ Maintenance window

Expected results:

- ▶ If the request content is either invalid or fails the reference data checks, it will be rejected and a rejection notification with the appropriate error code(s) will be sent to the sender of the message.
- ▶ If the request content is valid and reference data checks have been passed successfully, the platform will mark the occurrence of reference data as being logically deleted and the platform will send a success notification to the sender of the message.

Triggers:

- ▶ The process will be initiated by a Party sending a request to the platform for the deletion of an existing occurrence of reference data.

2.4.3 User Requirements

2.4.3.1 PERFORM TECHNICAL VALIDATION

Task Ref: SHRD.TR.CRDM.DELRD.010

Technical validation shall perform checks such as field level validation (fields have correct data type and size) for messages received.

If the validation fails, a rejection notification with the appropriate error code(s) shall be sent to the sender of the message.

Id	SHRD.UR.CRDM.DELRD.010.010
Name	Validation of messages received
Description	CRDM shall parse the message received and validate it against the relevant schema to ensure all attributes are of the correct data type and length.

Id	SHRD.UR.CRDM.DELRD.010.020
Name	Check mandatory fields
Description	CRDM shall ensure that all mandatory attributes are populated.

2.4.3.2 PERFORM BUSINESS VALIDATION

Task Ref: SHRD.TR.CRDM.DELRD.020

Where the result of the technical validation is positive, the message is submitted for business validation. The business validation comprises checks on the values of the attributes, cross-field consistency checks (where the value of one field is dependent upon, or has a relationship with, the value of another field, either in the same message or in the data already present in the database) and authorisation checks to ensure that the sender of the deletion request has suitable permissions.

If the validation fails, a rejection notification with the appropriate error code(s) shall be sent to the sender of the message.

Id	SHRD.UR.CRDM.DELRD.020.010
Name	Identify occurrence of Common Reference Data entity to be deleted
Description	CRDM shall ensure that the occurrence of reference data to be deleted has already been created (regardless of whether it is currently valid or not).

Id	SHRD.UR.CRDM.DELRD.020.020
Name	Check Valid From Date
Description	The deletion request may include a Valid From Date, although it may not be populated. The value indicates the business date on which the occurrence of Common Reference Data will be logically deleted. If not stated, the next business date shall be used by default. Valid From Date must be a valid date that must be on or after the current business date.

Id	SHRD.UR.CRDM.DELRD.020.030
Name	Check Valid From Event
Description	The deletion request may include a Valid From Event, although it may not be populated. The value indicates the event that, when it occurs, will be the point at which the occurrence of Common Reference Data will be logically deleted, on the Valid From Date. If the Valid From Event is not populated the amendment will be valid from the Start of Day on the business date indicated by the Valid From Date, or from the Start of Day on the next business date, if the Valid From Date is not populated. The default value for Valid From Event is thus 'Start of Day'. The Valid From Event shall be populated from a list of possible values, each of which shall be an event recognisable by the system and recorded in the scheduler.

2.4.3.3 DELETE OCCURRENCE OF COMMON REFERENCE DATA

Task Ref: SHRD.TR.CRDM.DELRD.030

After processing all validation successfully the reference data entity will be logically deleted.

Although the reference data entity will be marked as logically deleted in the system immediately after it has passed the validation, it can only be regarded as logically deleted once the business date indicated by the Valid From Date has been reached and the Valid From Event has occurred, where the reference data entity includes date/event validity attributes.

Id	SHRD.UR.CRDM.DELRD.030.010
Name	Logical deletion of Common Reference Data
Description	CRDM shall mark a reference data entity as logically deleted, instead of a physical deletion. Where the entity has date/event validity attributes but these are not stated then, by default, an entity is considered to be deleted as of the start of the next business day. Alternatively the user may specify a future date and/or event when the reference data entity will be logically deleted by using the Valid From Date and the Valid From Event. Where the entity does not have date/event validity attributes then the logical deletion shall become effective immediately.

2.5 PROPAGATE CHANGES

Business Process Ref: SHRD.BP.CRDM.PROP

2.5.1 Process Overview

Process goal:

This business process describes the propagation of changes made to Common Reference Data.

Common Reference Data is maintained centrally for use by any of the Eurosystem Market Infrastructure Services, including TIPS, ECMS, T2S, RTGS and CLM.

Process context:

- ▶ This is the process through which all changes to Common Reference Data (create, amend or delete) are propagated throughout the Eurosystem Market Infrastructure Services.

Pre-conditions:

- ▶ Changes have been made to Common Reference Data.

Time constraints:

- ▶ Maintenance window.

Expected results:

The process propagates any successful change made to any occurrence of Common Reference Data, including:

- ▶ Creating an occurrence of Common Reference Data;
- ▶ Amending an occurrence of Common Reference Data:
 - Changing the value of an attribute;
 - Adding an attribute;
 - Deleting an attribute.
- ▶ Deleting an occurrence of Common Reference Data.

Each change is propagated either intraday or as specified in Valid From (Date/ Event) to each service, component or application that is known to be a user of the Common Reference Data entity associated with the change.

Triggers:

- ▶ The process will be initiated by any successful change made to any occurrence of Common Reference Data.

2.5.2 General User Requirements

Id	SHRD.UR.CRDM.PROP.000.010
Name	Record service, component and application subscribing as user of Common Reference Data entity
Description	For each specific type of reference data entity maintained in the system CRDM shall maintain a list of services, components and applications that shall be informed about any change.

Id	SHRD.UR.CRDM.PROP.000.020
Name	Detect change to an occurrence of Common Reference Data
Description	CRDM shall initiate the process of propagating the change to services, components and applications that need the information for their processing, as soon as the change completed successfully.

Id	SHRD.UR.CRDM.PROP.000.030
Name	Determine services, components and applications impacted by change to an occurrence of Common Reference Data
Description	CRDM shall provide information to the services, components and applications that need the information for their processing whenever an occurrence of Common Reference Data is created, amended or deleted.

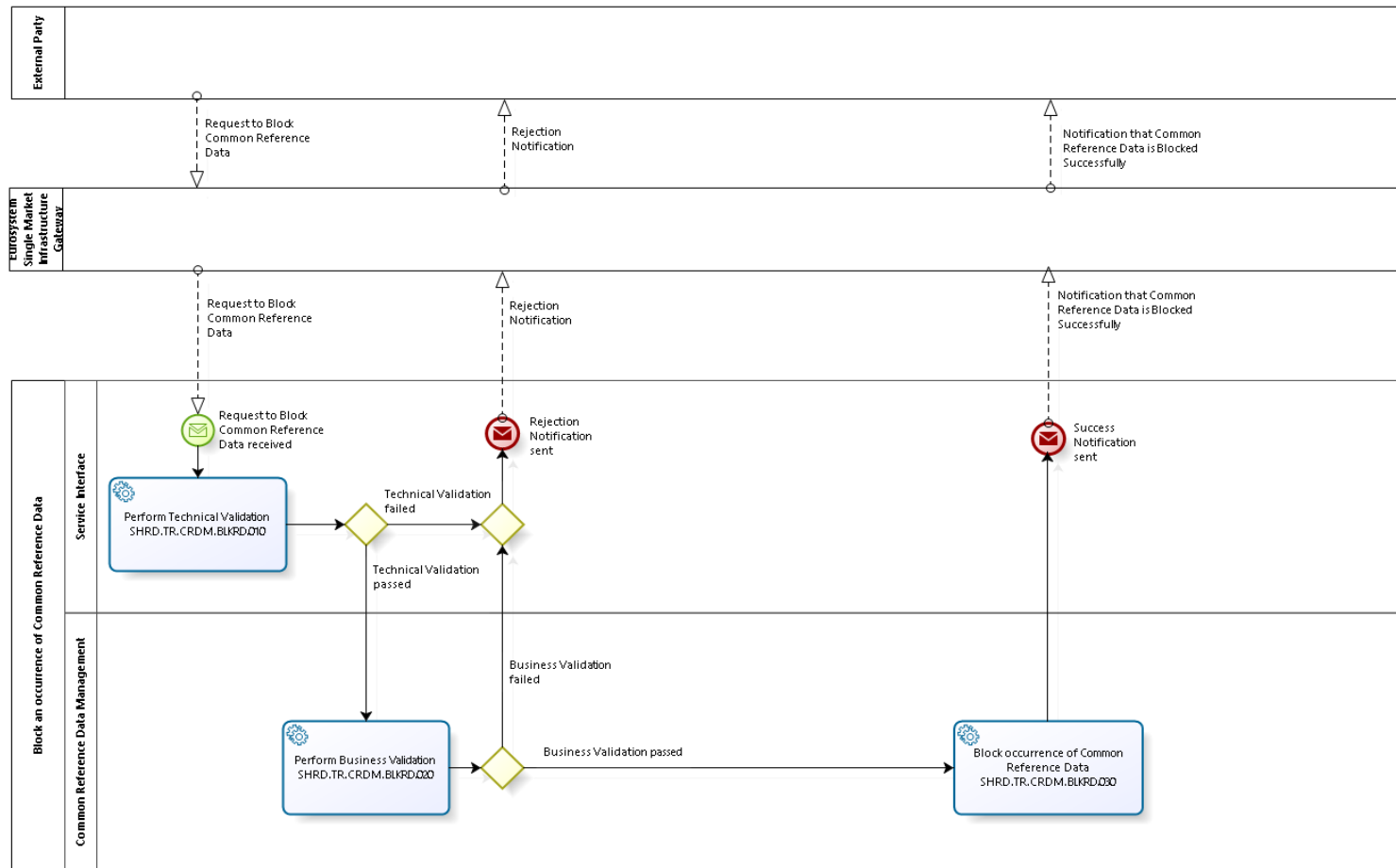
Id	SHRD.UR.CRDM.PROP.000.040
Name	Propagate change to an occurrence of Common Reference Data
Description	CRDM shall indicate whether the occurrence was added, amended or deleted, the values of the attributes held before and after the change, the date and time the change was made.

Id	SHRD.UR.CRDM.PROP.000.050
Name	Service-specific Reference Data maintenance
Description	Any changes to reference data made locally in any service, component or application will not be propagated to Common Reference Data and shall therefore need to be made also in Common Reference Data, if applicable. Once the change has been done in Common Reference Data, it shall be propagated to all services, component and applications that need the information for their processing impacted by the change, including the service, component or application in which the change was first made locally.

2.6 BLOCK AN OCCURRENCE OF COMMON REFERENCE DATA

Business Process Ref: SHRD.BP.CRDM.BLKRD

2.6.1 Business Process Model



Business Process Model 4: Block an occurrence of Common Reference Data

2.6.2 Process Overview

Process goal:

This business process describes the blocking of Cash Accounts and Parties.

Where the Common Reference Data entity includes a Valid From Date and a Valid From Event, these shall be used to determine which version of the Common Reference Data entity is valid at the time.

The Valid From Date in the blocking request indicates the business date from which the occurrence of reference data will become blocked in the system, which by default will be the next business date. If the Valid From Date is specified as immediate by entering the current business date, the Cash Accounts and/or Parties will become blocked immediately.

When a Common Reference Data entity requires date/event validity attributes for determining which version of the entity shall become blocked, this is explicitly specified in the definition of the entity in section 9 on Business Data Definitions in this User Requirements Document.

Process context:

- ▶ The generic process and its descriptions are valid for Cash Accounts and Parties.

Pre-conditions:

- ▶ None

Time constraints:

- ▶ Maintenance window

Expected results:

- ▶ If the request content is either invalid or fails the reference data checks, it will be rejected and a rejection notification with the appropriate error code(s) will be sent to the sender of the message.
- ▶ If the request content is valid and the reference data checks have been passed successfully, the platform will block the occurrence of reference data and the platform will send a success notification to the sender of the message.

Triggers:

- ▶ The process will be initiated by a Party (CB or TARGET Service Desk acting on behalf) via sending a request to the platform to block an occurrence of reference data.

2.6.3 User Requirements

2.6.3.1 PERFORM TECHNICAL VALIDATION

Task Ref: SHRD.TR.CRDM.BLKRD.010

Technical validation will perform checks such as field level validation (fields have correct data type and size) for messages received.

If the validation failed, rejection notifications with appropriate error code(s) must be sent to the sender of the message.

Id	SHRD.UR.CRDM.BLKRD.010.010
Name	Validation of messages received
Description	CRDM shall parse the message received and validate it against the relevant schema to ensure that all attributes are of the correct data type and length.

Id	SHRD.UR.CRDM.BLKRD.010.020
Name	Check mandatory fields
Description	CRDM shall ensure that all mandatory attributes are populated.

2.6.3.2 PERFORM BUSINESS VALIDATION

Task Ref: SHRD.TR.CRDM.BLKRD.020

Where the result of the technical validation is positive, the message is submitted for business validation. The business validation comprises checks on the values of the attributes, cross-field consistency checks (where the value of one field is dependent upon, or has a relationship with, the value of another field, either in the same message or in the data already present in the database) and authorisation checks to ensure that the sender of the amendment request has suitable permissions.

If the validation failed, rejection notifications with appropriate error code(s) must be sent to the sender of the message.

Id	SHRD.UR.CRDM.BLKRD.020.010
Name	Identify occurrence of Common Reference Data entity to be blocked
Description	CRDM shall ensure that the occurrence of reference data to be blocked has already been created (regardless of whether it is currently valid or not).

Id	SHRD.UR.CRDM.BLKRD.020.020
Name	Check attribute values
Description	CRDM shall check that the values of all attributes that are populated (mandatory or optional) are valid according to the allowed values or value ranges.

Id	SHRD.UR.CRDM.BLKRD.020.030
Name	Check data integrity
Description	CRDM shall check that all cross-field validations (data integrity) are satisfied, either between attributes within the message or between an attribute in the message and one or more items of data held in the system.

Id	SHRD.UR.CRDM.BLKRD.020.040
Name	Check status of Common Reference Data entity to be blocked
Description	CRDM shall check the status of the occurrence of reference data to be blocked to ensure that it is not already blocked.

Id	SHRD.UR.CRDM.BLKRD.020.050
Name	Check Valid From Date
Description	The blocking request may include a Valid From Date, although it may not be populated. The value indicates the business date from which the occurrence of Common Reference Data will be blocked. If not stated, the next business date shall be used by default. Valid From Date must be a valid date that must be on or after the current business date. If the Valid From Date is the current business date, then the occurrence of Common Reference Data will become blocked immediately.

2.6.3.3 BLOCK OCCURRENCE OF COMMON REFERENCE DATA

Task Ref: SHRD.TR.CRDM.BLKRD.030

After processing all validation successfully the occurrence of Common Reference Data will be blocked.

Although the blocking will be present in the system immediately after it has passed the validation, it will not necessarily become effective immediately as the change may be post-dated through the use of date validity attributes.

Processes using the Common Reference Data will need to determine at the time whether the occurrence of Common Reference Data is blocked, by checking whether it has been marked as blocked.

Blocking of a Party:

Id	SHRD.UR.CRDM.BLKRD.030.010
Name	Block Party accounts
Description	CRDM shall ensure that the blocking of a Party shall result in the blocking of all Cash Accounts belonging to the Party.

Blocking of an Ancillary System:

Id	SHRD.UR.CRDM.BLKRD.030.020
Name	Block Ancillary System
Description	CRDM shall mark the Ancillary System as blocked.

Blocking of a Cash Account:

Id	SHRD.UR.CRDM.BLKRD.030.030
Name	Block Cash Account
Description	CRDM shall mark the Cash Account as blocked for credit and debit. No credits or debits are allowed on the Cash Account.

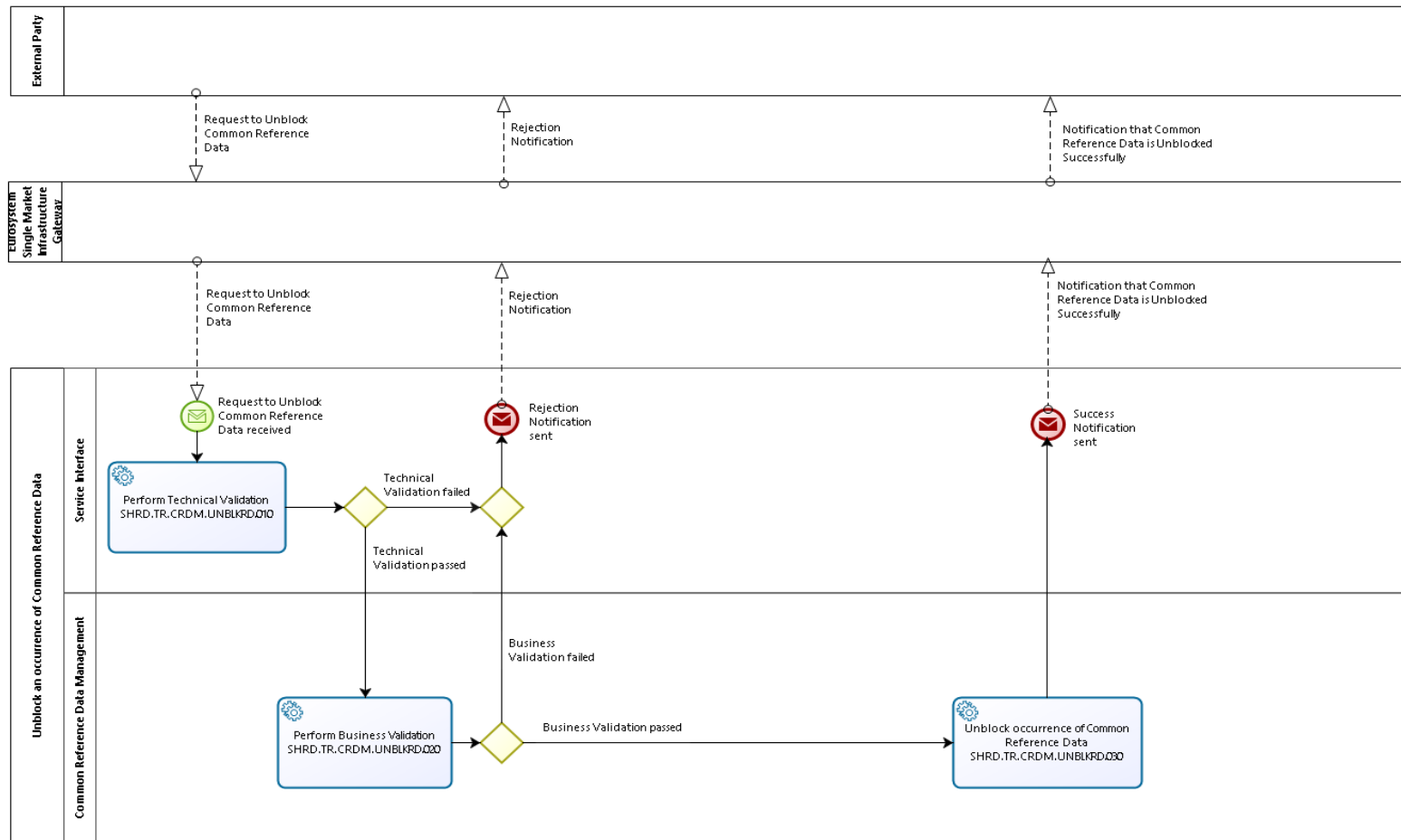
Id	SHRD.UR.CRDM.BLKRD.030.040
Name	Block account only for debit
Description	CRDM shall mark the Cash Account as blocked for debit. This would then allow credits still to be made into the Cash Account.

Id	SHRD.UR.CRDM.BLKRD.030.050
Name	Block account only for credit
Description	CRDM shall mark the Cash Account as blocked for credit. This would then allow debits still to be made into the Cash Account.

2.7 UNBLOCK AN OCCURRENCE OF COMMON REFERENCE DATA

Business Process Ref: SHRD.BP.CRDM.UNBLKRD

2.7.1 Business Process Model



Business Process Model 5: Unblock an occurrence of Common Reference Data

2.7.2 Process Overview

Process goal:

This business process describes the unblocking of Cash Accounts and Parties.

Where the Common Reference Data entity includes a Valid From Date and a Valid From Event, these shall be used to determine which version of the Common Reference Data entity is valid at the time.

The Valid From Date in the unblocking request indicates the business date from which the occurrence of reference data will become unblocked in the system, which by default will be the next business date. If the Valid From Date is specified as immediate then the Common Reference Data entity will become unblocked immediately.

When a Common Reference Data entity requires the above described date/event validity attributes for determining which version of the entity shall become unblocked, this is explicitly specified in the definition of the entity in section 9 on Business Data Definitions in this User Requirements Document.

Process context:

- ▶ The generic process and its descriptions are valid for Cash Accounts and Parties.

Pre-conditions:

- ▶ None

Time constraints:

- ▶ Maintenance window

Expected results:

- ▶ If the request content is either invalid or fails the reference data checks, it will be rejected and a rejection notification with the appropriate error code(s) will be sent to the sender of the message.
- ▶ If the request content is valid and the reference data checks have been passed successfully, the platform will unblock the occurrence of reference data and the platform will send a success notification to the sender of the message.

Triggers:

- ▶ The process will be initiated by a Party (CB or TARGET Service Desk acting on behalf) via sending a request to the platform to unblock an occurrence of reference data.

2.7.3 User Requirements

2.7.3.1 PERFORM TECHNICAL VALIDATION

Task Ref: SHRD.TR.CRDM.UNBLKRD.010

Technical validation will perform checks such as field level validation (fields have correct data type and size) for messages received.

If the validation failed, a rejection notification with appropriate error code(s) must be sent to the sender of the message.

Id	SHRD.UR.CRDM.UNBLKRD.010.010
Name	Validation of messages received
Description	CRDM shall parse the message received and validate it against the relevant schema to ensure that all attributes are of the correct data type and length.

Id	SHRD.UR.CRDM.UNBLKRD.010.020
Name	Check mandatory fields
Description	CRDM shall ensure that all mandatory attributes are populated.

2.7.3.2 PERFORM BUSINESS VALIDATION

Task Ref: SHRD.TR.CRDM.UNBLKRD.020

Where the result of the technical validation is positive, the message is submitted for business validation. The business validation comprises checks on the values of the attributes, cross-field consistency checks (where the value of one field is dependent upon, or has a relationship with, the value of another field, either in the same message or in the data already present in the database) and authorisation checks to ensure that the sender of the amendment request has suitable permissions.

If the validation failed, rejection notifications with appropriate error code(s) must be sent to the sender of the message.

Id	SHRD.UR.CRDM.UNBLKRD.020.010
Name	Identify occurrence of Common Reference Data entity to be unblocked
Description	CRDM shall ensure that the occurrence of reference data to be unblocked has already been created (regardless of whether it is currently valid or not).

Id	SHRD.UR.CRDM.UNBLKRD.020.020
Name	Check attribute values
Description	CRDM shall check that the values of all attributes that are populated (mandatory or optional) are valid according to the allowed values or value ranges.

Id	SHRD.UR.CRDM.UNBLKRD.020.030
Name	Check data integrity
Description	CRDM shall check that all cross-field validations (data integrity) are satisfied, either between attributes within the message or between an attribute in the message and one or more items of data held in the system

Id	SHRD.UR.CRDM.UNBLKRD.020.040
Name	Check status of Common Reference Data entity to be unblocked
Description	CRDM shall check the status of the occurrence of reference data to be unblocked to ensure that it is currently blocked

Id	SHRD.UR.CRDM.UNBLKRD.020.050
Name	Check Valid From Date
Description	The unblocking request may include a Valid From Date, although it may not be populated. The value indicates the business date from which the occurrence of Common Reference Data will be unblocked. If not stated, the next business date shall be used by default. Valid From Date must be a valid date that must be on or after the current business date.

2.7.3.3 UNBLOCK OCCURRENCE OF COMMON REFERENCE DATA

Task Ref: **SHRD.TR.CRDM.UNBLKRD.030**

After processing all validation successfully the occurrence of the Common Reference Data entity will be unblocked.

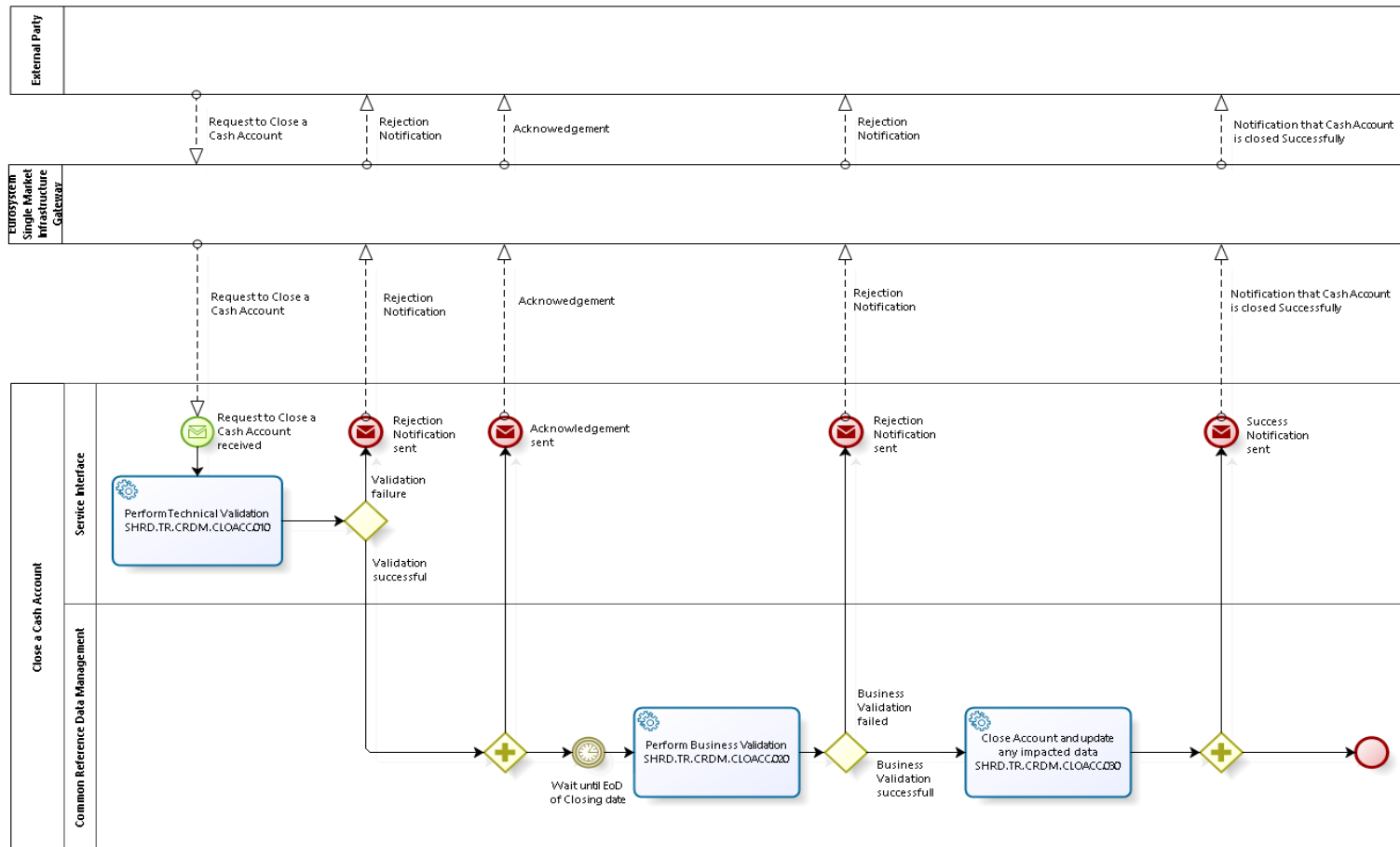
Although the unblocking will be present in the system immediately after it has passed the validation, it will not necessarily become effective immediately as the change may be post-dated through the use of date/event validity attributes.

Processes using the Common Reference Data will need to determine at the time whether the occurrence of the Common Reference Data is unblocked, by checking whether it is currently still marked as blocked.

2.8 CLOSE A CASH ACCOUNT

Business Process Ref: SHRD.BP.CRDM.CLOACC

2.8.1 Business Process Model



Business Process Model 6: Close a Cash Account

2.8.2 Process Overview

Process goal:

This business process describes the closing of a Cash Account.

Where the Common Reference Data entity includes a Valid From Date and a Valid From Event, these shall be used to determine which version of the Common Reference Data entity is valid at the time.

The Valid From Date in the request to close a Cash Account indicates the business date on which the Cash Account will be closed in the system, which by default will be the current business date. The Cash Account will be closed at the end of the business day indicated by the Valid From Date.

Process context:

- ▶ This process may be used to close any type of Cash Account.

Pre-conditions:

- ▶ The Cash Account must exist and must be active.

Time constraints:

- ▶ Maintenance window.

Expected results:

- ▶ If the request content is either invalid or fails the reference data checks, it will be rejected and a rejection notification with the appropriate error code(s) will be sent to the sender of the message.
- ▶ If the request content is valid and the reference data checks have been passed successfully, the platform will close the cash account and the platform will send a success notification to the sender of the message.

Triggers:

- ▶ The process will be initiated by a Party via a request to the platform to close a Cash Account.

2.8.3 User Requirements

2.8.3.1 PERFORM TECHNICAL VALIDATION

Task Ref: SHRD.TR.CRDM.CLOACC.010

Technical validation will perform checks such as field level validation (fields have correct data type and size) for messages received.

After successful technical validation an acknowledgement will be sent to the sender of the message. If the validation failed, a rejection notification with appropriate error code(s) must be sent to the relevant Parties.

Id	SHRD.UR.CRDM.CLOACC.010.010
Name	Validation of messages received
Description	CRDM shall parse the message received and validate it against the relevant schema to ensure that all attributes are of the correct data type and length.

Id	SHRD.UR.CRDM.CLOACC.010.020
Name	Check mandatory fields
Description	CRDM shall ensure that all mandatory attributes are populated.

2.8.3.2 PERFORM BUSINESS VALIDATION

Task Ref: SHRD.TR.CRDM.CLOACC.020

Where the result of the technical validation is positive, the message is submitted for business validation. The business validation comprises checks on the values of the attributes, cross-field consistency checks (where the value of one field is dependent upon, or has a relationship with, the value of another field, either in the same message or in the data already present in the database) and authorisation checks to ensure that the sender of the request to close the account has suitable permissions.

If the validation failed, rejection notifications with appropriate error code(s) must be sent to the sender of the message.

Before continuing the closing process there is a waiting period until the End of Day of the closing date is reached. Until this point in time the processing on the Cash Account will continue as usual.

Id	SHRD.UR.CRDM.CLOACC.020.010
Name	Identify Cash Account to be closed
Description	CRDM shall ensure that the Cash Account to be closed has already been created (regardless of whether it is currently valid or not).

Id	SHRD.UR.CRDM.CLOACC.020.020
Name	Check attribute values
Description	CRDM shall check that the values of all attributes that are populated (mandatory or optional) are valid according to the allowed values or value ranges.

Id	SHRD.UR.CRDM.CLOACC.020.030
Name	Check data integrity
Description	CRDM shall check that all cross-field validations (data integrity) are satisfied, either between attributes within the message or between an attribute in the message and one or more items of data held in the system.

Id	SHRD.UR.CRDM.CLOACC.020.040
Name	Transfer any remaining balance from Cash Account to be closed
Description	CRDM shall ensure that even after the Cash Account is closed; it shall always be possible for the relevant Central Bank to transfer any remaining balance to another Cash Account. No other actors shall be allowed to transfer liquidity from/to a closed Cash Account.

Id	SHRD.UR.CRDM.CLOACC.020.050
Name	Check Valid From Date
Description	The request to close a Cash Account may include a Valid From Date, although it may not be populated. The value indicates the business date on which the Cash Account will be closed. If not stated, the next current date shall be used by default. Valid From Date must be a valid date that must be on or after the current business date.

2.8.3.3 CLOSE ACCOUNT AND UPDATE ANY IMPACTED DATA

Task Ref: **SHRD.TR.CRDM.CLOACC.030**

The Cash Account will be closed, so that no processing can be performed on the Cash Account any longer. Additionally, further actions required due to the closure have to be triggered.

Id	SHRD.UR.CRDM.CLOACC.030.010
Name	Check on Standing Orders
Description	CRDM shall ensure that all Standing Orders related to the Cash Account to be closed are no longer valid before the Cash Account can be closed.

Id	SHRD.UR.CRDM.CLOACC.030.020
Name	Setting credit line to zero
Description	CRDM shall allow the relevant Central Bank to set the credit line of the closed Main Cash Account to zero.

Id	SHRD.UR.CRDM.CLOACC.030.030
Name	Retain reference data for closed Cash Account
Description	CRDM shall ensure that no reference data relating to the closed Cash Account shall be deleted automatically from the system. This will allow the Cash Account to be reopened if required at a later point in time, using the Amend an occurrence of Common Reference Data process (SHRD.BP.CRDM.AMDRD) defined in section 2.3 in this User Requirements Document on the Cash Account and the Create an occurrence of Common Reference Data process (SHRD.BP.CRDM.CRERD) defined in section 2.2 in this User Requirements Document to set up the Standing Orders again.
Id	SHRD.UR.CRDM.CLOACC.030.040
Name	Closed account referenced as account to be debited
Description	If the closed account is referenced as account to be debited in the billing common component, a U2A or A2A notification will be sent to the central bank of the party which has configured the account as account to be debited (which may be different from the system entity of the closed account).

2.9 DIRECTORY SERVICE

Business Process Ref: SHRD.BP.CRDM.DIR

2.9.1 Process Overview

The process describes the compilation, the content and delivery of the directories. The directories shall provide valuable business information to the actors of the settlement services, e.g. the reachability of Parties.

Process context:

- ▶ This process is a background process providing information for Parties.

Pre-conditions:

- ▶ None

Time constraints:

- ▶ Maintenance window

Expected results:

- ▶ Directories based on CRDM contents are compiled and delivered in time and format as requested by the settlement service.

Triggers:

- ▶ Scheduled process

2.9.2 User Requirements

Id	SHRD.UR.CRDM.DIR.000.010
Name	Service-specific population of directories
Description	CRDM shall compile directories for the settlement services. The content of each directory shall be based on the Party's participation type in the settlement service, identified by its BIC11.

Each settlement service might require its own set of data to be published to the Parties. The CRDM's function is to provide the data needed for instructing in the settlement service. The directories shall be limited to the participation type (direct and indirect participants, multi-addressee access as well as addressable BIC) of the settlement service, e.g. participants of TIPS shall not see a list of participants of RTGS in the TIPS directory.

The participation type in the settlement service will be published in the directory, however upon decision of the respective Party a BIC could not be published in the directory.

Id	SHRD.UR.CRDM.DIR.000.020
Name	Application of wildcard rules
Description	CRDM shall enrich service-specific data containing wildcard rules with the data of the SWIFT BIC directory for the building of the directories.

The wildcard rules, as specified for the TARGET2 directory today, shall be kept.

Id	SHRD.UR.CRDM.DIR.000.030
Name	Service-specific distribution of directories
Description	CRDM shall distribute the directories to the Parties of the settlement service. The directories shall be available in both, push and pull mode. Also, it shall be possible to retrieve a full copy of the directories upon request.

It is up to the chosen delivery method whether the data is distributed in delta mode or full mode. This shall depend on the underlying technique. The directories shall be distributed only to the Parties of a settlement service.

Id	SHRD.UR.CRDM.DIR.000.040
Name	Frequency of directory distribution
Description	CRDM shall distribute a directory update on a regular basis

Id	SHRD.UR.CRDM.DIR.000.050																
Name	Structure of the TIPS directory																
Description	CRDM shall provide the TIPS directory according to the following structure: <table border="1"> <thead> <tr> <th>Field name</th><th>Note</th></tr> </thead> <tbody> <tr> <td>BIC</td><td>Participant's BIC</td></tr> <tr> <td>TIPS Participation Type</td><td>TIPS Participant Reachable Party</td></tr> <tr> <td>Institution Name</td><td>Participant's company name</td></tr> <tr> <td>Type of Change</td><td>A: added M: modified D: deleted U: unchanged</td></tr> <tr> <td>Valid From</td><td>Business day from which the entry is valid</td></tr> <tr> <td>Valid To</td><td>Business day up to which the entry is valid</td></tr> <tr> <td>Reserve</td><td>Space</td></tr> </tbody> </table>	Field name	Note	BIC	Participant's BIC	TIPS Participation Type	TIPS Participant Reachable Party	Institution Name	Participant's company name	Type of Change	A: added M: modified D: deleted U: unchanged	Valid From	Business day from which the entry is valid	Valid To	Business day up to which the entry is valid	Reserve	Space
Field name	Note																
BIC	Participant's BIC																
TIPS Participation Type	TIPS Participant Reachable Party																
Institution Name	Participant's company name																
Type of Change	A: added M: modified D: deleted U: unchanged																
Valid From	Business day from which the entry is valid																
Valid To	Business day up to which the entry is valid																
Reserve	Space																

Id	SHRD.UR.CRDM.DIR.000.060	
Name	Structure of the RTGS directory	
Description	CRDM shall provide the RTGS directory according to the following structure:	
	Field name	Note
	BIC	Participant's BIC
	Addressee	BIC identifying the party receiving the messages
	Account Holder	BIC identifying the settlement bank
	Institution Name	Participant's company name
	City Heading	Participant's establishment
	National Sorting Code	Participant's national sorting code
	Main BIC Flag	Y: yes N: no Yes means that this BIC could be used to address the payments if the sender has no other information where to send to
	Type of Change	A: added M: modified D: deleted U: unchanged
	Valid From	Date from which the entry is valid
	Valid To	Date up to which the entry is valid
	Participation type	01 - "Direct" 02 - "Indirect" 03 - multi addressee - Credit institutions 04 - multi addressee - Branch of Direct participant 05 - addressable BIC – Correspondent (including CB customer) 06 - addressable BIC - Branch of Direct participant 07 - addressable BIC - Branch of Indirect participant 08 - addressable BIC - Branch of correspondent
	Reserve	Space

2.10 COMMON REFERENCE DATA MANAGEMENT – NON-FUNCTIONAL REQUIREMENTS

2.10.1 Availability

Id	SHRD.UR.CRDM.NFR.020
Name	Availability
Description	Availability, calculated on a quarterly basis, shall be at least 99.7%.

CRDM may be subject to incidents or failures, which may cause a temporary and unforeseen interruption of the service. Regardless of the total number of such unplanned interruptions, the overall availability calculated on a quarterly basis shall be at least 99.7%.

2.10.2 Disaster Recovery

Id	SHRD.UR.CRDM.NFR.030
Name	Recovery Point Objective
Description	CRDM shall ensure a recovery point objective value of zero minutes in the event of site failures. Where there is a loss of a complete region the RPO shall not exceed two minutes.

The recovery point objective (RPO) is a point of consistency to which a user wants to recover or restart the service. It is measured as the amount of time between the moment when the point of consistency was created and the moment when the failure occurred.

CRDM ensures synchronous point of consistency creations and, as a consequence, no data loss in the event of failures, unless the component cannot be restarted in the same region and a failover to the backup-region has to be conducted. In this case a data loss of two minutes will be tolerated.

Id	SHRD.UR.CRDM.NFR.040
Name	Recovery Time Objective
Description	CRDM shall have a RTO according to the requirements of the connected services components and applications.

The recovery time objective (RTO) is the maximum amount of time required for recovery or restart of the service to a specified point of consistency. In the event of a site failure, CRDM shall ensure a maximum time of unavailability of one hour starting from the time when the decision to restart the component is made up to the time the component is restored. Where there is a major failure or a regional disaster, CRDM shall ensure maximum time of unavailability two hours starting from the time when the decision to restart the component is made up to the time the component is restored.

2.10.3 Performance Requirements

Id	SHRD.UR.CRDM.NFR.050
Name	Response Time for CRDM updates
Description	CRDM shall have completed updates of Common Reference Data within 2 minutes for 95% of the updates and within 5 minutes for 100%.

Id	SHRD.UR.CRDM.NFR.060
Name	Peak workload
Description	CRDM shall be able to handle a maximum of ten updates per second. The peak workload has to be endured for half an hour.

3 BUSINESS DAY (BD)

3.1 OVERVIEW

3.1.1 Context Diagram

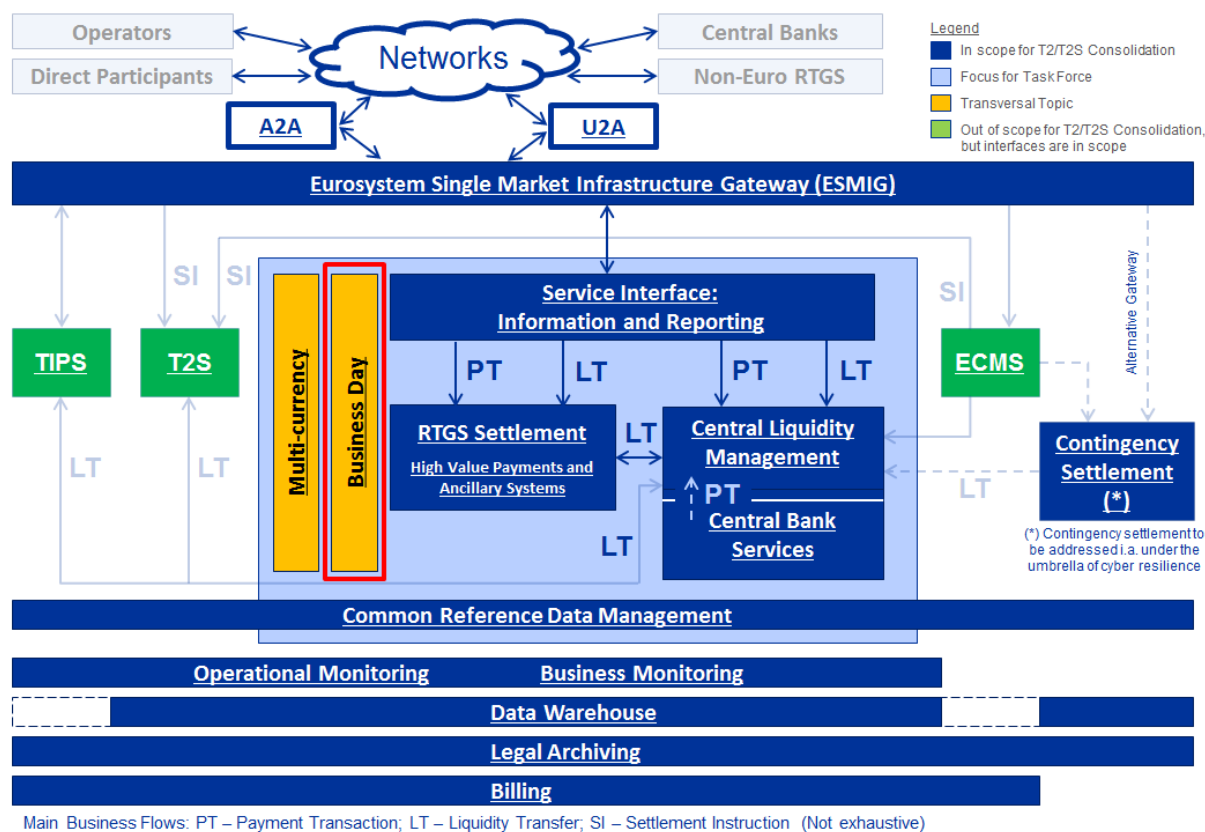


Figure 3: Context diagram for Business Day

3.1.2 Business Processes

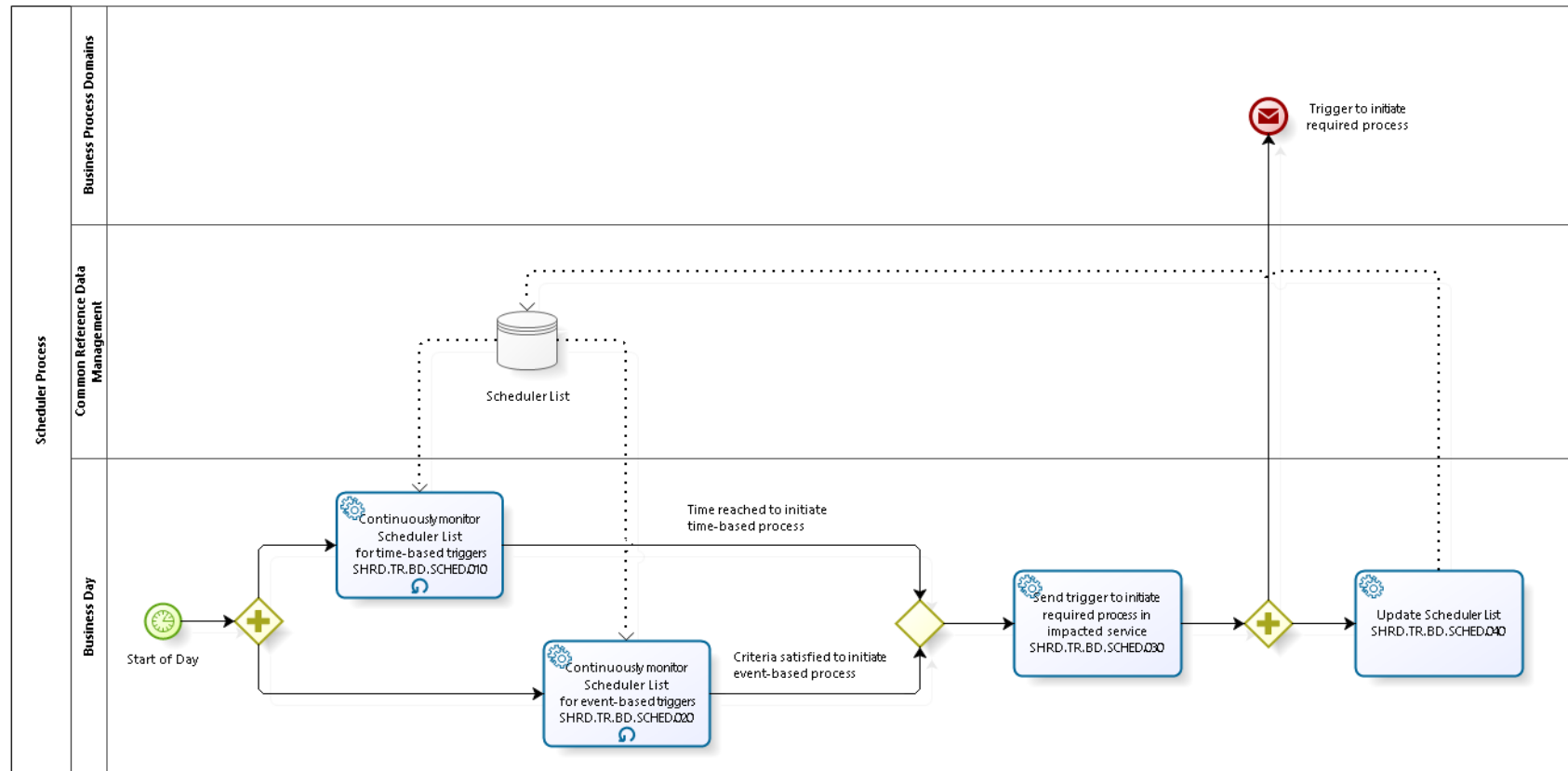
Business Process	BP Reference	Business Process Description
Scheduler Process	SHRD.BP.BD.SCHED	Process to initiate processes within any service, component and application that need to be performed either at a scheduled date/time or when specified criteria occur
End of Day/Start of Day Process	SHRD.BP.BD.EODSOD	Processes performed at the End of Day and during the following Start of Day

Table 2: Business Processes for Business Day

3.2 SCHEDULER PROCESS

Business Process Ref: SHRD.BP.BD.SCHED

3.2.1 Business Process Model



Business Process Model 7: Scheduler Process

3.2.2 Process Overview

The purpose of the scheduler is to initiate and coordinate overarching processes between different Eurosystem Market Infrastructure Services, e.g. RTGS, CLM, CRDM, TIPS, T2S or ECMS, as well as managing processes of the different Eurosystem Market Infrastructure Services. This is achieved by recognising the trigger events associated with the processes and then sending triggers to the services, components and applications to start these required processes. The trigger events can be either time-based or event-based, such as the receipt of a file or message or the completion of another process. Processes may be triggered on a repeating basis, or as one-off requests. Events may also be currency specific.

The details of each process to be initiated, and the criteria that define when this should happen, will be created and maintained in Common Reference Data Management (CRDM) in a scheduler list.

The Scheduler process will constantly monitor the scheduler list in order to recognise when the date and time has been reached, or the defined criteria are satisfied, to initiate a defined process. A trigger will then be sent immediately to the appropriate service, component and application for the required process to be initiated within that service, component or application. For some events, when required, the scheduler will wait for a feedback from the triggered process (e.g. processes on the critical path), for other events the scheduler is not awaiting for a feedback.

A list of potential processes to be initiated by the scheduler may include:

- ▶ Generation of reports;
- ▶ Generation of Standing Orders based on definitions in Common Reference Data Management;
- ▶ Sending information to the account holders (e.g. information about change of business day); and
- ▶ Management of events related to the business day schedule.

3.2.3 User Requirements

3.2.3.1 GENERAL USER REQUIREMENTS FOR SCHEDULER PROCESS

Id	SHRD.UR.BD.SCHED.000.010
Name	Scheduler - Maintain scheduler list
Description	The scheduler shall maintain the scheduler list and initiate a defined process based on a predefined set of conditions (trigger events) as soon as these are met.

Id	SHRD.UR.BD.SCHED.000.020
Name	Scheduler - Time-based trigger
Description	The scheduler shall generate a time-based trigger as soon as a predefined set of conditions based on CET time are met to initiate a specific process within services, components and applications.

Id	SHRD.UR.BD.SCHED.000.023
Name	Scheduler – Time-based trigger
Description	In a situation where a business day lasts for more than one calendar day, such as over a weekend, the same time will occur more than once. In such a case the scheduler shall generate a time-based trigger only once (on the first occasion) during the same business day.

Id	SHRD.UR.BD.SCHED.000.025
Name	Scheduler – Change time for a trigger
Description	The time of an event can be changed by the TARGET Service Desk unless the event has already been triggered.

Id	SHRD.UR.BD.SCHED.000.030
Name	Scheduler - Event-based trigger
Description	The scheduler shall generate an event-based trigger as soon as a predefined set of conditions are met, to initiate a specific process within services, components and applications.

Id	SHRD.UR.BD.SCHED.000.040
Name	Scheduler - Update of scheduler list
Description	The scheduler shall mark the request in the scheduler list as having been executed when the trigger to initiate the required process has been sent to the service, component or application, including the date and time when the event was triggered. This means that the process was started but does not imply that the initiated process has completed. For some events, when required, the scheduler will wait for a feedback from the triggered process (e.g. processes on the critical path), for other events the scheduler is not waiting for a feedback.

Id	SHRD.UR.BD.SCHED.000.050
Name	Scheduler – Information on scheduler events
Description	The scheduler shall generate a notification to account holders upon triggering a scheduled event (e.g. change of business day).

3.2.3.2 CONTINUOUSLY MONITOR SCHEDULER LIST FOR TIME-BASED TRIGGERS

Task Ref: SHRD.TR.BD.SCHED.010

Throughout the day the system shall monitor all unexecuted time-based process requests in the scheduler list. As soon as the time indicated in the process request is reached, the process will be initiated.

3.2.3.3 CONTINUOUSLY MONITOR SCHEDULER LIST FOR EVENT-BASED TRIGGERS

Task Ref: SHRD.TR.BD.SCHED.020

Throughout the day the system shall monitor all unexecuted event-based process requests in the scheduler list. As soon as the criteria stated in the process request are satisfied, the process will be initiated.

3.2.3.4 SEND TRIGGER TO INITIATE REQUIRED PROCESS IN IMPACTED SERVICE

Task Ref: SHRD.TR.BD.SCHED.030

For each process requests in the scheduler list a trigger is sent to the impacted service, component or application to initiate the required process.

3.2.3.5 UPDATE SCHEDULER LIST

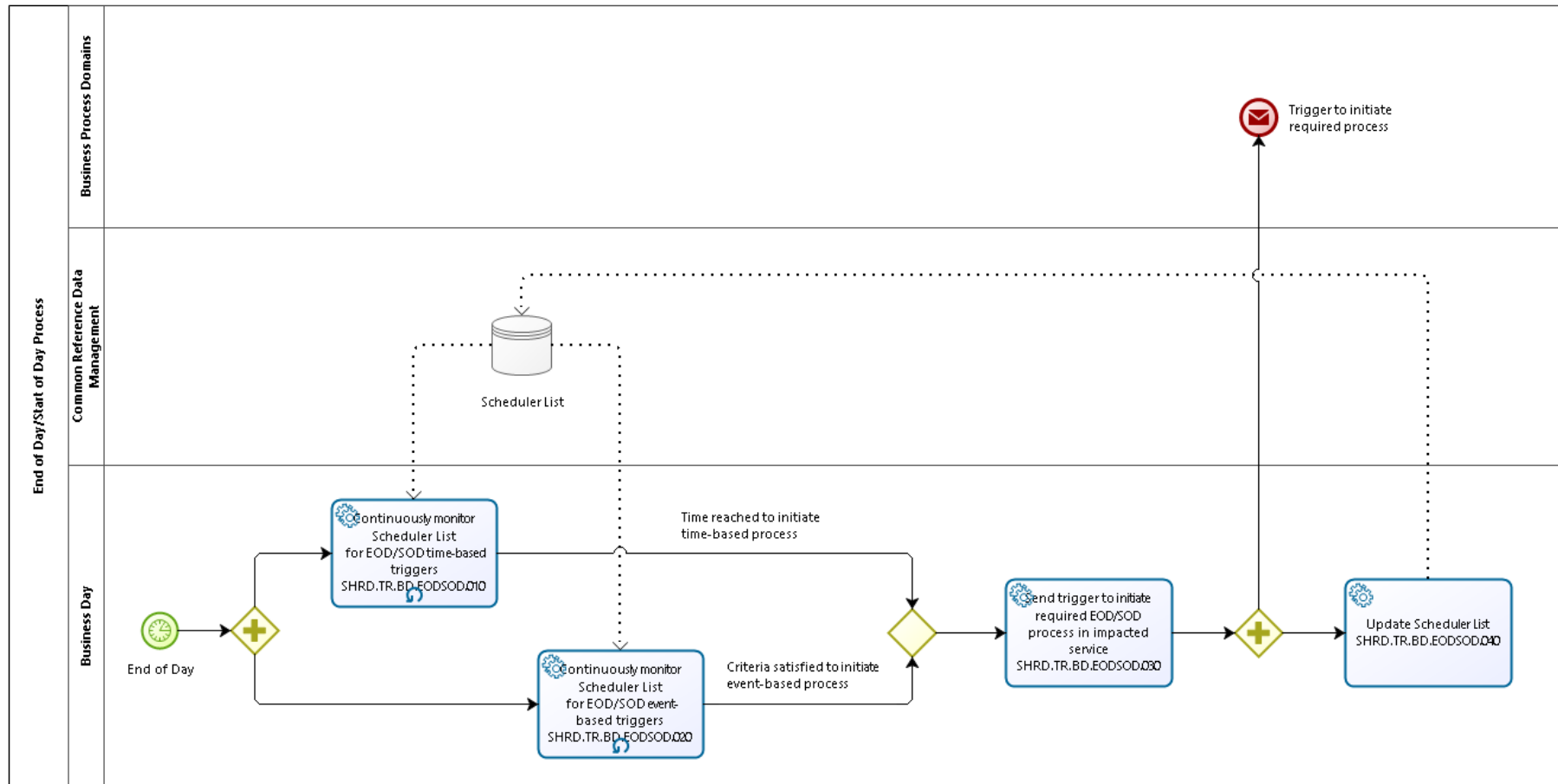
Task Ref: SHRD.TR.BD.SCHED.040

Once the trigger to initiate the required process has been sent, the process request in the scheduler list is marked as having been executed, including the date and time when the trigger was sent. For some events, when required, the scheduler will wait for a feedback from the triggered process (e.g. processes on the critical path), for other events the scheduler is not waiting for a feedback.

3.3 END OF DAY/START OF DAY PROCESS

Business Process Ref: SHRD.BP.BD.EODSOD

3.3.1 Business Process Model



Business Process Model 8: End of Day/Start of Day Process

3.3.2 Process Overview

The End of Day/Start of Day process (EoD/SoD) describes the tasks to be performed by RTGS, CLM and other components during this period of the business day schedule including the change of business day.²

During End of Day the closure of the current business day is performed, while during Start of Day the technical preparation of the new business day takes place.

This includes the processing of overarching events as well as component-specific ones for CLM, RTGS and the common components.

The End of Day and Start of Day periods are initiated by the scheduler via time-based or event-based triggers.

The tasks to be performed may include sending requests or notifications to one or more other services and applications, such as TIPS, T2S or ECMS, for tasks to be performed within those services and applications and/or for information to be provided to CLM, RTGS or the common components.

A non-exhaustive list of potential tasks during End of Day (including tasks on the critical and non-critical path) may include:

- ▶ Closure for liquidity transfer orders for all settlement services (i.e. RTGS, CLM, T2S, TIPS)
 - No new liquidity transfer orders will be accepted and therefore new ones will be rejected.
 - This would be the first task to be performed during End of Day.
- ▶ Closure of RTGS
 - Inform all other settlement services (i.e. CLM, T2S, TIPS) about the closure of RTGS.
- ▶ Rejection of pending payment orders, liquidity transfer orders and credit line changes
 - Pending payment orders, liquidity transfer orders not executed by the start of the End of Day process of the current business day will be rejected.
- ▶ Rejection of pending verifications related to payment orders (four-eyes principle)
 - Pending verifications for creations, amendments or deletions in four-eyes principle related to payment orders will be rejected.
 - Pending credit line changes not executed by the CLM CB cut-off of the current business day will be rejected.
- ▶ Collection of End of Day balances from each settlement service
 - Triggers are sent by the scheduler to all settlement services to send a report of End of Day balances (general ledger file) directly to Central Bank Services (CBS).³

² Additional tasks performed in the other services and applications as T2S, TIPS, ECMS are not described in this section.

³ The minimum reserve is calculated by a process within CBS when all balances are available. CBS also summarises all bilateral credits and bilateral debits between CBs and then books them on the ECB account of each CB.

- ▶ End of Day reporting
 - Triggers are sent by the scheduler to build the reports scheduled for End of Day.
- ▶ Change of business day
 - Close the current business day and open the next business day.
 - This would be the last task to be performed during End of Day.

A non-exhaustive list of potential tasks during Start of Day:

- ▶ Receiving of reference data from Common Reference Data Management.

3.3.3 User Requirements

3.3.3.1 GENERAL USER REQUIREMENTS FOR END OF DAY / START OF DAY PROCESS

Id	SHRD.UR.BD.EODSOD.000.010
Name	End of Day - Rejection of new liquidity transfer orders
Description	No new liquidity transfer orders will be accepted during End of Day and therefore they will be rejected and a notification will be sent to the sender with the respective error code.

Id	SHRD.UR.BD.EODSOD.000.020
Name	End of Day - Rejection of pending payment orders, liquidity transfer orders and credit line changes
Description	Pending payment orders (excluding connected payment orders) and liquidity transfer orders not executed by the start of the End of Day process of the current business day will be rejected and a notification will be sent to the sender with the respective error code. Pending credit line changes not executed by the CB cut-off will be rejected and a notification will be sent to the sender with the respective error code.

Id	SHRD.UR.BD.EODSOD.000.030
Name	End of Day - Rejection of pending verifications related to payment orders (four-eyes principle)
Description	Pending verifications related to payment orders for creations, amendments or deletions in four-eyes principle will be rejected.

Id	SHRD.UR.BD.EODSOD.000.040
Name	End of Day - Information on closure of RTGS
Description	The scheduler shall send a trigger to each settlement service (i.e. CLM, T2S, TIPS) when RTGS is closed.

Id	SHRD.UR.BD.EODSOD.000.050
Name	End of Day - Triggers are sent by the scheduler for several tasks
Description	The scheduler shall send triggers for several tasks after the closure of settlement services for liquidity transfers, e.g. • Requesting End of Day balances (general ledger file) from each settlement service to be sent to CBS • Building End of Day reporting

Id	SHRD.UR.BD.EODSOD.000.060
Name	End of Day - Liquidity on Cash Accounts
Description	The liquidity can remain on the Cash Accounts of the settlement services also at the end of business day; i.e. a cash sweep is executed only on an optional basis.

Id	SHRD.UR.BD.EODSOD.000.070
Name	End of Day - Collection of End of Day balances from each settlement service
Description	The End of Day balances shall be taken at one point in time from each settlement service. The scheduler will send a trigger to each settlement service when RTGS is closed.

Id	SHRD.UR.BD.EODSOD.000.080
Name	End of Day - Change of business day
Description	When all tasks of End of Day are initiated and certain tasks (including the tasks executed by CBS) have been completed, the current business day will be closed and the next business day will be opened. The scheduler will initiate the change of business day when the defined criteria are satisfied.

Id	SHRD.UR.BD.EODSOD.000.085
Name	End of Day - Change of business day
Description	The scheduler shall allow different timing for the change of business day per settlement service, but shall prevent liquidity transfers between settlement services in the period when one settlement service is already on the new business day, while for the other settlement service the End of Day processing is ongoing. For example, TIPS will start with a new business day shortly after 18:00, after closure of RTGS, while other settlement services will change the business day at 18:45 when End of Day processing is finished. The time for change of business day for cash should be coordinated for all currencies within all settlement services. Different calendars per settlement service and per currency have to be managed to operate different closing days.

Id	SHRD.UR.BD.EODSOD.000.090
Name	End of Day - Information on change of business day
Description	The scheduler shall send a trigger to each settlement service (i.e. RTGS, CLM, T2S, TIPS) when the business day was changed.

Id	SHRD.UR.BD.EODSOD.000.100
Name	End of Day - Same value date for all cash services
Description	All cash services shall use the same value date outside the End of Day period (see SHRD.UR.BD.EODSOD.000.085) and in contingency situations.

Id	SHRD.UR.BD.EODSOD.000.110
Name	Start of Day - Performance of several tasks
Description	During Start of Day several tasks triggered by the scheduler are performed, e.g. receiving of reference data from Common Reference Data Management

Id	SHRD.UR.BD.EODSOD.000.120
Name	Start of Day - Point in time
Description	The Start of Day may deviate for the different settlement services.

3.3.3.2 CONTINUOUSLY MONITOR SCHEDULER LIST FOR EOD/SOD TIME-BASED TRIGGERS

Task Ref: SHRD.TR.BD.EODSOD.010

As soon as the time for the End of Day is reached the scheduler initiates the relevant time-based processes for the EoD processing.

As soon as the time for the Start of Day is reached the scheduler initiates the relevant time-based processes for the SoD processing.

3.3.3.3 CONTINUOUSLY MONITOR SCHEDULER LIST FOR EOD/SOD EVENT-BASED TRIGGERS

Task Ref: SHRD.TR.BD.EODSOD.020

As soon as the closure of liquidity transfer orders has been performed the scheduler initiates all event-based processes, e.g. End of Day reporting and requests to send End of Day balances from each settlement service to CBS.

The final task of the End of Day is the change of business day which will be initiated by the scheduler when all other tasks of End of Day process are initiated and certain tasks (including the tasks executed by CBS) have been completed.

3.3.3.4 SEND TRIGGER TO INITIATE REQUIRED EOD/SOD PROCESS IN IMPACTED SERVICE

Task Ref: SHRD.TR.BD.EODSOD.030

For each process request in the scheduler list, a trigger is sent to the impacted settlement service to initiate the required process.

3.3.3.5 UPDATE SCHEDULER LIST

Task Ref: SHRD.TR.BD.EODSOD.040

Once the trigger to initiate the required process has been sent, the process request in the scheduler list is marked as having been executed, including the date and time when the trigger was sent. For some events, when required, the scheduler will wait for a feedback from the triggered process (e.g. processes on the critical path), for other events the scheduler is not waiting for a feedback.

3.4 AVAILABILITY OF SERVICES

This section describes the availability of the services and components (e.g. HVP, AS, CLM/CBS, CRDM, DWH) and the relationship between all services, components and applications (e.g. HVP, AS, CLM/CBS, CRDM, DWH, T2S, TIPS, ECMS).

3.4.1 Business day schedule

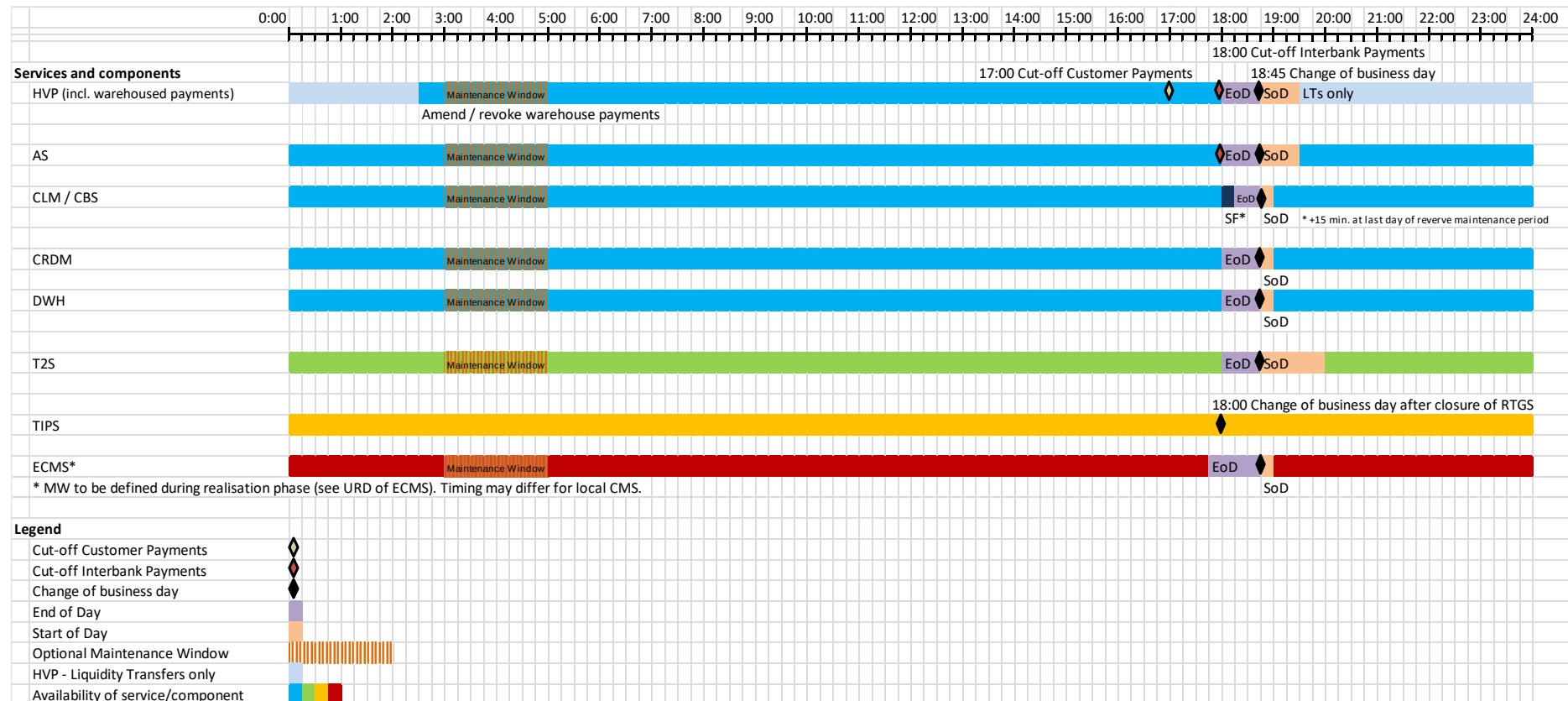


Figure 4: Business day schedule (Tuesdays, Wednesdays, Thursdays, Fridays except T2 closing days)

The cut-offs shall be configurable with parameters. The mentioned points in time are only indicative values to define the order of the different cut-offs and the timing regarding the phase of business day when the cut-offs have to take place.

3.4.2 User Requirements

3.4.2.1 GENERAL USER REQUIREMENTS FOR ALL SERVICES, COMPONENTS AND APPLICATIONS

Id	SHRD.UR.BD.OPER.000.010
Name	De-coupling of services, components and applications
Description	The different services, components and applications (.e.g. HVP, AS, CLM/CBS, CRDM, T2S, TIPS, ECMS) shall be de-coupled in terms of availability.

Id	SHRD.UR.BD.OPER.000.020
Name	Maintenance window
Description	The point in time of the maintenance window shall be aligned for all services, components and applications (.e.g. HVP, AS, CLM/CBS, CRDM, T2S, ECMS). [CSLD CR-12] It shall start at 03: 00 and end at 05:00 on Tuesdays, Wednesdays, Thursdays and Fridays, if it is activated. It shall start at 02:30 on Saturdays and end at 02:30 on Mondays.

3.4.2.2 USER REQUIREMENTS FOR THE DIFFERENT SERVICES AND COMPONENTS

RTGS service (HVP and AS):

Id	SHRD.UR.BD.OPER.000.030
Name	Cut-off
Description	RTGS shall ensure that after a cut-off at least one settlement attempt takes place. Note: Payment orders received, respectively, before the cut-off for customer or for interbank payment orders must have at least one possibility to settle.

Id	SHRD.UR.BD.OPER.000.040
Name	High Value Payments functionality - Availability
Description	HVP shall operate from 02:30 – 18:00. It shall be closed for payment orders between 19:30 and 02:30, but shall be open for liquidity transfer orders during the same period. (Immediate Liquidity Transfers can be submitted from 19.00 and will be parked until 19.30) It will be closed between 18:00 – 19:30 (EoD/SoD) and may be closed between 03:00 and 05:00 (on Tuesdays, Wednesdays, Thursdays, Fridays) if the maintenance window is activated. It will be closed on weekends and T2 closing days, i.e. from Saturday starting at 02:30 until Monday 02:30 and from 02:30 on a T2 closing day to 02:30 on the next working day.

Id	SHRD.UR.BD.OPER.000.050
Name	High Value Payments functionality - Cut-offs
Description	For HVP the following cut-offs shall take place: • Cut-off for customer payment orders at 17:00. • Cut-off for interbank payment orders at 18:00. Note: The cut-offs shall be configurable with parameters. The mentioned points in time are only indicative values to define the order of the different cut-offs and the timing regarding the phase of business day when they have to take place.

Id	SHRD.UR.BD.OPER.000.060
Name	Maintenance of warehoused payment orders
Description	Warehoused payment orders may be maintained between the start of the day and the opening of HVP, i.e. from 19:30 – 02:30.

Id	SHRD.UR.BD.OPER.000.070
Name	Settlement of warehoused payment orders
Description	Warehoused payment orders shall be queued for settlement at the time of opening of HVP on the indicated value date, unless the payment instruction includes FROM time.

Id	SHRD.UR.BD.OPER.000.080
Name	Ancillary Systems functionality - Availability
Description	AS shall operate from 19:30 – 18:00 (except during maintenance window if it is activated). It will be closed on weekends and T2 closing days, i.e. from Saturday starting at 02:30 until Monday 02:30 and from 02:30 on a T2 closing day to 02:30 on the next working day.

Id	SHRD.UR.BD.OPER.000.090
Name	Ancillary Systems functionality - Cut-offs
Description	For AS the following cut-off shall take place: • Cut-off interbank payment orders at 18:00. It is assumed that most of the Ancillary Systems have settled before the cut-off for customer payment orders, which takes place at 17:00. Specific types of transfer orders stemming from AS (e.g. money market, DVP) can be settled until 18:00. Note: The cut-offs shall be configurable with parameters. The mentioned points in time are only indicative values to define the order of the different cut-offs and the timing regarding the phase of business day when they have to take place.

Id	SHRD.UR.BD.OPER.000.100
Name	RTGS - Usage of Cash Accounts
Description	It will be possible to use the same Cash Account for HVP and AS. A technical solution shall be put in place to respect the different service hours of the functionalities, i.e. the system will ensure that only “eligible” orders will be settled during the respective timeframe.

Id	SHRD.UR.BD.OPER.000.110
Name	Ancillary Systems functionality - Settlement procedures
Description	For AS all offered settlement procedures are available during the operational hours of RTGS. AS will follow the change of business day logic and as such the underlying business in the Ancillary System will do the same.

CLM/CBS:

Id	SHRD.UR.BD.OPER.000.120
Name	CLM - Availability
Description	CLM shall operate from 19:00 – 18:00 (except during maintenance window, if it is activated). However, processing of liquidity transfer orders will not be possible from 19:00 – 19:30 (but automated liquidity transfer orders triggered by central bank operations can be generated during that time and immediate liquidity transfer submitted during that time will be parked). It will be closed on weekends and T2 closing days, e.g. from Saturday starting at 02:30 until Monday 02:30 and from 02:30 on a T2 closing day to 02:30 on the next working day.

Id	SHRD.UR.BD.OPER.000.130
Name	CLM - Cut-offs
Description	For CLM the following cut-offs shall take place: • Cut-off for Standing Facilities takes place 15 minutes after the start of End of Day process (+15 minutes on last business day of reserve maintenance period). • CB Cut-off: It shall be possible for CBs to insert requests for connected payments, standing facility transactions and credit line modifications (and, after the transition period, for the ECMS to insert requests) into the system until 40 minutes after the start of the End of Day process (+15 minutes on last business day of reserve maintenance period). Note: The cut-offs shall be configurable with parameters. The mentioned points in time are only indicative values to define the order of the different cut-offs and the timing regarding the phase of business day they have to take place.

CRDM:

Id	SHRD.UR.BD.OPER.000.140
Name	CRDM - Availability
Description	CRDM shall operate from 19:00 – 18:00 (except during maintenance window). It will be closed on weekends and TARGET holidays following the operational hours of RTGS.

DWH:

Id	SHRD.UR.BD.OPER.000.150
Name	DWH - Availability
Description	DWH shall operate from 19:00 – 18:00 (except during maintenance window). It will be opened on weekends on a best effort basis, without support.

4 USER ROLES AND ACCESS (URA)

4.1 OVERVIEW

This section describes the processing of the *Two-Eyes* and *Four-Eyes* principle. For accessing a Eurosystem Market Infrastructure Service via U2A or A2A a User has to be created first. While setting up a User, one or more Roles have to be assigned to the User, from a list of predefined Roles for each Service in which the User will participate. Each Role grants a set of Privileges to the User. Each Privilege relates to one business function, following either the two-eyes or the four-eyes principle. The assigned principle will be applied to each action by the User when performing the business function.

The descriptions of the setup and maintenance of the User and the association of Roles are provided in section 2 on Common Reference Data Management in this User Requirements Document.

For accessing a Eurosystem Market Infrastructure Service the User has to connect via Eurosystem Single Market Infrastructure Gateway (ESMIG). One of the functions performed by ESMIG is the authentication of the User, i.e. the check that the User is registered in CRDM, and verify whether the User is allowed to access to the requested service, component or application. However, it is up to each service, component and application to check that the User is allowed to perform each business function through its list of Roles and Privileges as well as the accessible data scope. Due to the fact that ESMIG supports a single sign on capability for all services, components and applications, the same User can be allowed to access various services, components and applications.

Regarding the data scope, the User shall have access to all of the data of the Party with which the User is primarily associated, via the Access Rights. Any User can also be granted access to the data scope of another Party through additional Access Rights. When logging in to a service, component or application in U2A mode, a User having multiple Access Rights can choose the Party for which the actions will be performed. The User shall have the option to change the Party during the same session. The data scope shall allow access to all data for any Party for which Access Rights have been granted; there shall be no facility to restrict access to any particular type(s) of data (although this is possible in T2S).

4.1.1 Business Processes

Business Process	BP Reference	Business Process Description
Two-Eyes Approval	SHRD.BP.URA.2EYE	Process to allow create, amend or delete actions to be performed by only one user
Four-Eyes Approval	SHRD.BP.URA.4EYE	Process to ensure that create, amend or delete actions performed by a first user have to be confirmed by a second user

Table 3: Business Processes for User Roles and Access

4.1.2 General User Requirements for URA

Id	SHRD.UR.URA.ALL.000.010
Name	Authorisation Principle
Description	Each service, component and application shall provide a list of predefined Roles that can be assigned to a User. Each Role grants a set of Privileges to the User. Each Privilege relates to one business function, following either the two-eyes or the four-eyes principle.

Id	SHRD.UR.URA.ALL.000.020
Name	Validation of Authorisation Principle
Description	The system shall allow for U2A usage Roles which contain Privileges with two-eyes or four-eyes principle. The system shall allow for A2A usage Roles which contain only Privileges with two-eyes principle.

Id	SHRD.UR.URA.ALL.000.025
Name	User access
Description	The same User shall be allowed to access various Eurosystem Market Infrastructure Services via ESMIG.

Id	SHRD.UR.URA.ALL.000.030
Name	Validation of Roles and accessible data scope
Description	Each service, component and application shall check that the User is allowed to perform a business function through its list of Roles as well as to access the respective data scope through the associated Access Rights.

Id	SHRD.UR.URA.ALL.000.040
Name	User access to data
Description	The User shall have access to the data of the Party to which it belongs, through the Access Rights indicating that this is the primary Party associated with the User.

Id	SHRD.UR.URA.ALL.000.050
Name	User access to data scope of another Party
Description	It shall be possible to grant a User access to the data scope of another Party, through additional Access Rights set up between the User and other Parties. The data scope shall allow access to all data for any Party for which Access Rights have been granted; there shall be no facility to restrict access to any particular type(s) of data (although this is possible in T2S).

4.2 TWO-EYES APPROVAL

Business Process Ref: SHRD.BP.URA.2EYE

This business process describes the processing of the two-eyes principle. If a User was assigned a Role containing a Privilege following the two-eyes principle and the User creates new data, amends or deletes existing data through the use of this Privilege, then there is no need for verification by another User.

For specific functionality related to payment order initiation (such as the current execution of back-up payment orders) a four-eyes verification shall be required even if a User has a Role which contains a Privilege following the two-eyes principle.

For “read only” operations (i.e. operations that cannot change any data) only the two eyes principle will be applied.

4.2.1 User Requirements

Id	SHRD.UR.URA.2EYE.000.010
Name	Two-eyes principle
Description	If a User was assigned a Role containing a Privilege following the two-eyes principle and the User creates new data, amends or deletes existing data through the use of this Privilege, then there is no need for verification by another User.

Id	SHRD.UR.URA.2EYE.000.020
Name	Two-eyes principle - Exceptional handling
Description	For specific business processes related to payment order initiation (such as the execution of back-up payment orders) a four-eyes verification shall be required even if a User has a Role which contains a Privilege following the two-eyes principle.

4.3 FOUR-EYES APPROVAL

Business Process Ref: SHRD.BP.URA.4EYE

This business process describes the processing of the four-eyes principle. If a User was assigned a Role containing a Privilege following the four-eyes principle and the User creates new data, amends or deletes existing data by using this Privilege, there is a need for verification by another User. This second User can have a Privilege following two-eyes or four-eyes principle.

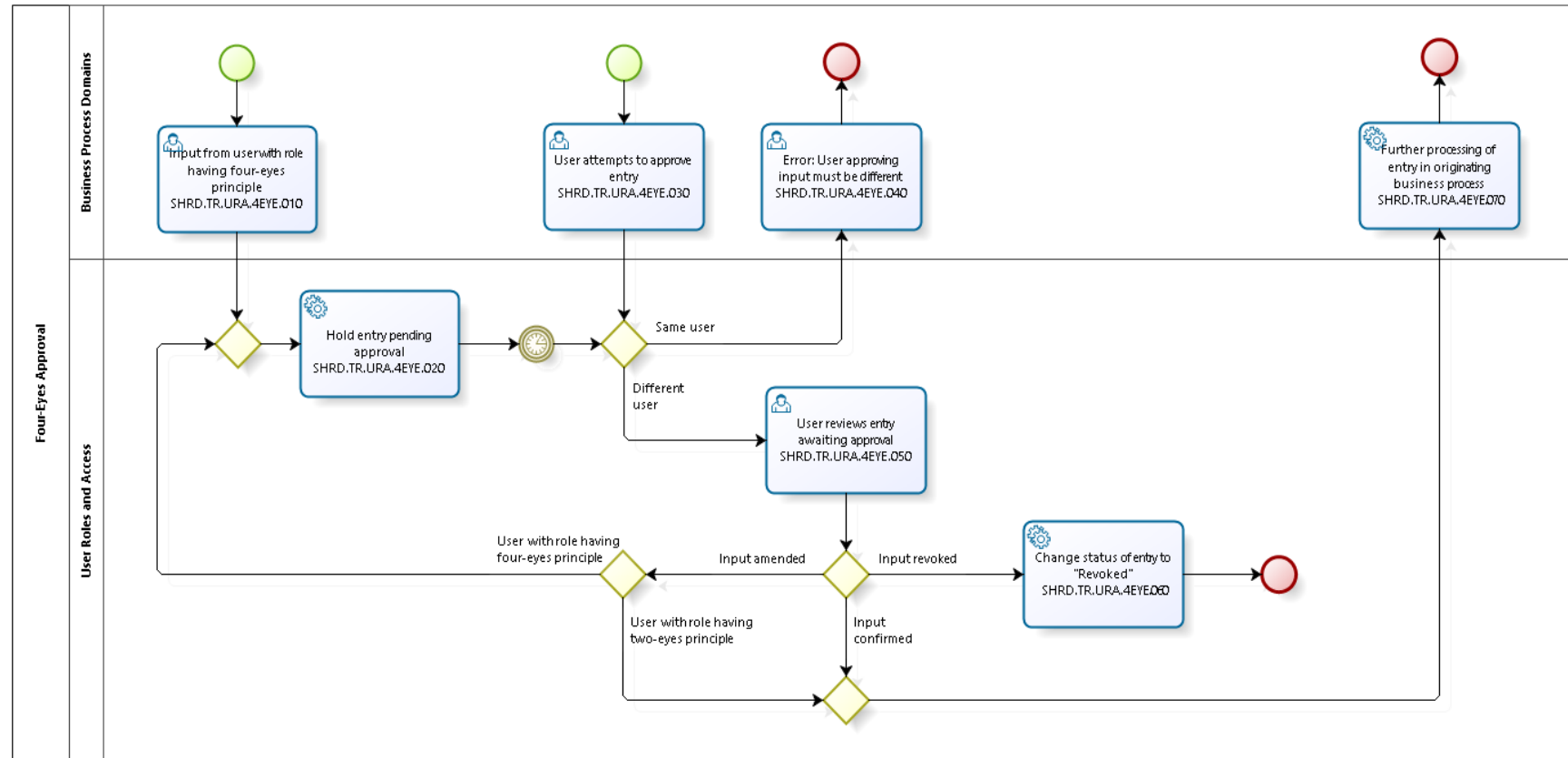
No four-eyes principle is foreseen for A2A. It will be the responsibility of the application sending the update in A2A mode to ensure that all appropriate security and access checks have been made prior to sending the request.

Where a User with a Role, which contains a Privilege following the four-eyes principle, has created new data, amended or deleted existing data, a second step for this update is required by another User to approve the change.

This User can perform the following actions:

- ▶ Confirm: The update is confirmed by the approval User and can therefore be processed.
- ▶ Revoke: The update is revoked by the approval User and therefore the status of the pending entry is changed to "Revoked".
- ▶ Amend: If the approval User needs to amend the order or data entered by the initial User the further processing is dependent on the Role of the approval User:
 - Approval User has a Role which contains a Privilege following the two-eyes principle:
The amendment of the approval User can be processed immediately.
 - Approval User has a Role which contains a Privilege following the four-eyes principle:
The amendment of the approval User needs verification by another User different from the approval User (but could potentially be the initial User). Therefore, the amended entry will be regarded as an initial creation or amendment of data.

Pending verifications for creations, amendments or deletions in four-eyes principle will be rejected at the start of the End of Day process.



Business Process Model 9: Four-Eyes Approval

4.3.2 User Requirements

4.3.2.1 GENERAL USER REQUIREMENTS FOR FOUR-EYES APPROVAL

Id	SHRD.UR.URA.4EYE.000.010
Name	Information on open tasks for verification
Description	Information on open tasks for verification by another User has to be available for the initiator of the order but also for the CB of the initiator.

Id	SHRD.UR.URA.4EYE.000.020
Name	Four-eyes principle - Check of different Users
Description	For a User who has a Role which contains a Privilege following the four-eyes principle it has to be checked that two different Users having the relevant Privileges perform the creation, amendment or deletion of data and the verification. This check shall ensure that the same User accessing the service, component or application via an alternative Network Service Provider is prevented from verifying an action previously performed by himself/herself. Note: The same User can perform for one task the creation, amendment or deletion of data and for another task the verification, providing that this is compliant with his/her Role.

Id	SHRD.UR.URA.4EYE.000.030
Name	Four-eyes principle - Creation, amendment or deletion
Description	If a User was assigned a Role containing a Privilege following the four-eyes principle and the User creates new data, amends or deletes existing data through the use of this Privilege, then there is a need for an additional verification by another User.

Id	SHRD.UR.URA.4EYE.000.040
Name	Four-eyes principle - Verification
Description	An approval User can perform the following actions: • Confirm: The update is confirmed by the approval User and can therefore be processed. • Revoke: The update is revoked by the approval User and therefore the status of the pending entry is changed to revoked. • Amend: Where the approval User edits the order or data entered by the first User, the further processing is dependent of the Role of the second User: – Approval User has a Role which contains a Privilege following the two-eyes principle: The amended update of the second User can immediately be processed. – Approval User has a Role which contains a Privilege following the four-eyes principle: The amended update of the approval User needs verification by another User. Therefore, the edit can be regarded as an initial creation or amendment of data. A confirmation, revocation or amendment can be performed as well by a CB User on behalf of the affected account holder independent from the user group profile of the initiator.

4.3.2.2 INPUT FROM USER WITH ROLE HAVING FOUR-EYES PRINCIPLE

Task Ref: SHRD.TR.URA.4EYE.010

User creates a new order or data, amends or deletes an existing order or data.

4.3.2.3 HOLD ENTRY PENDING APPROVAL

Task Ref: SHRD.TR.URA.4EYE.020

The creation, amendment or deletion is held pending verification by an approval User.

4.3.2.4 USER ATTEMPTS TO APPROVE ENTRY

Task Ref: SHRD.TR.URA.4EYE.030

Another User attempts to approve the entry through the appropriate verification screen.

If the same User, who made the initial entry, attempts to approve the entry, the attempt will not be possible.

4.3.2.5 ERROR: USER APPROVING INPUT MUST BE DIFFERENT

Task Ref: SHRD.TR.URA.4EYE.040

An error message is displayed on the User's screen stating that the entry cannot be approved by the same User that made the initial entry.

4.3.2.6 USER REVIEWS ENTRY AWAITING APPROVAL

Task Ref: SHRD.TR.URA.4EYE.050

The approval User reviews the entry awaiting approval. The system shall verify that the approval User has the relevant Privileges.

If the approval User revokes the entry, then creation, amendment or deletion will not take place and the entry will be changed into status "Revoked".

If the approval User confirms the entry, then the entry will be processed with the originating process.

If the approval User amends the entry and the approval User has only a Role which contains a Privilege following the four-eyes principle, then the amended entry will be held for further approval.

If the approval User amends the entry and the approval User has a Role which contains a Privilege following the two-eyes principle, then the amended entry will be processed with the originating process.

4.3.2.7 CHANGE STATUS OF ENTRY TO "REVOKED"

Task Ref: SHRD.TR.URA.4EYE.060

The status of creation, amendment or deletion entries that are revoked by the approval User is changed to "Revoked".

4.3.2.8 FURTHER PROCESSING OF ENTRY IN ORIGINATING BUSINESS PROCESS

Task Ref: SHRD.TR.URA.4EYE.070

Creation, amendment or deletion entries that are confirmed by the approval User are processed in the originating business process.

5 INFORMATION AND REPORTING (IR)

5.1 OVERVIEW

5.1.1 Context Diagram

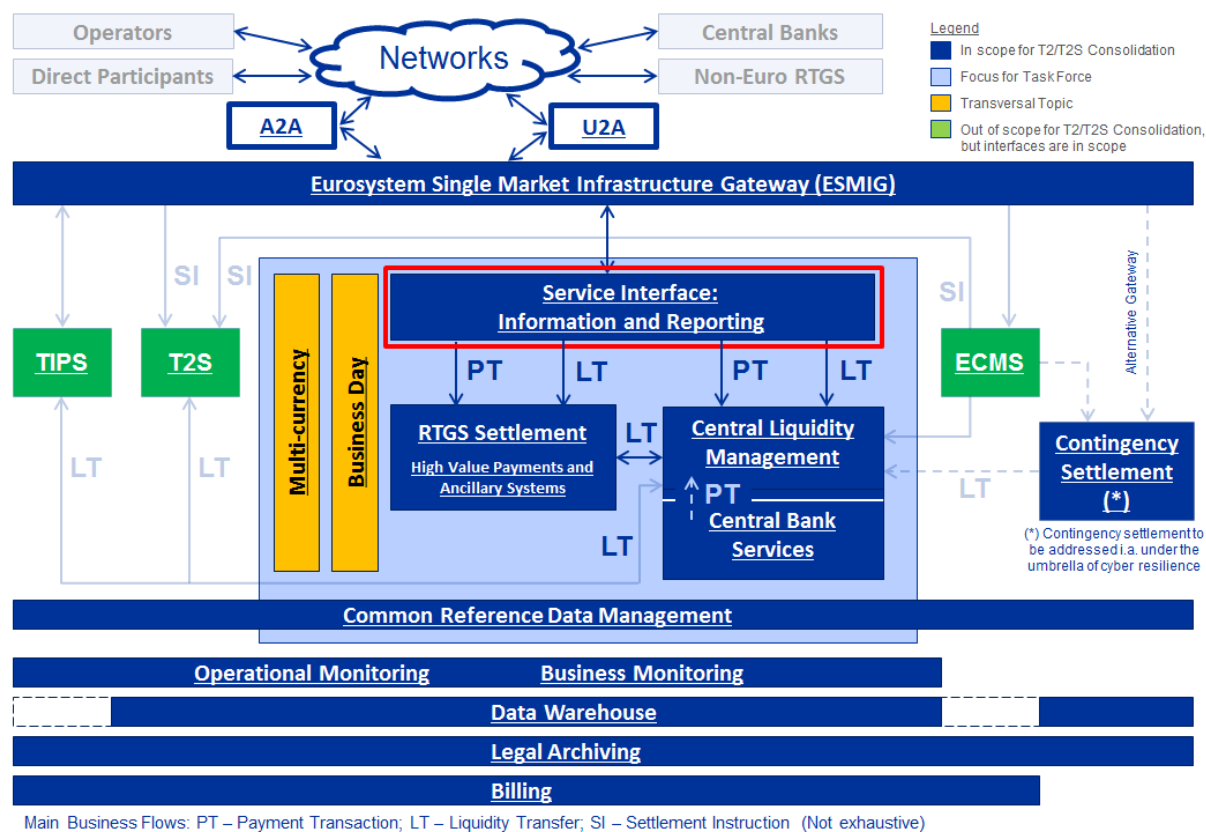


Figure 5: Context diagram for Information and Reporting

This section describes Information and Reporting. It includes the requirements for queries as well as reports. The business processes described in this section are working based on operational data.

However, requirements related to business and operational monitoring as well as information to be stored in the Data Warehouse for statistical and regulatory reporting are out of scope of the processes described in this section.

5.1.2 Business Processes

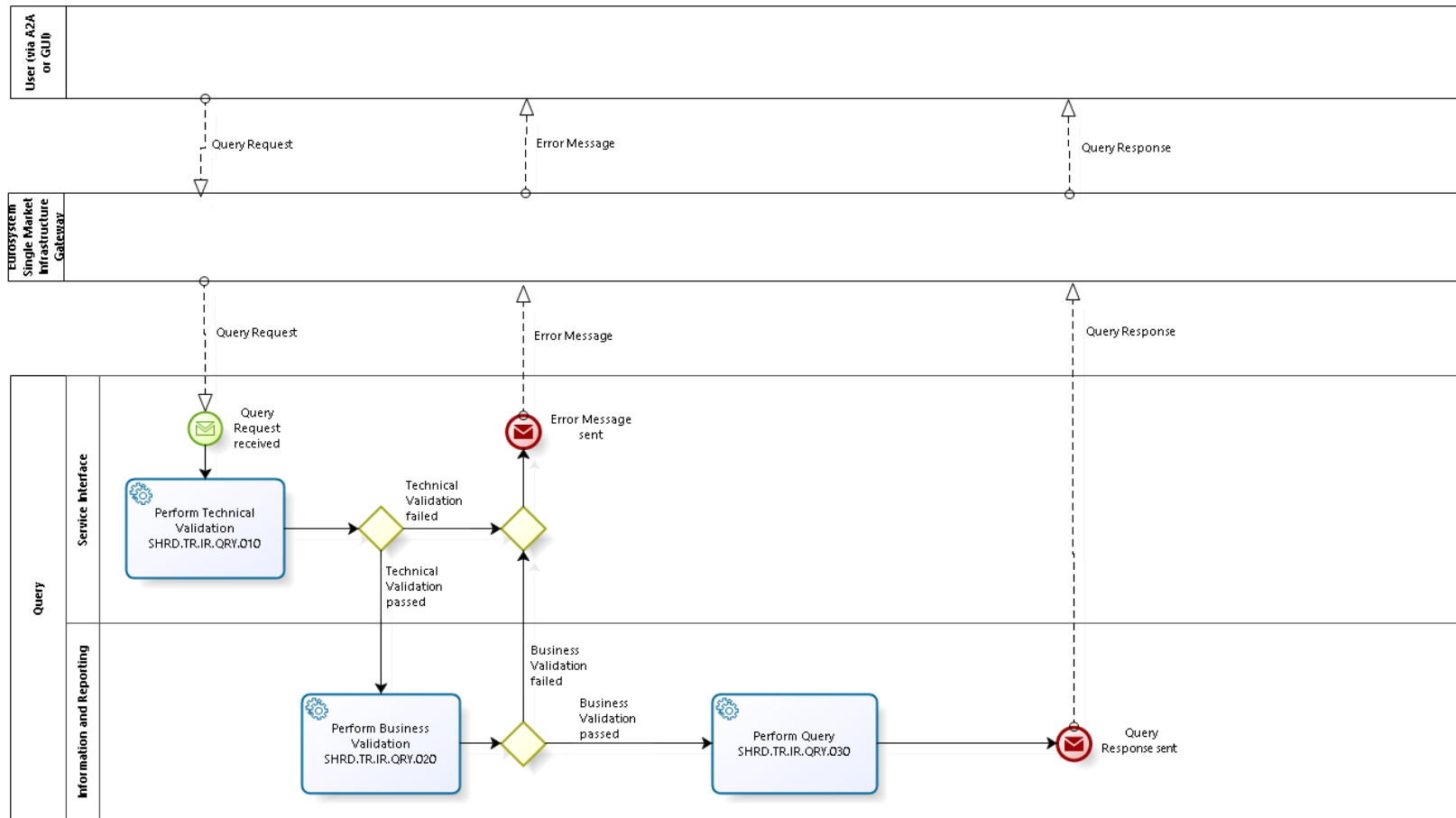
Business Process	BP Reference	Business Process Description
Query	SHRD.BP.IR.QRY	An user performs interactive query via the GUI (U2A) or via A2A
Produce Scheduled Report and Send (A2A) / Store for Download (U2A)	SHRD.BP.IR.SCHRPT	Reports produced on a regular basis are created and sent to all registered recipients in A2A (Push mode) Reports produced are also stored and available for U2A download (Pull mode)

Table 4: Business Processes for Information and Reporting

5.2 QUERY

Business Process Ref: SHRD.BP.IR.QRY

5.2.1 Business Process Model



Business Process Model 10: Query

5.2.2 Process overview

Process goal:

The purpose of this process is to perform a query requested by an user either via A2A or via the GUI (U2A) and to present the corresponding response provided by the service, component or application back to the user via the same mode as the request.

Process context:

- ▶ This process is the mechanism to allow an user to enquire about information held within the service, component or application.
- ▶ This process provides the opportunity
 - to download an already created report produced on a regular basis via U2A query
 - to query the latest version of an already created (and sent or downloaded) report until replaced by the next version via A2A and U2A

Pre-conditions:

- ▶ None

Time constraints:

- ▶ Not available during maintenance window

Expected results:

- ▶ If the query content is either invalid or fails the reference data checks, it will be rejected and a notification with error code(s) will be sent in A2A or the error message(s) are displayed in the GUI. If the query content is valid and reference data checks have been passed successfully, the platform will perform the query and will send the corresponding response either A2A or to the GUI.

Triggers:

- ▶ The process will be initiated by A2A or a U2A query.

5.2.3 User Requirements

5.2.3.1 PERFORM TECHNICAL VALIDATION

Task Ref: SHRD.TR.IR.QRY.010

When a query input is received via U2A or A2A, the component interface shall complete technical validation performing checks such as field level validation (fields have correct data type and size). The validation procedure will not stop after the detection of the first error but continues until the end and all errors found will be reported back (error codes are provided).

Id	SHRD.UR.IR.QRY.010.010
Name	Validation of query input
Description	The query process shall validate the query input to ensure that all attributes are of the correct data type and length.

Id	SHRD.UR.IR.QRY.010.020
Name	Check mandatory attributes
Description	The query process shall ensure that all mandatory attributes are populated.

Id	SHRD.UR.IR.QRY.010.030
Name	Processing where technical validation is successful
Description	Where the result of the technical validation is positive, the query shall be sent for further processing.

Id	SHRD.UR.IR.QRY.010.040
Name	Processing where technical validation fails
Description	Where the result of the technical validation is negative, the rejection notification shall be displayed directly on the screen with the appropriate error message where the query is via the GUI (U2A). If the request was received via A2A a rejection notification with the appropriate error code(s) shall be sent to the user performing the query. The validation will not stop after the first error was detected but continue until the end and all errors found will be reported back.

5.2.3.2 PERFORM BUSINESS VALIDATION

Task Ref: SHRD.TR.IR.QRY.020

Where the result of the technical validation is positive, the message is submitted for business validation. The business validation comprises checks such as cross-field consistency checks (where the value of one field is dependent upon, or has a relationship with, the value of another field, either within the query or in the data already present in the database) and authorisation checks to ensure that the user has suitable permissions.

If the validation failed, either an error message shall be displayed via the GUI or a rejection notification with the appropriate error code shall be sent to the user performing the query.

The validation procedure will not stop after the detection of the first error but continue until the end and all errors found will be reported back (with error codes being provided).

Id	SHRD.UR.IR.QRY.020.010
Name	Authorisation check
Description	The query process shall check that only authorised users are allowed to send a query and that the user is allowed to have “read” access to all values of all attributes (mandatory or optional according to the user’s access rights).

Id	SHRD.UR.IR.QRY.020.020
Name	Business validation of the mandatory and optional attributes
Description	The query process shall check that the values of all attributes that are populated (mandatory or optional) are valid according to the allowed values or value ranges.

Id	SHRD.UR.IR.QRY.020.030
Name	Check data integrity
Description	The query process shall check that all cross-field validations (data integrity) are satisfied, either between attributes within the query input or between an attribute in the query and one or more items of data held in the system.

Id	SHRD.UR.IR.QRY.020.040
Name	Processing where business validation fails
Description	Where the result of the business validation is negative, the rejection notification shall be displayed directly on the screen with the appropriate error message(s) where the query is via the GUI (U2A). If the request was received via A2A a rejection notification with the appropriate error code(s) shall be sent to the user performing the query. The validation will not stop after the first error was detected but continue until the end and all errors found will be reported back.

5.2.3.3 PERFORM QUERY

Task Ref: SHRD.TR.IR.QRY.030

After processing all validation successfully the query is performed and an adequate response is generated. The query response is either sent A2A or displayed in the GUI.

Id	SHRD.UR.IR.QRY.030.010
Name	Execution
Description	The query is executed. It shall take into account all criteria provided in the query. All data matching the given search criteria are retrieved.

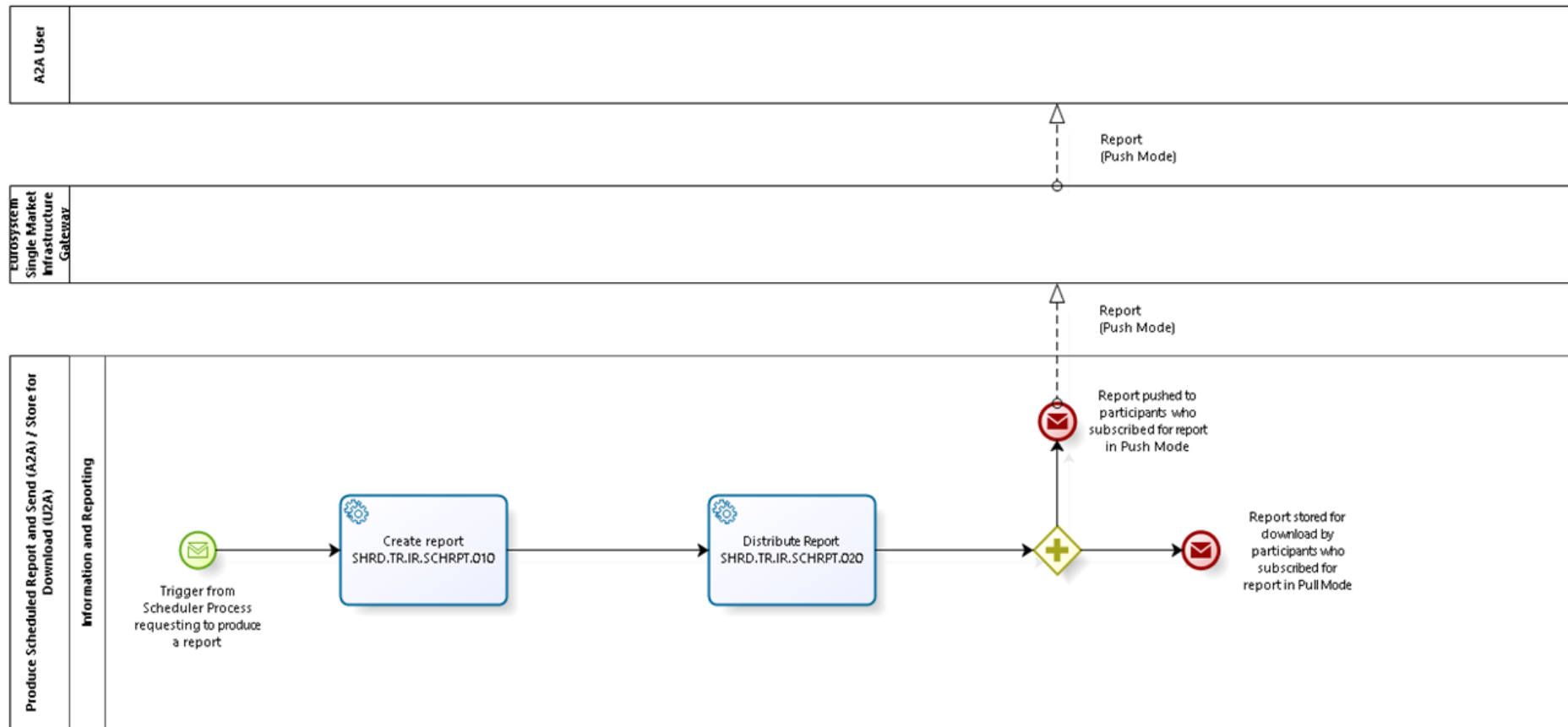
Id	SHRD.UR.IR.QRY.030.020
Name	Feedback where the execution of the query was successful
Description	The result shall be sent in the requested mode either to screen in U2A or via A2A.

Id	SHRD.UR.IR.QRY.030.030
Name	Export query results from the GUI
Description	Where the query has been executed via the GUI (U2A) and the results have been displayed on the screen, the user shall be able to export the results in various file formats (i.e. csv, pdf)

5.3 PRODUCE SCHEDULED REPORT AND SEND (A2A) / STORE FOR DOWNLOAD (U2A)

Business Process Ref: SHRD.BP.IR.SCHRPT

5.3.1 Business Process Model



Business Process Model 11: Produce Scheduled Report and Send (A2A) / Store for Download (U2A)

5.3.2 Process overview

Process goal:

The purpose of this process is to create reports, based on a time or an event trigger, and to either distribute them automatically or to store them and make them available for download.

Process context:

- ▶ This process is the mechanism whereby all regular standard reports will be produced and either distributed via A2A (Push mode) or only provided for U2A download (Pull mode), depending on the report subscription configured in CRDM.

Pre-conditions:

- ▶ None

Time constraints:

- ▶ Not available during maintenance window
- ▶ Account statements and general ledger files will only be provided after finalisation of the business day.

Expected results:

- ▶ The report will be created and sent to all registered recipients in A2A mode or made available for download via GUI (U2A).

Triggers:

- ▶ The process will be initiated by the scheduler.

5.3.3 User Requirements

5.3.3.1 CREATE REPORT

Task Ref: SHRD.TR.IR.SCHRPT.010

Id	SHRD.UR.IR.SCHRPT.010.010
Name	Report creation
Description	Each report request received from the Scheduler process for which the time-based or event-based trigger has occurred shall be created according to the predefined selection criteria and in the predetermined report format.

Id	SHRD.UR.IR.SCHRPT.010.020
Name	Update scheduler list
Description	Once the report request has been received, the Scheduler process will mark the request in the scheduler list as having been triggered.

5.3.3.2 DISTRIBUTE REPORT

Task Ref: **SHRD.TR.IR.SCHRPT.020**

Id	SHRD.UR.IR.SCHRPT.020.010
Name	Subscription check for recipients
Description	The report production process shall identify the participants for which there is an active report subscription for the report.

Id	SHRD.UR.IR.SCHRPT.020.020
Name	Report delivery
Description	The report production process will send out the report via A2A push mode for the participants who subscribed to it in push mode.

Id	SHRD.UR.IR.SCHRPT.020.030
Name	Report storage
Description	The report produced will be stored and will be available for participants who subscribed to the report in pull mode to be downloaded via U2A query.

5.4 INFORMATION AND REPORTING – NON-FUNCTIONAL REQUIREMENTS

5.4.1 Availability

Id	SHRD.UR.IR.NFR.020
Name	Unplanned downtime
Description	The Information and Reporting facilities shall be available during the same times as their underlying services, components and applications.

5.4.2 Disaster Recovery

Id	SHRD.UR.IR.NFR.030
Name	Recovery Time Objective
Description	Information and Reporting shall ensure a recovery time objective value of one hour in the event of site failures. Where there is a loss of a complete region the RTO shall not exceed two hours.

The recovery time objective (RTO) is the maximum amount of time required for recovery or restart of the service to a specified point of consistency. In the event of a site failure, Information and Reporting shall ensure a maximum time of unavailability of one hour starting from the time when the decision to restart the component is made up until the time the component is restored. Where there is a major failure or a regional disaster, the maximum time of unavailability is two hours starting from the time when the decision to restart the component is made up until the time the component is restored.

5.4.3 Performance Requirements

Id	SHRD.UR.IR.NFR.040
Name	Peak Workload per second
Description	Information and Reporting shall be able to handle an estimated peak workload of 20 interactions per second. This peak workload has to be endured for at least one hour.

Id	SHRD.UR.IR.NFR.050
Name	A2A Query Response Time
Description	Information and Reporting shall handle 100% of A2A queries related to CLM and RTGS within a maximum of 60 seconds. Limits shall be enforced (row, column and size) on the amount of data that can be downloaded via an A2A query. An option to abort long-running queries shall be provided.

Id	SHRD.UR.IR.NFR.060
Name	U2A Query Response Time
Description	Information and Reporting shall handle 100% of U2A queries related to CLM and RTGS within a maximum of 60 seconds. Limits shall be enforced (row, column and size) on the amount of data that can be downloaded via a U2A query. An option to abort long-running queries shall be provided.

6 DATA WAREHOUSE (DWH)

6.1 OVERVIEW

6.1.1 Context Diagram

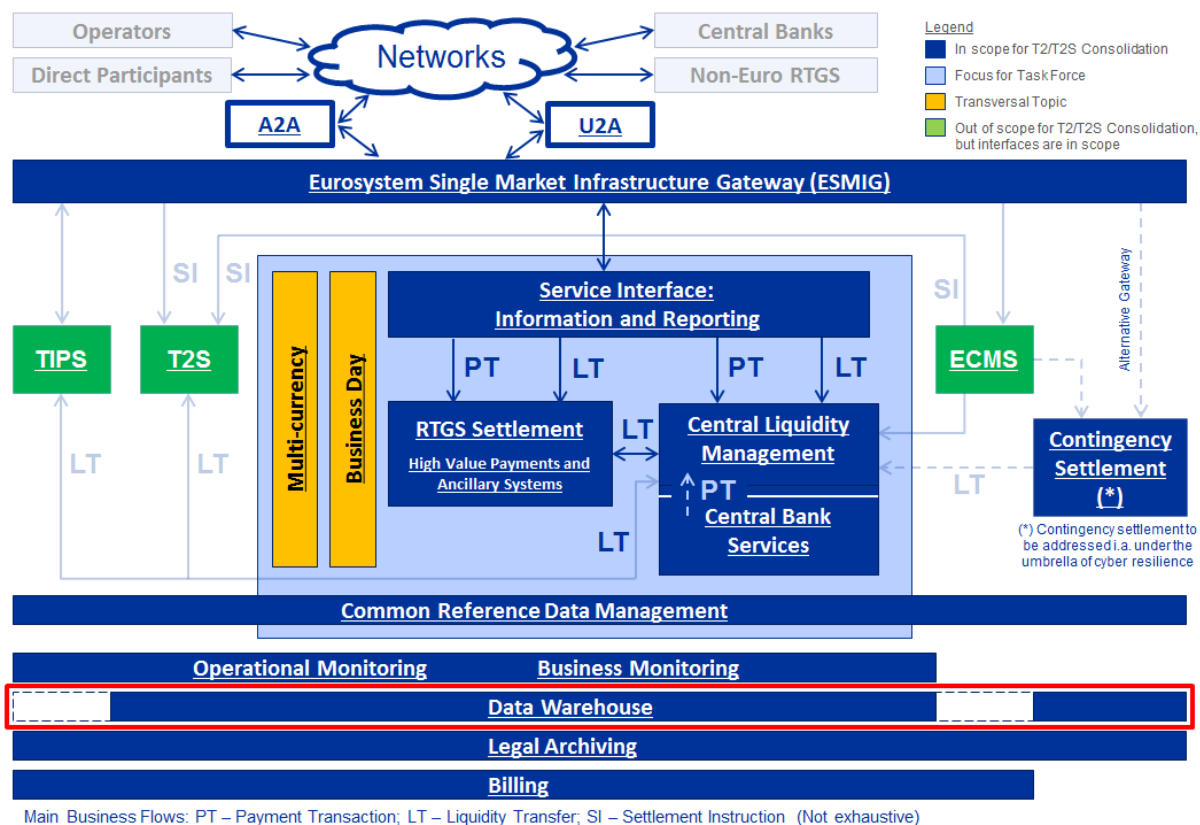


Figure 6: Context diagram for Data Warehouse

Data Warehouse provides data for historical, statistical and regulatory reporting. Data from the previous business days are available as of the next business day. The access to DWH is provided via U2A and A2A to:

- ▶ Participants, which have access to the predefined reports described in the User Interaction sections in the User Requirements Documents for CLM and RTGS and which may have additionally the possibility to save query/report templates (e.g. adapting a predefined report)
- ▶ CBs, which have access to further reports as described in the User Interaction sections in the CB annexes to the User Requirement Documents for CLM, RTGS and Common Components

6.1.2 Business Processes

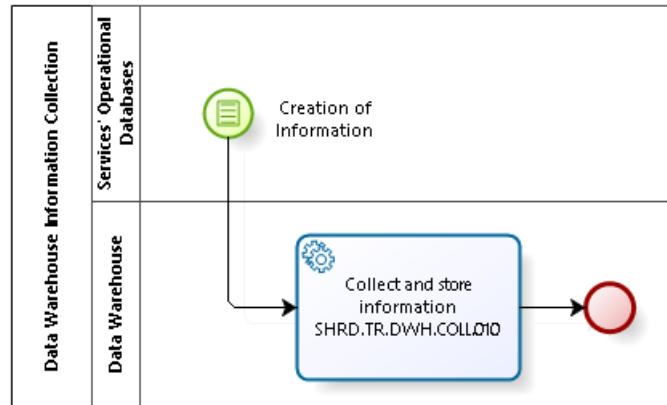
Business Process Name	BP Reference	Business Process Description
Data Warehouse Information Collection	SHRD.BP.DWH.COLL	Process to collect data within the various services and components
Data Warehouse Gather Information	SHRD.BP.DWH.GATH	Process to access collected information for the various needs

Table 5: Business Processes for Data Warehouse

6.2 DATA WAREHOUSE INFORMATION COLLECTION

Business Process Ref: SHRD.BP.DWH.COLL

6.2.1 Business Process Model



Business Process Model 12: Data Warehouse Information Collection

6.2.2 Process Overview

This business process describes the collection of business related data originating in the different services' and components' operational databases for queries, reports and regulatory reporting. In general, all available business relevant information shall be reflected in the Data Warehouse as granular data (order/account/participant level depending on type of data) for further analysis.

Disclaimer: The process flow description is not intended to predetermine any solution, e.g. that data need to be sent to DWH on the one hand, or sending of data to DWH might not be needed on the other hand. That will ultimately depend on the technology chosen.

6.2.3 User Requirements

6.2.3.1 COLLECT AND STORE INFORMATION

Task Ref: SHRD.TR.DWH.COLLO10

Id	SHRD.UR.DWH.COLLO10.010
Name	Information Collection
Description	Upon the creation of data entries the services and components shall provide data for Data Warehouse.

It should be possible to mirror all relevant data to Data Warehouse (further information can be found in the User Interaction section for each service and component).

Id	SHRD.UR.DWH.COLL.010.020
Name	Scope of collected information
Description	The scope of the information to be kept in DWH shall be derived from the requirements defined in the User Interaction sections of the User Requirements Documents for CLM, RTGS and Common Components as well as from their CB Annexes.

Id	SHRD.UR.DWH.COLL.010.030
Name	No service degradation of data source
Description	The provision of data shall not influence the operational behaviour of the underlying data sources.

Id	SHRD.UR.DWH.COLL.010.040
Name	Information age
Description	The services and components shall provide data to the Data Warehouse in time to meet the access needs. Data shall be available as of the next business day at the latest.

For queries, reports and regulatory reporting a provision of the data on the next business day is sufficient.

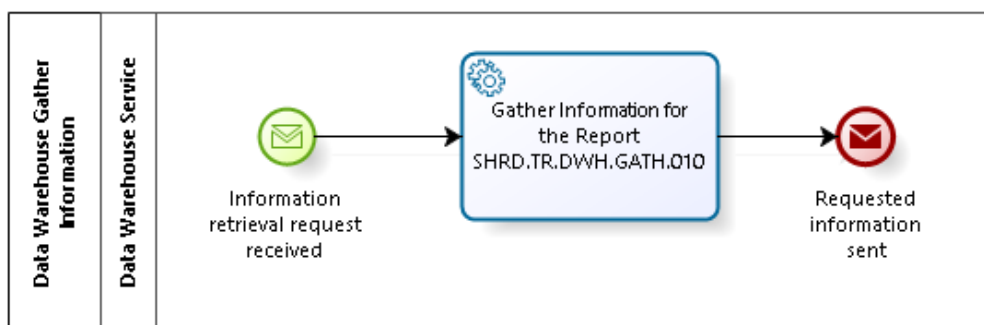
Id	SHRD.UR.DWH.COLL.010.050
Name	Retention period
Description	The collected information shall be kept for a retention period according to the business requirements, which preferably should be unlimited, but for at least 10 years. The retention period shall be configurable per data source.

Subject to the needs for queries and reports, it shall be possible to keep data in DWH for the retention period needed. Not each detailed data occurrence has to be kept for the full retention period. For example aggregated transaction data would be relevant for a longer time span.

6.3 DATA WAREHOUSE GATHER INFORMATION

Business Process Ref: SHRD.BP.DWH.GATH

6.3.1 Business Process Model



Business Process Model 13: Data Warehouse Gather Information

6.3.2 Process Overview

This business process describes the access to warehoused information. Data Warehouse only describes the data gathering process. Other aspects as e.g. report generation, data preparation or available views will be covered in the Information and Reporting and User Interaction sections of the User Requirement Documents for CLM, RTGS and Common Components as well as in their CB Annexes.

6.3.3 User Requirements

6.3.3.1 GATHER INFORMATION FOR THE REPORT

Task Ref: SHRD.TR.DWH.GATH.010

Id	SHRD.UR.DWH.GATH.010.010
Name	Information Access
Description	Upon request, access to the collected information shall be available to authorised users and processes. The user requirements on User Roles and Access apply (see section 4 on User Roles and Access in this document).

Id	SHRD.UR.DWH.GATH.010.020
Name	Information preparation
Description	Aggregated or otherwise prepared data to accelerate result generation will be subject to the information needs defined in the User Interaction sections of the User Requirements Documents for CLM, RTGS and Common Components as well as in their CB Annexes. Notably, a classification of the operations as used in the current TARGET2 statistical framework should be implemented.

Id	SHRD.UR.DWH.GATH.010.030
Name	Information display
Description	The display of information will be defined in the User Interaction sections of the User Requirements Documents for CLM, RTGS and Common Components as well as in their CB Annexes.

6.4 NON-FUNCTIONAL REQUIREMENTS FOR DATA WAREHOUSE

6.4.1 Availability

Id	SHRD.UR.DWH.NFR.020
Name	Availability
Description	Availability, calculated on a quarterly basis, shall be at least 97%.

DWH may be subject to incidents or failures, which may cause a temporary and unforeseen interruption of the service. Regardless of the total number of such unplanned interruptions, the overall availability calculated on a quarterly basis shall be at least 97%.

6.4.2 Disaster Recovery

Id	SHRD.UR.DWH.NFR.040
Name	Recovery Point Objective
Description	DWH shall ensure a recovery point objective of zero minutes to recover to the complete set of DWH data in the event of site failures and where there is a loss of a complete region.

The recovery point objective (RPO) is a point of consistency to which a user wants to recover or restart the service.

Id	SHRD.UR.DWH.NFR.050
Name	Recovery Time Objective
Description	DWH shall ensure a recovery time objective value of one day in the event of site failures and where there is a loss of a complete region

The recovery time objective (RTO) is the maximum amount of time required for recovery or restart of the service to a specified point of consistency. In the event of a site failure, Data Warehouse shall ensure a maximum time of unavailability of one day starting from the time when the decision to restart the component is made up until the time the component is restored. Where there is a major failure or a regional disaster, Data Warehouse shall ensure a maximum time of unavailability of one day starting from the time when the decision to restart the component is made up until the time the component is restored.

7 GENERAL NON-FUNCTIONAL REQUIREMENTS

The general non-functional requirements cover all requirements which are not service or component specific but apply to all services and components. Within the description of each of the services and components in the User Requirements Documents for CLM, RTGS and Common Components as well as in their CB Annexes the availability, disaster recovery and performance requirements have already been considered.

7.1 GENERAL FRAMEWORK

Id	SHRD.UR.NFR.ALL.000.010
Name	Language
Description	The services and components shall only use the English language.

This includes all documentation as well as all communication.

Id	SHRD.UR.NFR.ALL.000.020
Name	Service Usage Statistics
Description	The services and components shall count the usage of their functions.

This purpose for this requirement is to be able to identify built-in functionality with little or no use. Also, it should enable developers to evaluate whether usage and resource consumption of functions meets the expectations.

7.2 INFORMATION SECURITY

Id	SHRD.UR.NFR.ALL.000.030
Name	Information Security
Description	The services and components shall be compliant with the Information Security Requirements and Controls.

7.3 CYBER RESILIENCE

Id	SHRD.UR.NFR.ALL.000.040
Name	Cyber Resilience
Description	The services and components shall be compliant with Cyber Resilience Requirements and Controls.

7.4 TARGET SERVICE DESK

Id	SHRD.UR.NFR.ALL.000.050
Name	TARGET Service Desk
Description	The TARGET Service Desk shall be available at the service provider to respond to any operational or technical issue concerning the services and components.

Id	SHRD.UR.NFR.ALL.000.060
Name	TARGET Service Desk Availability
Description	The TARGET Service Desk shall be available both during standard support and non-standard support hours with different service levels.

The TARGET Service Desk's support hours shall be harmonised across the services and components. The definition of standard and non-standard support hours and reaction times will be part of the Service Level Agreement.

Id	SHRD.UR.NFR.ALL.000.070
Name	Trouble Management System
Description	The TARGET Service Desk shall be supported by a Trouble Management System (TMS).

The TARGET Service Desk shall be supported by a Trouble Management System (TMS). All activities connected to outages shall be tracked in and supported by the TMS, which covers the workflow and serves as the information base.

Id	SHRD.UR.NFR.ALL.000.080
Name	Access to Trouble Management System
Description	Parties other than the Central Banks shall have access to TMS with the possibility to view information related to broadcast incidents and problems and their own incidents and problems.

Id	SHRD.UR.NFR.ALL.000.090
Name	Contacting the TARGET Service Desk
Description	The TARGET Service Desk and the National Service Desks shall be reachable via phone, fax and email.

7.5 GENERAL BUSINESS CONTINUITY REQUIREMENTS

Id	SHRD.UR.NFR.ALL.000.100
Name	IT Service Continuity Management process is in place
Description	An IT Service Continuity Management (ITSCM) process shall be in place to

	ensure that services and components can be recovered within the required and agreed time-scales.
--	--

The goal for ITSCM is to support the overall Business Continuity Management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and Service Desk) can be recovered within required, and agreed, business time-scales.

Id	SHRD.UR.NFR.ALL.000.110
Name	Independent remote sites
Description	All services and components shall have independent remote sites to restart the services and components in the event of site failures.

The services and components shall have both technically and organisationally, independent remote sites with different risk profiles to be able to cope with incidents and crises which might affect the primary sites.

Id	SHRD.UR.NFR.ALL.000.120
Name	Crisis management
Description	Crisis management procedures and crisis management structures shall be defined and agreed.

The service provider shall have a structure and procedures in place to manage incidents and events that exceed a pre-agreed severity threshold. This covers e.g.:

- ▶ Coordination of crises;
- ▶ Communication of crises;
- ▶ Decision making procedures;
- ▶ Escalation procedures; and
- ▶ Resilient communication tools.

The goal is to provide clear information to the external parties, coordinate the incident resolution and enable business continuity during and after the crisis.

Id	SHRD.UR.NFR.ALL.000.130
Name	Access of support staff
Description	Support staff must have access to the systems at all times, including during crises.

7.6 SERVICE MANAGEMENT

Id	SHRD.UR.NFR.ALL.000.140
Name	Service Management Processes
Description	IT service management processes following the ITIL v.3 framework shall be in place.

The maintenance of the services shall be subject to efficient IT management processes.

7.7 CLOCK SYNCHRONISATION

Id	SHRD.UR.NFR.ALL.000.150
Name	Clock synchronisation method
Description	The services and components shall use atomic clock time as a reference.

The services' and components' clocks have to be synchronised to an atomic clock time (in UTC). The time will be CET; wintertime and summertime adjustments shall be observed.

7.8 TESTING REQUIREMENTS

The testing organisation is defined in the Testing Strategy document. Currently no functional user requirements for support of testing have been identified.

8 USER INTERACTION

The objective of this section is to provide the user requirements related to user interactions covering the usage of user-to-application (U2A) or application-to-application (A2A) mode. A Graphical User Interface (GUI) shall be provided for components, offering facilities to access information in U2A mode. The GUIs shall be harmonised to the best possible extent.

These requirements do not imply any particular consideration with regard to the design and implementation of the actual screens.

8.1 GENERAL USER REQUIREMENTS FOR USER INTERACTION

The following general requirements shall apply to the RTGS, CLM and Common Components.

8.1.1 Query

Id	SHRD.UR.ALL.UI.010
Name	Query Audit Trail
Description	Each component shall provide the functionality to query through U2A interface the modified data at the attribute level, the user performing the change and the timestamp of the change. It should be visible which attributes were changed, together with the new values. The query shall return relevant business attributes of the Audit Trail.

Id	SHRD.UR.ALL.UI.020
Name	Query System time
Description	All components shall provide the functionality to query system time to align the time of a connected application through an A2A interface. The query shall return the System time.

8.1.2 Action

Id	SHRD.UR.ALL.UI.030
Name	Amend / Revoke Task(s)
Description	All components shall provide the functionality to amend/revoke task(s) through the U2A interface.

Id	SHRD.UR.ALL.UI.040
Name	Act on behalf
Description	All components shall provide the functionality to act on behalf through U2A and A2A interfaces for: • Central Banks, to act on behalf of any Party belonging to their banking community; and • The TARGET Service Desk, to act on behalf of any Party.

Id	SHRD.UR.ALL.UI.050
Name	Access rights
Description	All components shall ensure that a user can only access functionality and data that is allowed by the access rights granted to the user through the Roles associated with the user.

Id	SHRD.UR.ALL.UI.060
Name	Four-eyes (confirm, revoke, amend)
Description	All components shall provide the functionality to use the four-eyes approval process through the U2A interface, allowing the authoriser to confirm, revoke or amend the input from the originator.

8.2 USER INTERACTION FOR EUROSISTEM SINGLE MARKET INFRASTRUCTURE GATEWAY

As stated in SHRD.UR.ALL.UI.050, all Services shall ensure that a user can only access functionality and data that is allowed by the access rights granted to the user through the Roles associated with the user. In particular, this shall mean that ESMIG user interface functionality shall only be accessible to authorised internal 4CB users.

8.2.1 Query

Id	SHRD.UR.ESMIG.UI.010
Name	Query message
Description	ESMIG shall provide the functionality to query the outgoing and incoming messages. The user shall specify all of the following mandatory selection criteria. In addition the query shall allow the user to specify any combination of mandatory or optional selection criteria. <u>Mandatory selection criteria:</u> • Entry date or range of date (current business day as default) • Entry time or range of time • Inbound or outbound • Message type • Service/component/application <u>Optional selection criteria:</u> • Status • Sender DN • Receiver DN The query shall return the message in xml format including the processing status. This query shall only be provided in U2A mode.

8.3 USER INTERACTION FOR COMMON REFERENCE DATA MANAGEMENT

8.3.1 Query

All queries described in this section shall be provided in both U2A and A2A mode unless otherwise stated.

For U2A queries, the Party BIC and the Cash Account number would be deduced from the data scope of the user. The data scope is described in section 4 on User Roles and Access in this User Requirements Document.

The extended list of the selection criteria and the output of the queries shall be defined in the UDFS.

The selection criteria listed in the queries may only refer to the business attributes as defined in section 9 Business Data Definitions in this User Requirements Document.

Id	SHRD.UR.CRDM.UI.010
Name	Query Party
Description	CRDM shall provide the functionality to query the Common Reference Data of a Party. The user can query within his data scope, which is determined by the Party BIC (Party BICs in case of a Central Bank as a user). The query shall allow the user to specify any combination of the following optional selection criteria. <u>Optional selection criteria:</u> • Party BIC • Status • Responsible CB • Party Type The query shall return all business attributes of the Party including the status.

Id	SHRD.UR.CRDM.UI.020
Name	Query participant
Description	CRDM shall provide the functionality to query the Common Reference Data of a participant. The user can query within his data scope. The query shall allow the user to specify any combination of the following optional selection criteria. <u>Optional selection criteria:</u> • Participant BIC • Status (U2A only) • Responsible CB • Party Type The query shall return all business attributes of the participant including the status.

Id	SHRD.UR.CRDM.UI.030
Name	Query Ancillary System
Description	CRDM shall provide the functionality to query the Common Reference Data of an Ancillary System. The user can query within his data scope. In addition the query shall allow the user to specify any combination of the following optional selection criteria. <u>Optional selection criteria:</u> • Party BIC • Status (U2A only) • Responsible CB The query shall return all business attributes of the Ancillary System including the status.

Id	SHRD.UR.CRDM.UI.040
Name	Query Central Bank
Description	CRDM shall provide the functionality to query the Common Reference Data of a Central Bank. The user can query within his data scope, which is determined by the Party BIC (Party BICs in case of a Central Bank as a user). In addition the query shall allow the user to specify any combination of the following optional selection criteria. <u>Optional selection criteria:</u> • Status (U2A only) • Party BIC The query shall return all business attributes of the Central Bank including the status.

Id	SHRD.UR.CRDM.UI.050
Name	Query directory (U2A only)
Description	CRDM shall provide the U2A functionality to query the list of reachable banks for payments. The user shall specify any combination of, but at least one of the following optional selection criteria. <u>Optional selection criteria:</u> • Status • BIC of reachable party • Name of reachable party • Responsible CB • Modification Date (from-to) • Service The query shall return all business attributes of the directory. All information in the directory shall be available to all users.

Id	SHRD.UR.CRDM.UI.060
Name	Query Standing Order
Description	CRDM shall provide the functionality to query the reference data of a Standing Order. The user can query within his data scope. In addition the query shall allow the user to specify any combination but at least one of the following optional selection criteria. <u>Optional selection criteria:</u> • Status (U2A only) • Party BIC • Cash Account number The query shall return all business attributes of the Standing Order.

Id	SHRD.UR.CRDM.UI.070
Name	Query Cash Account reference data
Description	CRDM shall provide the functionality to query reference data of Cash Accounts. The user can query within his data scope, which is determined by the Party BIC (Party BICs in case of a Central Bank as a user). In addition the query shall allow the user to specify any combination but at least one of the following optional selection criteria. <u>Optional selection criteria:</u> • Party BIC • Cash Account number The query shall return all business attributes of the Cash Account including the status.

Id	SHRD.UR.CRDM.UI.080
Name	Query Direct Debit Mandate
Description	CRDM shall provide the functionality to query the values for Direct Debit Mandates. The user can query within his data scope. In addition the query shall allow the user to specify any combination but at least one of the following optional selection criteria. <u>Optional selection criteria:</u> • Party BIC • Cash Account number • Status (U2A only) • Reference The query shall return all business attributes of the Direct Debit Mandate in U2A mode. In A2A mode, the query shall return all mandatory and optional, but not transactional attributes of the Direct Debit Mandate (see SHRD.UR.BDD.140 on Direct Debit Mandate in this User Requirements Document)

Id	SHRD.UR.CRDM.UI.090
Name	Query Calendar
Description	CRDM shall provide the functionality to query a calendar. The user shall specify at least one of the following selection criteria: • Year • Month The query shall return all business attributes of the calendar.

Id	SHRD.UR.CRDM.UI.110
Name	Query Error Codes
Description	CRDM shall provide the functionality to query the description of the Error Codes. The user shall specify at least one of the following selection criteria: • Error Code • Error Code description The query shall return all business attributes of the error code. The query is available in U2A mode only.

8.3.2 Action

Id	SHRD.UR.CRDM.UI.120
Name	Create a Standing Order for Limit
Description	CRDM shall provide the functionality to create a Limit through the U2A interface.

Id	SHRD.UR.CRDM.UI.130
Name	Amend a Standing Order for Limit
Description	CRDM shall provide the functionality to amend a Limit through the U2A interface and the A2A interface.

Id	SHRD.UR.CRDM.UI.140
Name	Delete a Standing Order for Limit
Description	CRDM shall provide the functionality to delete a Limit through the U2A interface and the A2A interface.

Id	SHRD.UR.CRDM.UI.150
Name	Create a Report Subscription
Description	CRDM shall provide the functionality to create a Report Subscription through the U2A interface.

Id	SHRD.UR.CRDM.UI.160
Name	Amend a Report Subscription
Description	CRDM shall provide the functionality to amend a Report Subscription through the U2A interface.

Id	SHRD.UR.CRDM.UI.170
Name	Delete a Report Subscription
Description	CRDM shall provide the functionality to delete a Report Subscription through the U2A interface.

Id	SHRD.UR.CRDM.UI.180
Name	Create a Message Subscription
Description	CRDM shall provide the functionality to create a Message Subscription through the U2A interface.

Id	SHRD.UR.CRDM.UI.190
Name	Amend a Message Subscription
Description	CRDM shall provide the functionality to amend a Message Subscription through the U2A interface.

Id	SHRD.UR.CRDM.UI.200
Name	Delete a Message Subscription
Description	CRDM shall provide the functionality to delete a Message Subscription through the U2A interface.

Id	SHRD.UR.CRDM.UI.210
Name	Create a Standing Order
Description	CRDM shall provide the functionality to create a Standing Order through the U2A interface and the A2A interface.

Id	SHRD.UR.CRDM.UI.220
Name	Amend a Standing Order
Description	CRDM shall provide the functionality to amend a Standing Order through the U2A interface and the A2A interface.

Id	SHRD.UR.CRDM.UI.230
Name	Delete a Standing Order
Description	CRDM shall provide the functionality to delete a Standing Order through the U2A interface and the A2A interface.

Id	SHRD.UR.CRDM.UI.231
Name	Create a Rule-based liquidity transfer order
Description	CRDM shall provide the functionality to create a Rule-based liquidity transfer order through the U2A interface, including non-technical attributes listed in SHRD.UR.BDD.130. Users will be able to perform this action only - for the full set of attributes of Rule-based liquidity transfer orders and the mandatory attributes of Rule-based floor liquidity transfer orders having an Account to be Debited for which they are defined as Account Owner or Co-Manager; - for the Floor Amount and Target Amount After Breaching Floor attributes of Rule-based floor liquidity transfer orders having an Account to be Credited for which they are defined as Account Owner or Co-Manager.

Id	SHRD.UR.CRDM.UI.232
Name	Amend a Rule-based liquidity transfer order
Description	CRDM shall provide the functionality to amend a Rule-based liquidity transfer order through the U2A interface, including non-technical attributes listed in SHRD.UR.BDD.130. Users will be able to perform this action only - for the full set of attributes of Rule-based ceiling liquidity transfer orders and the mandatory attributes of Rule-based floor liquidity transfer orders having an Account to be Debited for which they are defined as Account Owner or Co-Manager; - for the Floor Amount and Target Amount After Breaching Floor attributes of Rule-based floor liquidity transfer orders having an Account to be Credited for which they are defined as Account Owner or Co-Manager.

Id	SHRD.UR.CRDM.UI.233
Name	Delete a Rule-based liquidity transfer order
Description	CRDM shall provide the functionality to delete a Rule-based liquidity transfer order through the U2A interface. Users will be able to perform this action only for Rule-based liquidity transfers having an Account to be Debited for which they are defined as Account Owner or Co-Manager.

Id	SHRD.UR.CRDM.UI.234
Name	Create a floor/ceiling notification configuration
Description	CRDM shall provide the functionality to create a floor/ceiling notification through the U2A interface, including attributes listed in SHRD.UR.BDD.131. Users will be able to perform this action only for the Cash Accounts for which they are defined as Account Owner or Co Manager.

Id	SHRD.UR.CRDM.UI.235
Name	Amend a floor/ceiling notification configuration
Description	CRDM shall provide the functionality to amend a Rule-based liquidity transfer through the U2A interface, including attributes listed in SHRD.UR.BDD.131. Users will be able to perform this action only for the Cash Accounts for which they are defined as Account Owner or Co Manager.

Id	SHRD.UR.CRDM.UI.236
Name	Delete a floor/ceiling notification configuration
Description	CRDM shall provide the functionality to delete a floor/ceiling notification through the U2A interface. Users will be able to perform this action only for the Cash Accounts for which they are defined as Account Owner or Co Manager.

Id	SHRD.UR.CRDM.UI.240
Name	Create a Standing Order for Reservation
Description	CRDM shall provide the functionality to create a Standing Order for Reservation through the U2A interface.

Id	SHRD.UR.CRDM.UI.250
Name	Amend a Standing Order for Reservation
Description	CRDM shall provide the functionality to amend a Standing Order for Reservation through the U2A interface and the A2A interface.

Id	SHRD.UR.CRDM.UI.260
Name	Delete a Standing Order for Reservation
Description	CRDM shall provide the functionality to delete a Standing Order for Reservation through the U2A interface and the A2A interface.

Id	SHRD.UR.CRDM.UI.360
Name	Grant access rights to individual users
Description	CRDM shall provide the functionality to grant access rights to individual users through the U2A interface.

Id	SHRD.UR.CRDM.UI.370
Name	Create a participant
Description	CRDM shall provide the functionality to create a participant through the U2A interface.

Id	SHRD.UR.CRDM.UI.380
Name	Amend a participant
Description	CRDM shall provide the functionality to amend a participant through the U2A interface.

Id	SHRD.UR.CRDM.UI.390
Name	Delete a participant
Description	CRDM shall provide the functionality to amend a participant through the U2A interface.

Query / Action	U2A	A2A
Query Standing Order	x	x
Query Cash Account reference data	x	x
Query Central Bank	x	x
Query participant	x	x
Query Ancillary System	x	x
Query Calendar	x	x
Query Direct Debit Mandate	x	x
Query Error Codes	x	
Query directory	x	x
Query Party	x	x
Grant access rights to individual users	x	
Create/ Amend /Delete a participant	x	
Create/Amend/ Delete a Standing Order	x	x
Amend/ Delete Standing Order for Limit	x	x
/Amend/Delete a Standing Order for Reservation	x	x
Create Standing Order for Limit	x	
Create Standing Order for Reservation	x	
Create/Amend/Delete a Report Subscription	x	
Create/ Amend/Delete a Message Subscription	x	

Table 6: Summary of queries and actions in U2A and A2A mode for Common Reference Data

Management

8.4 USER INTERACTION FOR BUSINESS DAY

8.4.1 Query

Id	SHRD.UR.BD.UI.010
Name	Query list of events
Description	Business Day shall provide the functionality to query the list of events scheduled for the current day including the actual time when these events took place.

8.5 USER INTERACTION FOR DATA WAREHOUSE (DWH)

8.5.1 Report

Id	SHRD.UR.DWH.UI.010
Name	Predefined report
Description	DWH shall offer a limited number of predefined reports to participants via the U2A and A2A interfaces.

9 BUSINESS DATA DEFINITIONS

This section describes the business data entities and attributes referred to within the business process descriptions either within this document, the User Requirements Document for Common Components, or those that are common to the business processes described in more than one of the User Requirements Documents of the Eurosystem Market Infrastructure Services (RTGS, CLM, TIPS, T2S).

Business data entities and attributes that are referred to uniquely within only one of the User Requirements Documents are described within that particular User Requirements Document.

The business data entities and attributes described include both Common Reference Data and also data that are transactional in nature.

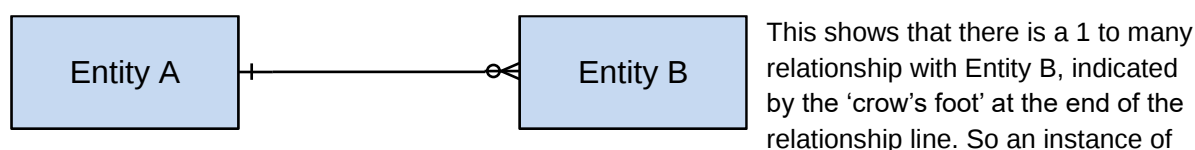
The definitions of the entities are based purely on a logical view of the data requirements implied by the understanding of the requirements for the business processes. These logical definitions do not in any way imply or predicate any design considerations or suggestions.

Within the context of the User Requirements Document, an 'entity' is a person, organisation, place, thing or concept which helps to define or is of interest to TARGET Services RTGS, such as Party, Service, Cash Account, Standing Order etc. These are shown as boxes in the Entity Relationship diagrams in the following section.

Each entity is described by a number of 'attributes' which are the individual pieces of information about that entity. The level of detail and the enumerations of the attributes in this document serve as an indication; the enumerations and description of entities and attributes are non-exhaustive. Additional entities or attributes may be deemed to be necessary during the detailed design.

The association between one entity and another is described by a 'relationship' and these are shown as lines connecting the two related entities (boxes) in the Entity Relationship diagrams. The relationship names indicate the nature of the relationship between the entities, and also the optionality and cardinality of the relationship (i.e. whether an entity has to be linked to the other entity or whether it is optional, and whether the relationship is 1 to many, 1 to 1 or many to many).

As an example, the diagram below depicts the relationship between Entity A and Entity B:



Entity A can be associated with any number of instances of Entity B (including zero, because of the 'O' on the line next to the crow's foot). Every instance of Entity B must be associated with one and only one instance of Entity A (because of the '1' on the line next to Entity A).

Currently the BDD for the Common Components, CLM and RTGS are described in detail. The BDD for T2S and TIPS are delivered within the requirements of the concerning services; an alignment is envisaged and ensured as far as possible.

The diagrams below illustrate how the model supports some of the various ways in which Parties will be associated with services, through the use of the Party Type.

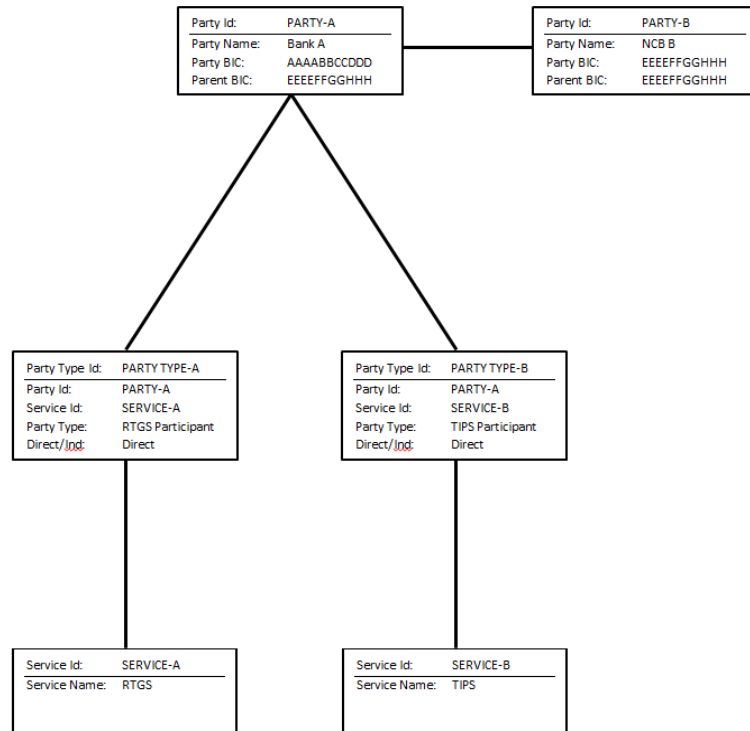
It has been agreed that Limit, Report Subscription and Message Subscription are at a Cash Account level.

Bank A is a participant in RTGS and TIPS

PARTY

PARTY TYPE

SERVICE



NCB A is a Central Bank for both T2 and T2S

PARTY

Party Id:	PARTY-A
Party Name:	NCB A
Party BIC:	AAAAABCCDDDD
Parent BIC:	AAAAABCCDDDD

PARTY TYPE

Party Type Id:	PARTY TYPE-A
Party Id:	PARTY-A
Service Id:	SERVICE-A
Party Type:	Central Bank
Direct/Ind:	Direct

Party Type Id:	PARTY TYPE-B
Party Id:	PARTY-A
Service Id:	SERVICE-B
Party Type:	Central Bank
Direct/Ind:	Direct

SERVICE

Service Id:	SERVICE-A
Service Name:	T2

Service Id:	SERVICE-B
Service Name:	T2S

Bank B is both a T2S Payment Bank and a CSD Participant in T2S. Bank B requires TWO Parties.

PARTY

Party Id:	PARTY-A
Party Name:	NCB A
Party BIC:	AAAAABCCDDDD
Parent BIC:	AAAAABCCDDDD

Party Id:	PARTY-B
Party Name:	Bank B
Party BIC:	BBBBCCDDDDD
Parent BIC:	AAAAABCCDDDD

Party Id:	PARTY-C
Party Name:	Bank B
Party BIC:	BBBBCCDDDDD
Parent BIC:	CCCCDDEEFF

Party Id:	PARTY-D
Party Name:	CSD A
Party BIC:	CCCCDDEEFF
Parent BIC:	CCCCDDEEFF

PARTY TYPE

Party Type Id:	PARTY TYPE-A
Party Id:	PARTY-A
Service Id:	SERVICE-A
Party Type:	Central Bank
Direct/Ind:	Direct

Party Type Id:	PARTY TYPE-B
Party Id:	PARTY-B
Service Id:	SERVICE-A
Party Type:	T2S Payment Bank
Direct/Ind:	Direct

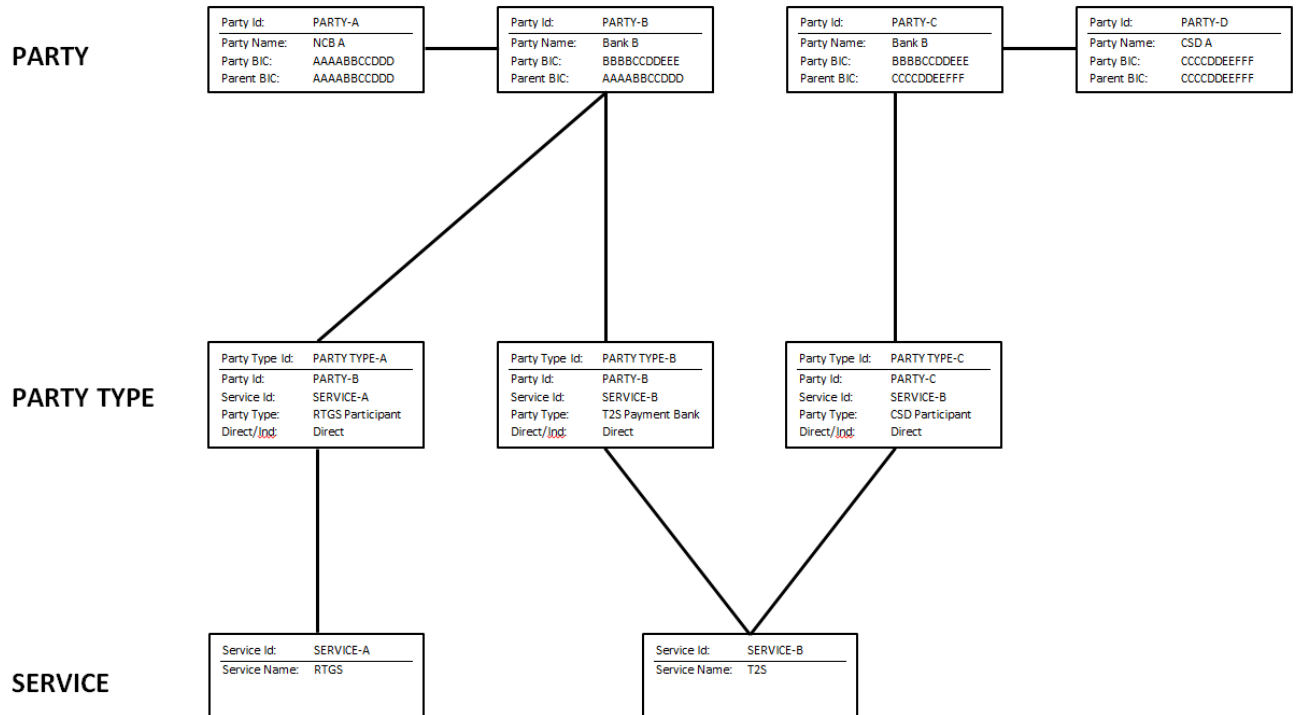
Party Type Id:	PARTY TYPE-C
Party Id:	PARTY-C
Service Id:	SERVICE-A
Party Type:	CSD Participant
Direct/Ind:	Direct

Party Type Id:	PARTY TYPE-D
Party Id:	PARTY-D
Service Id:	SERVICE-A
Party Type:	CSD
Direct/Ind:	Direct

SERVICE

Service Id:	SERVICE-A
Service Name:	T2S

Bank B is a participant in RTGS, a T2S Payment Bank and also a CSD participant in T2S



9.1.2 Cash Account

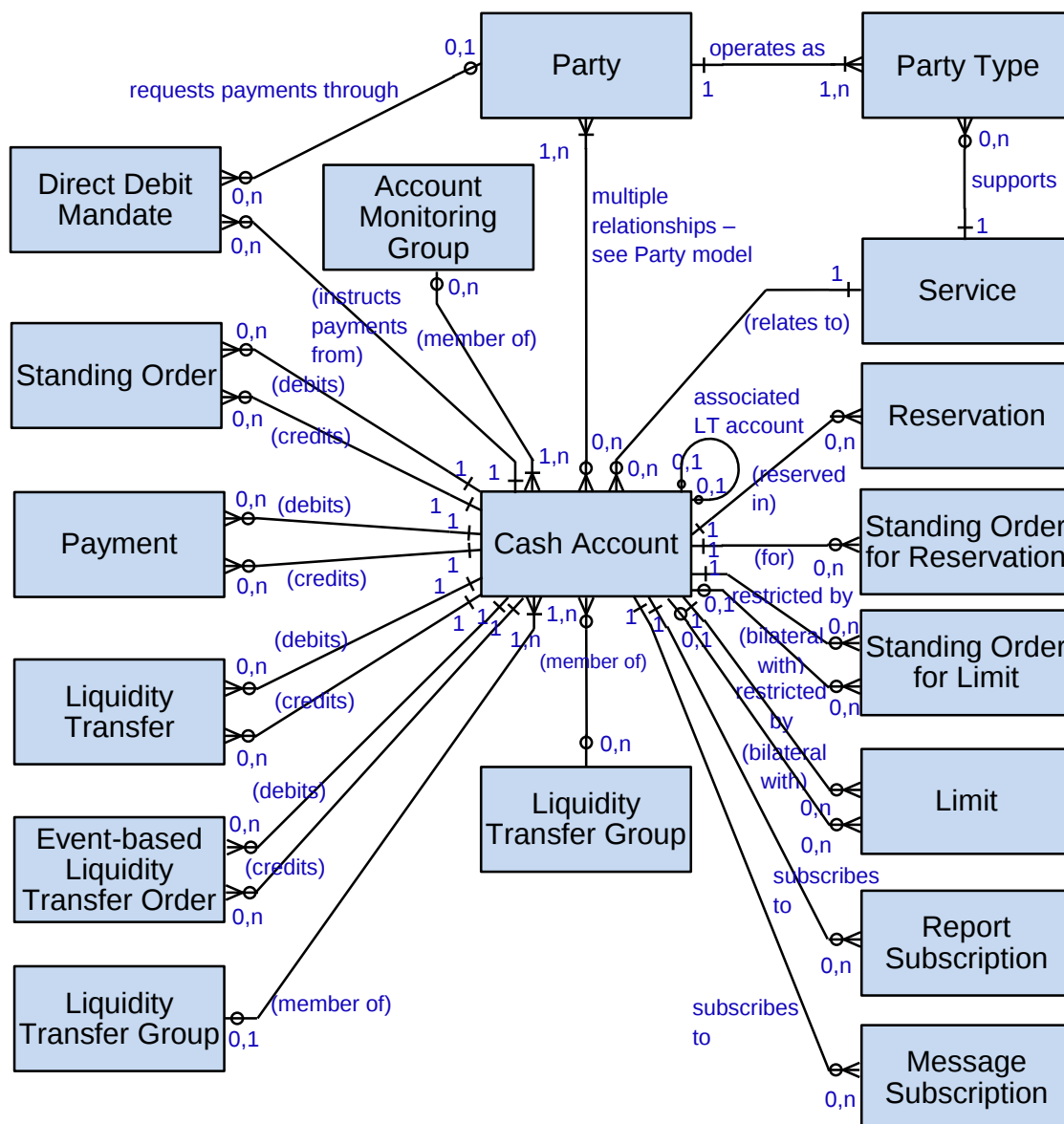


Figure 8: Entity Relationship Diagram for Cash Account

9.1.3 User

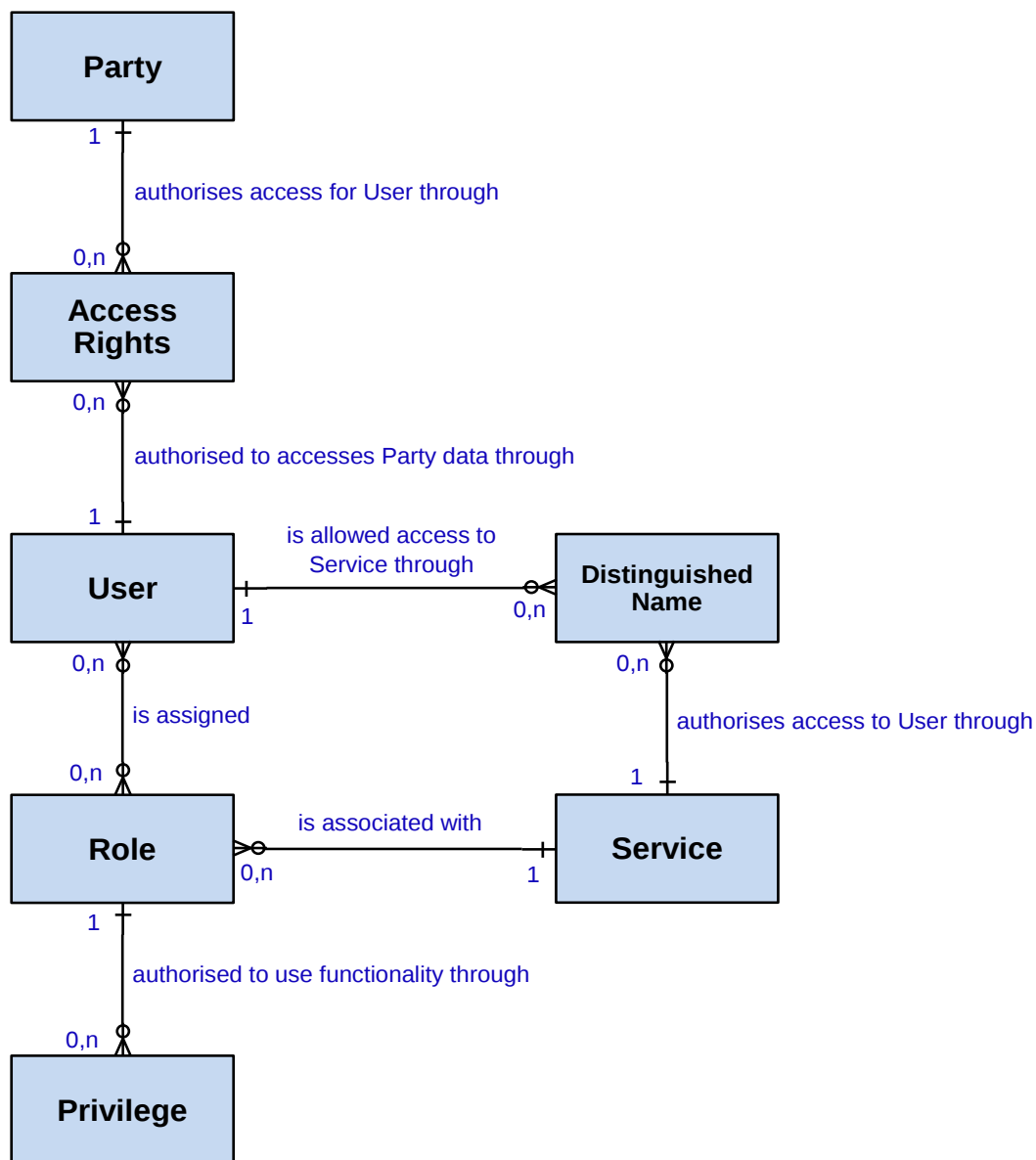


Figure 9: Entity Relationship Diagram for User

9.2 ENTITIES AND ATTRIBUTES

Id	SHRD.UR.BDD.000
Name	Audit Trail
Description	The following Attributes are implied to be included within each of the Entities described in this section, without being stated explicitly in every case. <u>Mandatory attributes:</u> • User Id The unique technical identifier of the user (individual or application) who updated the occurrence of the entity • Timestamp The timestamp is a snapshot of the operating system date and time when a change is committed • Approval Status Indicates whether the change requires four-eyes approval and if so whether the change has been approved or not <u>Optional attributes:</u> n/a

Id	SHRD.UR.BDD.010
Name	Party
Description	This entity shall denote any legal or organisational entity required in the Eurosystem Market Infrastructure Services <u>Mandatory attributes:</u> • Party Identifier (KEY) (for internal use only) The unique technical identifier of the Party • Party BIC BIC11 identifying the Party • Parent BIC BIC11 of the Parent responsible for the Party. Where the Party is a Parent and there is no other Party having responsibility over it, then Parent BIC will be the same as the Party BIC • Institutional Sector Code Identifies the financial corporations sector classification to which the Party belongs with respect to the nature of its business. Should take a value defined by ESA 2010 Standards • Party Status The business status of a Party for processing in the system • Intraday Credit Indicator (i.e. allowed/not allowed) • Overnight Deposit Indicator (i.e. allowed/not allowed) • Marginal Lending Indicator (i.e. allowed/not allowed) • Minimum Reserve Obligation (i.e. the Party is subject to / exempted from minimum reserve requirement) • Opening Date The date on which the contractual relationship with the Party was legally established • Notification and Broadcast Messages Subscription Y/N flag, indicating whether the party wishes to subscribe to settlement-related notifications and operations-related-broadcast in A2A <u>Optional attributes:</u> • Banking Group Identifier The unique technical identifier of a Banking Group • Billing Group Identifier The unique technical identifier of a Billing Group • LEI (mandatory for Parties using RTGS or CLM) The unique identifier of the legal entity in accordance with the ISO 17442 standard • Global End of Day Balance Balance composed of the individual End of Day balances within each settlement service for the participant • Monetary Financial Institution (MFI) Code This attribute shall identify the MFI code of the Party

- **Leading CLM Account Holder**
 - BIC of the Party designated as the Minimum Reserve Leader where minimum reserves are managed in a pool
 - Party BIC of the intermediary party in case of indirect holding of minimum reserve
 - Party's own BIC in case of direct holding of minimum reserves (same value as Party BIC attribute in that case)
 - Empty in case the party is not subject to minimum reserves.
 - **Marginal Lending Account**
Account Number of the Marginal Lending Account managed within CLM and maintained by a Central Bank to settle all marginal lending orders submitted by CBS and processed by CLM (applies until the go-live of ECMS)
 - **Overnight Deposit Account**
Account Number of the Overnight Deposit Account managed within CLM and maintained by a Central Bank to settle all overnight deposit orders submitted by CBS and processed by CLM
 - **Closing Date**
The date that the contractual relationship with the Party has legally ended
 - **Currency Code**
The national currency associated with a Central Bank
 - **Country Code**
 - **VAT Rates**
(Only relevant for system entities; Multiple occurrences allowed)
The additional national rate of Value Added Tax associated with a Central Bank or a CSD.
Mandatory where Party Type is Central Bank (CB) or Central Securities Depository (CSD), but can be zero.
 - **VAT Exempt**
True/false flag set to Y if VAT is not applicable to the party
 - **Tariffs**
(Multiple occurrences allowed)
For each service item defined in the billing component, the party may be assigned to a specific tariff.
 - **Account To Be Credited (Central Banks only)**
(Multiple occurrences allowed)
The Cash Account to be credited within the billing process. Different accounts may be specified for each different settlement service (T2S, T2, TIPS, ECMS)
 - **Procedure E notification (Ancillary Systems only)**
Single or global Procedure E Notification
- Transactional data (only for MFI with direct or indirect minimum reserves management and for Lead CLM Account Holder in case of pool management):**
- **Minimum Reserves (EUR)**
Minimum reserve requirement
 - **Running Average (EUR)**
Value of running average calculated at the end of the previous day
 - **Adjustment Balance (EUR)**
Value of adjustment balance

Id	SHRD.UR.BDD.015
Name	Central Bank Accounts for Interest Payments
Description	This entity shall denote the attributes related to minimum reserve for Central Bank Parties in CLM. These attributes are applicable for Eurosystem National Central Banks. <u>Optional attributes:</u> • CB account for standing facilities interests Identifier of the CLM CB Account (among those held by the CB itself) for standing facilities interests. • CB account for minimum reserve interests and penalties Identifier of the CLM CB Account (among those held by the CB itself) for reserve interests and penalties. • CB account for other interests Identifier of the CLM CB Account (among those held by the CB itself) for other interests.

Id	SHRD.UR.BDD.020
Name	Party Type
Description	This entity shall denote the type of participation or business role of a Party within a settlement service. <u>Mandatory attributes:</u> • Party Type Identifier (KEY) (for internal use only) The unique technical identifier of the Party Type • Party Identifier The unique technical identifier of a Party. It shall link the Party Type to the Party • Service Identifier The unique technical identifier of the settlement service with which the Party is associated within the capacity of this Party Type. It shall link the Party Type to the settlement service • Party Type Description Describes the nature of the business role performed by the Party within the settlement service. This will include (but is not restricted to): – TARGET Service Desk – Central Bank (CB) – T2S Payment Bank – RTGS account holder – CLM account holder – TIPS account holder – TIPS Operator – Credit Institution – Ancillary System (AS) – Central Securities Depository (CSD) – CSD Participant – External CSD – Reachable Party • Valid From Date <u>Optional attributes:</u> • Valid To Date • Direct/Indirect The nature of the participation in the settlement service by the Party, where appropriate • AS sub-type The type of AS where appropriate in RTGS. Multiple values are not allowed. Exactly one value is mandatory when the party is an AS. No value allowed when the party is not an AS.

Id	SHRD.UR.BDD.025
Name	Authorised Account User
Description	An Authorised Account User defines a three-way relationship between a Cash Account, a Party acting as a participant and a BIC. This relationship enables the participant, using a specific BIC, to instruct payment orders on the Cash Account. In other words, the BIC specified in a payment order on a Cash Account must be authorized through this entity. <u>Mandatory attributes:</u> • Authorised Account User Identifier (KEY) (for internal use only) The unique technical identifier of the Authorised Account User • Account Number The Account Number uniquely identifies the Cash Account authorised for use by the Authorised Account User • Payment BIC Code BIC11 code identifying the participant authorised to instruct payment orders on the Cash Account • Valid From Date The date from which the Authorised Account User is valid. <u>Optional attributes:</u> • Party Identifier The unique technical identifier of a Party. • Valid To Date

Id	SHRD.UR.BDD.030
Name	Party Name
Description	This entity shall denote a Party Name. <u>Mandatory attributes:</u> • Party Identifier (KEY) The unique technical identifier of a Party. It shall link the name back to the Party • Valid From Date The date from which the Party Name is valid. Since the Party Name may change over time, it is necessary to define period in which a name is valid • Party Long Name The full name of the Party • Party Short Name The short name of the Party <u>Optional attributes:</u> • Valid To Date

Id	SHRD.UR.BDD.040
Name	Party Address
Description	This entity shall denote the address of a Party. <u>Mandatory attributes:</u> • Address Identifier (KEY) (for internal use only) The unique technical identifier of the Party Address • Party Identifier The unique technical identifier of a Party. It shall link the address to the Party • Valid From Date The date from which the Party Address is valid <u>Optional attributes:</u> • Jurisdiction The country of jurisdiction for the Party. This attribute shall be mandatory for a legal address. It shall be the same country as in the legal address, except for supranational institutions • Street The name of the street for the address • House Number The house number for the address • City The name of the city for the address • Postal Code The postal code for the address • State or Province The state or province for the address. Its use shall depend on the country code of the address • Country Code The country code of the address. The two-character ISO country code (ISO3166-1) shall identify the country • Valid To Date

Id	SHRD.UR.BDD.045
Name	Party Contact
Description	This entity shall denote the name and contact details for an individual acting as a contact for a Party <u>Mandatory attributes:</u> • Party Contact Identifier (KEY) (for internal use only) The unique technical identifier of the Party Contact • Party Identifier The unique technical identifier of a Party. It shall link the Address to the Party • Contact Name The name of the contact for the Party • Contact Position The position or role of the contact for the Party • Valid From Date The date from which the Party Contact is valid <u>Optional attributes:</u> • Office Telephone Number The Office Telephone Number for the Party Contact • Mobile Number The Mobile Number for the Party Contact • Email Address The Email Address for the Party Contact • Valid To Date

Id	SHRD.UR.BDD.050
Name	Banking Group
Description	This entity shall denote a Banking Group, allowing a number of Parties acting as Payment Banks or Ancillary Systems to be viewed collectively for certain business purposes, such as oversight and regulation. Payment Banks and Ancillary Systems within a Banking Group may be associated with more than one Central Bank. <u>Mandatory attributes:</u> • Banking Group Identifier (KEY) (for internal use only) The unique technical identifier of the Banking Group. • Banking Group Name The name of the Banking Group. <u>Optional attributes:</u> n/a

Id	SHRD.UR.BDD.055
Name	Account Monitoring Group
Description	This entity shall denote a consolidation group, allowing a number of Cash Accounts of Parties acting as participants (RTGS or CLM) to be viewed collectively for certain business processes, such as the monitoring of liquidity. This is similar to the Consolidated Account Information concept in TARGET2. Cash Accounts within an Account Monitoring Group may be owned by different Parties (banks), and these Parties may be associated with more than one Central Bank. Furthermore, a Cash Account may belong to more than one Account Monitoring Group. <u>Mandatory attributes:</u> • Account Monitoring Group Identifier (KEY) (for internal use only) The unique technical identifier of the Account Monitoring Group • Account Monitoring Group Name The name of the Account Monitoring Group <u>Optional attributes:</u> n/a

Id	SHRD.UR.BDD.060
Name	Billing Group
Description	This entity shall denote a Billing Group, allowing a number of Parties acting as Payment Banks to be viewed collectively for the purpose of aggregating RTGS payments to derive volume-based tariffs. Payment Banks within a Billing Group may be associated with more than one Central Bank. <u>Mandatory attributes:</u> • Billing Group Identifier (KEY) (for internal use only) The unique technical identifier of the Billing Group. • Billing Group Name The unique name of the Billing Group. • Billing Group Leader References a party <u>Optional attributes:</u> n/a

Id	SHRD.UR.BDD.065
Name	Minimum reserve configuration
Description	<u>This entity shall store reference data for the current period of minimum reserve</u> <u>Mandatory attributes:</u> • Current Maintenance Period From Date range of the current maintenance period • Current Maintenance Period To Date range of the current maintenance period • Minimum reserve interest rate Interest rate applied to the average minimum reserve holding at the end of the maintenance period • Minimum reserve penalty rate type 1 Interest rate applied to compute the minimum reserve penalty in case of single infringement • Minimum reserve penalty rate type 2 Interest rate applied to compute the minimum reserve penalty in case of repeated infringement • Excess reserve interest rate (exempt tier) Interest rate applied to the average excess reserve exempt tier at the end of the maintenance period • Excess reserve interest rate (non-exempt tier) Interest rate applied to the average excess reserve non-exempt tier at the end of the maintenance period • Overnight deposit interest rate Interest rate applied to overnight deposit • Marginal lending interest rate Interest rate applied to marginal lending • Excess reserve exemption factor Factor for the calculation of the excess reserve exemption amount <u>Optional attributes:</u> • n/a

Id	SHRD.UR.BDD.070
Name	Limit
Description	This entity shall denote a limit at account level which will restrict the settlement of normal payment orders in a Cash Account, either towards a specified party (bilateral) or in general (multilateral). <u>Mandatory attributes:</u> • Limit Identifier (KEY) The unique technical identifier of the Limit • Limit Type Type of the Limit i.e.: – Bilateral – Multilateral • Defined Limit The initial value of the Limit pertaining to the Cash Account • From Cash Account Cash Account for which normal payment orders are restricted by the Limit <u>Optional attributes:</u> • To Cash Account Cash Account with which the Bilateral Limit exists (mandatory for Bilateral Limits; not used for Multilateral Limits). Cannot be an account of a Central Bank, i.e. normal payment orders towards a Central Bank cannot be restricted. • <u>Transactional data:</u> • Free Limit Position The current value of the remaining Limit. This is adjusted dynamically during the day as payments and transfers are made into or out of the Cash Account.

Id	SHRD.UR.BDD.080
Name	Standing Order for Limit
Description	A template for limits initiated at Start of Day. <u>Mandatory attributes:</u> • Limit Type Type of the Limit i.e.: – Bilateral – Multilateral • Defined Limit The initial value of the Limit pertaining to the Cash Account • From Cash Account Cash Account for which normal payment orders are restricted by the Limit • Valid From Date <u>Optional attributes:</u> • To Cash Account Cash Account with which the Bilateral Limit exists (mandatory for Bilateral Limits; not used for Multilateral Limits). Cannot be an account of a Central Bank, i.e. normal payment orders towards a Central Bank cannot be restricted. • Valid To Date

Id	SHRD.UR.BDD.090
Name	Cash Account
Description	This entity shall denote any cash account required by the Eurosystem Market Infrastructure Services. For certain Cash Account Types, the Account Owner may not have any other Cash Accounts. <u>Mandatory attributes:</u> • Service Identifier Possible values are: • RTGS • CLM • TIPS • T2S • Account Number (KEY) The Account Number uniquely identifies the Cash Account • Cash Account Type • For RTGS: - RTGS DCA, - Guarantee account, - Sub account for AS settlement, - CB Account, - Dedicated Transit Account, - AS Technical Account, - Technical account • For Ancillary Systems: - Guarantee account, - Technical account • For CLM: - Main Cash Account (MCA), - Overnight Deposit (OD) account, - CB Account, - CB ECB Account, - ECB mirror account, - Dedicated Transit Account, - Marginal Lending Account • For TIPS: - TIPS DCA, - Dedicated Transit Account • For T2S: - T2S DCA, - CB Account, - Dedicated Transit Account • Currency Code

	The Cash Account's currency, which is an eligible settlement currency • Account Owner The Party who owns the Cash Account • Status Current blocking status of the Cash Account; unblocked, blocked for debiting, blocked for crediting or blocked for both • Opening Date The date as of which a Cash Account is legally opened <u>Optional attributes:</u> • Party To Be Billed The Party to whom the invoice will be addressed • Party To Be Charged The Party to whom the billable item is assigned, due to a contractual agreement • MCA to be debited The Main Cash Account to be debited within the billing process • Ancillary System Used Party Identifier of the Ancillary System used for the Cash Account • Ancillary System Model Used Ancillary System Model used for the Cash Account • Associated Liquidity Transfer Account A 1 to 1 link between an MCA and a DCA for liquidity transfer orders • Automated generation of Interest payment (System generated) Indicates whether interest payment is automatically generated by CLM (yes/no) • Minimum Reserve Party Party for which this Cash Account is included for minimum reserve calculation (applicable for RTGS DCA and sub account for AS settlement) • Management of Minimum Reserve The method by which the Minimum Reserve is managed. Possible values are: • Direct • Pool • No • Default Flag Indicating whether the Cash Account is the default choice of the Party (RTGS, CLM) • Contingency Account The Account Number of the corresponding contingency account (in the Contingency Settlement) (must be provided for the first MCA or RTGS DCA created) • Account Monitoring Group Identifier (Multiple occurrences allowed) The unique technical identifier of an Account Monitoring Group • Liquidity Transfer Group Identifier (Multiple occurrences allowed) The unique technical identifier of a Liquidity Transfer Group • Maximum Amount for Direct Debit Orders The maximum amount allowed to be debited from the Cash Account
--	---

based on direct debit orders per business day

- **Closing Date**
The date as of which a Cash Account is legally closed
- **Rule-based liquidity transfers for queued urgent payment/AS transfer orders**

Boolean attribute specifying whether a rule-based liquidity transfer should be triggered from the Associated LT Account when an urgent payment order or AS transfer order is queued.

- **Rule-based liquidity transfers for queued urgent payment/AS transfer/high priority payment orders**

Boolean attribute specifying whether a rule-based liquidity transfer should be triggered from the Associated LT Account when an urgent payment order, AS transfer order or high priority payment order is queued.

- **Linked Account**

Indicates another Cash Account (defined in the same currency) referenced for different purposes depending on the Cash Account Type.

-For RTGS Sub-Account it should reference an RTGS DCA or an RTGS CB Account [CR-65] (for AS settlement).

-For Overnight Deposit Account and Marginal Lending Account it should reference a Main Cash Account (to allow the CLM Account Holder of the MCA to reverse money from the Overnight Deposit account and view the balances on both types of accounts).

Transactional data:

- **Cash Balance**
Current cash balance
- **Credit Line**
Current maximum collateralised overdraft position of the Cash Balance (CLM MCA)

Note: A negative balance is only allowed for the CB Accounts, the Dedicated Transit Accounts and all T2S CB Accounts; for all other Cash Accounts the liquidity is restricted to the balance plus credit line if available

Id	SHRD.UR.BDD.100
Name	Payment / AS transfer (TRANSACTIONAL DATA)
Description	Within RTGS, High-Value payments and Ancillary System transfers are possible. For CLM, only payment orders linked to Central Bank Operations and Cash Withdrawals as well as payment orders that the Central Bank initiates in order to transfer liquidity from the reservation for seizure of funds are possible. <u>Mandatory attributes:</u> • Payment Identifier (KEY) (for internal use only) The unique technical identifier of the payment • Service Identifier Possible values are: – RTGS – CLM • Payment Category Mandatory for RTGS, not used for CLM. Possible values are: – High-Value Payment – Ancillary System transfer • Payment Type Possible values are: e.g. – Credit transfer – Direct debit – Connected payment – Warehoused payment – Back Value payment – Backup payment • Priority Possible values are: – Urgent – High – Normal • Transaction Reference (AS transaction) or UETR (one and only one of those two references should be present) Reference given by the original instructor of the payment / UETR • Internal Reference Reference assigned by RTGS or CLM for the payment • Transfer Amount Amount to be credited or debited with the payment order • Currency • Account To Be Debited • Account To Be Credited • Entry Timestamp • Settlement Timestamp Timestamp specifying the date and the time the payment was settled • Actual Amount Amount actually settled with the payment

- **Settlement Status**

Possible values are :

- Rejected
- Pending
- Settled

Optional attributes:

- **Credit Line Update Amount**

Used for connected payments

- **From Time**

Where From Time is specified, a payment order can only be submitted to settlement after this has been reached

- **Reject Time**

If Reject Time is specified, then Till Time cannot be specified.

Where Reject Time is specified, a payment order can only be submitted to settlement if this has not yet been reached. As soon as the Reject Time is reached and if the payment order has not been settled, the payment order will be rejected and a settlement failure notification will be sent out.

- **Till Time**

If Till Time is specified, then Reject Time cannot be specified.

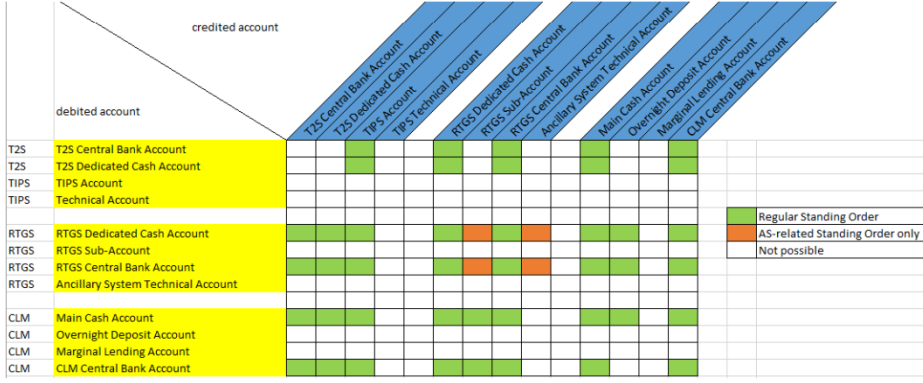
Where Till Time has been specified, if this time is reached and the payment order has not been settled, then the payment order shall not be rejected and it may still be submitted for settlement beyond this time. Till Time is only used to trigger a warning notification.

- **Origin UETR**

For a return payment, UETR of the initial transaction

Id	SHRD.UR.BDD.110
Name	Liquidity Transfer (TRANSACTIONAL DATA)
Description	An instruction to transfer Central Bank Money from a cash account to another cash account which can be in the same settlement service or in a different settlement service. <u>Mandatory attributes:</u> • Liquidity Transfer Identifier (KEY) (for internal use only) The unique technical identifier of the liquidity transfer • Service Identifier Possible values are: – RTGS – CLM – T2S – TIPS • Transfer Type Possible values are: – inter-service liquidity transfer from MCA to DCA – inter-service liquidity transfer from DCA to MCA – intra-service liquidity transfer – liquidity transfer between two DCAs in two different settlement services • Underlying Transfer Order Type Identifies the underlying liquidity transfer order type of the liquidity transfer Possible values are: – Immediate liquidity transfer order – Rule-based liquidity transfer order (RTGS and CLM only) – Standing order liquidity transfer order • Reference of Instruction Reference given by the original instructor of the liquidity transfer • Transfer Amount Amount to be credited or debited with the liquidity transfer order • Currency • Account To Be Debited • Account To Be Credited • Entry Timestamp • Settlement Timestamp Timestamp specifying the date and the time the settlement was attempted • Actual Amount Amount actually settled with the liquidity transfer order • Settlement Status Possible values are: – Rejected – Partially Settled – Settled <u>Optional attributes:</u> • Service-Related Reference Reference assigned by the individual sending settlement service

	• Partial Execution Flag identifying whether partial execution is possible or not
Id	SHRD.UR.BDD.115
Name	Liquidity Transfer Group
Description	This entity shall denote a group of Cash Accounts within one settlement service for which intra-service liquidity transfer orders are allowed. Cash Accounts within a Liquidity Transfer Group may be owned by different Parties (banks), and these banks may be associated with more than one Central Bank. Furthermore, a Cash Account may belong to more than one Liquidity Transfer Group. <u>Mandatory attributes:</u> • Liquidity Transfer Group Identifier (KEY) (for internal use only) The unique technical identifier of the Liquidity Transfer Group • Liquidity Transfer Group Name The name of the Liquidity Transfer Group <u>Optional attributes:</u> n/a

Id	SHRD.UR.BDD.120
Name	Standing Order Liquidity Transfer Order
Description	An instruction template to transfer Central Bank Money from a debited account to a credited account. The following debited/credited account combinations are supported:  Mandatory attributes: • Standing Order Identifier (KEY) (for internal use only) The unique technical identifier of the Standing Order • Reference of Instruction Reference given by the original instructor of the liquidity transfer • Transfer Amount Amount to be credited or debited with the liquidity transfer order • Currency • Account To Be Debited • Account To Be Credited • Trigger An event-based trigger that will initiate the Standing Order • Valid From Date Optional attributes: • Valid To Date • AS Procedure Standing Order link to an AS procedure initiation. Possible values: - Procedure C, automated start of mandatory procedure - Procedure C, manual start of optional procedure - Procedure D, automated start of mandatory procedure • Creditor BIC, only allowed if "Procedure D, automated start of mandatory procedure" is selected • ASTN creditor account, only allowed if "Procedure D, automated start of mandatory procedure" is selected

- **Debtor BIC**, only allowed if “Procedure D, automated start of mandatory procedure” is selected

- **ASTN debtor account**, only allowed if “Procedure D, automated start of mandatory procedure” is selected **{CSLD CR0116}**

Id	SHRD.UR.BDD.130
Name	Rule-based Liquidity Transfer Order
Description	An instruction to transfer Central Bank money from a debited account to a credited account whenever a particular event occurs, such as a floor or ceiling value being reached. The following debited/credited account combinations are supported:  Mandatory attributes: • Rule-based Liquidity Transfer Identifier (KEY) (for internal use only) The unique technical identifier of the rule-based liquidity transfer order • Trigger event The event that will trigger the transfer of liquidity • Reference of Instruction Reference given by the original instructor of the liquidity transfer • Transfer Parameters Parameters needed by the system to calculate the amount to be credited or debited with the liquidity transfer order • Currency • Account To Be Debited • Account To Be Credited Optional attributes: • Floor amount A lower threshold which may trigger the sending of a liquidity transfer order if it is breached from above (absolute numbers). If a floor notification has been configured for the account to be credited, they must have the same floor amount. • Ceiling amount An upper threshold which may trigger the sending of a liquidity transfer order if it is breached from below (absolute numbers). If a ceiling notification has been configured for the account to be debited, they must have the same ceiling amount. • Target Amount After Breaching Floor Target amount to be reached if the Floor is breached • Target Amount After Breaching Ceiling Target amount to be reached if the Ceiling is breached

Id	SHRD.UR.BDD.131
Name	Floor/ceiling notification configuration
Description	A notification triggered when a floor or ceiling has been breached on a given account. <u>Mandatory attributes:</u> • Account Number <u>Optional attributes:</u> • Floor amount A lower threshold which may trigger the sending of a notification message if it is breached from above (absolute numbers). If Floor Rule-based Liquidity Transfer Order has been configured to credit the account, they must have the same floor amount. • Ceiling amount An upper threshold which may trigger the sending of a notification message if it is breached from below (absolute numbers). If a Ceiling Rule-based Liquidity Transfer Order has been configured to debit the account, they must have the same ceiling amount. Either the Floor or the Ceiling attributes must be present, but not both.

Id	SHRD.UR.BDD.140
Name	Direct Debit Mandate
Description	Details of an instruction mandate to allow a Party (the payee) to submit payment orders for payment by direct debit from an account of another Party (the payer). The payer Party is the owner of the specified Cash Account to be debited. <u>Mandatory attributes:</u> • Direct Debit Identifier (KEY) (for internal use only) The unique technical identifier of the Direct Debit Mandate • From Cash Account Account Number of the Cash Account to be debited • Payee Party Identifier The Party from whom payment orders have been authorised under this mandate and to whom the corresponding payments will be made • Payee Reference The reference provided by the payee Party to be included in the payment order details for recognition of the payment • Valid From Date The date from which the direct debit instruction is valid <u>Optional attributes:</u> • Maximum Amount per counterparty Maximum Amount allowed to be debited by the payee Party during a business day • Maximum Amount of a direct debit order per counterparty Maximum Amount of a direct debit order allowed to be debited by the payee Party • Valid To Date <u>Transactional data:</u> • Used Amount Amount used during the current day, increased after each booking of a direct debit. This should be lower than the Maximum Amount, if defined.

Id	SHRD.UR.BDD.150
Name	Reservation (TRANSACTIONAL DATA)
Description	Within the RTGS reservation facility, liquidity can be reserved by RTGS DCA holders for the execution of special transactions with a certain priority class. Within the CLM reservation facility, liquidity can be reserved by CLM MCA holders for the execution of Central Bank Operations and Cash Withdrawals. <u>Mandatory attributes:</u> • Reservation Identifier (KEY) (for internal use only) The unique technical identifier of the Reservation • Service Identifier Possible values are: – RTGS – CLM • Priority Type Type of the Priority: – Urgent (U) – High (H) • Reservation Type Origin of the Reservation e.g.: – Regular Reservation from Standing Order – One-Time Reservation • Reservation Amount Reservation required for the Cash Account, as requested in the Reservation Order or the Standing Order for Reservation. This does not change after this Reservation has been created. • Pending Value The current amount remaining in order to meet the Reservation Amount for the Reservation. This is adjusted dynamically during the day as available liquidity is reserved for the Cash Account. • Defined Value The amount reserved currently from the available liquidity for this Reservation. This is adjusted dynamically during the day as available liquidity is reserved for the Cash Account. • Cash Account Account Number of the Cash Account for which the Reservation is made • Internal Reference Reference assigned by RTGS or CLM for the Reservation • Entry Timestamp • Settlement Timestamp Timestamp specifying the date and the time the settlement was attempted • Settlement Status Possible values are: – Not executed – Partially settled – Settled

Id	SHRD.UR.BDD.160
Name	Standing Order for Reservation
Description	A repeatable order to create a Reservation which is initiated automatically at Start of Day. Within the RTGS reservation facility, liquidity can be reserved by RTGS DCA holders for the execution of special transactions with a certain priority class. Within the CLM reservation facility, liquidity can be reserved by CLM MCA holders for the execution of Central Bank Operations and Cash Withdrawals. <u>Mandatory attributes:</u> • Standing Order for Reservation Identifier (KEY) (for internal use only) The unique technical identifier of the Standing Order for Reservation • Service Identifier Possible values are: – RTGS – CLM • Priority Type Type of the Priority: – Urgent (U) – High (H) • Reservation Amount The amount of the required Reservation to be created for the Cash Account at Start of Day • Cash Account Account Number of the Cash Account for which the Reservations will be made • Valid From Date <u>Optional attributes:</u> • Valid To Date

Id	SHRD.UR.BDD.180
Name	Report Subscription
Description	This entity shall denote the subscription to a report for a Cash Account. The settlement service to which the report relates shall be identified via the Cash Account. <u>Mandatory attributes:</u> • Report Subscription Identifier (KEY) The unique technical identifier of a Report Subscription • Report The report subscribed for the Cash Account • Cash Account Account Number of the Cash Account for which the report has been subscribed • Recipient The Party Identifier of the participant subscribing to the report for the Cash Account • Parameters for Report Specifies whether the relevant report will be received in full or delta mode, and whether in push or pull mode • Subscription Valid From The date from which the subscription is valid <u>Optional attributes:</u> • Scheduled Time The scheduled time when the report is provided. Either Scheduled Time or Scheduled Event must be specified, but not both. • Scheduled Event The event that shall trigger the report to be produced. Either Scheduled Time or Scheduled Event must be specified, but not both. • Subscription Valid To The date until which the subscription is valid

Id	SHRD.UR.BDD.190
Name	Message Subscription
Description	This entity shall denote the subscription to a message for a Cash Account. The settlement service to which the message relates shall be identified via the Cash Account. <u>Mandatory attributes:</u> • Message Subscription Identifier (KEY) The unique technical identifier of a Message Subscription • Message Id The identifier of the message subscribed to by the participant • Cash Account Account Number of the Cash Account for which the message has been subscribed • Recipient The Party Identifier of the participant subscribing to the message for the Cash Account • Subscription Valid From The date from which the subscription is valid <u>Optional attributes:</u> • Business Case Business case for which a message has to be sent • Priority Priority of the underlying payment order • Message type Message type of the underlying payment order • Multi-addressee BIC BIC of the multi-addressee credit institution that sent the underlying payment order • Subscription Valid To The date until which the subscription is valid

Id	SHRD.UR.BDD.200
Name	Scheduled Event
Description	This entity shall denote a scheduled event that will automatically trigger a specified process within a Eurosystem Market Infrastructure Service. <u>Mandatory attributes:</u> • Scheduled Event Identifier The unique technical identifier of a Scheduled Event • Process Identifier The unique technical identifier of a business process • Service Identifier Possible values are: – RTGS – CLM – TIPS – T2S • Scheduled Event Status Indicates whether the Scheduled Event has occurred and the business process has been initiated • Event Triggered Timestamp The system date and time at which the Scheduled Event occurred and the business process was triggered • Repeat Flag Indicates whether another instance of the Scheduled Event should be created when this instance has occurred <u>Optional attributes:</u> • Trigger Date Either the Trigger Date and Trigger Time or the Trigger Event Identifier must be populated • Trigger Time • Trigger Event Identifier The unique technical identifier of another Scheduled Event that shall trigger this Scheduled Event when it occurs

Id	SHRD.UR.BDD.210
Name	Currency
Description	This entity shall denote any valid currency and information whether the currency is settled in the Eurosystem Market Infrastructure Services. <u>Mandatory attributes:</u> • Currency Code (KEY) The three-character ISO currency shall identify the currency • Currency Name • Number of Decimals • RTGS Settlement Currency Specification of the currency is an RTGS settlement currency (y/n) • T2S Settlement Currency Specification of the currency is a T2S settlement currency (y/n) • TIPS Settlement Currency Specification of the currency is a TIPS settlement currency (y/n) • CLM Settlement Currency Specification of the currency is a CLM settlement currency (y/n) • CONT Settlement Currency Specification of the currency is a CONT settlement currency (y/n) <u>Optional attributes:</u> n/a

Id	SHRD.UR.BDD.220
Name	SWIFT BIC Directory
Description	SWIFT, as the global authority for registering BIC codes, provides the BIC directory. The directory, as provided by SWIFT, shall be part of CRDM. The directory shall be updated on a regular basis. The attributes shall be derived from the structure of the SWIFT BIC directory

Id	SHRD.UR.BDD.230
Name	Service
Description	This entity shall denote any Eurosystem Market Infrastructure Service, application or component which is accessible via ESMIG. <u>Mandatory attributes:</u> • Service Identifier (KEY) The unique technical identifier of a service or a component • Service Short Name e.g. RTGS, CLM, CRDM, T2S, TIPS, CONT, DWH, BILL and LEA. • Service Long Name • Service Availability Timeframe when service is available – Start Time: Start time of service – End Time: End time of service <u>Optional attributes:</u> • Cut-off (Multiple occurrences allowed) Definition of cut-off of the service

Id	SHRD.UR.BDD.240
Name	User
Description	A user is an individual or application that interacts with one or more of the available Eurosystem Market Infrastructure Services. This entity shall denote any information required by ESMIG to direct inbound and outbound communications. <u>Mandatory attributes:</u> • User Id (KEY) The unique technical identifier of a User • ID of Sender The ID shall result out of authentication process • External Party Address Information required that the correct Network Service Provider, target address, communication mode and protocol (i.e. right external user address) are used • Accessible Service (Multiple occurrences allowed) Enumeration of Eurosystem Market Infrastructure Services the user is allowed to access • Role Identifier (Multiple occurrences allowed) One or more roles assigned to the user <u>Optional attributes:</u> n/a

Id	SHRD.UR.BDD.250
Name	Distinguished Name
Description	This entity shall denote the Distinguished Name assigned (via a digital certificate) to one or many User(s) to allow access to a service, application or component. <u>Mandatory attributes:</u> • Distinguished Name (KEY) • User Id The unique technical identifier of a User • Service Identifier Unique identifier of a Eurosystem Market Infrastructure Service, application or component the user is allowed to access • Certificate Information Information related to the digital certificate <u>Optional attributes:</u> n/a

Id	SHRD.UR.BDD.260
Name	Role
Description	A role is a set of defined privileges that allows or denies the user access to specific functionality within the service, application or component or to view specific data. A role consists of one or more privileges. <u>Mandatory attributes:</u> • Role Identifier (KEY) The unique technical identifier of a Role • Role Name • Service Identifier The unique technical identifier of the service, application or component with which the Role is associated <u>Optional attributes:</u> n/a

Id	SHRD.UR.BDD.270
Name	Privilege
Description	A Privilege defines a specific functional capability within a process or application in any of the Eurosystem Market Infrastructure Services. For example, within Common Reference Data, possible privileges are: create new Cash Account, delete Party Address, or amend a Limit. The definition of Privileges is the means of granting access to functionality for specific Roles. <u>Mandatory attributes:</u> • Privilege Identifier (KEY) The unique technical identifier of a Privilege • Role Identifier the Role with which the Privilege is associated • Privilege Description • Function Identifier Identifier of the functionality to which the privilege applies (e.g. Amend Party Address) • Authorisation Principle Two-eyes or Four-eyes Principle • Access Mode U2A or A2A • Allowed/Denied Indicator (For Common Components, CLM and RTGS this will always be 'Allowed') <u>Optional attributes:</u> n/a

Id	SHRD.UR.BDD.280
Name	Access Rights
Description	Access Rights define the ability for a User to view and maintain any information relating to a Party, subject to the functionality granted to the User through the associated Roles and Privileges. The definition of Access Rights is the means of granting access to data for specific roles. <u>Mandatory attributes:</u> • Access Rights Identifier (KEY) The unique technical identifier of an Access Rights • User Id the User with which the Access Rights is associated • Party Id the Party with which the Access Rights is associated • Access Rights Description The nature of the Access Rights to the data of the Party that have been granted to the User. In particular, this will identify the primary Party with which the User is associated • Allowed/Denied Indicator (For Common Components, CLM and RTGS this will always be 'Allowed') <u>Optional attributes:</u> n/a

List of Business Process Models

Business Process Model 1: Create an occurrence of Common Reference Data.....	21
Business Process Model 2: Amend an occurrence of Common Reference Data.....	28
Business Process Model 3: Delete an occurrence of Common Reference Data.....	35
Business Process Model 4: Block an occurrence of Common Reference Data.....	43
Business Process Model 5: Unblock an occurrence of Common Reference Data	49
Business Process Model 6: Close a Cash Account.....	53
Business Process Model 7: Scheduler Process.....	64
Business Process Model 8: End of Day/Start of Day Process.....	68
Business Process Model 9: Four-Eyes Approval.....	86
Business Process Model 10: Query	92
Business Process Model 11: Produce Scheduled Report and Send (A2A) / Store for Download (U2A)	97
Business Process Model 12: Data Warehouse Information Collection.....	104
Business Process Model 13: Data Warehouse Gather Information.....	106

List of Figures

Figure 1: Context diagram for Eurosystem Single Market Infrastructure Gateway	6
Figure 2: Context Diagram for Common Reference Data Management.....	17
Figure 3: Context diagram for Business Day	63
Figure 4: Business day schedule (Tuesdays, Wednesdays, Thursdays, Fridays except T2 closing days)	75
Figure 5: Context diagram for Information and Reporting	90
Figure 6: Context diagram for Data Warehouse	102
Figure 7: Entity Relationship Diagram for Party.....	127
Figure 8: Entity Relationship Diagram for Cash Account	131
Figure 9: Entity Relationship Diagram for User.....	132

List of Tables

Table 1: Business Processes for Common Reference Data Management.....	18
Table 2: Business Processes for Business Day.....	63
Table 3: Business Processes for User Roles and Access	81
Table 4: Business Processes for Information and Reporting.....	91
Table 5: Business Processes for Data Warehouse	103

Table 6: Summary of queries and actions in U2A and A2A mode for Common Reference Data Management.....	124
---	-----