Common Reference Data Management for TIPS

User Detailed Functional Specifications

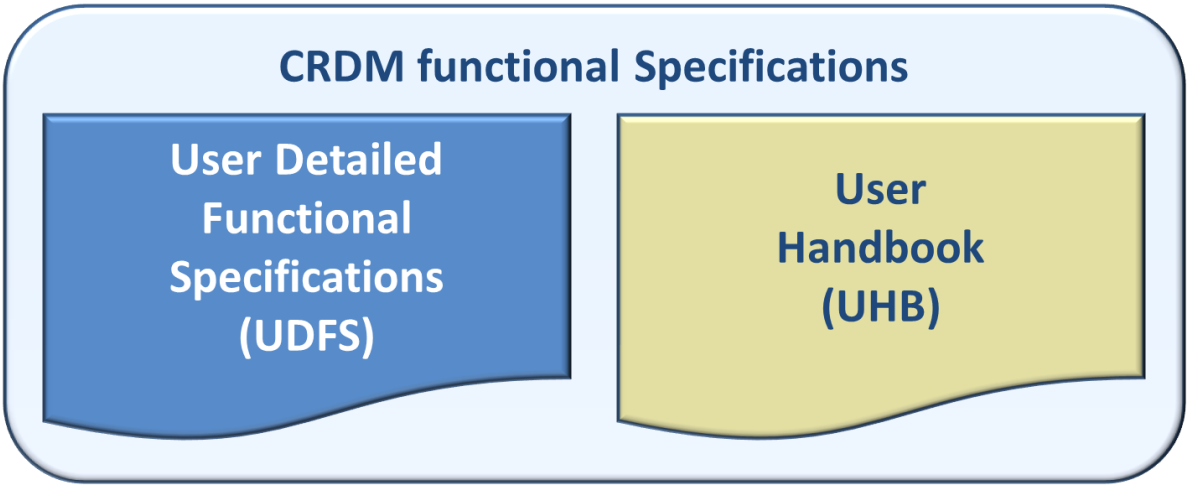
~~V1~~V2.~~1~~0.0

Author	4CB
Version	2.0.0~~1.1.0~~
Date	~~31/~~14/06/~~08/2018~~2019

Introduction

The User Detailed Functional Specifications (UDFS) of the Common Reference Data Management (CRDM) common component are part of the documentation of the T2-T2S Consolidation project. The diagram below presents an overview of all the documents foreseen to allow CRDM Actors to understand how requirements described in the T2-T2S Consolidation User Requirements Document (URD) for the Common Reference Data Management common component are implemented.

DIAGRAM 1 - OVERVIEW OF CRDM SPECIFICATIONS

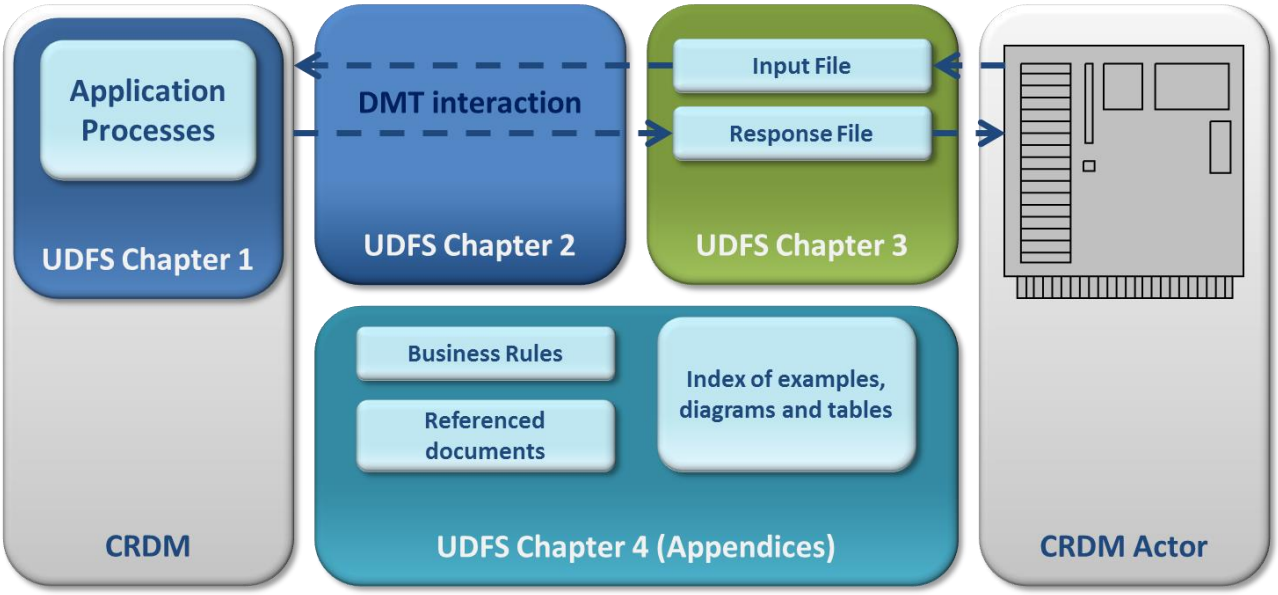


The UDFS focus on the provision of information to CRDM Actors to design and build the interface of their business applications with the Common Reference Data Management common component, while the UHB describes the Graphical User Interface (GUI) screens in detail.

The UDFS are designed to provide information to Business analysts of the CRDM Actors, who will find in the UDFS a description of the application processes and the information flows between their own business applications and the Common Reference Data Management common component.

The UDFS are a self-contained document, structured along 4 different but complementary Chapters.

DIAGRAM 2 - SCOPE OF UDFS CHAPTERS



Chapter 1: General features of the Common Reference Data Management common component

UDFS chapter 1 provides concise and descriptive information on the Common Reference Data Management common component behaviour as it is seen from a CRDM Actor point of view. The background information provided in Chapter 1 on the Common Reference Data Management common component internal behaviour facilitates the understanding of Chapters 2 and 3 (in particular to understand the information flows described in Chapter 2).

Information provided in Chapter 1 on the Common Reference Data Management common component application processes is user-oriented and does not include detailed descriptions of the internal Common Reference Data Management processes. Furthermore, it does not provide descriptions of the internal behaviour of CRDM Actors interacting with the Common Reference Data Management common component: it is not the purpose of the UDFS to predicate the business conduct of future CRDM users.

The following table presents the scope and user objective for each section of UDFS Chapter 1:

***TABLE 1* - STRUCTURE OF UDFS CHAPTER 1**

SECTION	SCOPE	USER OBJECTIVE
1.1 Introduction to CRDM	Overall presentation of the CRDM business functionalities	To understand the general behaviour of CRDM.
1.2 Access to CRDM	CRDM Interface	To understand the main principles for the exchange of information between CRDM and CRDM Actors.
1.3 Reference data model	Common reference data structure	To understand how reference data structures can be organised in CRDM.
1.4 CRDM features	Common reference data maintenance	To understand how reference data can be managed in CRDM.

SECTION	SCOPE	USER OBJECTIVE
1.5 Interactions with other services	Interactions between CRDM and other Eurosystem services	To understand the links in place between CRDM and other existing and planned Eurosystem market infrastructure services.
1.6 Operations and support	Operational aspects and actions to be performed by the CRDM Operator	To understand the features supporting operational activities and the actions the CRDM Operator can perform for CRDM configuration and CRDM operation monitoring.
1.7 Limitations of the system	Features and processes that are not covered by CRDM	To understand the exact perimeter of CRDM and what processes should not be expected from CRDM.

Chapter 2: Dialogue between the Common Reference Data Management common component and CRDM Actors

Chapter 2 of the UDFS provides a formalised description of the dialogue between CRDM users and the Data Migration Tool (DMT), which allows CRDM Actors to interact with the Common Reference Data Management common component. The objective of this Chapter is to describe the behaviour of the Common Reference Data Management DMT regarding the interactions with CRDM Actors, i.e. when sending/receiving files to/from the latter. Consistently with the approach of Chapter 1, UDFS Chapter 2 does not enter into any description of the behaviour of Actors' systems interacting with the Common Reference Data Management common component.

Chapter 2 describes the dialogue between the Common Reference Data Management DMT and a CRDM Actor in the form of a "Universal Use Case".

Chapter 3: Data Migration Tool

Chapter 3 of the UDFS provides a detailed description of the file specifications to be used to communicate with the Data Migration Tool. It describes the entire set of reference data objects which are processed by the DMT, in the form of structured files which can be exchanged between the Common Reference Data Management common component and the CRDM Actors. The initial subsections describe general structure, format and processing rules valid for all objects, while the following subsections describe, for each object, the structure of the relevant file with mandatory/optional fields, rules and purpose of each field in the context of the DMT.

The objective of the Chapter is to allow the reader to find all the necessary information related to DMT communications which are needed to establish a functioning communication between the Common Reference Data Management common component and its users.

Chapter 4: Appendices

The UDFS appendices provide:

- Information on the CRDM business rules applying to incoming DMT files, with the respective messages and error codes associated;
- Indexes:
  - Index of diagrams;
  - Index of tables;
  - List of acronyms;
  - List of referenced documents.

Reader's guide

The UDFS document is available for the whole community of CRDM Actors: in order to ensure the same level of information for all CRDM Actors, information relevant for CBs and directly connected Payment Banks is contained in one single book of UDFS.

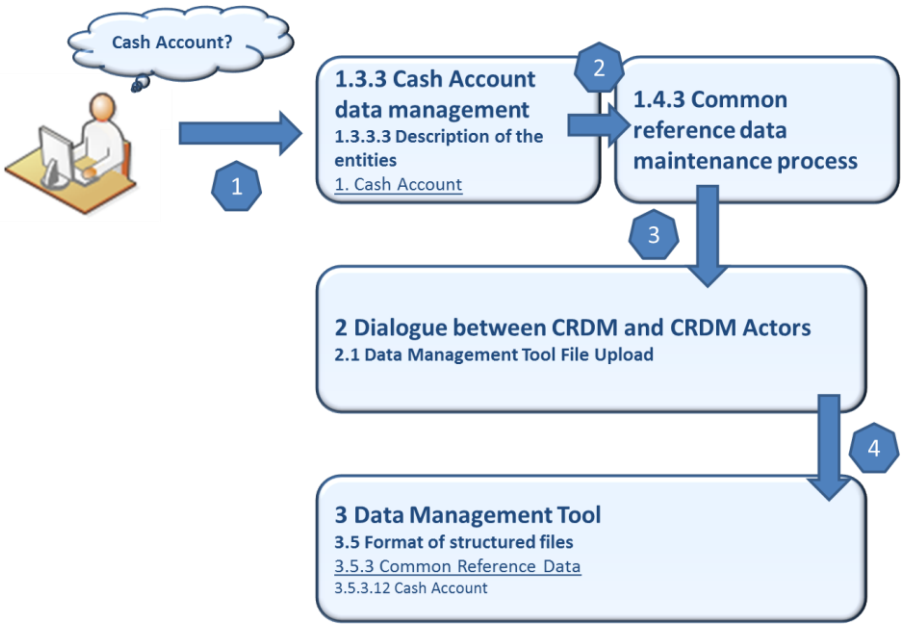
Nevertheless, different readers may have different needs and priorities. For instance, "business" readers interested mainly in organisational issues may not wish to enter into the full details of the DMT file descriptions, while technical readers may not be interested in the thorough description of the Common Reference Data Management application processes that are leading to the sending of a given file. Not every reader wants to read the entire UDFS, or even want to follow the same reading plan.

However, all readers, whether "business" or "technical", may find it useful to read the following UDFS sections, which are providing a background to the understanding of any other UDFS section:

- 1.1 "Introduction to CRDM", which is a summary providing the basis for the understanding of the main Common Reference Data Management concepts.
- 1.3 "Reference data model", which provides the basis for data organisation in CRDM.

Business and technical readers may be interested in the way information is structured in the Common Reference Data Management common component. This user may want to follow the reading plan described below to find information about cash accounts and the relevant maintenance operations that can be performed on a cash account in CRDM:

EXAMPLE 1 - "CRDM DATA AND RELATED PROCESSING" READING PLAN



- 1 The business reader finds in section 1.3.3 "Cash Account data management" a general description of Cash Accounts specifying the different attributes that make up this object in CRDM.
- If the reader requires more information on the Reference data management process, they can refer to section 1.4.3 "Common reference data maintenance process" 2 which offers a general description applicable to all reference data objects.
- From this point, he may jump to Chapter 2.1 "Data Migration Tool File Upload" 3 to find a description of the maintenance process which can be carried out via DMT. This process is the same for all reference data objects that are available via DMT.
- If the reader need to enter into further details on how to update a cash account via DMT, he may access through a hyperlink section 3.5.3.12 "Cash Account" 4 to find the detailed description of the file used to update a cash account in CRDM.

1. General features of CRDM

The present chapter, after a short introduction of the Common Reference Data Management common component, describes all the features it provides. Section 1.2 introduces the details regarding the access of CRDM Actors to CRDM, covering the different modes of connectivity, the authentication and the authorisation processes, as well as, security aspects and an introduction to the Graphical User Interface (GUI). Section 1.3 describe the reference data model of the CRDM, including a description of all the relevant entities and relationships. Section 1.4 describes the various features of CRDM, such as the structure of reference data objects, the different types of available maintenance operations, the management of objects with limited and unlimited valid period, the archiving and purging processes and the life-cycle management of reference data objects. Finally, section 1.5 describes the interactions that CRDM, as a common component, has with other services and common components provided by the Eurosystem, whereas section 1.6 describes supporting the CRDM Operator in the management of the component.

1.1. Introduction to CRDM

CRDM provides a common reference data management feature that allows all CRDM Actors to create and maintain common reference data for the configuration of data related to parties, cash accounts, rules and parameters. The following list shows the main configuration areas for common reference data in CRDM:

- Party reference data;
- Cash account reference data;
- Access rights management;
- Message subscription configuration;
- Network configuration;
- Report configuration;
- Restriction type management;
- Configuration parameters.[1]

CRDM Actors set up the appropriate configuration by creating and maintaining common reference data objects in CRDM. A common reference data object is a set of logically related, self-consistent information (see section 1.4.3.1). Parties and cash accounts are examples of common reference data objects.

CRDM allows CRDM Actors to create, update and delete common reference data objects in CRDM. Deletion of a common reference data object is always logical and it is possible, for a duly authorised user, to restore a previously deleted common reference data object (see section 1.4.3.2).

CRDM provides versioning facilities and validity periods allowing the implementation of data revision and data history features, in order to keep track of all past data changes, to enter changes meant to become effective as of a future date and to define common reference data objects with limited or unlimited validity.

1 This area includes reference data for countries, currencies, currency service links, system entities, services, TIPS directory.

All types of CRDM Actors, i.e. CBs, payment banks and the CRDM Operator have access to the common data management, each of them to different functions and data, according to the access rights granted to their users (see section 1.2.2).

Duly authorised users can create and maintain common reference data objects in CRDM submitting common reference data maintenance instructions.

1.2. Access to CRDM

1.2.1. Connectivity

CRDM supports the connectivity of CRDM Actors as follows:

- Communication via files (DMT mode);
- Online screen-based activities performed by CRDM Actors (U2A mode).

The Data Migration Tool (DMT) functionality is described extensively in chapters 2 and 3.

U2A connectivity to CRDM will be handled through the ESMIG Portal. Please refer to the ESMIG documentation for more details.

1.2.2. Access rights

This section provides information on access rights management in the CRDM. More into detail, section 1.2.2.1 presents some basic concepts (e.g. user, privilege, role and data scope) related to access rights management. On this basis, section 1.2.2.2 illustrates all the available options for the configuration of access rights. Finally, section 1.2.2.3 describes the access rights configuration process that each type of CRDM Actor has to put in place in order to set up the appropriate assignment of roles and privileges for all its users.

1.2.2.1. Access rights concepts

This section presents the main concepts related to access rights management in the CRDM.

1.2.2.1.1. User function

DMT files and GUI functions are the atomic elements users can trigger through the DMT and in U2A mode respectively to interact with CRDM and TIPS. Based on these set of files and GUI functions, it is possible to define the set of all user functions, i.e. of all the possible actions that a user can trigger in CRDM or TIPS, either in the DMT or in U2A mode.

1.2.2.1.2. Privilege

A privilege identifies the capability of triggering one or several user functions and it is the basic element to assign access rights to users. This means that a user U_X owns the access right to trigger a given user function F_Y if and only if U_X was previously granted with the privilege P_Y identifying the capability to trigger F_Y.

The following tables provide the exhaustive list of privileges covering all the user functions of CRDM and TIPS available in the DMT:

Table 109 – Other

TABLE 2 – ACCESS RIGHTS MANAGEMENT

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
Administer Party[2]	n/a	n/a	n/a
Create Certificate Distinguish Name	Certificate DN – New	Any Certificate DN	Yes
Create DN-BIC Routing	DN-BIC Routing - New	DN-BIC Routing data within own System entity (for CBs) or for DNs linked to own Users and BICs authorised to own Cash Accounts (for Payment Banks).	Yes
Create Role	Role – New	Roles within own System Entity (for CBs).	Yes
Create User	User – New	Users within own System Entity (for CBs) or own Party (for Payment Banks).	Yes
Create User Certificate Distinguish Name Link	User Certificate DN Link – New	Links within own System Entity (for CBs) or for own Users (for Payment Banks).	Yes
Delete Certificate Distinguish Name	Certificate DN – Delete	Any Certificate DN	No
Delete DN-BIC Routing	DN-BIC Routing - Delete	DN-BIC Routing data within own System entity (for CBs) or for DNs linked to own Users and BICs authorised to own Cash Accounts (for Payment Banks).	No
Delete Role	Role – Delete	Roles within own System Entity (for CBs).	No
Delete User	User – Delete	Users within own System Entity (for CBs) or own Party (for Payment Banks).	No
Delete User Certificate Distinguish Name Link	User Certificate DN Link – Delete	Links within own System Entity (for CBs) or for own Users (for Payment Banks).	No
Grant Privilege	Grant Privilege	Privileges granted to Parties, Roles and Users within own System Entity (for CBs) or to own Users (for Payment Banks)	Yes
Grant/Revoke Role	Grant/Revoke Role	Roles granted to Parties and Users within own System Entity (for CBs) or to own Users (for Payment Banks)	Yes (Grant only)

[2] This privilege enables a User to act as Party Administrator for their own Party.

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
Revoke Privilege	Revoke Privilege	Privileges granted to Parties, Roles and Users within own System Entity (for CBs) or to own Users (for Payment Banks)	No
Update DN-BIC Routing	DN-BIC Routing - Edit	DN-BIC Routing data within own System entity (for CBs) or for DNs linked to own Users and BICs authorised to own Cash Accounts (for Payment Banks).	No
Update Role	Role – Edit	Roles within own System Entity (for CBs)	No
Update User	User – Edit	Users within own System Entity (for CBs) or own Party (for Payment Banks).	No

TABLE 3 – PARTY DATA MANAGEMENT

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
Create Party	Party – New	Parties within own System Entity (for CB)	Yes
Create Party-Service Link	Party-Service Link - New	Links within own System Entity (for CBs)	Yes
Create Technical Address Network Service Link	Technical Address Network Service Link - New	Links within own System Entity (for CBs)	Yes
Delete Party	Party - Delete	Parties within own System Entity (for CB) excluding own Party	No
Delete Party-Service Link	Party-Service Link - Delete	Links within own System Entity (for CBs)	No
Delete Technical Address Network Service Link	Technical Address Network Service Link - Delete	Links within own System Entity (for CBs)	No
Update Party	Party – Edit	Parties within own System Entity (for CB)	No
Update Party-Service Link	Party-Service Link - Edit	Links within own System Entity (for CBs)	No

TABLE 4 – CASH ACCOUNT DATA MANAGEMENT

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
Create Authorised Account User	Authorised Account User - New	Links within own System Entity (for CBs) or for own Cash Accounts (for Payment Banks).	Yes
Create Limit	Limit – New	Limits on CMBs defined on Cash Accounts within own System Entity (for CB) or linked to	Yes

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
		Cash Accounts owned by own Party (for Payment Bank)	
Create Cash Account	Cash Account – New	Cash Accounts within own System Entity (for CB) or CMBs linked to Cash Accounts owned by own Party (for Payment Bank)	Yes
Delete Authorised Account User	Authorised Account User - Delete	Links within own System Entity (for CBs) or for own Cash Accounts (for Payment Banks).	No
Delete Limit	Limit – Delete	Limits on CMBs defined on Cash Accounts within own System Entity (for CB) or linked to Cash Accounts owned by own Party (for Payment Bank)	No
Delete Cash Account	Cash Account – Delete	Cash Accounts within own System Entity (for CB) or CMBs linked to Cash Accounts owned by own Party (for Payment Bank)	No
Update Authorised Account User	Authorised Account User - Edit	Links within own System Entity (for CBs) or for own Cash Accounts (for Payment Banks).	No
Update Limit	Limit – Edit	Limits on CMBs defined on Cash Accounts within own System Entity (for CB) or linked to Cash Accounts owned by own Party (for Payment Bank)	No
Update Cash Account	Cash Account – Edit	Cash Accounts within own System Entity (for CB) or CMBs linked to Cash Accounts owned by own Party (for Payment Bank)	No

TABLE 5 – MESSAGE SUBSCRIPTION CONFIGURATION

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
Create Message Subscription Rule	Message Subscription Rule – New	Message Subscription Rules within own System Entity (for CBs) or for own Party (for Payment Banks)	Yes
Create Message Subscription Rule Set	Message Subscription Rule Set – New	Message Subscription Rule Sets within own System Entity (for CBs) or for own Party (for Payment Banks)	Yes
Delete Message Subscription Rule	Message Subscription Rule – Delete	Message Subscription Rules within own System Entity (for CBs) or for own Party (for	No

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
		Payment Banks)	
Delete Message Subscription Rule Set	Message Subscription Rule Set – Delete	Message Subscription Rule Sets within own System Entity (for CBs) or for own Party (for Payment Banks)	No
Update Message Subscription Rule	Message Subscription Rule – Edit	Message Subscription Rules within own System Entity (for CBs) or for own Party (for Payment Banks)	No
Update Message Subscription Rule Set	Message Subscription Rule Set – Edit	Message Subscription Rule Sets within own System Entity (for CBs) or for own Party (for Payment Banks)	No

TABLE 6 – REPORT CONFIGURATION

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
Create Report Configuration	Report Configuration – New	Report Configurations within own System Entity (for CBs) or for own Party (for Payment Banks)	Yes
Delete Report Configuration	Report Configuration – Delete	Report Configurations within own System Entity (for CBs) or for own Party (for Payment Banks)	No
Update Report Configuration	Report Configuration – Edit	Report Configurations within own System Entity (for CBs) or for own Party (for Payment Banks)	No

TABLE 7 – ROUTING CONFIGURATION

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
Create Routing	Routing – New	Routing configurations within own System Entity (for CBs) or linked to own Party Technical Addresses (for Payment Banks)	No
Delete Routing	Routing – Delete	Routing configurations within own System Entity (for CBs) or linked to own Party Technical Addresses (for Payment Banks)	No
Update Routing	Routing – Edit	Routing configurations within own System Entity (for CBs) or linked to own Party Technical Addresses (for Payment Banks)	No

TABLE 8 – REFERENCE DATA QUERIES

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
Authorised Account User Query	Authorised Account User - List	Links within own System Entity (for CBs) or for own Cash Accounts (for Payment Banks).	No
Certificate Query	Certificate Query	Any Certificate DN	No
Country Query	Countries – Select + List	Any Country	No
Currency Query	Currencies – Select + List	Any Currency	No
Data Changes of a Business Object Details Query	Data Changes of a Business Object Details Query	Data within own System Entity (for CBs) or linked to own Party (for Payment Banks)	No
Data Changes of a Business Object List Query	n/a	Data within own System Entity (for CBs) or linked to own Party (for Payment Banks)	No
DN-BIC Routing Query	DN-BIC Routing Query	Links within own System Entity (for CBs) or linked to own Party (for Payment Banks)	No
Granted Roles List Query	Granted Roles – Search	Roles granted to Parties and Users within own System Entity (for CBs) or to own Users (for Payment Banks)	No
Granted Roles List Query	Grant/Revoke Role – Details	Roles granted to Parties and Users within own System Entity (for CBs) or to own Users (for Payment Banks)	No
Granted System Privileges List Query	Grant/Revoke System Privileges List Query	Privileges granted to Parties, Roles and Users within own System Entity (for CBs) or to own Users (for Payment Banks)	No
Limit Query	Limit Query	Limits on CMB defined on Cash Accounts within own System Entity (for CB) or owned by own Party (for Payment Bank)	No
Market-specific Restriction List Query	Market-specific Restriction List Query	Restrictions defined by the Operator	No
Market-specific Restriction Type Rule Detail Query	Market-specific Restriction Type Rule –Detail Query	Restrictions defined by the Operator	No
Market-specific Restriction Type Rule Parameter Details Query	Market-specific Restriction Type Rule Parameter Details Query	Restrictions defined by the Operator	No
Market-specific Restriction	Market-specific Restriction	Restrictions defined by the Operator	No

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
Type Rule Set List Query	Type Rule Set List Query		
Message Subscription Rule List Query	Message Subscription Rule List Query	Message Subscriptions within own System Entity (for CBs) or for own Party (for Payment Banks)	No
Message Subscription Rule Set Details Query	Message Subscription Rule Sets Details Query	Message Subscriptions within own System Entity (for CBs) or for own Party (for Payment Banks)	No
Message Subscription Rule Set List Query	Message Subscription Rule Set List Query	Message Subscriptions within own System Entity (for CBs) or for own Party (for Payment Banks)	No
Network Service List query	Network Service List Query	Any Network Service	No
Party Audit Trail Query	Static Data Audit Trail Query	Data within own System Entity (for CB) or linked to own Party (for Payment Bank)	No
Party List Query	Party List Query	Parties within own System Entity (for CB) or own Party (for Payment Bank)	No
Party Reference Data Query	Party Reference Data Query	Parties within own System Entity (for CB) or own Party (for Payment Bank)	No
Party-Service Link List Query	Party-Service Link List Query	Links within own System Entity (for CBs) or linked to own Party (for Payment Banks)	No
Privilege Query	Privilege – Selection Criteria + List	Any Privilege	No
Queued Data Changes Query	Queued Data Changes - Select+List	Data within own System Entity (for CBs) or linked to own Party (for Payment Banks)	No
Report Configuration Details Query	Report Configuration Details Query	Report Configurations within own System Entity (for CBs) or for own Party (for Payment Banks)	No
Report Configuration List Query	Report Configuration List Query	Report Configurations within own System Entity (for CBs) or for own Party (for Payment Banks)	No
Residual Static Data Audit Trail Query	Static Data Audit Trail Query	Data within own System Entity (for CBs) or linked to own Party (for Payment Banks)	No
Role List Query	Role List Query	Roles created or granted to Parties and Users within own System Entity (for CBs) or to own	No

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
		Users (for Payment Banks)	
Routing List Query	Routing List Query	Routing configurations within own System Entity (for CBs) or linked to own Party Technical Addresses (for Payment Banks)	No
System Entity Query	System Entities – Select + List	Own System Entity (for CBs)	No
TIPS Directory Query	TIPS Directory Query	Any BIC reachable in TIPS	No
Cash Account Audit Trail Query	Revisions - Selection Criteria + List	Data within own System Entity (for CB) or linked to own Party (for Payment Bank)	No
Cash Account List Query	Cash Account List Query	Cash Accounts within own System Entity (for CB) or owned by own Party (for Payment Bank)	No
Cash Account Reference Data Query	Cash Account Reference Data Query	Cash Accounts within own System Entity (for CB) or owned by own Party (for Payment Bank)	No
System User Link Query	System User Link Query	Links within own System Entity (for CBs) or linked to own Users (for Payment Banks)	No
Technical Address Network Service Link Details Query	Technical Address Network Service Link Details Query	Links within own System Entity (for CBs) or linked to own Party (for Payment Banks)	No
Technical Address Network Service Link Details Query	Technical Address Network Service Link Details Query	Links within own System Entity (for CBs) or linked to own Party (for Payment Banks)	No

***TABLE 9 –* TIPS FUNCTIONS**

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
Adjust CMB Limit	Adjust CMB Limit	Data within own System Entity (for CB) or linked to own Party (for Payment Bank)	No
Instruct Instant Payment	Initiate Instant Payment Confirm/reject Instant Payment Request Instant Payment recall	Data related to Accounts within own System Entity (for CB) or for which own Party is set as authorised user (for Payment Bank)	No

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
	Confirm Instant Payment recall Reject Instant Payment recall Instant Payment Status Investigation		
Instruct Liquidity Transfer	Initiate Outbound Liquidity Transfer	Accounts within own System Entity (for CB) or owned by own Party (for Payment Bank)	No
Modify All Blocking Status	Block/unblock Participant Block/unblock Account Block/unblock CMB	Data within own System Entity (for CB) or linked to own Party (for Payment Bank)	No
Modify CMB Blocking Status	Block/unblock CMB	Data within own System Entity (for CB) or linked to own Party (for Payment Bank)	No
Query All	Query Account Balance and Status Query CMB Limit and Status Query Instant Payment Transaction	Data related to Accounts within own System Entity (for CB) or owned by own Party (for Payment Bank)	No
Query as Reachable Party	Query CMB Limit and Status Query Instant Payment Transaction	Data related to Accounts within own System Entity (for CB) or for which own Party is set as authorised user (for Payment Bank)	No

TABLE 10 – OTHER

PRIVILEGE	USER FUNCTION	DATA SCOPE	DMT AVAILABILITY
Data Migration Tool Access	n/a	n/a	Yes

See section 1.2.2.2.2. for information on the configuration of privileges.

1.2.2.1.3. Role

A role is a set of privileges. See section 1.2.2.2.3. for information on the configuration of roles.

1.2.2.1.4. User

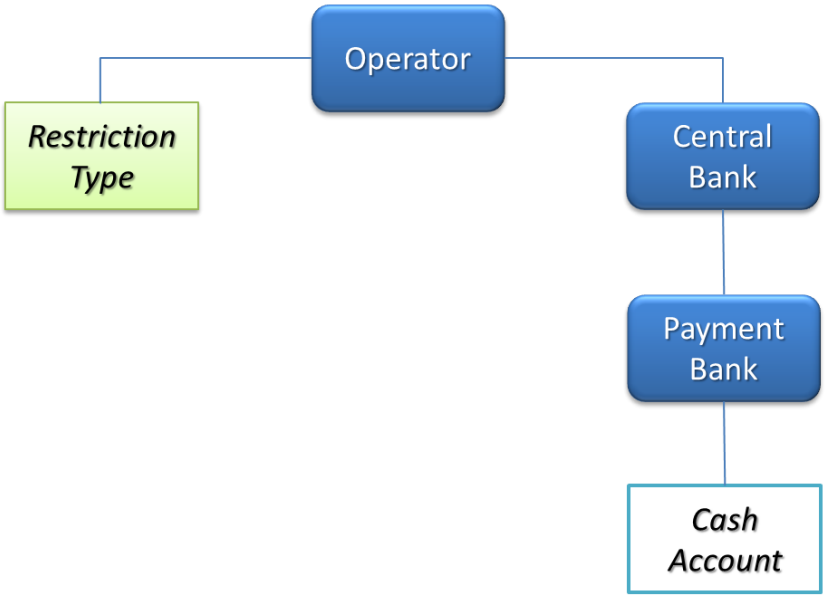
A user is an individual or application that interacts with CRDM triggering the available CRDM user functions. See section 1.2.2.2.1. for information on the configuration of users.

1.2.2.1.5. Common reference data objects and the hierarchical party model

All parties in the CRDM are linked to each other according to a hierarchical model (see section 1.3.2). As shown in the following diagram and on the basis of this hierarchical party model, the Operator is the only party at level 1, all the Central Banks are level 2 parties, all payment banks are level 3 parties[3]. All the other reference data objects are linked to a party. For example:

- A cash account is linked to its Central Bank or payment bank;
- A restriction type is linked to the Operator.

DIAGRAM 1 – COMMON REFERENCE DATA OBJECTS AND THE HIERARCHICAL PARTY MODEL



1.2.2.1.6. Data scope

For each privilege, the hierarchical party model determines the data scope of the grantee, i.e. the set of reference data objects on which the grantee can trigger the relevant user function. More precisely:

- Users of the Operator have visibility on all reference data objects, and can act on objects belonging to participants only in exceptional circumstances, following a specific agreement;
- Users of the Central Banks have visibility on all reference data objects belonging to the same system entity;[4]
- Users of the payment banks have visibility on reference data objects that are (directly or indirectly) linked to the same party.

The following example describes the concept of data scope.[5]

3 Participation types may be further detailed with information specific to each individual Service, if the Service foresees this possibility; for more information see section 1.3.2.

4 A system entity in the CRDM corresponds to a partition of data equating to the scope of a Central Bank or of the Operator. For example, the system entity of a Central Bank includes all the data related to its payment banks.

5 The following example presents only the configuration data that are relevant for the example. All the possible configuration options are defined in the following sections.

EXAMPLE 1 - DATA SCOPE

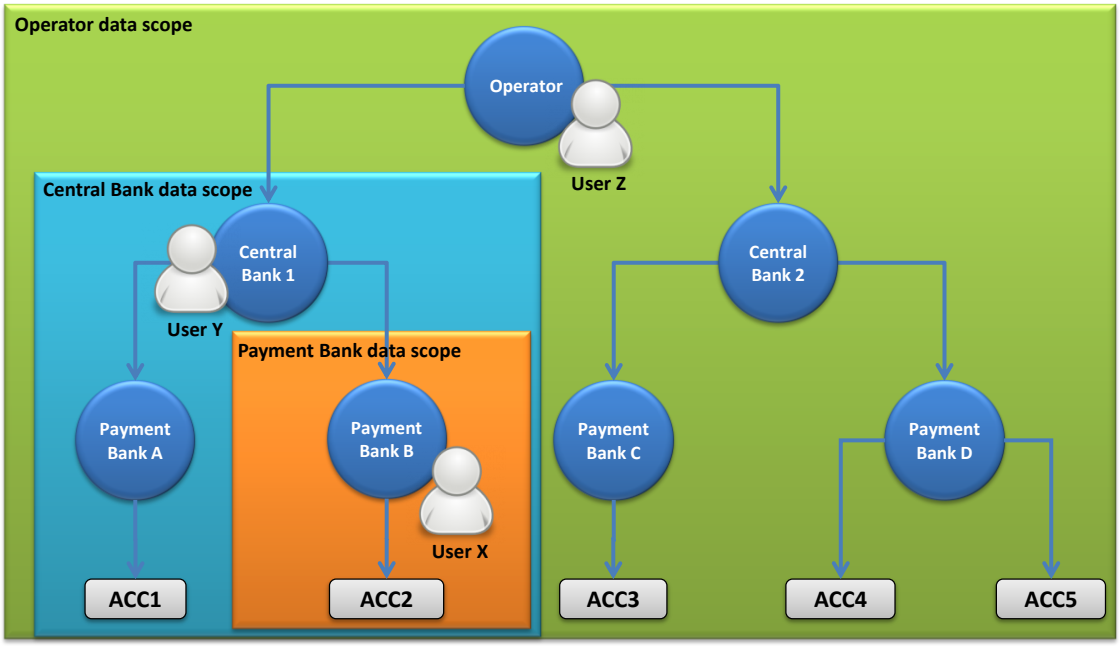
Three users, X, Y and Z, belonging to a Payment Bank, to a Central Bank and to the Operator respectively, are granted with the same privilege to query cash accounts:

TABLE 11 - USER PRIVILEGES (DATA SCOPE)

USER	PRIVILEGE
X	Cash Account Reference Data Query
Y	Cash Account Reference Data Query
Z	Cash Account Reference Data Query

The following diagram shows the data scopes stemming from this access rights configuration for the three users.

DIAGRAM 2 - DATA SCOPES



The diagram shows that users X, Y and Z are given different data scopes, owing to the fact that they belong to different parties located at different levels of the hierarchical party model. More precisely:

- User X of Payment Bank B gets a data scope including the cash account ACC2 only, as ACC2 is the only account of Payment Bank B. User X cannot query any other cash account in CRDM;
- User Y of Central Bank 1 gets a data scope including cash accounts ACC1 and ACC2, as these accounts belong to Payment Banks of Central Bank 1. User Y cannot query any other cash account in CRDM, i.e. any cash account falling under the data scope of any other Central Bank;
- User Z of the Operator gets a data scope including all cash accounts in CRDM, as the Operator is at the top level of the hierarchical party model.

1.2.2.2. Access rights configuration

This section presents how roles and privileges can be configured in the CRDM in order to grant each user with the appropriate set of access rights.

1.2.2.2.1. Configuration of users

Links between users and parties

Each new user is linked to the same party which the creator user belongs to. An exception takes place when creating the first user of a party, i.e.

- When a CRDM Operator system administrator creates a new system administrator for a Central Bank;
- When a Central Bank system administrator creates a new system administrator for one of its payment banks.

In all these cases the created user is linked to the party this user is going to administer.

Through the link with the relevant party, each user inherits a data scope (see section 1.2.2.1.6.).The link between a user and a party cannot be changed, i.e. a user is always linked to the same party.

Party administrators

Each party must have at least one party administrator, i.e. a user being granted specific system privileges that allow its grantee to grant any roles and privileges previously granted to the grantee's party.

1.2.2.2.2. Configuration of privileges

Availability of privileges

Each privilege, just after its creation, is available to the party administrator(s) of the CRDM Operator only. This means that party administrators of all the other parties cannot grant this privilege to their users.

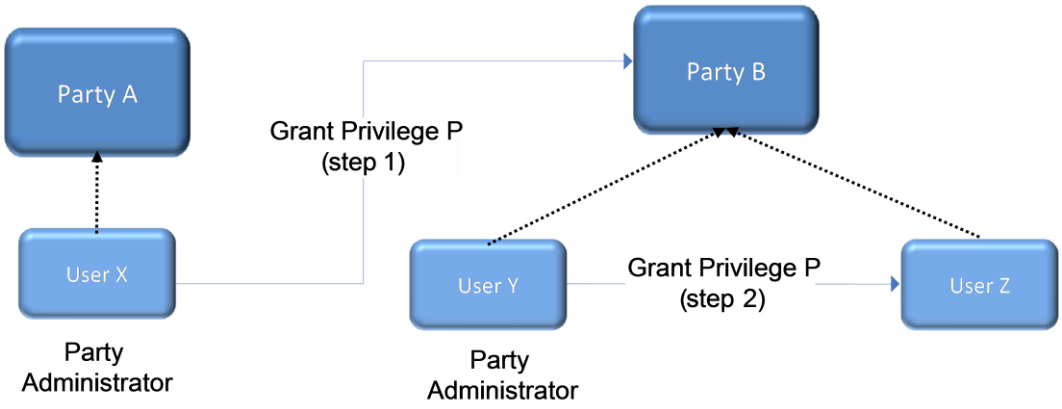
A privilege becomes available to a party administrator of a party different from the CRDM Operator only after this privilege has been granted to this party. From this moment on, the party administrator can grant this privilege, according to the rules defined in the following sections.

This implies that a two-step process is required in order to grant a specific privilege to a user belonging to a party different from the CRDM Operator. In the first step, the privilege is granted to the relevant party (so that it becomes available to the party administrator(s) of this party). With the second step, one of the party administrators grants the privilege to the relevant user.

The following diagram illustrates the access rights configuration steps needed to grant a user Z of a Party B a given privilege P that is already available to the party administrator X of another party A.[6]

6 Party A may be the Operator or any other party which was previously granted privilege P.

DIAGRAM 3 - ACCESS RIGHTS CONFIGURATION STEPS



The two configuration steps are as follows:

- User X, as a party administrator of party A, grants privilege P to party B. From this moment on, privilege P becomes available to the party administrator Y of party B.
- User Y, as a party administrator of party B, grants privilege P to user Z. From this moment on, user Z can trigger the user functions linked to privilege P.

At Party level, Access rights are propagated following the hierarchical Party model, i.e. the Operator propagates access rights to Central Banks which in turn propagate them to their Payment Banks. If necessary, the Operator can act on behalf of a Central Bank following a specific request to propagate access rights directly to its Payment Banks.

While the features described above apply to all privileges related to CRDM functions, it should be noted that TIPS privileges cannot be granted directly to Parties or Users, but can only be granted to Roles, which can in turn be granted to Parties and Users. This implies that the above described configuration steps remain valid for TIPS as well, but in this case Privileges have to be granted to Roles in the first place and then Roles can be granted to Parties and Users. For details on the configuration of Roles see section 1.2.2.2.3.

Granting privileges

CRDM privileges can be granted to roles, users and parties, whereas TIPS privileges can be granted to roles only. When granting a privilege, the grantor specifies appropriate values for the three following assignment options: Deny option, Administration option and Four-Eyes option.

TABLE 12 - PRIVILEGE ASSIGNMENT OPTIONS

OPTION	DESCRIPTION
Deny	This option specifies whether the associated user function is allowed (Deny is False) or explicitly denied (Deny is True).
Administration	If the grantee of the privilege is a user or a role, this option specifies whether the grantee is allowed to grant the same privilege to another user or role of the same party (Administrator is True) or not (Administrator is False). If the grantee of the privilege is a party, this option specifies whether the party administrators of the grantee party is allowed to grant the same privilege only to users and roles of the same party (Administrator is False) or also to other parties (Administrator is True).
Four-Eyes	This option specifies whether the grantee of the privilege is allowed to use the function associated to the privilege according to the Two-Eyes (Four-Eyes is False) or Four-Eyes (Four-Eyes is True) principles. This option is relevant only when the Deny option is set to False and it is always not relevant for privileges related to queries.

EXAMPLE 2 - ASSIGNMENT OF PRIVILEGES TO ROLES

The following table shows some examples of assignment of privileges to roles:

TABLE 13 - ASSIGNMENT OF PRIVILEGES TO ROLES

ROW	ROLE	PRIVILEGE	DENY	ADMIN	FOUR-EYES
1	Cash Account Management	Cash Account Reference Data Query	False	False	not relevant
2	Cash Account Administration	Cash Account Reference Data Query	True	True	not relevant
3	Party Management	Create Party	False	False	True
4	Party Management	Update Party	False	False	True
5	Party Management	Delete Party	False	False	True
6	Party Management	Party Reference Data Query	False	True	not relevant

For each assignment of a privilege to a role, three additional attributes define the features of such assignment.

For example, according to row 1, the privilege to query Cash Account data is assigned to the Cash Account Management role:

- Without Deny, i.e. users linked to the Cash Account Management role can query cash account data [7];

7 In this case the setting for the Four Eyes assignment option is not applicable, as the privilege refers to a query.

- Without Admin, i.e. users linked to the Cash Account Management role cannot grant the privilege to query cash account data to other roles and users.

According to row 2, the privilege to query Cash Account data is assigned to the Cash Account Administration role:

- With Deny, i.e. users linked to the Cash Account Administration role cannot query cash account data;
- With Admin, i.e. users linked to the Cash Account Administration role can grant the privilege to query cash account data to other roles and users of the same party.

As a whole, rows 1 and 2 result in a segregation of duties between business users and access rights administrators. In fact, users linked to the Cash Account Management role can query accounts, but they cannot configure the same access rights for any other user. On the contrary, users linked to the Cash Account Administration role cannot query accounts, but they can configure these access rights for other users.

According to row 3, the privilege to create parties is assigned to the Party Management role:

- Without Deny and with 4-Eyes set to True, i.e. users linked to the Party Management role can create parties according to the Four-Eyes principle only;
- Without Admin, i.e. users linked to the Party Management role cannot grant the privilege to create parties to other roles and users.

As per rows 4 and 5 , the privileges to maintain and delete parties are assigned to the Party Management role with the same assignment options.

Finally, according to row 6, the privilege to query parties is assigned to the Party Management role:

- Without Deny, i.e. users linked to the Party Management role can query parties;
- With Admin, i.e. users linked to the Party Management role can grant the privilege to query parties to other roles and users of the same party.

As a whole, rows from 3 to 6 only result in a partial segregation of duties between business users and access rights administrators. In fact:

- Business users linked to the Party Management role can create, maintain, delete and query parties, they can only configure the same access rights for any other user limited to the query privilege;
- On the contrary, access rights administrators linked to the Party Management role, and whose Party is also linked to the same role, can create, maintain, delete and query parties and they can also grant the same privilege to other users of the same party; in addition, they can also grant the query privilege to other parties.

EXAMPLE 3 - ASSIGNMENT OF PRIVILEGES TO USERS

The following table shows two examples of assignment of privileges to users:

TABLE 14 - ASSIGNMENT OF PRIVILEGES TO USERS

ROW	PRIVILEGE	USER	DENY	ADMIN	FOUR-EYES
1	Create Cash Account	U_X	False	False	False
2	Create Cash Account	U_Y	True	True	False

For each assignment of a privilege to a user, three additional attributes define the features of such assignment.

According to row 1, the privilege to create cash accounts is assigned to user U_x:

- Without Deny, i.e. user U_X can create cash accounts according to the Two-Eyes principle (as the privilege is assigned without Four-Eyes);
- Without Admin, i.e. user U_X cannot grant the privilege to create cash accounts to other roles and users.

Similarly, row 2 stipulates that the privilege to create cash accounts is assigned to user U_Y:

- With Deny, i.e. user U_Y cannot create cash accounts;
- With Admin, i.e. user U_Y can grant the privilege to create cash accounts to other roles and users of the same party, according to the Two-Eyes principle or to the Four-Eyes principle (as the privilege is assigned without Four-Eyes).

As a whole, this configuration results in a full segregation of duties between business users and access rights administrators. In fact, user U_X can create cash accounts, but without having the possibility to grant the same privilege to any other user. Vice versa, user U_Y can configure this privilege for other users, but without having the possibility to use it.

EXAMPLE 4 - ASSIGNMENT OF PRIVILEGES TO PARTIES

The following table shows one example of assignment of a privilege to a party:

TABLE 15 - ASSIGNMENT OF PRIVILEGES TO PARTIES

PRIVILEGE	PARTY	DENY	ADMIN	FOUR-EYES
Cash Account Reference Data Query	Payment Bank A	False	True	False

For each assignment of a privilege to a party, three additional attributes define the features of such assignment. In this example, the privilege to query cash accounts is assigned to the payment bank A:

- Without Deny, i.e. party administrators of the payment bank A can grant the privilege to query cash accounts to other roles and users of the same party;
- With Admin, i.e. party administrators of the payment bank A can grant the privilege to query cash accounts to other parties.

The Four-Eyes attribute is set to false but it is not relevant for this example, as the privilege refers to a Query.

Revoking privileges

Privileges can be revoked from roles, users and parties.

When revoking a privilege from the user, this just results in the removal of the privilege from the list of privileges linked to the user.

When revoking a privilege from a role, this results in the removal of the privilege from the list of privileges linked to the role. Consequently, all the users and parties linked to the role are not linked anymore to the privilege, with immediate effect.

When revoking a privilege from a party, CRDM applies a cascade effect. This results in the removal of the privilege:

- from the list of privileges linked to the party and
- from the list of privileges linked to all the roles and users of the party.

The following table shows all the possible scenarios for revoking privileges that are allowed in CRDM, their link with the cascade process and how party administrators of CBs can ensure that all the privileges revoked from one of their parties are revoked also from all the users of the same party:

TABLE 16 – CASCADE PROCESS WHEN REVOKING PRIVILEGES

FUNCTION	FROM	CASCADE	PROPAGATION TO USERS
Revoke Privilege	User	n/a	As the grantee is already a user, there is no need to trigger any cascade process.
Revoke Privilege	Role	n/a	If the party administrator of the Payment Bank granted a privilege included in the role directly to other users of the Payment Bank, then the removal of this privilege from the role would not revoke the same privilege from these users. In fact, when revoking a privilege from a role, CRDM does not trigger the cascade process as this may result in unintended removal of privileges from the users of the Payment Bank. For example, even a simple movement of a privilege between two roles assigned to the same Payment Bank (i.e. revoking the privilege from the first role and granting it to the latter) would imply the removal of the same privilege from all the users of this Payment Bank and this would oblige the party administrator of the Payment Bank to grant again this privileges to all the impacted users. In order to ensure that the relevant privilege is revoked also from the users of the Payment Bank (if this is the intended goal), the party administrator of the CB should grant directly this privilege to the Payment Bank and then revoke it, as this will trigger the cascade process related to the Revoke Privilege function from Party (see next row of this table).
Revoke Privilege	Party	Yes	CRDM triggers automatically the cascade process, which ensures that privileges revoked from a party are also revoked from all the users and roles of the same party.

The cascade process is automatically triggered in a deferred mode one time per business day. However, in case the party administrator needs the cascade process to take place immediately, this can be achieved by contacting the CRDM Operator, as the CRDM Operator can trigger this process on demand also intraday.

1.2.2.2.3. Configuration of roles

Links between roles

CRDM supports a role-based access control (RBAC) model. This results in the possibility to inherit privileges from one or more roles.

Granting roles

Roles can be granted to users and parties.

When granting a role to a user, the grantee user immediately inherits all the privileges of the granted role, i.e. all the privileges linked to the granted role.

When granting a role to a party, the grantee party immediately inherits all the privileges of the granted role, i.e. all the privileges linked to the granted role.

Revoking roles

Roles can be revoked from users and parties.

When revoking a role from a user, this user immediately loses all the privileges of the revoked role, i.e. all the privileges linked to the revoked role.

When revoking a role from a party, this party immediately loses all the privileges of the revoked role, i.e. all the privileges linked to the revoked role.

Both when revoking roles from users and from parties, CRDM does not apply a cascade effect.

The following table shows all the possible scenarios for revoking roles that are allowed in CRDM, their link with the cascade process and how party administrators of CBs can ensure that all the roles revoked from one of their parties (and all the privileges included in these roles) are revoked also from all the users of the same party:

TABLE 17 – CASCADE PROCESS WHEN REVOKING ROLES

FUNCTION	FROM	CASCADE	PROPAGATION TO USERS
Revoke Role	User	n/a	As the grantee is already a user, there is no need to trigger any cascade process.
Revoke Role	Party	n/a	If the party administrator of the Payment Bank granted the role (or a privilege included in the role) directly to other users of the Payment Bank, then the removal of this role from the party would not revoke the same role (or the privilege included in the role) from these users. In fact, when revoking a role from a party, CRDM does not trigger the cascade process as this may result in unintended removal of roles (or privileges) from the users of the Payment Bank. In order to ensure that the relevant role is revoked also from the users of the Payment Bank, the party administrator of the CB should revoke all the privileges included in the role from the role itself and then delete the role. It should be noted that this approach can be applied without unintended side effects on other Payment Banks only if the role was specifically created for (and assigned to) the relevant

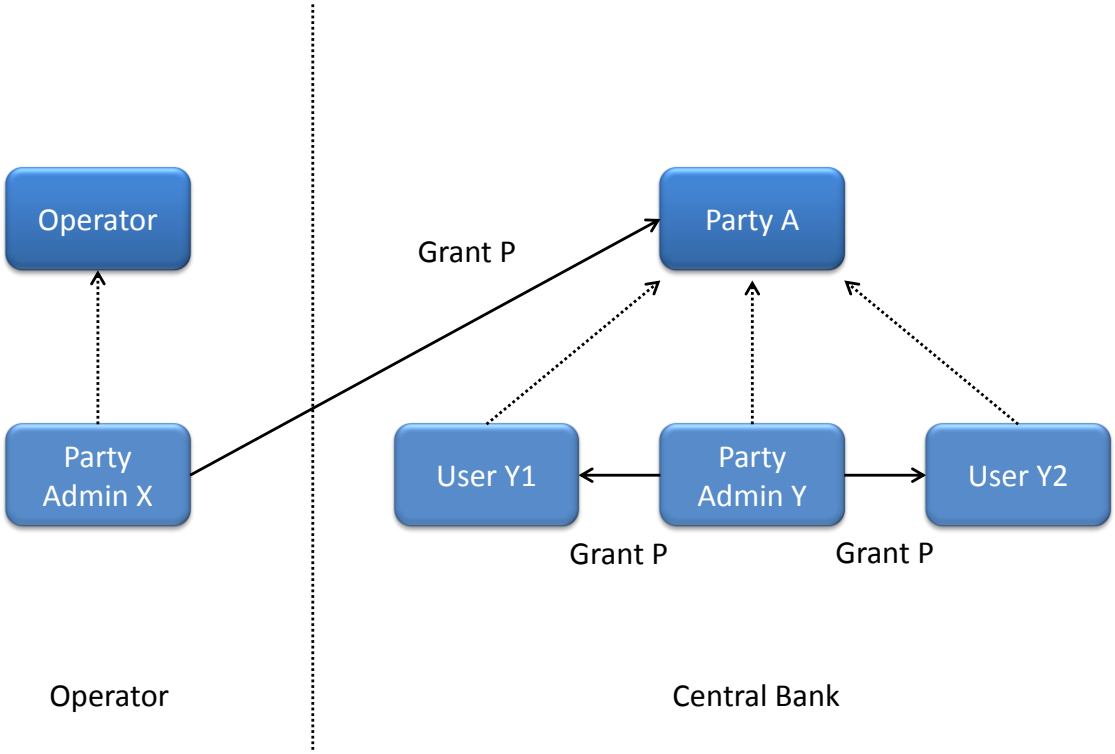
FUNCTION	FROM	CASCADE	PROPAGATION TO USERS
			Payment Bank only, otherwise the procedure just described would also have an effect on all Payment Banks (and on all their users) being granted with the same role. Furthermore, in order to ensure that any privilege belonging to the role and that was granted directly to users of the Payment Bank is also revoked from these users, the party administrator of the CB should grant directly this privilege to the Payment Bank and then revoke it, as this will trigger the cascade process related to the Revoke Privilege function from Party (see Table 11 – Cascade Process when Revoking Privileges).

1.2.2.3. Access rights configuration process

As described in section 1.2.2.2. , before the party administrator of a given party can grant a privilege to a user of the same party, the same privilege has to be granted to the same party, so that it becomes available to the party administrator(s) of the party.

On this basis, the following diagram illustrates the steps needed for granting a given privilege P to the users of a Central Bank (identified as Party A in the diagram).

DIAGRAM 4 - ACCESS RIGHTS CONFIGURATION PROCESS (A)



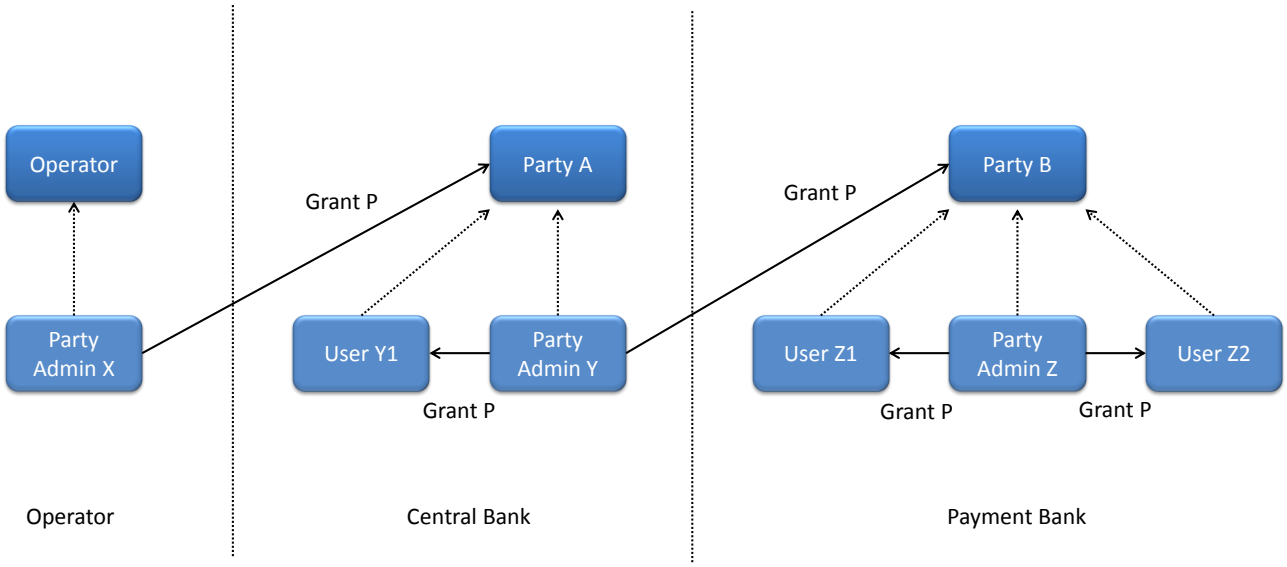
The diagram shows that the two required steps are as follows:

- User X, as a party administrator of the Operator, grants the privilege P to the party A;

- User Y, as a party administrator of the party A, grants the privilege P to all the relevant users (in this case, users Y_1 and Y_2).

The same process applies when a Central Bank needs to configure access rights for their payment banks. The following diagram illustrates all the steps needed for granting a given privilege P to the users of a payment bank (party B in the diagram), via the relevant Central Bank (party A in the diagram).

***DIAGRAM* 5 - ACCESS RIGHTS CONFIGURATION PROCESS (B)**



The diagram shows that the three required steps are as follows:

- User X, as a party administrator of the Operator, grants the privilege P to the party A (i.e. to a Central Bank);
- User Y, as a party administrator of the party A, grants the privilege P to the party B (i.e. to a payment bank);
- User Z, as a party administrator of the party B, grants the privilege P to the relevant users (in this case users Z_1 and Z_2).

In addition, the diagram shows that user Y, as a party administrator of the party A, can also grant the privilege P to the user Y_1, as this user belongs to the same party.

These two examples illustrates that the access rights configuration process in the CRDM consists in two main tasks:

- Configuration of access rights at party level;
- Configuration of access rights at user level.

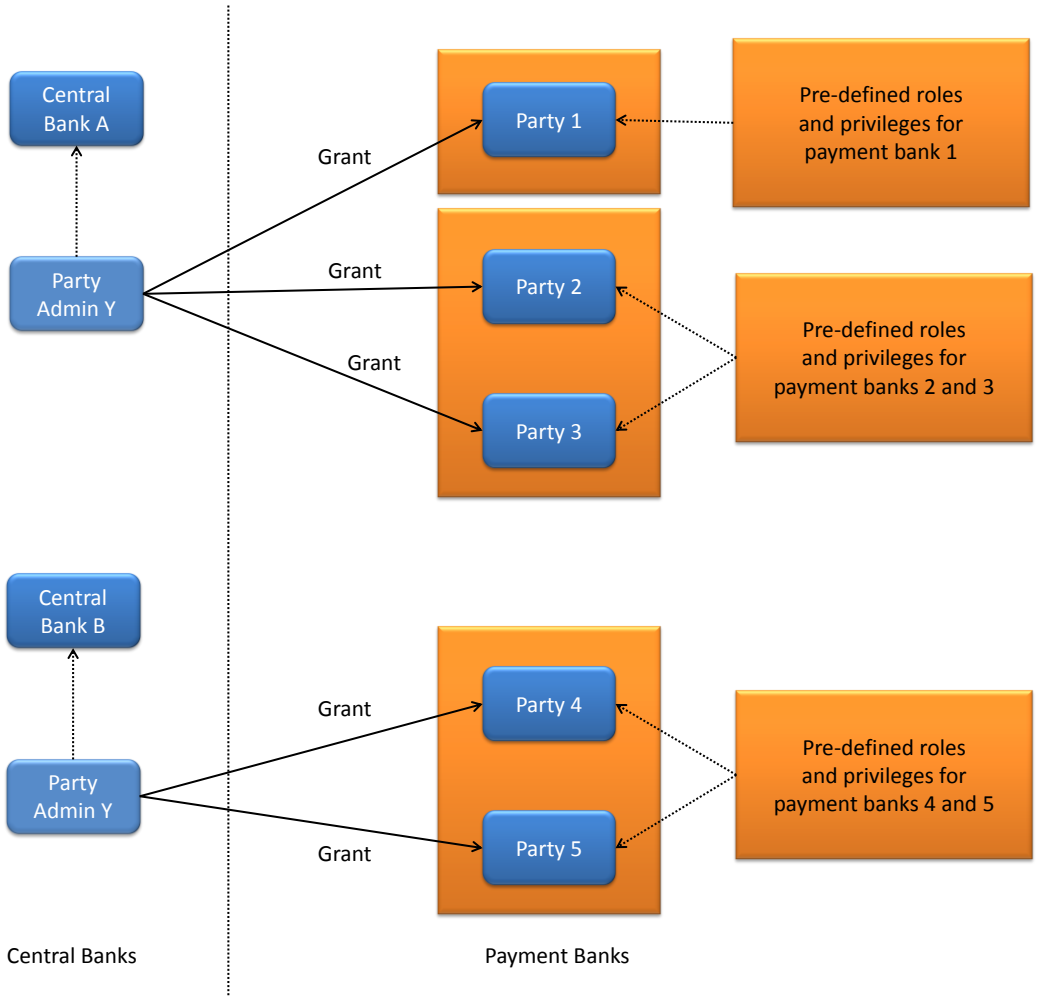
As stated in section 1.2.2.2.2. , the above process is not directly applicable for TIPS Privileges; in this case Privileges have to be granted to Roles in the first place and then Roles can be granted to Parties and Users. For details on the configuration of Roles see section 1.2.2.2.3.

1.2.2.3.1. Configuration of access rights at party level

This task consists in the assignment of the relevant set of roles and privileges to a given party in the CRDM. A party administrator of the CRDM Operator performs this task for the configuration of access rights of Central Banks.

The following diagram shows an example in which the party administrator of the CRDM Operator grants to all the Central Banks the same set of roles and privileges. This set includes all the privileges needed by the Central Banks and all the privileges needed by the Payment Banks.

EXAMPLE 5 - CONFIGURATION OF ACCESS RIGHTS AT PARTY LEVEL BY THE CRDM OPERATOR



A party administrator of each Central Bank assigns the relevant set of roles[8] and privileges to all its payment banks. In this example the party administrator of a Central Bank A configures the relevant access rights for three payment banks Party 1, Party 2 and Party 3. This results in two different set of roles and privileges, the first one being granted to the payment bank Party 1 only, the latter being assigned to both payment banks Party 2 and Party 3. Similarly, the party administrator of a Central Bank B assigns the relevant access

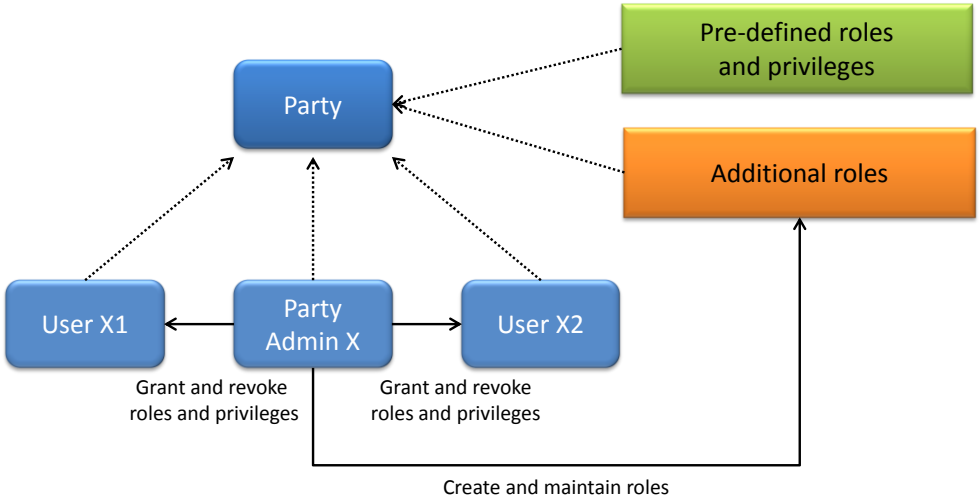
[8] New Roles can only be created and maintained by the CRDM Operator and Central Bank parties. Payment Banks can only grant/revoke Roles that have previously been granted to them by their Central Banks.

rights to two payment banks Party 4 and Party 5, this task resulting in the configuration of the same set of access rights for both payment banks Party 4 and Party 5.

1.2.2.3.2. Configuration of access rights at user level

After the configuration of access rights at party level has been set up for a given party, its party administrator(s) can perform the configuration of access rights at user level, in order to assign the appropriate roles and privileges to all the users of the given party.

DIAGRAM 6 - CONFIGURATION OF ACCESS RIGHTS AT USER LEVEL



The above diagram shows that the party administrator(s) can set up the appropriate access rights configuration for the users of the same party:

- By possibly creating and maintaining[9] additional roles, besides the ones previously granted at party level[10];
- By granting (and revoking) the (default and additional) roles and the (default) privileges to the users of the same party.

1.2.3. Message subscription

1.2.3.1. Message subscription configuration

Central Banks can configure, for payment banks they are responsible for, the subscription for credit notifications for liquidity transfers occurring on selected TIPS Accounts owned by the payment banks.

Each message subscription rule set is defined by the following elements:

- The name and the description of the message subscription rule set;
- A validity period, specified by a mandatory initial date of validity and an optional final date of validity.

9 New Roles can only be created and maintained by the CRDM Operator and Central Bank parties. Payment Banks can only grant/revoke Roles that have previously been granted to them by their Central Banks.

10 These additional roles can only be granted with available privileges, i.e. privileges previously granted at party level.

- The payment bank to which TIPS sends all the messages matching the rule set.
- A set of rules defining the TIPS accounts for which TIPS sends the credit notifications. Each rule is assigned a validity period, specified by a mandatory initial date of validity and an optional final date of validity. The validity period of a rule cannot exceed the validity period of the message subscription rule set it belongs to, i.e. the validity period of a rule cannot start before or end after the validity period of the relevant message subscription rule set.
- A positive/negative parameter which for TIPS shall always be set to Positive, as only positive message subscription rule sets are propagated from CRDM to TIPS.

If deemed necessary, CBs can decide to hand over the control to their DCPs by granting them the privilege for message subscription configuration (for more information on privilege granting see section 1.2.2).

1.2.3.2. Message subscription parameter types

The table below describes the exhaustive list of parameter types that Central Banks can use for configuring their message subscription rule sets.

TABLE 18 - MESSAGE SUBSCRIPTION PARAMETER TYPES

PARAMETER TYPE	DESCRIPTION
Message Type	It specifies the type of message (i.e. BankToCustomerDebitCreditNotification).
Cash Account	It specifies the TIPS account for which credited notifications shall be sent.

1.2.3.3. Message subscription examples

The above described message subscription configuration is illustrated below.

EXAMPLE 6 - SUBSCRIBING FOR LIQUIDITY TRANSFER CREDIT NOTIFICATION

This example is about a message subscription configuration which allows a payment bank A to receive from TIPS credit notifications related to settlement of liquidity transfers.

This message subscription configuration must be valid as of 1st of July 2019. The general features of the new message subscription rule set for the payment bank A, i.e. the rule set name, the starting validity date and the relevant interested party can be specified as follows:

TABLE 19 - DEFINITION OF A NEW MESSAGE SUBSCRIPTION RULE SET

MESSAGE SUBSCRIPTION RULE SET	
Name	CREDIT_NOTIFY_ACCOUNT_A
Description	Receive credit notifications for account A
Interested Party	Payment Bank A

MESSAGE SUBSCRIPTION RULE SET	
Valid From	1-July-2019
Valid To	-
Positive/Negative	Positive

The rule that the payment bank A needs to specify for itself in order to fulfil the requirements described before is as follows:

TABLE 20 - DEFINITION OF THE RULES FOR A NEW MESSAGE SUBSCRIPTION RULE SET

RULE SET	VALID FROM	VALID TO	MESSAGE TYPE	TIPS ACCOUNT
Rule 1	2019-07-01	-	BankToCustomerDebitCreditNotification	ACCOUNT A

1.2.4. Graphical user interface

Users of CRDM Actors granted with the appropriate privileges can communicate with the CRDM in U2A mode via a web-based graphical user interface (GUI).

The following CRDM functionalities are available in U2A mode:

TABLE 21 – CRDM U2A FUNCTIONS

Function	Actor[11]
Create Party	CRDM Operator, Central Bank
Update Party	CRDM Operator, Central Bank
Delete/Restore Party	CRDM Operator, Central Bank
Query Party List	CRDM Operator, Central Bank, Payment Bank
Query Party Details	CRDM Operator, Central Bank, Payment Bank
Create Party Service Link	CRDM Operator, Central Bank
Update Party Service Link	CRDM Operator, Central Bank
Delete/Restore Party Service Link	CRDM Operator, Central Bank
Query Party Service Link List	CRDM Operator, Central Bank, Payment Bank
Create Cash Account	CRDM Operator, Central Bank, Payment Bank[12]
Update Cash Account	CRDM Operator, Central Bank, Payment Bank[12]
Delete/Restore Cash Account	CRDM Operator, Central Bank, Payment Bank[12]
Query Cash Account List	CRDM Operator, Central Bank, Payment Bank
Query Cash Account Details	CRDM Operator, Central Bank, Payment Bank
Create Limit	Payment Bank
Update Limit	Payment Bank
Delete/Restore Limit	Payment Bank
Query Limit List	Payment Bank
Query Limit Details	Payment Bank
Create Authorized Account User	Payment Bank
Update Authorized Account User	Payment Bank

[11] The Actor types listed for each function refer to the default responsible Actor in normal operating conditions. However it is possible for the CRDM Operator to act on behalf of Central Banks (and of Payment Banks, upon request of the relevant Central Bank) and for the Central Banks to act on-behalf of their Payment Banks, under well-defined contingency scenarios.

[12] Payment Banks are only allowed to Create/Update/Delete/Restore Cash Accounts of type "TIPS Credit Memorandum Balance".

Function	Actor[11]
Delete/Restore Authorized Account User	Payment Bank
Query Authorized Account User List	Payment Bank
Create User	CRDM Operator, Central Bank, Payment Bank
Update User	CRDM Operator, Central Bank, Payment Bank
Delete/Restore User	CRDM Operator, Central Bank, Payment Bank
Query User List	CRDM Operator, Central Bank, Payment Bank
Query User Details	CRDM Operator, Central Bank, Payment Bank
Create Role	CRDM Operator, Central Bank
Update Role	CRDM Operator, Central Bank
Delete/Restore Role	CRDM Operator, Central Bank
Query Role List	CRDM Operator, Central Bank
Create Certificate DN	CRDM Operator, Central Bank, Payment Bank
Delete/Restore Certificate DN	CRDM Operator, Central Bank, Payment Bank
Query Certificate DN List	CRDM Operator, Central Bank, Payment Bank
Create User Certificate DN Link	CRDM Operator, Central Bank, Payment Bank
Delete/Restore User Certificate DN Link	CRDM Operator, Central Bank, Payment Bank
Query User Certificate DN Link List	CRDM Operator, Central Bank, Payment Bank
Grant Privilege	CRDM Operator, Central Bank, Payment Bank
Revoke Privilege	CRDM Operator, Central Bank, Payment Bank
Query Granted Privilege List	CRDM Operator, Central Bank, Payment Bank
Query Granted Privilege Details	CRDM Operator, Central Bank, Payment Bank
Grant Role	CRDM Operator, Central Bank, Payment Bank
Revoke Role	CRDM Operator, Central Bank, Payment Bank
Query Granted Role List	CRDM Operator, Central Bank, Payment Bank
Query Granted Role Details	CRDM Operator, Central Bank, Payment Bank
Create Message Subscription Rule	Central Bank, Payment Bank
Update Message Subscription Rule	Central Bank, Payment Bank
Delete/Restore Message Subscription Rule	Central Bank, Payment Bank

Function	Actor[11]
Query Message Subscription Rule List	Central Bank, Payment Bank
Query Message Subscription Rule Details	Central Bank, Payment Bank
Create Message Subscription Rule Set	Central Bank, Payment Bank
Update Message Subscription Rule Set	Central Bank, Payment Bank
Delete/Restore Message Subscription Rule Set	Central Bank, Payment Bank
Query Message Subscription Rule Set List	Central Bank, Payment Bank
Query Message Subscription Rule Set Details	Central Bank, Payment Bank
Create Technical Address Network Service Link	CRDM Operator, Central Bank
Delete/Restore Technical Address Network Service Link	CRDM Operator, Central Bank
Query Technical Address Network Service Link List	CRDM Operator, Central Bank, Payment Bank
Create DN BIC Routing	Payment Bank
Update DN BIC Routing	Payment Bank
Delete/Restore DN BIC Routing	Payment Bank
Query DN BIC Routing List	Payment Bank
Create Report Configuration	Payment Bank
Update Report Configuration	Payment Bank
Delete/Restore Report Configuration	Payment Bank
Query Report Configuration List	Payment Bank
Query Report Configuration Details	Payment Bank
Create Routing	CRDM Operator, Central Bank, Payment Bank
Update Routing	CRDM Operator, Central Bank, Payment Bank
Delete Routing	CRDM Operator, Central Bank, Payment Bank
Query Routing	CRDM Operator, Central Bank, Payment Bank

Via U2A mode, CRDM offers to CRDM Actors a dual authorisation concept, the Four-Eyes-Principle (See section 1.2.5.2).

Detailed description of the CRDM graphical user interface is provided into the CRDM User Handbook.

1.2.5. Security

This section aims at describing the main processes performed by CRDM in terms of security principles applied to ensure to CRDM users that they can securely exchange information with CRDM.

Secure means that the following security conditions are met:

- Confidentiality: Ensuring that information is accessible only to authenticated and authorised CRDM Actors;
- Integrity: Safeguarding the accuracy and completeness of information;
- Monitoring: Detecting operational and technical problems and recording appropriate information for crisis management scenarios and future investigations;
- Availability: Ensuring that authorised users have access to information and associated assets when required;
- Auditability: Ensuring the possibility to establish whether a system is functioning properly and that it has worked properly.

1.2.5.1. Confidentiality

The confidentiality of data in CRDM is ensured by the possibility to grant specific access rights for any given set of data, as detailed in section 1.2.2. In conjunction with mechanisms of authentication[13] and authorisation applying to all requests received by CRDM in both the DMT and U2A mode, this guarantees that each CRDM Actor's data is treated confidentially and is not accessible to non-authorized CRDM Actors.

In addition to these standard mechanisms, the principle of data segregation is applied on the reference and transactional data belonging to CBs and Payment Banks in order to ensure a strict separation of their respective data in CRDM.

1.2.5.2. Integrity

Within CRDM, various business validations ensure the integrity of information. If a business validation fails, CRDM has a concept of Error handling in place. The requested action is not processed and CRDM provides the user with detailed information regarding the nature of the error via DMT or U2A.

In U2A mode, CRDM offers users in addition the possibility to further ensure the integrity of data, data requests and communications via usage of a dual authorisation concept, the Four-Eyes-Principle. In case this option is chosen for a specified set of CRDM operations, a second independent verification and confirmation is required before an operation becomes active in CRDM. If, for example, a critical set of Reference Data should be modified and the person requesting the change is only allowed to do so under the Four-Eyes-Principle, then a second person of the same Party has to confirm the correctness of the request. Otherwise, the requested change of Reference Data is not implemented.

1.2.5.3. Monitoring

CRDM operational monitoring provides tools to the CRDM Operator for the detection in real-time of functional or operational problems.

Technical monitoring allows for the detection of hardware and software problems via real-time monitoring of the technical components involved in the processing, including the network connections.

In addition, the monitoring provides the CRDM Operator with an overview of the message flows in CRDM.

13 Authentication means determining whether someone or something (function, component...) is who or what it is declared to be

1.2.5.4. Availability

The overall availability of the CRDM is ensured by the infrastructure design. The technical environment for the CRDM core system follows a "two regions/four sites" approach to ensure availability throughout the widest possible range of system failures.

1.2.5.5. Auditability

CRDM provides an audit trail with which it is possible e.g. to reconstruct who updated which data when. All this data is available to authorised users via queries.

1.3. Reference data model

This section provides a detailed description of all the reference data objects stored by CRDM. More in detail, section 1.3.1 identifies some common information that are used for all reference data objects and the validity period attributes that have to be specified for all reference data objects having a limited validity period (see section 1.4.3.3). The following sections describe into detail the conceptual data model of the different CRDM reference data components, i.e.:

- party data management (§.1.3.2)
- cash account data management (§.1.3.3)
- access rights management (§.1.3.4)
- message subscription configuration (§.1.3.5)
- network configuration (§.1.3.6)
- report configuration (§.1.3.7)
- restriction type management (§.1.3.8)
- configuration parameters (§.1.3.9)

1.3.1. Common information

All reference data items have the following set of attributes in common for audit trail and reference data change management purposes:

TABLE 22 – COMMON INFORMATION ATTRIBUTES

Attribute	Description
Technical Identifier	This attribute is the automatically assigned primary identifier for a new item of reference data. The technical identifier in combination with a sequential revision number is used to ensure uniqueness within multiple occurrences of a single reference data item, which has undergone multiple updates.
Revision Number	Given a technical identifier, this attribute marks every update of the item's attributes so as to ensure the uniqueness of a given item which has undergone several revisions.
Deletion Status	It defines whether the reference data may be available for processing in other services or common components. The exhaustive list of possible values is as follows: • Active • Deleted The reference data item is available for processing only if its deletion status is "Active" and it approval status (see below) is "Approved".
Approval Status	The attribute defines whether the reference data object is approved or revoked by an authorised system user, is awaiting approval by the system user, or was rejected owing to business validation errors. The exhaustive list of possible values is as follows: • Approved • Awaiting Approval

Attribute	Description
	• Rejected • Revoked. In case of updates of a reference data item submitted according to the Four-Eyes principle, the modified version of the data is created with status "Awaiting Approval" and it becomes either “Approved” or “Revoked” only after the decision of the second, independent, authorised system user.

Furthermore, a System Entity Identifier attribute links each new reference data item to a Central Bank or to the CRDM Operator for data segregation purposes.

Finally, some reference data items may have one or two additional attributes specifying a validity period:

TABLE 23 – VALIDITY PERIOD ATTRIBUTES

Attribute	Description
Valid From[14]	It specifies the date (inclusive) from which the reference data item is valid.
Valid To[15]	It specifies the date (inclusive) until when the reference data item is valid.

These two attributes are indicated explicitly for the relevant entities in the data model descriptions.

To ensure the audit trail documenting events and status changes, Common Reference Data Management keeps the date and time of every change and the unique identifier of the system user requesting the change.

TABLE 24 – AUDIT TRAIL ATTRIBUTE

Attribute	Description
Timestamp	Timestamp of the change

The audit trail record has an association with the system user (or the application) responsible for the change and to the before and after images of the records, resulting from the change.

Some examples below illustrate the concepts of revision and history in combination with the status transitions related to the attribute Deletion Status and Approval Status of Reference Data objects.

Example 1: Common Reference Data Management allows the maintenance of a reference data object (not requiring a data history), i.e. some of its attributes are updated according to the Four-Eyes principle. In this scenario, the latest revision of the object with Deletion Status = “Active” and Approval Status = “Approved” is used as a baseline for the maintenance request processing.

TABLE 25 – BEFORE THE PROCESSING

Technical Identifier	Revision	Attributes	Deletion Status	Approval Status
20101968	5	ABCD	Active	Approved

[14] Opening Date for certain items.

[15] Closing Date for certain items.

When processed according to the Four-Eyes principle, the processing immediately creates a new revision of the object with an Approval Status set to “Awaiting Approval”. The status allows authorised users (i.e. the ones authorised either to approve or revoke it), to access the object for approval or revocation, but excludes this revision of the object for any other types of processing in other services or components. After the processing (and until the approval of the new revision by a second authorised user), the old revision of the object is still available for processing in other services or components.

TABLE 26 – AFTER THE FIRST STEP OF THE PROCESSING

Technical Identifier	Revision	Attributes	Deletion Status	Approval Status
20101968	5	ABCD	Active	Approved
20101968	6	XYZ	Active	Awaiting Approval

When the second user approves the maintenance, a new revision of the object is created in order to update its Approval Status and set it to "Approved". This makes the new version of the object (i.e. with the new values for the updated attributes) available for processing in other services.

TABLE 27 – AFTER THE PROCESSING

Technical Identifier	Revision	Attributes	Deletion Status	Approval Status
20101968	5	ABCD	Active	Approved
20101968	6	XYZ	Active	Awaiting Approval
20101968	7	XYZ	Active	Approved

Example 2: A duly authorised system user maintains an item of a reference data object subject to a data history and based on the Two-Eyes principle to create a new version of that item valid as of a future date.

TABLE 28 – BEFORE THE PROCESSING

Technical Identifier	Revision	Valid From	Attributes	Deletion Status	Approval Status	Ref. Tech. Identifier
20101968	3	2020-01-01	ABC	Active	Approved	19581027

In this scenario, a new version of the item is created with the specified validity period and it is linked to the same object. As a result, two different items exist for the same object, but with different validity periods.

TABLE 29 – AFTER THE PROCESSING

Technical Identifier	Revision	Valid From	Attributes	Deletion Status	Approval Status	Ref. Tech. Identifier
20101968	3	2020-01-01	ABC	Active	Approved	19581027
13021972	0	2020-03-15	XYZ	Active	Approved	19581027

Example 3: For a reference object with a data history, a duly authorised system user maintains an existing item of a reference data object for an existing validity date and based on the Two-Eyes principle.

TABLE 30 – BEFORE THE PROCESSING

Technical Identifier	Revision	Valid From	Attributes	Deletion Status	Approval Status	Ref. Tech. Identifier
20101968	3	2020-01-01	ABC	Active	Approved	19581027

In this scenario, a new revision of the item is created with the new attributes and the same validity period and it is linked to the same object. As before the processing, one single item is linked to the relevant object, but with different values of the attributes when compared to the previous revision.

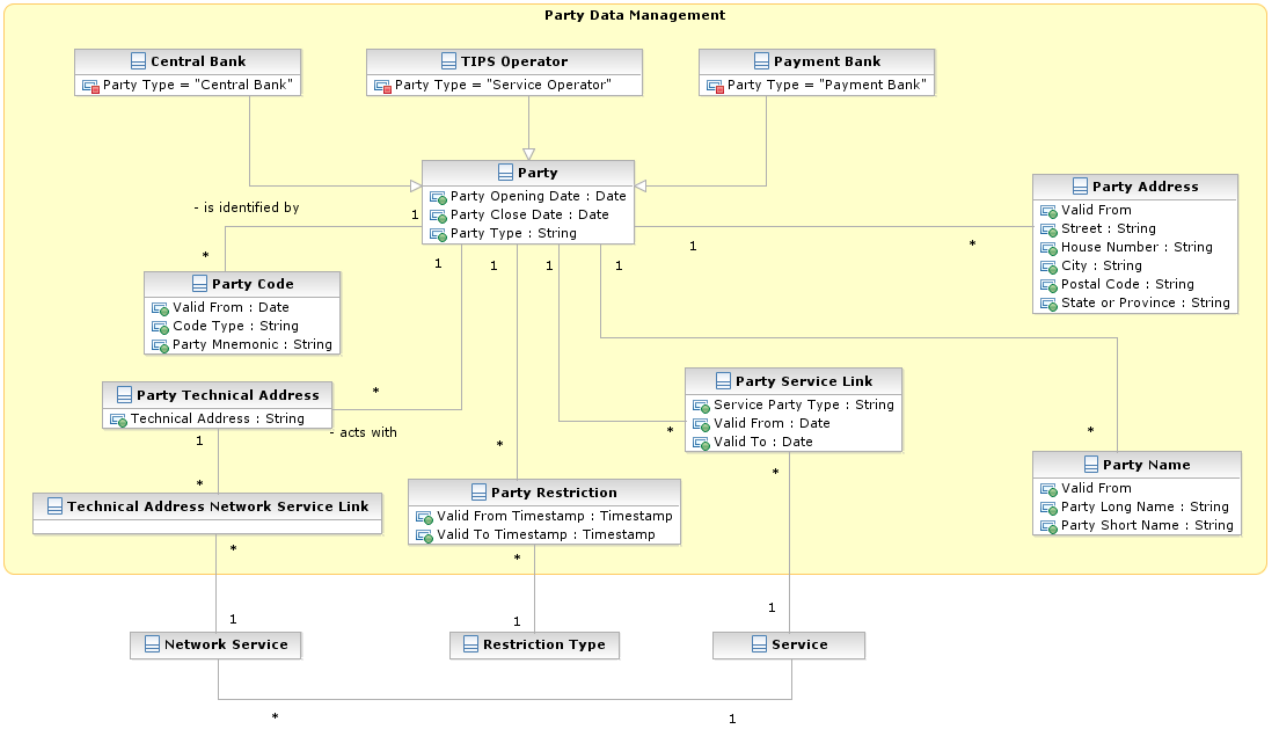
TABLE 31 – AFTER THE PROCESSING

Technical Identifier	Revision	Valid From	Attributes	Deletion Status	Approval Status	Ref. Tech. Identifier
20101968	3	2020-01-01	ABC	Active	Approved	19581027
20101968	4	2020-01-01	DEF	Active	Approved	19581027

1.3.2. Party data management

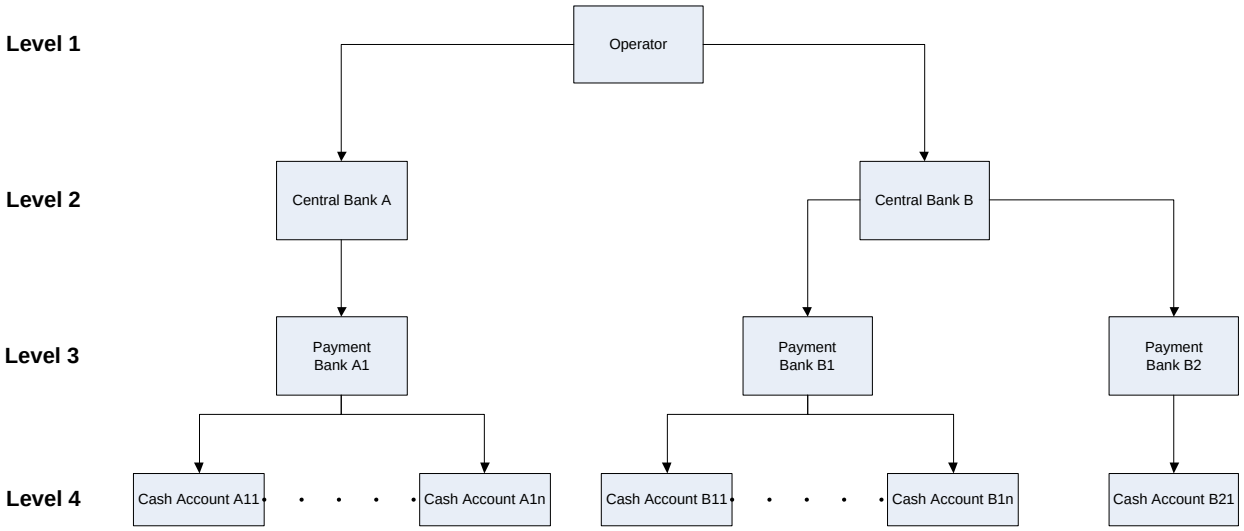
1.3.2.1. Data Model of the component

The following diagram shows the conceptual data model for Party Data Management.



1.3.2.2. Description of the component

This component allows the management of reference data related to parties, according to the hierarchical structure described in the following diagram.



The party model of CRDM is based on a hierarchical three-level structure. The CRDM Operator is the only party on the top level of the hierarchy and it is responsible for the setup of each party of the second level, i.e. each Central Bank. Similarly, each party belonging to the second level (i.e. a Central Bank) is responsible for the setup of all parties of its community (i.e. Payment Banks), represented by parties of the third level. Finally, the lowest level of the hierarchy describes the links between each payment bank and its cash account(s).

The Party Data Management component allows the managements of all the relationships between all the parties belonging to the first three levels of the hierarchy, but not the links between a party and its cash accounts. The management of these links is performed within the Cash Account Data Management component (see section 1.3.3).

In order for a Party to be active within a specific Service (e.g. TIPS), the same Party must be linked to the Service. One Party may be configured to participate in different Services and may play different roles in each Service it participates in.

As far as Payment Banks are concerned, when they are linked to the TIPS Service, the relevant Central Bank must specify whether the Payment Bank participates in TIPS as a TIPS Participant or as a reachable Party.

The following section describes all the reference data objects related to the Party Data Management component.

1.3.2.3. Description of the entities

1. Party

This entity includes all party reference data that do not require a data history, i.e. all the attributes having only one valid value for a given party, regardless the point in time taken into account.

ATTRIBUTE	DESCRIPTION
Party Opening Date	Opening date of the party.
Party Closing Date	Closing date of the party.
Party Type	It specifies a classification for the party. The exhaustive list of possible values is as follows: - Operator - Payment Bank - Central Bank

The party reference data that require a data history are the entities *Party Code*, *Party Name*, *Party Address* and *Party-Service Link*, described below. Each party is linked at least to one *Party Code*, *Party Name* and *Party Address*. One or more Party-Service Links may be defined to link a specific Party to one or more Services. In addition, each party is linked to one or many *Party Technical Addresses*.

Each *Party* may be linked to one or many *Party Restrictions*[16].

2. Party Code

This entity includes the information used to identify a *Party* from a business perspective. Each legal entity is identified in the financial market by its primary BIC, based on ISO 9362 standard. A legal entity may establish multiple legal relationships with several Central Banks in the hierarchical party model. As a consequence, a legal entity may be defined multiple times in the hierarchical party model, possibly multiple times for each legal relationship with a Central Bank. The combination of <Central Bank BIC, Party BIC> ensures the uniqueness of the *Party* in the hierarchical party model, i.e. any BIC is unique within a given *System Entity* (see section 1.3.9).

Party codes may change in time, but only one *Party code* for each *Party* must be valid at any given point in time. For this reason, it is also necessary to specify the validity period for each *Party Code*.

ATTRIBUTE	DESCRIPTION
Valid From	Starting validity date for the party code.
Code Type	Code type for the party. Currently, only BIC (as defined by ISO 9362 standard) is foreseen.
Party Mnemonic	Actual value for the party code, i.e. a BIC11 for the party.

Each *Party Code* is linked to its relevant *Party*.

[16] For each party restriction, a period of validity and a restriction type must be specified.

3. Party Name

This entity includes a Party Long Name and Party Short Name in a chronological basis. This is due to the fact that party names may change in time, but only one long name and one short name for each *Party* are valid at any given point in time.

ATTRIBUTE	DESCRIPTION
Valid From	Starting validity date for the party name.
Party Long Name	Full name of the party.
Party Short Name	Short name of the party.

Each *Party Name* is linked to its relevant *Party*.

4. Party Address

This entity includes legal address information in a chronological basis. This is due to the fact that party legal addresses may change in time, but only one legal address for each *Party* is valid at any given point in time.

ATTRIBUTE	DESCRIPTION
Valid From	Starting validity date for the party address.
Street	Name of the street for the address.
House Number	House number for the address.
City	Name of the city for the address.
Postal Code	Postal code for the address.
State or Province	State or province for the address.

Each *Party Address* is linked to its relevant *Party* and *Country*.

5. Party Technical Address

This entity includes information related to all technical addresses defined for a *Party*. Each Party Technical Address uniquely identifies a possible recipient technical address the *Party* can use for the receipt of specific messages from the different services.

ATTRIBUTE	DESCRIPTION
Technical Address	Unique technical address of a party (i.e. a distinguished name)

Each *Party Technical Address* is linked to its relevant *Party* and to one or many *Network Services* (see section 1.3.6). At any given point in time, each Party may have no more than one Technical Address linked to any TIPS Network Service.

6. Party Service Link

This entity links *Parties* to *Services* on a many-to-many basis. Each *Party-Service Link* uniquely identifies a link between a single *Party* and a single *Service*, but multiple links can be defined in order to allow the same *Party* to access different *Services* and the same *Service* to be accessed by different *Parties*.

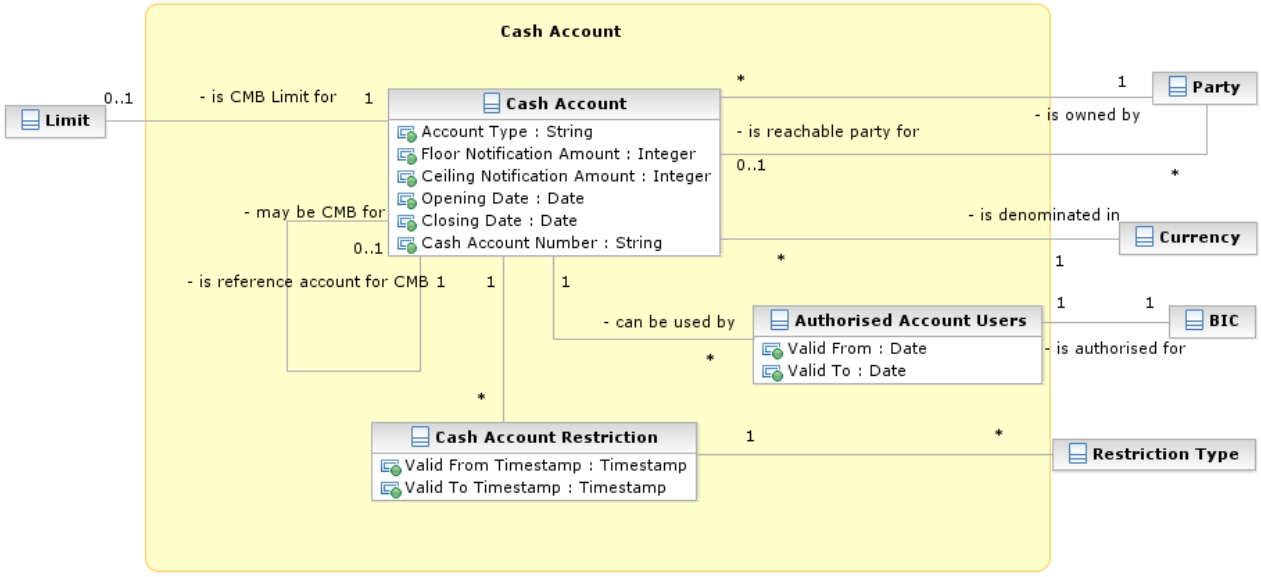
ATTRIBUTE	DESCRIPTION
Service Party Type	Service-specific classification for the Party. Certain values may be used only in conjunction with specific Services and specific Party Types defined at Party level. The exhaustive list of possible values for the TIPS Service is as follows: - TIPS Operator - TIPS Central Bank - TIPS Participant - TIPS Reachable Party
Valid From	Date from which the Party Service Link is valid.
Valid To	Date until which the Party Service Link is valid.

Each *Party Service Link* is linked to its relevant *Party* and *Service*. Due to the requirements of the TIPS participation model, multiple Payment Banks identified with the same Party Code (i.e. BIC) cannot be linked to the TIPS *Service* at the same time.

1.3.3. Cash account data management

1.3.3.1. Data model of the component

The following diagram shows the conceptual data model for Cash Account Data Management.



1.3.3.2. Description of the component

This component allows the management of reference data related to *Cash Accounts* and their links to the relevant *Limits*, *Currencies* and *Cash Accounts Restrictions*.

1.3.3.3. Description of the entities

1. Cash Account

This entity includes all *Cash Account* reference data. An authorised Central Bank user can create and maintain TIPS Accounts for its Parties. An authorised Payment Bank user (corresponding to a TIPS Participant) can create and maintain TIPS Credit Memorandum Balances (CMB) on the TIPS Accounts owned by its Party.

ATTRIBUTE	DESCRIPTION
Cash Account Number	It specifies the unique cash account number.
Floor Notification Amount	It specifies the lower threshold for notifying the cash manager.
Ceiling Notification Amount	It specifies the upper threshold for notifying the cash manager.
Account Type	It specifies a classification for the cash account. The exhaustive list of possible values is as follows: - TIPS Account - TIPS Transit Account - TIPS Credit Memorandum Balance A Transit Account per currency exists in TIPS and it belongs to a Central Bank. The Transit Account for euro belongs to the European Central Bank.
Opening Date	Opening date of the cash account.
Closing Date	Closing date of the cash account.

Each *Cash Account* is linked to its relevant owner *Party* and *Currency*. In addition, it may be linked to one or many *Cash Account Restrictions*[17]. *Cash Accounts* with type equal to "TIPS Credit Memorandum Balance" are additionally linked to a Cash Account with type equal to "TIPS Account". Finally, each TIPS Account may be linked to one or many BICs defined as "Authorised Account Users"[18]. Each TIPS Credit Memorandum Balance may be linked to only one "Authorised Account User".

2. Limit

This entity includes all reference data related to *Limits* defined on TIPS Credit Memorandum Balances. Common Reference Data Management shall allow a Payment Bank (linked to the TIPS

[17] For each cash account restriction, a period of validity and a restriction type must be specified.

[18] For each Authorised Account User a period of validity must be specified.

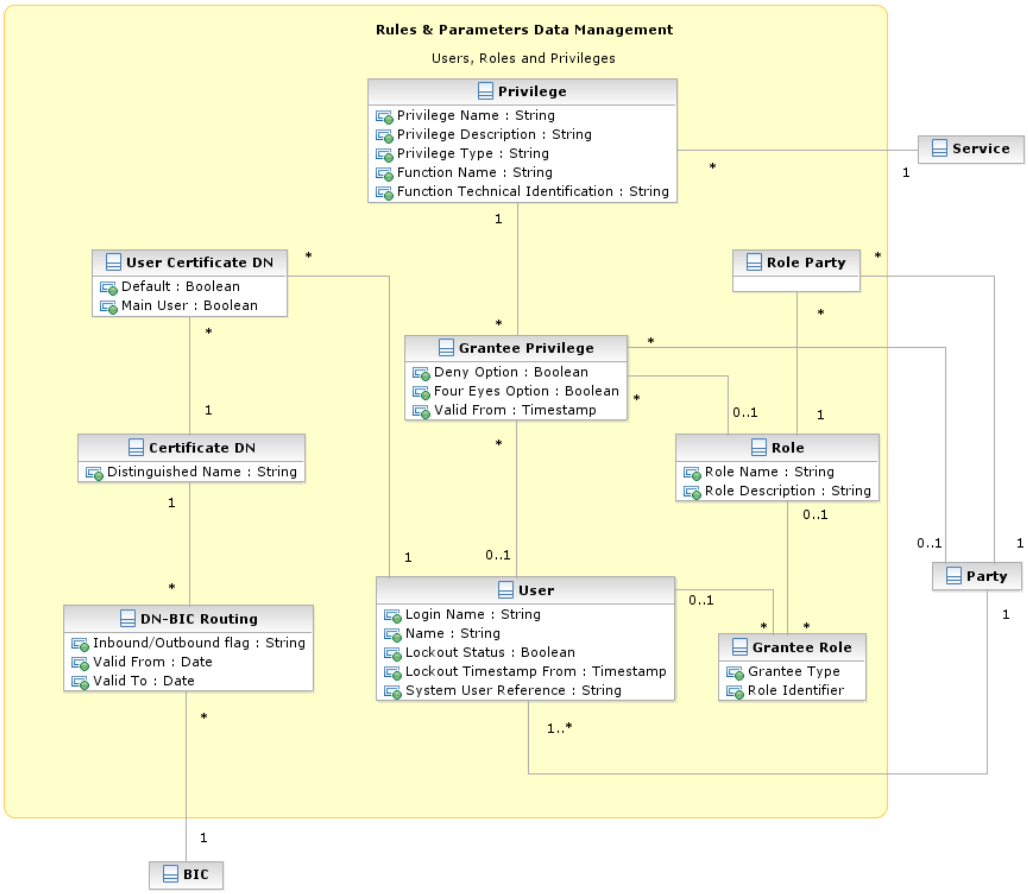
Service as a TIPS Participant) to define and maintain credit limits for their individual customers related to the usage of a TIPS Credit Memorandum Balance defined on the TIPS Account of said TIPS Participant.

ATTRIBUTE	DESCRIPTION
Limit Type	It specifies a classification for the limit. The exhaustive list of possible values is as follows: - TIPS CMB Limit
Limit Amount	It specifies the value set for the limit amount. If set to zero, the relevant Cash Account (i.e. TIPS CMB) cannot be debited.
Valid From Timestamp	It specifies the date from which the limit is valid.

Each *Limit* is linked to its relevant *Cash Account*, whose type must be equal to "TIPS Credit Memorandum Balance".

1.3.4. Access rights management

The following diagram shows the conceptual data model for *Users*, *Roles* and *Privileges* management.



Each function of any given *Service* is linked to a *Privilege* (i.e. the privilege that allows triggering this function), which is the means used for granting (or denying) access to functions (and possibly data) to selected *Parties*, *Users* and *Roles*.

Privileges are created and maintained by the CRDM Operator. *Privileges* can be granted or revoked by a system administrator. A set of *Privileges* can be grouped into a *Role*. Each *Role* can be assigned one or more *Privileges*. Each *Party* and *User* can be assigned several *Privileges,* optionally through one or more *Roles*. *Roles* are created and managed by the CRDM Operator and Central Bank system administrators. The management of *Roles* includes both their maintenance (i.e. update and logical deletion) and the possibility to grant or revoke other *Privileges*. Central Banks may configure specific roles to be granted to their own Payment Banks (i.e. Participants and Reachable Parties), in order to grant them with proper access to functions. In turn, system administrators of Payment Banks can use *Roles* and *Privileges* granted by the relevant Central Bank in order to assign proper access rights to their own system users.

Based on the granted set of *Roles* and *Privileges*, all system users are authorised to input their own reference data objects and to access and maintain them, i.e. to create new objects or to update or delete already existing objects. For each system user, the specific set of available functions and data are determined by the relevant access rights.

1. User

This entity includes all reference data for *Users* . This concept includes not only users interacting with the different services in U2A mode and triggering functions via ad hoc screens, but also connecting through the DMT and using functions via DMT files.

ATTRIBUTE	DESCRIPTION
Login Name	Username to be provided for authentication.
Name	Full name of the user.
Lockout Status	Boolean attribute specifying whether the user is blocked from logging.
Lockout Timestamp From	Timestamp specifying the date and the time from which the user is locked out.
System User Reference	The unique system user reference associated to the user.

Users are linked to the *Party* they belong to and to one or many *Roles*. Each User can be linked to one or many *Certificate DNs*[19].

2. Certificate DN

This entity includes all reference data for *Certificate DN* .

[19] The link between a User and a Certificate DN also contains a "Default" flag specifying whether the Certificate DN identifies the default User associated to the related Distinguished Name and a "Main User" flag specifying that it is the single User enabled for the TIPS Service.

ATTRIBUTE	DESCRIPTION
Distinguished Name	It specifies the distinguished name.

Each *Certificate DN* can be linked to one or many *Users*[20].

3. Privilege

This entity includes all reference data for *Privileges*.

ATTRIBUTE	DESCRIPTION
Privilege Name	Name of the privilege.
Privilege Description	Description of the privilege.
Privilege Type	It specifies a classification for the privilege. The exhaustive list of possible values is as follows: - System, i.e. the associated function does not apply to a specific static data object type. - Object, i.e. the associated function applies to a specific static data object type.
Function Name	Name of the function associated to the privilege.
Function Technical Identification	It specifies all the data needed in order to identify and to trigger the function, e.g. the type of function (query, report, etc.), the type of interaction (push, pull, interactive), the set of required input parameters for the function and so forth.

Each *Privilege* can be granted to one or many *Roles, Users* or *Parties,* and is linked to a single *Service*. When granting a *Privilege* to a *Role*, *User* or *Party,* the following Boolean attributes are set:

- Deny Option, to specify whether the associated function is allowed or explicitly denied to the grantee;
- Administration Option, to specify whether the grantee of the privilege is allowed to grant the same privilege to another *Party*, *User* or *Role;*
- Four-Eyes Option, to specify whether the grantee of the privilege is allowed to use the associated function according to the Two-Eyes or Four-Eyes principle (this attribute is relevant only for privileges related to functions that can be used both according to the Two-Eyes and to the Four-Eyes principle) .

4. Role

This entity includes all reference data for *Roles*.

[20] The link between a User and a Certificate DN also contains a "Default" flag specifying whether the Certificate DN identifies the default User associated to the related Distinguished Name and a "Main User" flag specifying that it is the single User enabled for the TIPS Service.

ATTRIBUTE	DESCRIPTION
Role Name	Name of the role.
Role Description	Description of the role.

Each *Role* can be linked to one or many *Privileges*. Moreover, each *Role* can be linked to many *Parties* and *Users*.

System administrators can grant Roles to *Parties* and *Users* in order to set up their change approval configuration, i.e. the applicable combination of change type (e.g. create, update, delete) and update type (i.e. Two-Eyes mode or Four-Eyes mode) for all the relevant functions and reference data objects.

5. DN-BIC Routing

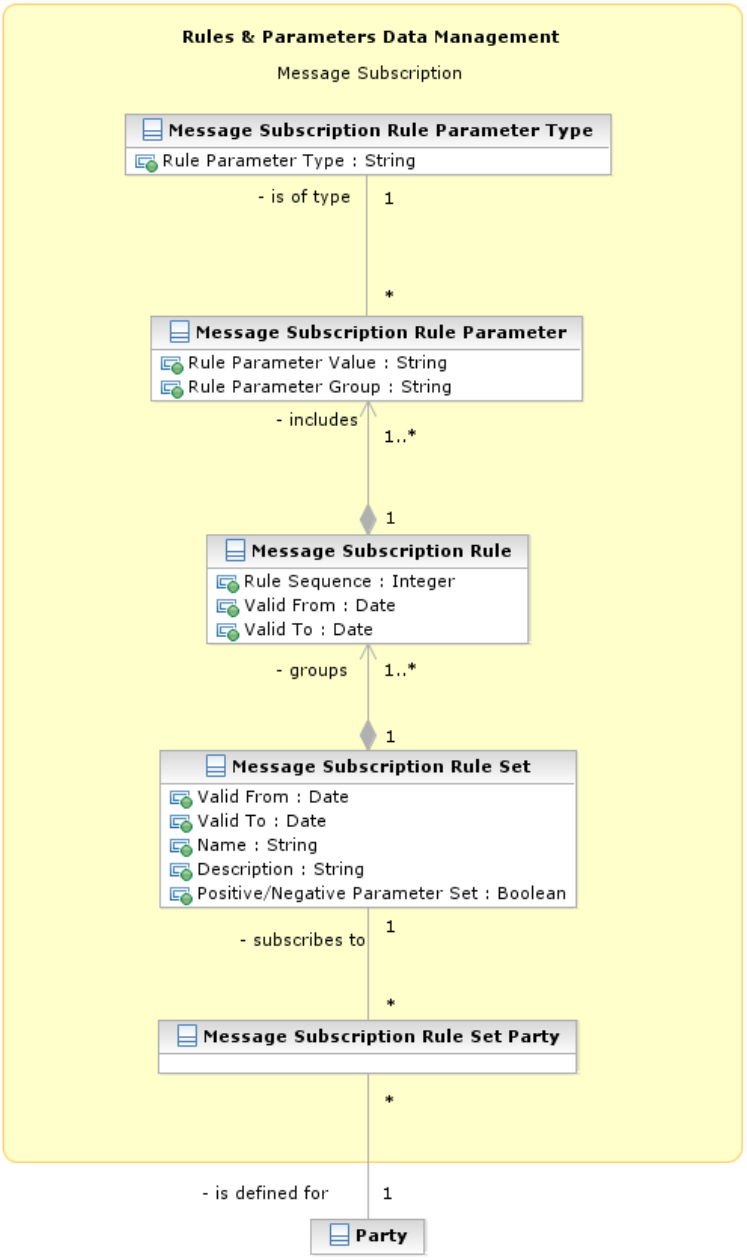
This entity includes all reference data for DN-BIC Routing, for inbound and outbound communication. In the former case, different DNs can be linked to different BICs and vice versa. In the outbound case, the same BIC can only be linked to a single DN. However different BICs can still be linked to the same DN.

ATTRIBUTE	DESCRIPTION
Inbound/Outbound flag	Attribute specifying whether the routing relationship is for inbound or outbound communications. If set to Outbound, a DN can only be linked to no more than one BIC.
Valid From	Date from which the DN-BIC Routing is valid.
Valid To	Date until which the DN-BIC Routing is valid.

Each *DN-BIC Routing entry* can be linked to one or many *Certificate DNs and one or many BICs.*

1.3.5. Message subscription configuration

The following diagram shows the conceptual data model for *Message Subscription* management.



Message Subscription allows *Parties* to configure the specific set of messages they want to receive from a given *Service*.

Each *Party* can set up several *Message Subscription Rule Sets*. Each *Message Subscription Rule Set* defines the messages one or many interested *Parties* receive via a sequence of *Message Subscription Rules*. Each *Message Subscription Rule* specifies the parameters (e.g. message type, cash account) that have to be taken into account to identify the messages to be sent to the interested *Parties*.

1. Message Subscription Rule Set

This entity defines the set of message subscription rules defined by each *Party*.

ATTRIBUTE	DESCRIPTION
Valid From	It specifies the date from which the rule set is valid.
Valid To	It specifies the date to which the rule set is valid.
Name	The name assigned to the message subscription rule set.
Description	It represents the description assigned to the message subscription rule set.
Positive/Negative Parameter Set	It specifies whether the message subscription rule set must be used in positive or negative way.

Each *Message Subscription Rule Set* is linked to the relevant *Party*, to one or many interested *Parties* (i.e. the parties that receive all the messages identified by the message subscription rule set), and to a set of *Message Subscription Rules*.

2. Message Subscription Rule

This entity defines the *Message Subscription Rules* defined by each *Party*.

ATTRIBUTE	DESCRIPTION
Rule Sequence	It specifies the order in which the rule is processed within the relevant rule set.
Valid From	It specifies the date from which the rule is valid.
Valid To	It specifies the date to which the rule is valid.

Each *Message Subscription Rule* belongs to a single *Message Subscription Rule Set* and it is linked to a set of *Message Subscription Rule Parameters*.

3. Message Subscription Rule Parameter

This entity includes the message subscription rule parameters defined within each message subscription rule.

ATTRIBUTE	DESCRIPTION
Rule Parameter Group	It specifies the group of the rule parameter. All the groups within a message subscription rule include the same number of rule parameters. A rule is matched when all the rule parameters of at least one of its groups are matched.
Rule Parameter Value	It specifies a valid value for the rule parameter.

Each *Message Subscription Rule Parameters* belongs to a single *Message Subscription Rule* and it is linked to a specific *Message Subscription Rule Parameter Type*.

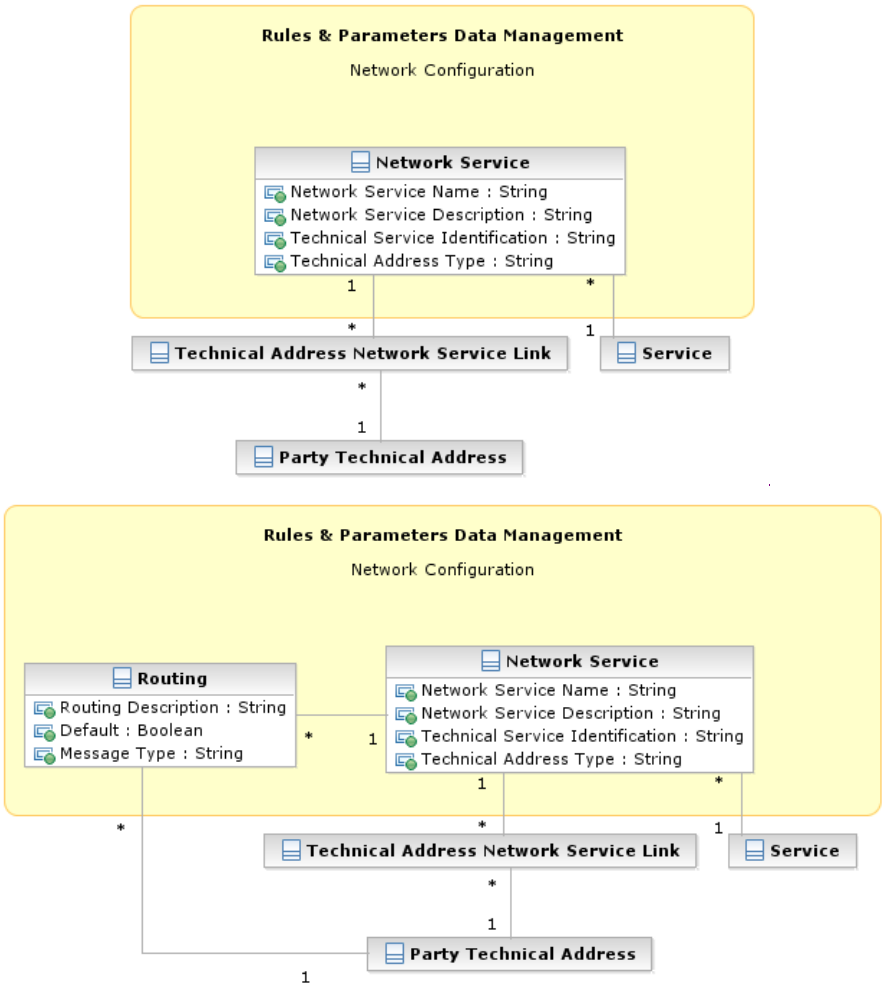
4. Message Subscription Rule Parameter Type

This entity defines all message subscription rule parameters types.

ATTRIBUTE	DESCRIPTION
Rule Parameter Type	It specifies a classification for the message subscription rule parameters. The exhaustive list of possible values is as follows: - Message type - Cash account number

1.3.6. Network configuration

The following diagram shows the conceptual data model for Network Configuration.



Network Configuration allows parties to configure routing information that the various *Services* use to deliver outgoing messages to them.

1. Network Service

This entity stores reference data of all network services available in the different *Services*.

ATTRIBUTE	DESCRIPTION
Network Service Name	Name of the network service.
Network Service Description	Description of the network service.
Technical Service Identification	It specifies all the data needed in order to identify and to use a network service[21].
Technical Address Type	It specifies the type of technical address for the network service (e.g. BIC, Distinguished Name, IP address).

Each *Network Service* is linked to all the *Party Technical Addresses* it provides and to the *Service* it refers to.

2. Routing

This entity allows Parties to configure routing information that TIPS uses to deliver outgoing messages to them. Each Party can define a default routing configuration that is used when no specific routing conditions are defined for the same party and for a specific outgoing message.

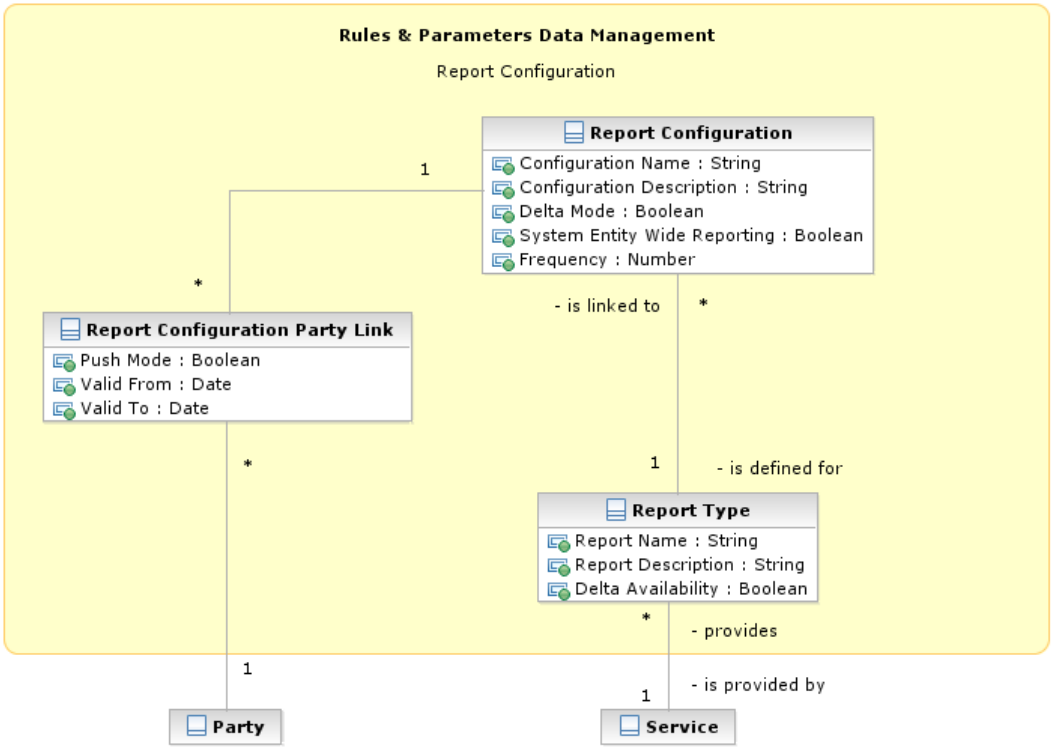
ATTRIBUTE	DESCRIPTION
Routing Description	Description of the routing configuration.
Default	Identifies the default routing configuration for a given Party.
Message Type	Specifies the message type for which a specific routing configuration applies.

Each *Routing* configuration is linked to the relevant *Party Technical Address* and *Network Service*.

1.3.7. Report configuration

The following diagram shows the conceptual data model for report configuration.

[21] The actual data to be stored for the technical identification of a network service is clarified during the detailed specification phase.



Report configuration allows parties to configure the specific set of reports they want either to receive (push mode) or to download (pull mode) from the various *Services*.

1. Report Type

This entity defines all types of reports available in the different *Services*.

ATTRIBUTE	DESCRIPTION
Report Name	Name of the report type.
Report Description	Description of the report type.
Delta Availability	Boolean attribute specifying whether the report is also available in delta mode, i.e. with the possibility for the recipient to get only the changes since the last time the recipient got the same report.

Each *Report Type* and can be referenced by many *Report Configurations* and is linked to one or more *Services*.

2. Report Configuration

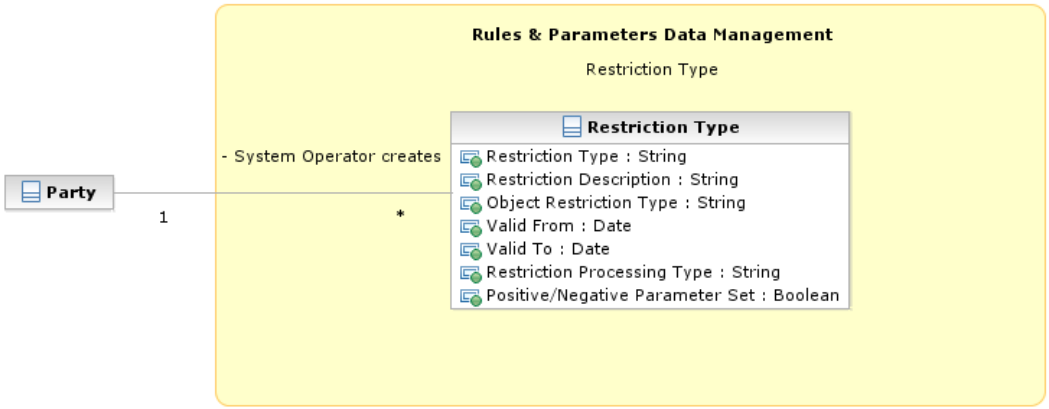
This entity stores all reference data for report configurations. Each *Report Configuration* specifies a type of report, its data scope (i.e. full or delta report), the set of parties entitled to get said type of report and the mode they get it (i.e. push or pull).

ATTRIBUTE	DESCRIPTION
Configuration Name	Name of the report configuration.
Configuration Description	Description of the report configuration.
Delta Mode	Boolean attribute specifying whether the recipient gets the report linked to the report configuration in delta mode or in full mode.
System Entity Wide Reporting	Boolean attribute specifying whether the recipient gets the report for data belonging to the entire system entity.
Frequency	Frequency in hours for the generation of the delta reports. Not relevant for full reports, which will be generated daily and cover a 24-hour period. The exhaustive list of possible values is as follows: - 3 hours - 6 hours - 12 hours

Each *Report Configuration* is linked to the relevant *Report Type* and to one or many *Parties* entitled to get the same *Report Type*[22].

1.3.8. Restriction type management

The following diagram shows the conceptual data model for *Restriction Types* management.



It is possible for the CRDM Operator to define restriction types. A restriction type is a set of attributes that define specific processing characteristics for *Parties and Cash Accounts*.

1. Restriction Type

This entity includes all the information concerning the harmonised restriction types defined and maintained by the CRDM Operator and available to all Parties.

22 For each of these links a Boolean value specifies whether the party receives its report in push mode or if it downloads it in pull mode. A validity period can be defined by giving a valid from and valid to date.

ATTRIBUTE	DESCRIPTION
Restriction Type	It specifies a code defined by the CRDM Operator to identify the restriction.
Restriction Description	Description of the restriction.
Valid From	It specifies the date from which the restriction type is valid.
Valid To	It specifies the date to which the restriction type is valid.
Object Restriction Type	It specifies a classification for the object type on which the restriction applies. The exhaustive list of possible values is as follows: - Party - Cash Account
Restriction Processing Type	It specifies a classification for the type of processing that shall apply for the restriction. The exhaustive list of possible values is as follows: - Blocking: blocking of a party or cash account from settlement
Positive / Negative Parameter Set	It specifies whether the rules of the restriction type represent a positive or negative set of parameters. A positive parameter set shall specify the conditions requiring the system to apply the restriction. A negative parameter set shall specify the conditions for which the system shall not apply the restriction.

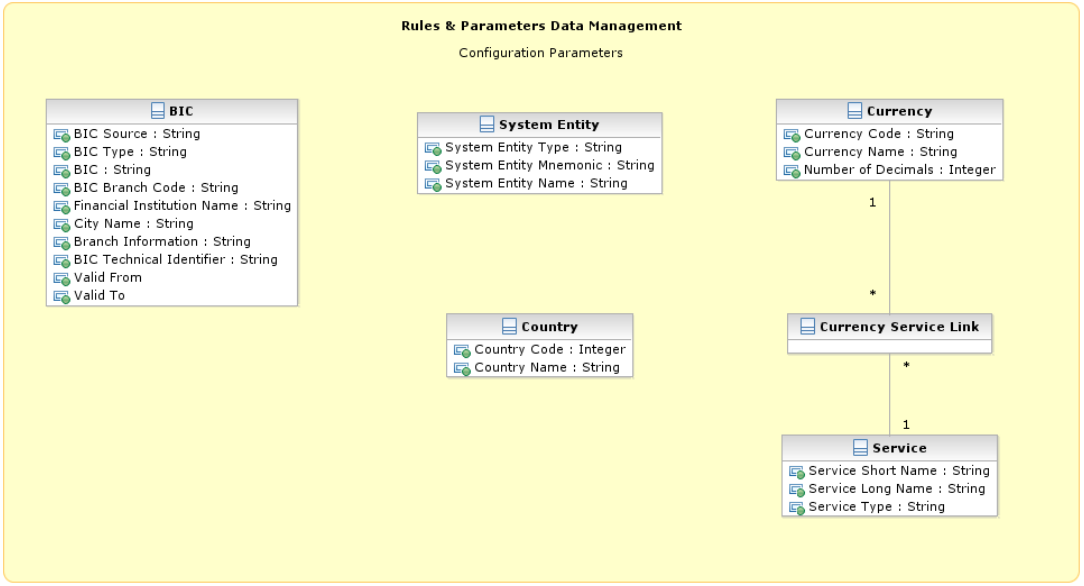
Each *Restriction Type* is linked to the specifying *Party* (i.e. the CRDM Operator).

1.3.9. Configuration parameters

This section describes all reference data concerning the following rules and parameters:

- Country;
- Currency;
- System entity;
- BIC Directory;
- Service.

The following diagram shows the conceptual data model for Configuration Parameters management.



1. Country

This entity includes all reference data related to countries defined in the different Services.

ATTRIBUTE	DESCRIPTION
Country Code	Numeric code of the country according to the ISO 3166-1 standard.
Country Name	Name of the country according to the ISO 3166-1 standard.

2. Currency

This entity includes all reference data related to *Currencies* defined in the different Services .

ATTRIBUTE	DESCRIPTION
Currency Code	Unique code of the currency according to the ISO 4217 standard.
Currency Name	Name of the currency.
Number of Decimals	Number of decimals in which the currency is expressed.

Each *Currency* is linked to one to many *Services* (which allow settlement for that *Currency*).

3. System Entity

This entity includes all reference data for system entities. System entities define the entities (i.e. Central Banks and the CRDM Operator) by which data is segregated.

ATTRIBUTE	DESCRIPTION
System Entity Type	It specifies a classification for the system entity. The exhaustive list of possible values is as follows: - Operator - Central Bank (CB)
System Entity Mnemonic	It specifies a unique short code used to identify the system entity.
System Entity Name	It specifies the full name of the system entity.

Every reference data entity has an association with the relevant *System Entity*, to inherit the System Entity Identifier attribute.

Each *System Entity* is linked to its relevant *Party*, i.e. to the CRDM Operator or the Central Bank defined as a *Party* and corresponding to the same *System Entity*.

4. BIC Directory

This entity includes all the information needed to identify the legal entities to which SWIFT assigned the BIC that is used to validate the input BICs as *Party* identifiers. Common Reference Data Management supports the automatic loading and update of the *BIC Directory* based on the BIC Data+.

ATTRIBUTE	DESCRIPTION
BIC Source	It specifies a classification for the BIC source. The exhaustive list of possible values is as follows: - Manual input - Automatic loading
BIC Type	It specifies a classification for the BIC type. The exhaustive list of possible values is as follows: - Official BIC - Internal technical BIC
BIC	8-character BIC, consisting of the bank code (financial institution), country code and location code.
BIC Branch Code	3-character branch code for the financial institution.
Financial Institution Name	Three text fields with a length of 35 characters each to store the name of the financial institution.
City Name	35-character name of the city in which the financial institution resides.
Branch Information	Two text fields with a length of 35 characters each to identify the branch of the financial institution.

ATTRIBUTE	DESCRIPTION
BIC Technical Identifier	This attribute specifies the unique technical identifier of a BIC.
Valid From	It specifies the date from which the BIC is valid.
Valid To	It specifies the date to which the BIC is valid.

5. Service

This entity stores information on all the different *Services* that rely on reference data stored in the Common Reference Data Management.

ATTRIBUTE	DESCRIPTION
Service Short Name	Identification of the Service.
Service Long Name	Extended identification of the Service.
Service Type	Defines whether the Service is a Service that belongs to the Single Shared Platform or not. The exhaustive list of possible values follows: - Internal (i.e. service belonging to the Eurosystem Market Infrastructures) - External

Each Service may be linked to one or multiple *Currencies*.

1.4. CRDM Features

1.4.1. Concept

The Common Reference Data Management common component allows duly authorised users to create and maintain reference data objects used by TIPS. Common Reference Data Management objects specify reference data for the configuration of parties, cash accounts and TIPS rules and parameters.

1.4.2. Overview

The Common Reference Data Management common component is in charge of executing reference data maintenance instructions for the creation or the maintenance of reference data objects.

Duly authorised users belonging to CBs, payment banks and to the CRDM Operator can trigger the Common Reference Data Management common component according to their own specific access rights, i.e. using the functions and maintaining the common reference data objects they have been granted.

Duly authorised users of the CRDM Operator are responsible for system configuration tasks and for the management of common reference data for CBs. These users can also act on behalf of other CRDM Actors in order to perform some specific actions or within some pre-defined contingency scenarios.

The Common Reference Data Management common component executes immediately all reference data maintenance instructions. However, the related reference data changes become effective in TIPS in a deferred way, by means of a daily reference data propagation process. The process takes place every business day at 17:00 CET, so to ensure a smooth and complete reference data propagation before TIPS receives the notification that a new business day is starting (see also section 1.5.4 of TIPS UDFS for more information).

All common reference data objects can be created and maintained in U2A mode, whereas only a sub-set of them can be maintained also through the DMT (See section 1.4.3.2). All reference data changes performed in U2A mode can be executed either in Two-Eyes or in Four-Eyes mode. Duly authorised users can specify the applicable mode for the functions and the common reference data objects they manage (See section 1.2.2).

Versioning facilities and validity periods allow the implementation of data revision and data history features, in order to keep track of all past data changes, to enter changes meant to become effective as of a future date and to define common reference data objects with limited or unlimited validity.

1.4.3. Common reference data maintenance process

1.4.3.1. Common reference data objects

Duly authorised users manage common reference data by creating and maintaining common reference data objects. A common reference data object is a set of logically related, self-consistent information. Parties and cash accounts are examples of common reference data objects. The following

table provides the exhaustive list of common reference data objects defined in the Common Reference Data Management common component and the CRDM Actors that are responsible for their management, i.e. for creating and maintaining them:

TABLE 32 - COMMON REFERENCE DATA OBJECTS

AREA	OBJECT	RESPONSIBLE CRDM ACTORS [23, 24]
Party	Party	CRDM Operator, Central Bank
	Party Service Link	CRDM Operator, Central Bank
Cash account	Cash account	All[25]
	Limit	Payment Bank
	Authorized Account User	Payment Bank
Access rights management	User	All
	Role	CRDM Operator, Central Bank
	Privilege	CRDM Operator
	Certificate DN	All
	User-Certificate DN Link	All
	Role User[26]	All
	Role Party[27]	CRDM Operator, Central Bank
	Grantee Privilege[28]	CRDM Operator, Central Bank, Payment Bank
Message subscription configuration	Message subscription rule	Central Bank, Payment Bank
	Message subscription rule set	Central Bank, Payment Bank
Network configuration	DN BIC Routing	Payment Bank
	Network service	CRDM Operator
	Technical address Network service link	CRDM Operator, Central Bank
	Routing	CRDM Operator, Central Bank, Payment Bank

23 "All" indicates that all types of CRDM Actors (CRDM Operator, CBs, Payment Banks) have the ability to manage the object type.

24 The Actor types listed for each function refer to the default responsible Actor in normal operating conditions. However it is possible for the CRDM Operator to act on behalf of Central Banks (and of Payment Banks, upon request of the relevant Central Bank) and for the Central Banks to act on-behalf of their Payment Banks, under well-defined contingency scenarios.

25 The Cash Account object includes both TIPS Accounts and TIPS CMBs. In this respect, Payment Banks may only create and maintain TIPS CMBs, whereas Central Banks create and maintain TIPS Accounts and may create and maintain TIPS CMBs on behalf of their Payment Banks.

26 This object is related to the granting/revoking of Roles to/from Users.

27 This object is related to the granting/revoking of Roles to/from Parties.

28 This object is related to the granting/revoking of Privileges to/from Roles, Parties and Users.

AREA	OBJECT	RESPONSIBLE CRDM ACTORS [23, 24]
Report configuration	Report configuration	Payment Bank
Restriction type management	Restriction type	CRDM Operator
Configuration parameters	Country	CRDM Operator
	Currency	CRDM Operator
	Currency Service Link	CRDM Operator
	System entity	CRDM Operator
	BIC directory	CRDM Operator
	Service	CRDM Operator

A common reference data object consists of one or more classes of information. For example, a party is a common reference data object, consisting of the following classes of information:

- Party;
- Party code;
- Party name;
- Party address;
- Party technical address.

Each class of information includes a defined set of attributes. For example, the class of information party name of the common reference data object party includes the following attributes:

- The long name of the party;
- The short name of the party;
- The starting validity date of the party name.

The Common Reference Data Management common component provides functions to maintain all common reference data objects (See section 1.4.3.2). Each maintenance operation on a common reference data object results in a new version of the same object. Each version of a common reference data object is called a revision of the object. Consequently, at any point in time, the Common Reference Data Management common component stores one or many revisions of each common reference data object, more precisely only one revision for newly created objects that were never maintained after their creation and N revisions for objects that were maintained N-1 times after they were created. The first revision of each common reference data object includes all the attribute values provided at creation time. After that, each maintenance request successfully processed creates a new revision for the object. This means that each revision may entail changes of many attributes of the same common reference data object at the same time. A new revision is also created when deleting and restoring a common reference data object.

Some classes of information are subject to data history, i.e. classes of information having multiple occurrences with continuous and non-overlapping validity periods. For example, the classes of information party name and party code of the common reference data object party can be subject to

data history. In fact, they include a Valid From attribute which determines the valid value of these classes of information at any given point in time.

1.4.3.2. Reference data maintenance types

The Common Reference Data Management common component allows a duly authorised user to perform the following types of reference data maintenance operations on common reference data objects:

- Create. It creates a new common reference data object.
- Update. It updates an already existing common reference data object. It is possible, with a single update, to create, update or delete one or many classes of information of a common reference data object at the same time.
- Delete. It deletes an already existing common reference data object. Deletion is always logical and not physical. Physical deletion is performed automatically by the Common Reference Data Management common component when performing the purge process following the archiving process (See section 1.4.3.4).
- Restore[29]. It reactivates a previously deleted common reference data object, i.e. it updates the approval status of this object from deleted to active.

Besides these operations, the Common Reference Data Management common component provides some specific types of reference data maintenance operations for the configuration of access rights (See section 1.2.2 for a detailed description of these operations).

CRDM allows all reference data maintenance types on all reference data objects in U2A mode, whereas it allows them only on a subset of reference data objects through the DMT. The following table shows the exhaustive list of all the available reference data maintenance types that are possible in the DMT:

TABLE 33 – MANAGEMENT OF REFERENCE DATA OBJECTS IN DMT

AREA	OBJECT	DMT FUNCTION
Party data management	Party	Create
	Technical address network service link	Create
Cash account data management	Cash account	Create
	Authorised account user	Create
	Limit	Create
Access rights management	User	Create
	Role	Create, Grant

29 This function is available in U2A mode only and it is granted, for each object, with the system privilege that allows deleting the same object as well.

AREA	OBJECT	DMT FUNCTION
	Privilege	Grant
	Certificate DN	Create
	User-Certificate DN Link	Create
Message subscription configuration	Message subscription rule set	Create
	Message subscription rule	Create
Report configuration	Report configuration	Create

1.4.3.3. Validity of common reference data objects

Some common reference data objects include attributes limiting the validity period of these objects. For example, each Party service link, which defines the participation of a given payment bank in TIPS, includes two attributes specifying the date from which and the date to which the link is valid, i.e. the period in which said payment bank can operate in TIPS. Between the creation date and the deletion date of the link, but outside the validity period just defined, the payment bank is not allowed to operate in TIPS, even though it is active in the Common Reference Data Management repository and it can be queried and maintained by a duly authorised user.

The Common Reference Data Management common component makes a distinction between the following two categories of common reference data objects:

- Common reference data objects with unlimited validity period,
- Common reference data objects with limited validity period.

The following table shows the exhaustive list of all the common reference data objects with unlimited validity period:

TABLE 34 - COMMON REFERENCE DATA OBJECTS WITH UNLIMITED VALIDITY PERIOD

AREA	OBJECT
Access rights management	User
	Role
	Privilege
	Certificate DN
	User-Certificate DN Link
	Role User Link
	Role Party Link
	Privilege Role Link
Network configuration	Network service

AREA	OBJECT
	Technical Address Network Service Link
	Routing
Configuration parameters	Country
	Currency
	System entity
	Service
	Currency Service Link

This type of common reference data object starts being valid immediately after it has been created. Similarly, a common reference data object with unlimited validity period may be immediately updated or deleted by a duly authorised user. However, in both cases the reference data change, i.e. the creation of a new object or the update or deletion of an already existing object is made effective in TIPS only by means of the daily reference data propagation process.

Regardless of the way common reference data object with limited validity period are propagated to TIPS, between the creation date and the deletion date of this object, it is active in the Common Reference Data Management common component and it can be queried and maintained by a duly authorised user.

Common reference data objects with limited validity period can be updated either intraday, i.e. while they are in their validity period or as of a future date, i.e. before they become valid.

The following table shows the exhaustive list of all the common reference data objects with limited validity period, with the columns on the right specifying the possible maintenance operations depending on the validity period:

TABLE 35 - COMMON REFERENCE DATA OBJECTS WITH LIMITED VALIDITY PERIOD [30]

AREA	OBJECT	CREATION	UPDATE	DELETION
Party	Party	Validity date may take the value of the current date.	May take effect on the current date [31].	May be performed only on objects that are not valid on the current date.
	Party Service Link	Validity date may take the value of the current date.	May take effect on the current date.	May be performed only on objects that are not valid on the current date.
Cash account	Cash account	Validity date may take the value of the current date.	May take effect on the current date.	May be performed only on objects that are not valid on the current date.
	Authorised Account User	Validity date may take the value of the current date.	May take effect on the current date.	May be performed only on objects that are not valid on the current date.
	Limit	Validity date may take the value of the current date.	May take effect on the current date.	May be performed only on objects that are not valid on the current date.
Message subscription	Message subscription rule set	Validity date may take value of the next business day at the earliest.	May take effect only as of a future date.	May be performed only on objects that are not valid on the current date.

30 In the following table, the columns 'Creation/Update/Deletion' clarify whether it is possible to perform a given maintenance operation on each object with immediate effect in the CRDM. For example, if a user updates an object on which updates "may take effect on the current date", they are able, should they wish to do so, to perform changes that become immediately valid in the CRDM. On the contrary, if the update "may take effect only as of a future date" then it is not possible to perform intraday changes on the object. The possibilities described in the table represent the level of flexibility offered to the user. Within these limitations, the user decides exactly when a specific modification should take effect.

31 This is not applicable to the Party Code, which cannot be updated if it is currently active.

AREA	OBJECT	CREATION	UPDATE	DELETION
	Message subscription rule	Validity date may take value of the next business day at the earliest.	May take effect only as of a future date.	May be performed only on objects that are not valid on the current date.
Report configuration	Report configuration	Validity date may take value of the next business day at the earliest.	May take effect only as of a future date.	May be performed only on objects that are not valid on the current date.
Restriction type management	Restriction type	Validity date may take value of the next business day at the earliest.	May take effect only as of a future date.	May be performed only on objects that are not valid on the current date.
Network configuration	DN-BIC Routing	Validity date may take the value of the current date.	May take effect on the current date.	May be performed only on objects that are not valid on the current date.
Configuration parameters	BIC Directory	Validity date may take the value of the current date.	May take effect on the current date.	May be performed only on objects that are not valid on the current date.

For parties and cash accounts the validity period is defined by an Opening Date and a Closing Date attribute. Between these two dates the common reference data object, i.e. the party or the cash account, is valid, meaning that TIPS can use it for processing (e.g. for settlement purpose). Outside this period, the common reference data object can only be queried or maintained in the Common Reference Data Management common component by a duly authorised user.

1.4.3.4. Common reference data archiving and purging

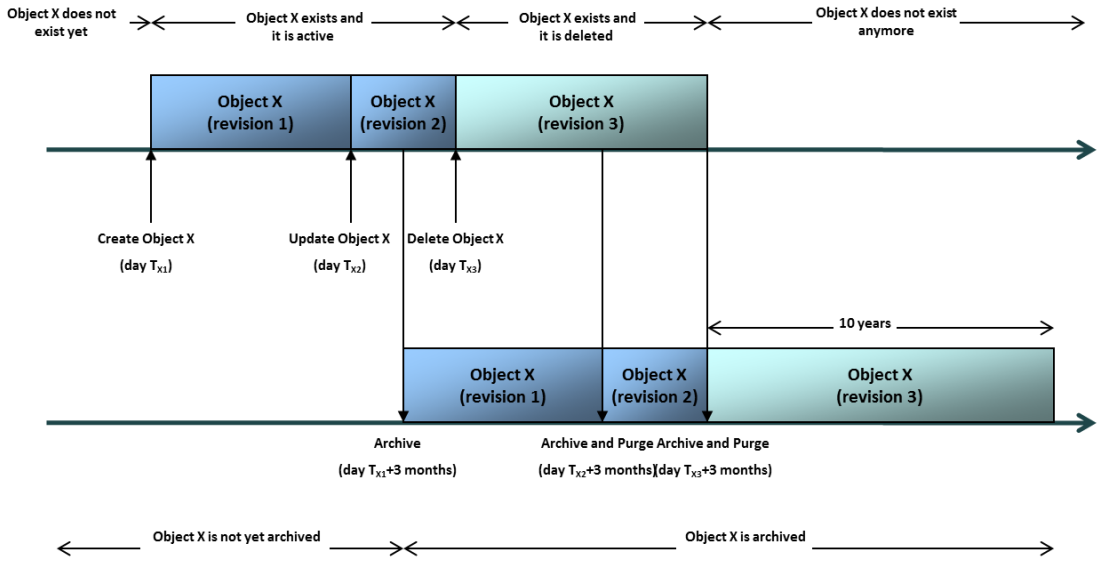
The following section refers to the implementation of the archiving and purging functionalities in the full CRDM. In its current version, the retention period for archiving/purging (what is described as three calendar months below) will be extended indefinitely, resulting in data not being archived/purged. For additional information, see section 1.7.3.

The Common Reference Data Management archives new reference data and their changes three calendar months after they were created or changed. The Common Reference Data Management

purges, i.e. physically deletes reference data from the production data base three calendar months after they were deleted. For example, a party has to be deleted before the Common Reference Data Management can purge it. This implies that a party is never purged, unless a duly authorised user makes the decision to delete it.

The following example illustrates how the Common Reference Data Management archives and purges the different revisions of a generic common reference data object.

EXAMPLE 7 - ARCHIVING AND PURGING AFTER DELETION OF A COMMON REFERENCE DATA OBJECT



In this example, a duly authorised user creates intra-day, on business day T_{X1}, a common reference data object X. This results in the creation of the first revision of the object X.

During business day T_{X2} (with $T_{X2}<T_{X1}$+ three calendar months) a duly authorised user updates the common reference data object X changing one (or many) of its attribute(s). This results in the creation of a new revision (2) for X.

On business day T_{X1}+ three calendar months, the archiving process copies the first revision of the common reference data object X into the archiving data base. It is worth mentioning that:

- The Common Reference Data Management does not purge the archived revision, as it still refers to a period of time that expired on T_{X2}, i.e. since less than three calendar months;
- The Common Reference Data Management does not archive the second revision of the common reference data object X, as it was created on T_{X2}, i.e. since less than the duration of the retention period.

During business day T_{X3} (with $T_{X3}<T_{X2}$+ three calendar months), a duly authorised user deletes the common reference data object X. This results in the creation of a new revision (3) for the same object.

On business day T_{X2}+ three calendar months, the archiving process copies the second revision of the common reference data object X into the archiving data base. In this case:

- The Common Reference Data Management does not purge this second revision, as it still refers to a period of time that expired on T_{X3}, i.e. since less than three calendar months ;

- The Common Reference Data Management does not archive the third revision of the common reference data object X, as it was created on T_{X3}, i.e. since less than three calendar months ;
- The Common Reference Data Management purges the first revision of the common reference data object X, as it refers to a period of time that expired exactly since three calendar months.

Finally, on business day T_{X3}+ three calendar months, the archiving process copies the third and final revision of the common reference data object X into the archiving data base. On the same day, just after the archiving process has been successfully performed, the Common Reference Data Management purges the common reference data object X, by physically deleting the last two revisions of the object X that are still present in the production data base.

From this moment on, all revisions of the common reference data object X are available only in the archiving data base, where the Archiving service keeps them for a period of ten years.

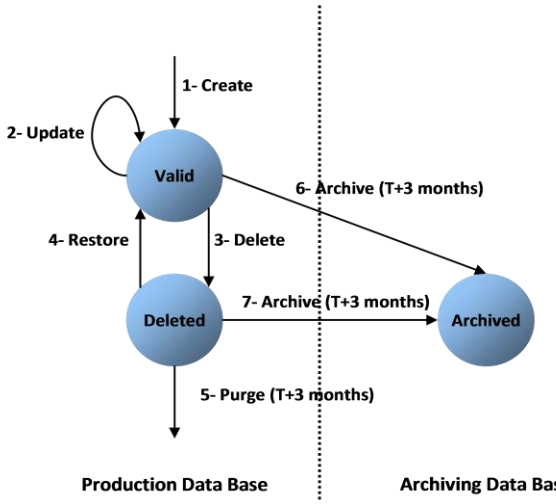
1.4.3.5. Lifecycle of common reference data objects

This section puts together all the concepts described so far and provides a general description of the lifecycle of common reference data objects.

Lifecycle of common reference data objects with unlimited validity period

The following diagram illustrates the lifecycle of a common reference data object with unlimited validity period both in the production data base and in the archiving data base:

DIAGRAM 7 - LIFECYCLE OF COMMON REFERENCE DATA OBJECTS WITH UNLIMITED VALIDITY PERIOD



When a duly authorised user submits to the Common Reference Data Management a reference data maintenance instruction to create a common reference data object with unlimited validity period, the Common Reference Data Management processes it and, in case of successful processing, it creates the relevant object. This object is valid and it exists in the production data base only (transition 1).

From this moment on, a duly authorised user may submit to the Common Reference Data Management common component one or many reference data maintenance instructions to update the common reference data object. Regardless of the result of the Common Reference Data Management processing, i.e. whether the reference data maintenance instruction is successfully or unsuccessfully processed, the common reference data object remains valid (transition 2).

When a duly authorised user submits to the Common Reference Data Management a reference data maintenance instruction to delete a common reference data object, the Common Reference Data Management processes it and, in case of successful processing, it deletes the relevant object. This object is logically deleted (transition 3), even if it is still physically present in the production data base.

From this moment on and within a period of three calendar months, if a duly authorised user submits to the Common Reference Data Management a reference data maintenance instruction to restore a previously deleted common reference data object, the Common Reference Data Management processes it and, in case of successful processing, it restores the relevant object. As a result, the object becomes valid again (transition 4).

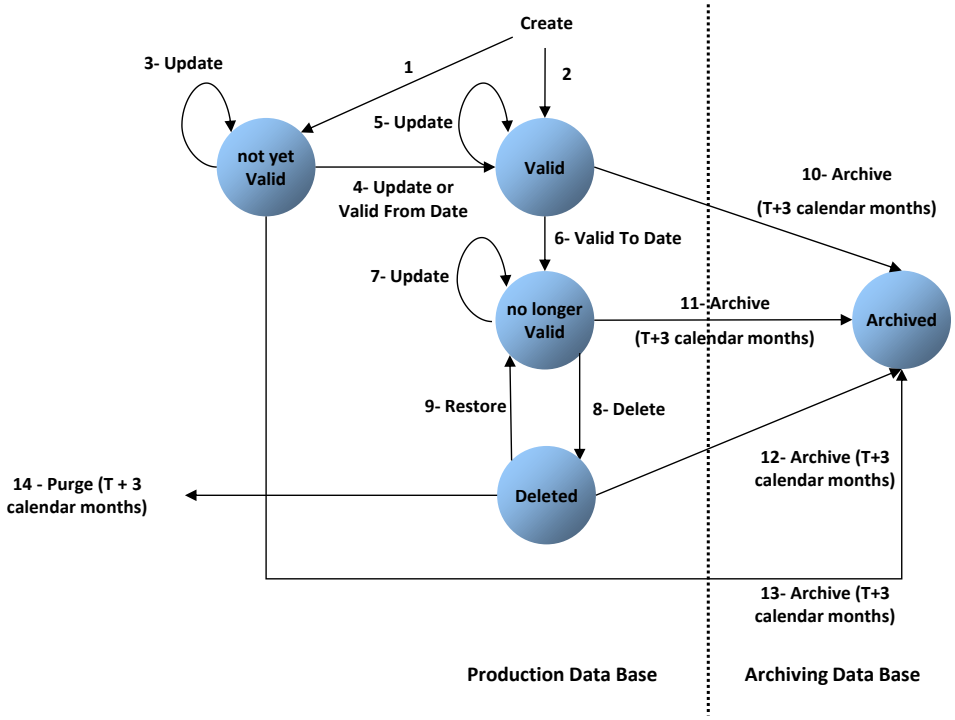
Three calendar months after a common reference data object has been deleted, the Common Reference Data Management physically deletes it from the production data base. This results in the object being purged by the production data base (transition 5), i.e. it exists only in the archiving data base.

Three calendar months after a common reference data object has been either created, updated or deleted, the Common Reference Data Management copies the revision of the common reference data object resulting from this reference data maintenance instruction from the production data base to the archiving data base. As a result the common reference data object is both in the production data base and archived in the archiving data base, in case it was created or updated, or only in the archiving data base, in case it was deleted (transitions 6 and 7).

Lifecycle of common reference data objects with limited validity period

The following diagram illustrates the lifecycle of a common reference data object with limited validity period both in the production data base and in the archiving data base

DIAGRAM 8 - LIFECYCLE OF COMMON REFERENCE DATA OBJECTS WITH LIMITED VALIDITY PERIOD



When a duly authorised user submits to the Common Reference Data Management a reference data maintenance instruction to create a common reference data object with limited validity period, the Common Reference Data Management processes it and, in case of successful processing, it creates the relevant object. This object is either valid or not yet valid, depending on the starting date of its validity period, and it exists in the production data base only (transitions 1 and 2).

From this moment on, a duly authorised user may submit to the Common Reference Data Management one or many reference data maintenance instructions to update the common reference data object. If the object is valid, then it remains valid, regardless of the result of the Common Reference Data Management processing, i.e. whether the reference data maintenance instruction is successfully or unsuccessfully processed (transition 5). If the object is not yet valid, two sub-cases are possible:

- If the reference data maintenance instruction also updates the starting date of the validity period to the current business date and it is successfully processed, then the common reference data object becomes valid (transition 4).
- In all other cases, whether the reference data maintenance instruction is successfully or unsuccessfully processed, the common reference data object remains not yet valid (transition 3).

A common reference data object becomes valid from the starting business date of the validity period (transition 4).

A common reference data object is valid until the end of day of the final date of the validity period (transition 6). As far as TIPS is concerned, this implies that the object is valid until TIPS receives from the RTGS system the message notifying the first business day greater than the final date of the validity period.

When a duly authorised user submits to the Common Reference Data Management a reference data maintenance instruction to delete a common reference data object, the Common Reference Data Management processes it and, in case of successful processing, it deletes the relevant object. This object is logically deleted (transition 8), even if it is still physically present in the production data base.

From this moment on and within a period of three calendar months, if a duly authorised user submits to the Common Reference Data Management a reference data maintenance instruction to restore a previously deleted common reference data object, the Common Reference Data Management processes it and, in case of successful processing, it restores the relevant object. As a result, the object becomes no longer valid again (transition 9).

Three calendar months after a common reference data object has been deleted, the Common Reference Data Management physically deletes it from the production data base. This results in the object being purged by the production data base (transition 14), i.e. it exists only in the archiving data base.

Three calendar months after a common reference data object has been either created, updated or deleted, the Common Reference Data Management copies the revision of the common reference data object resulting from this reference data maintenance instruction from the production data base to the archiving data base. As a result the object is both in the production data base (as a not yet valid,

valid, no longer valid or deleted object) and archived in the archiving data base, in case it was created or updated, or only in the archiving data base, in case it was deleted (transitions 10, 11, 12 and 13).

1.4.4. TIPS Directory

1.4.4.1. Purpose

To support the routing of instant payment in TIPS, the needed routing information is provided in a structured TIPS Directory.

It includes the list of all BICs of TIPS Participants and Reachable Parties that are addressable within TIPS.

1.4.4.2. Structure

TIPS Directory is generated as a fixed length record flat file encapsulated in a XML envelope.

The structure of the records of the TIPS Directory is as follows:

TABLE 36 – TIPS DIRECTORY STRUCTURE

O/M	FIELD No.	FIELD NAME	FORMAT	DESCRIPTION
M	1	User BIC	CHAR(11)	BIC configured as Authorised Account User in TIPS. This BIC can be authorised for payments on one and only one TIPS Account or CMB in TIPS and it is the BIC that shall be used to address Instant Payments in TIPS.
M	2	Institution Name	CHAR(105)	It is the name stored in the CRDM BIC Directory together with the User BIC.
M	3	Party BIC	CHAR(11)	BIC that identifies a TIPS Participant or a Reachable Party in TIPS. This BIC is for information purpose only and it allows grouping all User BICs configured by a given TIPS Participant or Reachable Party. It cannot be used to address Instant Payments in TIPS.
M	4	Account Owner BIC	CHAR(11)	BIC of the TIPS Participant owning the TIPS Account for which the User BIC has been authorised, also through a CMB.
M	5	Type of Change	CHAR(1)	Exhaustive list of possible values: A – Added M – Modified D – Deleted U – Unchanged
M	6	Valid From	DATE(YYYYMMDD)	Date from which the entry is valid.

O/M	FIELD No.	FIELD NAME	FORMAT	DESCRIPTION
M	7	Valid To	DATE(YYYYMMDD)	Date up to which the entry is valid. Value "99991231" is used whenever the ending of validity has not been specified.
M	8	Participation Type	CHAR(2)	Exhaustive list of possible values for Party BIC: 01 – TIPS Participant 02 – Reachable Party

Each version of the TIPS Directory is identified by the name of its file (see section 1.4.4.4).

The following table shows the usage of the "Type of Change" field:

TABLE 37 – TYPE OF CHANGE USAGE

CHANGE	VERSION N-1	VERSION N	VERSION N+1
A new record is issued in the version N of the TIPS Directory (the "Valid From" date must be greater than the validity date of the version N-1).	not present	A	U
A field (different from the BIC) is changed in the version N.	U	M	U
A BIC is no more reachable in TIPS (the "Valid To" date + 1 must be strictly lower than the validity date of the version N+1).	U	D	not present

1.4.4.3. Generation

CRDM generates both a full version and a delta version of the TIPS Directory every business day at 17:00 CET. The full version includes all BICs of TIPS Participants and Reachable Parties that are addressable within TIPS, whereas the delta version only includes changes with respect to the previous version of the TIPS Directory (i.e. record with "Type of Change" equal to "A", "D" or "M"). In case there are no changes between two versions of the TIPS Directory, the delta version consists of an empty file.

Immediately after the generation is completed, CRDM forwards both the full version and the delta version to TIPS for push distribution (see section 1.4.4.4).

1.4.4.4. Distribution

TIPS Actors may receive the TIPS Directory in two ways:

- **push mode**: each day, after having received the end-of-day message from TARGET2, TIPS sends the full version or the delta version of the TIPS Directory to all TIPS Actors who created for this an appropriate Report Configuration.
- **pull mode**: at any time during the service hours of CRDM, a TIPS Actor may download either the full version or the delta version of the TIPS Directory from a CRDM web-page.

The name of the flat file that contains the TIPS Directory is as follows: TIPSDIRTTTTYYYYMMDD where:

- TTTT is the type, i.e. FULL for the full version and DLTA for the delta version;
- YYYYMMDD specifies the year, month and day as of which the TIPS Directory is valid.

1.4.4.5. XML Envelope

To adhere to ISO20022 compliance, TIPS Directory content is embedded into a XML Envelope.

The following is the XML schema used to embed the file into a message:

```
<?xml version="1.0" ?>
<xs:schema xmlns="urn:TIPS:TIPSDirectory"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
 targetNamespace=" urn:TIPS:TIPSDirectory "
 elementFormDefault="qualified">
<xs:simpleType name="RestrictedFileType">
 <xs:restriction base="xs:string">
  <xs:pattern value="(.{157,157}\n)+"/>
 </xs:restriction>
</xs:simpleType>
<xs:element name="File" type="File"/>
 <xs:complexType name="File">
  <xs:simpleContent>
   <xs:extension base="RestrictedFileType">
    <xs:attribute name="fileId" type="xs:string" default="" />
   </xs:extension>
  </xs:simpleContent>
 </xs:complexType>
</xs:schema>
```

This XML Schema Definition can be used by recipient actor to validate the content of the directory, if deemed necessary.

The produced XML file should look as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<File fileId = “TIPSDIRFULL20200101” xmlns=" urn:TIPS:TIPSDirectory ">Record1
Record2
…
Recordn
</File>
```

1.5. Interactions with other services

This section describes the interactions in place between the Common Reference Data Management common component and other Eurosystem Market Infrastructure Services.

1.5.1. TARGET2-Securities

The Common Reference Data Management common component is built as an enhancement of the T2S Static Data Management (SDMG) domain. The reference data objects and management functionalities featured in CRDM are based on the result of a gap analysis between the functionalities available in T2S SDMG and the TIPS requirements, as a first step in the long term framework of the T2-T2S Consolidation project. CRDM functionalities relate to T2S SDMG in one of three possible ways:

- SDMG functions which highlighted no gap with the TIPS requirements are reused in full in CRDM;
- SDMG functions which highlighted specific gaps with the TIPS requirements were modified in order to extend their scope and satisfy the requirements in CRDM;
- New functions which did not exist in SDMG were developed specifically for CRDM.

While the user interfaces are different, CRDM and SDMG share the same logical environments, database and back-end software, meaning that steps have been taken to ensure that the coexistence of data relating to both components does not interfere with the ongoing T2S settlement business. Based on the T2-T2S Consolidation requirements, the reference data model was set up in order to ensure that certain types of data are shared and relevant for both components. In this respect, three different object categories can be identified:

- Fully shared objects where the same instances are relevant and used by both components (e.g. Parties, Users). These objects can be viewed, created and maintained from both the CRDM and the T2S interface. The same instance will be valid and taken into account in both components, regardless of the channel from which it is created/maintained. For example, a Payment Bank Party created through the CRDM interface is used and taken into account by T2S processes as if it has been created through the T2S interface.
- Categorised shared objects which are used in both components but each instance has a specific link to a single component (e.g. Cash Accounts, Limits). These objects can be created and maintained from both the CRDM and the T2S interface, however instances related to one component cannot be viewed or created/maintained from the other component's interface and are not taken into account by the other component's application processes.
- Service-specific objects which only have meaning for one service (e.g. Authorised Account User and DN-BIC Routing for CRDM-TIPS; Securities and CSD Account Links for T2S). Among these objects, those relevant for CRDM-TIPS can only be viewed and maintained from the CRDM interface and have no bearing on the T2S application processes.

1.5.2. TARGET2

CRDM utilises BIC data for internal validations and addressing checks. The BIC Directory stores information needed to identify the legal entity linked to each BIC. This information is used, for example, to validate BICs used as Party identifiers or Authorised Account Users. CRDM executes a monthly loading of the SWIFT BIC directory on the basis of information provided by SWIFT through TARGET2 and forwarded to CRDM.

The CRDM Operator, in any case, has the ability to perform CRDM-specific updates on individual BICs. For example, this would allow to insert BICs that are not published in the SWIFT BIC Directory in order to use them in TIPS payments, if required.

1.5.3. TARGET Instant Payment Settlement

The CRDM allows users to configure reference data to be used in TIPS. With the exception of a very limited set of attributes which are required to be modified on a 24/7 basis (see section 1.7.2), all reference data used in TIPS is created and maintained in CRDM.

Data set up in CRDM is propagated to TIPS on a regular basis, typically once a day, at a preset time before the change of business date. If needed, participants can request an ad-hoc propagation to be run at different times of day. There is no technical limit on the number of times a data propagation can run during a given business date.

No data propagation flow exists from TIPS to CRDM; data modified in TIPS does not influence the existing data in CRDM.

1.6. Operations and support

1.6.1. Data configuration

The CRDM Operator is responsible for defining and maintaining a number of rules and parameters as reference data objects for the configuration of the CRDM business application. The rules and parameters the CRDM Operator may configure are the following:

- System Entity: a system entity in CRDM corresponds to a partition of data equating to the scope of a Central Bank or of the CRDM Operator. For example, the system entity of a Central Bank includes all the data related to its payment banks. The CRDM Operator is responsible for the creation and maintenance of system entities for all the Central Banks. The creation of a system entity is a necessary preliminary step for the creation of a Central Bank as a party in CRDM (and, consequently, for the creation of payment banks).
- Party reference data for Central Banks: the CRDM Operator is responsible for creating and maintaining Central Banks as parties in CRDM. Subsequently, users from these parties may create their own payment banks. For more details, see section 1.3.2.
- Access rights configuration for Central Banks: after having created the system entity and the related party, the CRDM Operator may set up the Central Banks' privileges to access CRDM and TIPS. Subsequently, Central Banks are able to set up their own participants' access rights and to manage the access rights of their users independently, without resorting to the CRDM Operator. For details on access rights management, see section 1.2.2 and 1.3.4.
- General restriction types: the CRDM Operator defines a set of general restriction types which each Central Bank or participant may use in order to block/unblock the participants or accounts/CMBs. See section 1.3.8 for details on restriction types.
- General system parameters: the CRDM Operator may define a set of system parameters that are applicable to all participants, e.g. the list of available report types and the list of privileges.
- Country: the country codes for all countries (for uses such as defining the country of origin of a payment bank) are stored and maintained by the CRDM Operator.
- Currency: the CRDM Operator is responsible for setting up and maintaining currency reference data and for specifying the settlement currencies for TIPS.
- Network Service: the CRDM Operator maintains all the data related to the available network services, including the data for technical identification of each service and the type of data expected to interact with each service (e.g. BIC or Distinguished Name).

1.6.2. Business and operations monitoring

The Business and operations monitoring integrates information coming from different sources in order to monitor the business and operational status of the Common Reference Data Management, to detect possible problems in real-time or to proactively recognise a possible deterioration of performance and to provide up-to-date information for crisis management scenarios.

Business and operations monitoring gives the CRDM Operator the possibility to perform a real-time supervision of the Common Reference Data Management in terms of:

- Performance;
- Transactions transit and response times;
- Ongoing fulfilment of SLA commitments and expectations;
- Volumes and values exchanged;
- Actors activity on the system;
- Hardware and software problems.

The goal is to allow an early detection of possible anomalies through the continuous comparison of reported data with standard patterns. Besides that, the data can be used to improve the component's behaviour or its usage through a better understanding of the relevant dynamics.

The Business and operations monitoring application process extracts, merges and organizes the data in forms of tables, grids and graphs to ensure both the depth of the underlying information and its prompt usability.

In order to exclude any even remote impact on the component's performances, the Business and operations monitoring application makes use of a different set of data which are replicated from the original ones.

The CRDM Operator is also provided with a tool for the detection in real-time of functional or operational problems, called Technical Monitoring. It allows for the detection of hardware and software problems via real-time monitoring of the technical components involved in the processing, including the network connections.

Business and operations monitoring interfaces are available in U2A mode only.

1.7. Limitations of the system

1.7.1. A2A channel

The fully-fledged CRDM will be accessible in U2A mode (for all functions) and in A2A mode (for a subset of functions). The A2A channel is intended to allow Central Banks and their participants to perform massive upload of reference data when needed.

The first version of CRDM is designed to interact and support the reference data configuration for TIPS. All the possible solutions for the inclusion of an A2A channel in this version of CRDM are suboptimal both from a technical connectivity standpoint and in terms of coverage of the required functional scope:

- The technical connectivity solution provided by ESMIG at this stage does not cover the full scope of connectivity services foreseen for the go-live of T2-T2S Consolidation. In particular, A2A connectivity towards the fully-fledged CRDM will only be available as of 2021;
- The existing A2A connectivity solution for T2S cannot be considered as it would be based on the assumption that all TIPS actors are also T2S actors;
- A specific solution for the interim period between 2018 and 2021 would be based on a throw-away investment.

In addition, since it is not foreseen to enlarge the scope of available XML messages, all of the above solutions would allow to perform massive reference data upload only for a limited set of reference data objects (specifically, the ones which are currently available through A2A in T2S, i.e. Parties and Cash Accounts, including TIPS CMBs). Several reference data objects expected to have high cardinality would still have to be loaded in U2A mode.

For these reasons the Data Migration Tool (DMT) was chosen as a solution to allow a massive upload of several reference data objects. This allows to avoid a throw-away investment for the implementation of an interim A2A channel and to implement via DMT the full scope of TIPS reference data objects with high cardinality.

1.7.2. Data propagation between CRDM and TIPS

In addition to the propagation of reference data from CRDM on a regular basis, TIPS offers its users a reference data management functionality specifically to maintain the limited set of data that is required to be modifiable on a 24/7 basis in real-time. This data is exhaustively listed below:

- Blocking status for TIPS Participants (represented in CRDM by Party restrictions)
- Blocking status for TIPS Accounts and TIPS Credit Memorandum Balances (represented in CRDM by Cash Account restrictions)
- Limit value for TIPS Credit Memorandum Balances (represented in CRDM by the Limit amount

The concurrent change of this data on either side (CRDM and TIPS), taking into consideration the delayed propagation of data from CRDM to TIPS, could lead to inconsistent and unexpected results. As such, the current version of CRDM does not allow to modify these attributes. While it is possible to

set a value for Limits upon creation, this value is propagated to TIPS only as an initial limit value. Following the initial propagation to TIPS, Limits can only be modified in TIPS. On the other hand, the blocking statuses can only be set and modified in TIPS.

1.7.3. Archiving management

CRDM is based on the existing T2S Static Data Management (SDMG) domain. As such it retains all the functionalities that are implemented therein. One notable limitation is that the current version of CRDM does not foresee a reference data archiving function, which is not part of T2S SDMG and is foreseen to be introduced as part of the fully-fledged CRDM.

As a consequence, maintaining the current setup for purging (i.e. physically removing) reference data could lead to unwanted results. In T2S, data is copied to the archiving database with a three-month delay from the production database. Likewise, data which is logically deleted is then purged from the production database after a retention period of three months and can then be consulted in the archiving database only.

The absence of a long-term archive in CRDM would entail that keeping the purging mechanism leads to data being removed for good from the system. For this reason, and until the deployment of the fully-fledged CRDM, it has been chosen to avoid purging logically deleted data from the database. Specifically, this means that the retention period (currently set to three months) is extended indefinitely for reference data objects that are also used in CRDM. These objects include Party, Technical Address Network Service Link, Party Service Link, Cash Account, Authorised Account User, Limit, Role, User, DN-BIC Routing, User-Certificate DN Link, Certificate DN, Message Subscription Rule Set, Message Subscription Rule, Restriction Type, Report Configuration[32].

[32] For all these objects, audit trail data will continue to be purged after three months and not be archived in any case.

2. Dialogue between CRDM and CRDM Actors

2.1. Data Migration Tool File Upload

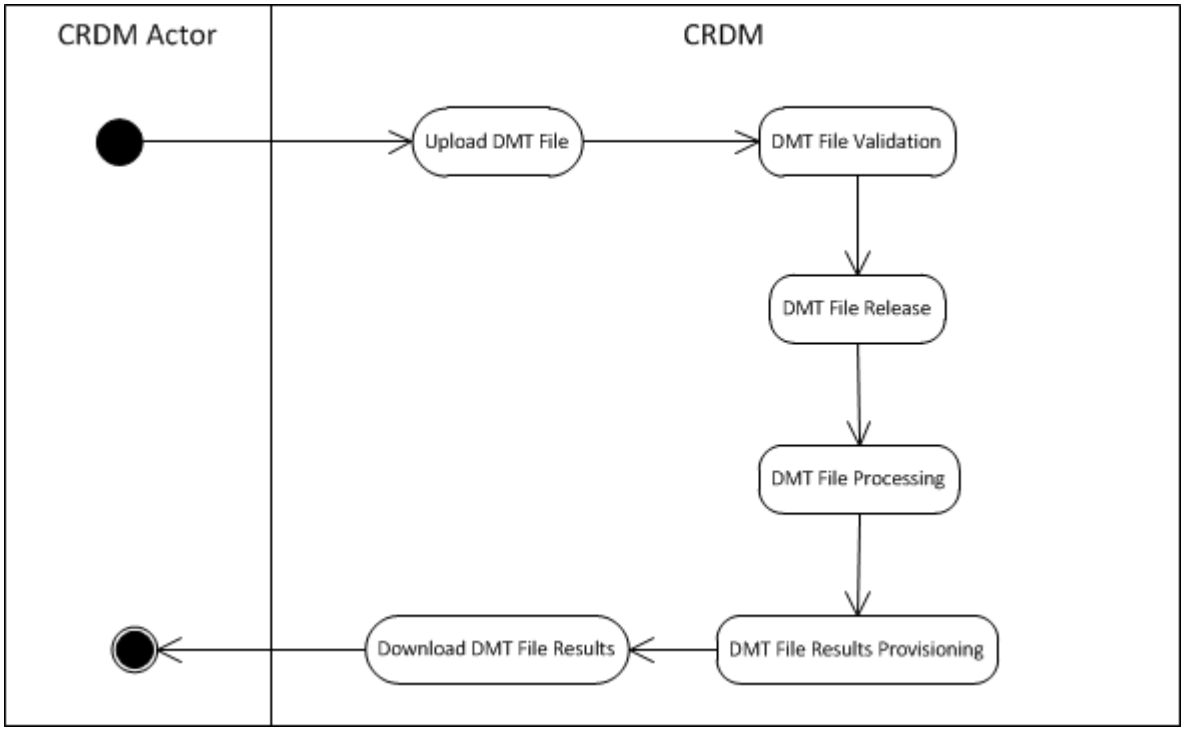
2.1.1. Introduction

This use case covers the standard situation of a Central Bank or Payment Bank CRDM Actor loading TIPS related reference data into Common Reference Data Management common component. Upload use case is available via U2A through a dedicated section.

The user uploading the file will be propagated to the related back-end functions and must have the appropriate access right configuration.

2.1.2. Activity Diagram

The following diagram details all the processing steps of the Data Migration Tool File Upload use case:



2.1.2.1. Upload DMT File

The CRDM Actor uploads the required DMT file containing the reference data to be created in CRDM.

The file can be generated in Excel or Comma Separated Value format and follow the specifications described in chapter 3.

2.1.2.2. DMT File Validation

CRDM performs a technical validation on the uploaded file to ensure that the technical constraints have been respected.

2.1.2.3. DMT File Release

CRDM System Operator release the file for the back end module processing as agreed with the Actor.

This step triggers the back end module function required by the file as described in the record type label.

2.1.2.4. DMT File Processing

The DMT triggers the related back end module function passing information record by record.

Every call to the back end module function generates a result processing.

2.1.2.5. DMT File Results Provisioning

Once all of the records in the uploaded file have been sent and processed by the back end module which provided the related result, the DMT File Result is consolidated.

For every record, the successful processing or the business errors received from the back end module are included in the DMT File Results.

The file is published for the CRDM Actor to download.

2.1.2.6. Download DMT File Results

CRDM Actor downloads the result file reporting the number of migrated records and the detailed list of errors for rejected records.

The following table maps the reference data maintenance operations available in the DMT with the related reference data objects and the file specifications contained in Chapter 3.

TABLE 38 – DMT FILES SPECIFICATIONS

REFERENCE DATA OBJECT	OPERATION	FILE SPECIFICATIONS SECTION
Authorised Account User	Create	3.5.3.14
Cash Account	Create	3.5.3.12
Certificate DN	Create	3.5.3.10
DN-BIC Routing	Create	3.5.3.16
Limit	Create	3.5.3.13
Message Subscription Rule	Create	3.5.3.8
Message Subscription Rule Set	Create	3.5.3.7
Party	Create	3.5.3.1
Party-Service Link	Create	3.5.3.15
Privilege	Grant	3.5.3.6
Report Configuration	Create	3.5.3.9
Role	Create	3.5.3.4
Role	Grant	3.5.3.5
Technical Address Network Service Link	Create	3.5.3.2
User	Create	3.5.3.3
User Certificate DN Link	Create	3.5.3.11

3. Data Migration Tool

3.1. Introduction

The TIPS Data Migration Tool (TIPS DMT) offers NCBs and Payment Banks the opportunity to load TIPS related reference data into Common Reference Data Management common component.

The data can be produced in Excel or flat file format by the user and submitted to CRDM via a web application.

3.2. Technical Specification

3.2.1. Data Record Definition

This chapter refers to Excel and the flat file in the same manner.

3.2.1.1. Rows and Columns

A spreadsheet consists of horizontal rows and vertical columns. Columns identify the attributes and are restricted to a specific data type. There is no mix-up of different attributes and data types in one column.

3.2.1.2. Header

The names of the columns appear in the first row. The names support the user to fill out the form but have no further functionality. Data Migration Tool identifies the attributes based on the location of the column and does not interpret the column names.

3.2.1.3. Records

A record is a data structure that contains all parameters for a certain business function. A record spans over several rows as it may contain attributes that are repeatable. The repeated attributes are placed in a separate row just below the initial row in the same column.

3.2.1.4. Record Type

The record type describes the business function of the record. A file may contain several records of the same record type. A mixture of different record types in one file is not possible.

The record type is indicated with a key word in the upper left corner of the file. Since there is only one record type per file the indication occurs only once. For example:

Record Type	Record Id	An Attribute
Party	1	aaa
	2	bbb

3.2.1.5. Record Identification

A record is identified with a unique record identifier. The identifier must be unique within the file. It is recommended that the record identifier starts with 1 and is consecutively numbered.

In case the record contains repeatable attributes and spans over several rows the record identifier is repeated in each row of the record. Rows with the same record identifier are located one after the other. These connected rows must not be interrupted by rows with another record identifier. For example:

Record Type	Record Id	A repeatable Attribute	A non-repeatable Attribute
Party	1	a1	c1
	1	b1	
	2	a2	c2
	2	b2	

3.2.1.6. Default Values

Default values are not used. When a field has no value the Excel field remains empty. For example:

aaa		ccc

In a flat file the length of a field with no value is 0. For example:

```
aaa,,ccc
```

Data Migration Tool does not provide default values for empty fields. Any input parameter must be stated within the files.

3.2.1.7. Format Types

The values appear in the format as in the table below:

Format Type	Excel	CSV[33]

[33] The CSV format matches to the Excel format when the regional settings of a Windows PC are „English (Great Britain)“

DATE	The format depends on the country and location of the user.	The format is « dd/mm/yyyy » with no timezone indication. Example: “30/06/2015”
TIME	The format depends on the country and location of the user.	The format is «hh:mm:ss» with no timezone indication. Times are in 24 hour format. Example: “15:30:59”
CHAR (n)	String with exactly n characters.	Same format as Excel.
VARCHAR (n)	String with n characters maximum.	Same format as Excel.
DEC (p,s)	Floating-point number with maximum p integer places and s decimal places. A dot ‘.’ is used as decimal separator. Due to Excel restriction, cell must be treated as text	Floating-point number with maximum p integer places and s decimal places. A dot ‘.’ is used as decimal separator.
NUMERIC (p)	Number with maximum p integer places and no decimal places.	Same format as Excel.
BOOLEAN	Possible values: • true • false	Same format as Excel.

3.2.1.8. EPC SCT^{Inst} Charset Interoperability

In order to ensure compliance to TIPS ISO20022 message implementation, the character set of all fields is restricted to the SWIFT X Character Set (see below).

Exceptions might occur if special chars are required. Character set restrictions will not apply on these fields which are not used in supported message payloads (e.g. Distinguish Name in Party Technical Address for Party) and will not hamper interoperability.

Exceptions are highlighted in the definition of the related fields.

3.2.1.9. Timezones

Timezones do to appear in the data. The timezone is considered the timezone of Frankfurt. This is either **CET** (GMT+01:00) or, when a daylight saving hour is applied, **CEST** (GMT+02:00).

3.2.1.10. Character Set

All characters belong to the SWIFT X Character Set. The character set is as follows:

a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
/ - ? : ( ) . , ' +
CR LF Space

3.2.1.11. Filenames

Any filename is permitted.

Remark:

Users are recommended to include the record type, e.g. “TIPS.DMT.CRDM.Party.100”, in the file name. This helps the Operator to identify the content of the uploaded file. This is not required by Data Migration Tool as only the record type is checked (see chapter 3.2.1.4 for details).

3.3. Technical Specification of the Excel File

3.3.1. Excel Version

The Excel files adhere to one single distinct version of Microsoft Office.

Detailed information:

- Version: Microsoft® Office Excel® 2007
- File Extension: xlsx

3.3.2. Restrictions

3.3.2.1. Worksheets

The option that one Excel file may contain several worksheets is not supported. TIPS DMT uses only the very first worksheet.

3.3.2.2. Number of Rows

Due to technical limitations the number of rows is restricted.

Detailed information:

- Maximum number of rows: 50.000

3.3.2.3. Size limits

In addition to the number of rows, the uploaded file cannot exceed 9 MB.

3.4. Technical Specification of the Flat File

3.4.1.1. Compliancy to RFC 4180

The flat file has a CSV format that follows closely RFC 4180. The RFC specifies a format that is widely used by many implementations and eases the development of an upload process.

Detailed information:

- File Extension: csv

3.4.1.2. Definition of the CSV Format (RFC 4180)

1. Each row is located on a separate line, delimited by a line break (CRLF). For example:

   aaa,bbb,ccc CRLF

zzz,yyy,xxx CRLF

1. The last row in the file has no ending line break. For example:

   aaa,bbb,ccc CRLF
   zzz,yyy,xxx

2. Within each row, there are one or more fields, separated by commas. Each row contains the same number of fields throughout the file. Spaces are considered part of a field and are not ignored. The last field in the record is not followed by a comma. For example:

   aaa,bbb,ccc

3. Each field may or may not be enclosed in double quotes. If fields are not enclosed with double quotes, then double quotes do not appear inside the fields. For example:

   aaa,"bbb","ccc" CRLF
   zzz,yyy,"xxx"

4. Fields containing line breaks (CRLF), double quotes, and commas are enclosed in double quotes. For example:

   aaa,"b CRLF bb",ccc CRLF
   zzz,yyy,xxx

5. A double quote appearing inside a field is escaped by preceding it with another double quote[34]. For example:

   "aaa","b""bb","ccc"

The escaping with double quotes ensures that all data can appear. Quotes, commas and line breaks may be included into the business data.

3.4.1.3. Control Characters

In order to structure the data in the flat file the following control characters are used:

Carriage Return (CR)	0x0d
Line Feed (LF)	0x0a

3.4.1.4. Encoding

The encoding of the flat file is UTF-8 with no Byte Order Mark (BOM).

3.4.1.5. Number of Rows

The number of rows is restricted.

Detailed information:

- Maximum number of rows: 50.000

[34] Currently, character « quote » is not allowed. See chapter 3.2.1.10 for details. Please note that the CSV format definition is independent from the character set.

3.4.1.6. Size limits

In addition to the number of rows, the uploaded file cannot exceed 9 MB.

3.5. Format of Structured Files

3.5.1. Format of Excel and Flat Files

See chapter 3.4for the specification and details of the format types.

3.5.2. Technical Prerequisites

3.5.2.1. Record Type Identifier

Prior to the static and dynamic data appears the record type identifier.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per File
1	A	Record Type	VARCHAR (50)	Indicates the business function. The required value can be found in the first line of the chapters 3.5.3.1 - 3.5.3.16.	Occurs in the 2nd row only.	1..1

3.5.3. Common Reference Data

3.5.3.1. Party Reference Data - New

- Record Type: “Party”

The record is used to create party reference data.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.	Must occur in each line of the record.	1..n	
Group “Party”						1..1	
3	C	Parent BIC	CHAR (11)				1..1
4	D	Type	Possible values: • PMBK •	Classification of the party: • PMBK = Payment bank •			1..1
5	E	Opening Date	DATE	Activation date of a party.	Must be equal or greater than the current date.		1..1
6	F	Closing Date	DATE	Closing date of the party.	Must be greater than the Opening Date.		0..1
7	G	BIC	CHAR (11)	Party BIC.			1..1
Group “Name”						1..1	
8	H	Long Name	VARCHAR (350)	Long name.			1..1
9	I	Short Name	VARCHAR (35)	Short name.			1..1
Group “Address”						1..1	
10	J	Street	VARCHAR (70)	Name of the street for the address.			1..1
11	K	House Number	VARCHAR (16)	House number for the address.			1..1
12	L	Postal Code	VARCHAR (16)	Postal code for the address.			1..1
13	M	City	VARCHAR (35)	City for the address.			1..1
14	N	State or Province	VARCHAR (35)	State or the province for the address.			0..1
15	O	Country Code	CHAR (2)	Country code of the address.			1..1
Group “Party Technical Address“						1..10	
16	P	Technical Address	VARCHAR (256)	Unique technical address of the party (distinguished name).	EPC SCT^{Inst} interoperability character set restriction does		1..1

					not apply		
Group “Auto-Collateralisation Rule”					This group is defined for keeping backward compatibility with T2S. It is not used in TIPS.	1..1	
17	Q	Collateralisation Procedure	Possible value: • REPO	Type of collateralisation procedure application. Possible value: • REPO	The value must be ‘REPO’ and has no impact in TIPS processing.		1..1
Group “Market-Specific Attributes”						0..10	
18	R	Market-Specific Party Attribute Name	VARCHAR (35)	Name of the market specific attribute.	This field is defined for keeping backward compatibility with T2S. It is not used in TIPS.		1..1
19	S	Market-Specific Party Attribute Value	VARCHAR (350)	Value of the market specific attribute.	This field is defined for keeping backward compatibility with T2S. It is not used in TIPS.		1..1
Group “Party Restriction List”						0..10	
20	T	Restriction Type	CHAR (4)	List of blocking restrictions.			1..1
21	U	Restriction Valid From Date	DATE	Valid from date and time of the restriction.	Must be equal or greater than the current date and time.		1..1
22	V	Restriction Valid From Time	TIME				1..1
23	W	Restriction Valid To Date	DATE	Valid to date and time of the restriction.	Date and time must occur together.		0..1
24	X	Restriction Valid To Time	TIME		Must be greater than the Valid From date and time.		0..1

3.5.3.2. Technical Address Network Service Link - New

- Record Type: “Technical Address Network Service Link”

The record is used to create a link between a technical address and a network service.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.	Must occur in each line of the record.	1..n	
Group “Party Identification”						1..1	
3	C	Parent BIC	CHAR (11)	BIC of the System Entity responsible for the party			1..1
4	D	Party BIC	CHAR (11)	BIC of the party			1..1
Group “Technical Address Network Service”						1..1	
5	E	Technical Address	VARCHAR (256)		EPC SCT^{Inst} interoperability character set restriction does not apply	1..1	
6	F	Network Service	VARCHAR (35)			1..1	

3.5.3.3. User - New

- Record Type: “User”

The record is used to create a user.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.	Must occur in each line of the record.	1..n	
Group “User”						1..1	
3	C	Login Name	VARCHAR (35)	Login name.			1..1
4	D	Name	VARCHAR (127)	Name of the user.			1..1
5	E	System User Reference	VARCHAR (35)	System reference of the user.			1..1
6	F	Lockout From Date	DATE	Date and time when the user is locked out from the system.	Must be equal or greater than the current date and time. Date and time cannot be specified when “Lockout” = false. Date and time are mandatory when “Lockout” = true		0..1
7	G	Lockout From Time	TIME				0..1
8	H	Lockout	BOOLEAN	• true = The user cannot enter the system after the Lockout From Date and Time			1..1
Group “Party”						1..1	
9	I	Parent BIC	CHAR (11)	Party parent BIC.			
10	J	BIC	CHAR (11)	Party BIC.			1..1

3.5.3.4. Roles - New

- Record Type: “Role”

The record is used to create a role.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.	Must occur in each line of the record.	1..n	
Group “Role”						1..1	
3	C	Role Name	VARCHAR (35)	Name of the role.			1..1
4	D	Role Description	VARCHAR (127)	Description of the role.			1..1

3.5.3.5. Grant Roles - New

- Record Type: “Grant Role”

The record is used to grant a role to a party and/or a user.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.	Must occur in each line of the record.	1..n	
Group “Role”						1..1	
3	C	Role Name	VARCHAR (35)	Name of the role to be granted.			1..1
Group “User”					Mandatory if group “Party” is not specified, Not allowed otherwise.	0..1	
4	D	User	VARCHAR (35)	Login name of the user.			1..1
Group “Party”					Mandatory if group “User” is not specified. Not allowed otherwise.	0..1	
5	E	Parent BIC	CHAR (11)	Parent BIC of the party.			1..1
6	F	BIC	CHAR (11)	BIC of the party.			1..1

3.5.3.6. Grant System Privilege - New

- Record Type: “Grant System Privilege”

The record is used to grant a system privilege to a role.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.	Must occur in each line of the record.	1..n	
Group “Role”						1	
3	C	Role Name	VARCHAR (35)	Name of the role.			1..1
Group “Party”					This group is defined for keeping backward compatibility with T2S. It is not allowed in TIPS.	0	
4	D	Parent BIC	CHAR (11)	Parent BIC of the party.			0
5	E	BIC	CHAR (11)	BIC of the party.			0
Group “User”					This group is defined for keeping backward compatibility with T2S. It is not allowed in TIPS.	0	
6	F	User	VARCHAR (35)	Login name of the user.			0
Group “Privilege”						1..1	
7	G	Privilege Name	VARCHAR (35)	Name of the system privilege.	EPC SCT Inst interoperability character set restriction does not apply		1..1
8	H	Deny Option	BOOLEAN	• true = The system privilege is explicitly denied • false = The system privilege is explicitly assigned			1..1
9	I	4-Eyes Option	BOOLEAN	• true = The 4-eyes principle is required to perform the activity linked to the system privilege • false = The 2-eyes principle is required to perform the activity linked to the system privilege			1..1
10	J	Administration Option	BOOLEAN	• true = If the grantee of the privilege is a			1..1

				user or a role the grantee is allowed to grant the same privilege to another user or role of the same party. If the grantee of the privilege is a party, the party administrators of the grantee party are allowed to grant the same privilege also to other parties. • false = If the grantee of the privilege is a user or a role the grantee is not allowed to grant the same privilege to another user or role of the same party. If the grantee of the privilege is a party, the party administrators of the grantee party are allowed to grant the same privilege only to users and roles of the same party.			

3.5.3.7. Message Subscription Rule Set - New

- Record Type: “Message Subscription Rule Set”

The record is used to create message subscription rule sets and the relationship among the rule set and a list of parties.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.	Must occur in each line of the record.	1..n	
Group “Message Subscription Rule Set”						1..1	
3	C	Name	VARCHAR (35)	Name of the message subscription rule set.			1..1
4	D	Description	VARCHAR (350)	Description of the message subscription rule set.			1..1
5	E	Valid From	DATE	Valid from date of the message subscription rule set.	Must be equal or greater than the current date.		1..1
6	F	Valid To	DATE	Valid to date of the	Must be greater		0..1

				message subscription rule set.	than the Valid From date.		
7	G	Positive/Negative Parameter Set	BOOLEAN	• true = The message subscription rule set must be used in positive way • false = The message subscription rule set must be used in negative way			1..1
Group “Interested Party”						0..10	
8	H	Parent BIC	CHAR (11)	Parent BIC of the interested party.			1..1
9	I	Party BIC	CHAR (11)	BIC of the interested party.			1..1

3.5.3.8. Message Subscription Rule - New

- Record Type: “Message Subscription Rule”

The record is used to create message subscription rules connected to an existing message subscription rule set.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.	Must occur in each line of the record.	1..n	
Group “Message Subscription Rule Set”						1..1	
3	C	Name	VARCHAR (35)	Name of the message subscription rule set.			1..1
Group “Message Subscription Rule”						1..1	
4	D	Sequence Number	NUMERIC (9)	Sequence related to the rule.			1..1
5	E	Valid From	DATE	Valid from date of the message subscription rule.	Must be equal or greater than the current date.		1..1
6	F	Valid To	DATE	Valid to date of the message subscription rule.	Must be equal or greater than the valid from date.		0..1
Group “Message Subscription Rule Parameter”					Each Message Subscription Rule may have up to 10 Message Subscription Rule Parameters.	1..10	
7	G	Group	VARCHAR (35)				1..1
8	H	Parameter	Name of the				1..1

		Type Name	parameter type to be set for the rule. Allowed values are: • CASH (TIPS Account) •				
9	I	Parameter Type Value	VARCHAR (35)	Value for the parameter type	This field is defined for keeping backward compatibility with T2S. It is not allowed in TIPS.		0
10	J	Parameter Parent BIC Identifier	CHAR(11)		This field is defined for keeping backward compatibility with T2S. It is not allowed in TIPS.		0
11	K	Parameter Party BIC Identifier	CHAR(11)		This field is defined for keeping backward compatibility with T2S. It is not allowed in TIPS.		0
12	L	Parameter Securities Account Identifier	VARCHAR(35)		This field is defined for keeping backward compatibility with T2S. It is not allowed in TIPS.		0
13	M	Parameter Securities Identifier	CHAR(12)		This field is defined for keeping backward compatibility with T2S. It is not allowed in TIPS.		0
14	N	Parameter Cash Account Identifier	VARCHAR(34)		This field must be an existing TIPS Account accessible by the requestor.		
15	O	Parameter Business Sending Parent BIC Identifier	CHAR(11)		This field is defined for keeping backward compatibility with T2S. It is		0

					not allowed in TIPS		
16	P	Parameter Business Sending Party BIC Identifier	CHAR(11)		This field is defined for keeping backward compatibility with T2S. It is not allowed in TIPS		0
17	Q	Parameter Instructing Party Parent BIC Identifier	CHAR(11)		This field is defined for keeping backward compatibility with T2S. It is not allowed in TIPS		0
18	R	Parameter Instructing Party Party BIC Identifier	CHAR(11)		This field is defined for keeping backward compatibility with T2S. It is not allowed in TIPS		0

3.5.3.9. Report Configuration - New

- Record Type: “Report Configuration”

The record is used to create a report configuration.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.	Must occur in each line of the record.	1..n	
Group “Report Configuration”						1..1	
3	C	Configuration Name	VARCHAR (35)	Name of the report configuration.			1..1
4	D	Configuration Description	VARCHAR (350)	Description of the report configuration.			1..1
5	E	Delta Mode	BOOLEAN	• true = The recipient gets the report in delta mode • false = The recipient gets the report in full mode			1..1
6	F	Report Name	Possible values: • TIPS Directory• TIPS Statement of Accounts • TIPS Statement of Account Turnover	Name of the report type.			1..1
7	G	System Entity Wide Reporting Flag	BOOLEAN	• true = System entity wide reporting			1..1
8	H	Frequency	DECIMAL (2,0)	Frequency in hours for the generation of the delta reports	Mandatory when Delta Mode = true. Not allowed otherwise.		0..1
Group “Report Configuration Party Link”						0..10	
9	I	Parent BIC	CHAR (11)	Parent BIC of the linked party.			1..1
10	J	Party BIC	CHAR (11)	Party BIC of the linked party.			1..1
11	K	Push Mode	BOOLEAN	• true = The recipient gets the report in push mode • false = The recipient gets the report in pull mode	Only allowed value in TIPS is “true”.		1..1

12	L	Execution Time	TIME	Time of the execution of the report.	This field is defined for keeping backward compatibility with T2S. It is not allowed in TIPS.		0
13	M	Event Type	CHAR (4)	Code of the event type that triggers the report.	This field is defined for keeping backward compatibility with T2S. It is not allowed in TIPS.		0
14	N	Valid From	DATE	Starting date for the validity period.	Must be equal or greater than the current date.		1..1
15	O	Valid To	DATE	Ending date for the validity period.	Must be greater than the Valid From date.		0..1
16	P	Currency	CHAR(3)	Currency linked to the Report Configuration	This field is defined for keeping backward compatibility with T2S. It is not allowed in TIPS.		0

3.5.3.10. Certificate Distinguished Name

- Record Type: “Certificate DN”

The record is used to create a certificate distinguished name.

Flat file	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.		1..1	
3	C	Certificate Distinguished Name	VARCHAR (256)		EPC SCT^{Inst} interoperability character set restriction does not apply	1..1	

3.5.3.11. User Certificate Distinguished Name Link

- Record Type: “User Certificate DN Link”

The record is used to create a link between a Certificate DN and a TIPSUser.

Flat file	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.		1..1	
3	C	Certificate Distinguished Name	VARCHAR (256)		Interoperability character set restriction does not apply	1..1	
4	D	Login Name	VARCHAR (35)	TIPS User’s login name.		1..1	
5	E	Default	BOOLEAN			1..1	
6	F	Main User	BOOLEAN	Link for enabling user in TIPS		1..1	

3.5.3.12. Cash Account

- Record Type: “Cash Account”

The record is used to create TIPS Cash Account.

Flat file	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.		1..1	
3	C	Cash Account Number	VARCHAR (34)	Unique number of the TIPS Cash Account		1..1	
4	D	Currency Code	CHAR (3)	Currency of the TIPS Cash Account	This field is not allowed if the Account Type is “TIPS Credit Memorandum Balance”. It is mandatory otherwise.	0..1	
5	E	Account Type	Possible values: • TACC • TCMB • TTAC	Classification of the TIPS Cash Account: • TACC = TIPS Account • TCMB = TIPS Credit Memorandum		1..1	

				Balance • TTAC = Transit Account			
6	F	Opening Date	DATE	Opening date of the TIPS Cash Account		1..1	
7	G	Closing Date	DATE	Closing date of the TIPS Cash Account		0..1	
8	H	Floor Notification Amount	DEC (13,5)	Threshold for floor notifications		0..1	
9	I	Ceiling Notification Amount	DEC (13,5)	Threshold for ceiling notifications		0..1	
10	J	Parent BIC	CHAR (11)	Parent BIC of the account owner		1..1	
11	K	BIC	CHAR (11)	BIC of the account owner		1..1	
12	L	Linked Account	VARCHAR (34)	TIPS Cash Account linked to the CMB	This field is mandatory when Account Type is “TIPS Credit Memorandum Balance”. It is not allowed otherwise.	0..1	
Group “Cash Account Restriction List”						0..10	
13	M	Restriction Type	CHAR (4)	List of blocking restrictions.			1..1
14	N	Restriction Valid From Date	DATE	Valid from date and time of the restriction.	Must be equal or greater than the current date and time.		1..1
15	O	Restriction Valid From Time	TIME				1..1
16	P	Restriction Valid To Date	DATE	Valid to date and time of the restriction.	Date and time must occur together. Must be greater than the Valid From date and time.		0..1
17	Q	Restriction Valid To Time	TIME				0..1

3.5.3.13. Limit

- Record Type: “Limit”

The record is used to create a Limit on a TIPS Credit Memorandum Balance.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.		1..1	
3	C	TIPS CMB Number	VARCHAR (34)	Unique number of the TIPS CMB		1..1	
4	D	Limit Type	Possible values: • BILI	Classification of the Limit: • BILI: ISO Code identifying a bilateral Limit set between an Account Owner and a counterparty (TIPS CMB User)		1..1	
5	E	Limit Amount	DEC (18,5)	Amount defined for the Limit		1..1	
6	F	Valid From	DATE	Starting validity date for the Limit		1..1	

3.5.3.14. Authorised Account User

- Record Type: “Authorised Account User”

The record is used to define Authorised Account Users for a TIPS Account.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.		1..1	
3	C	Cash Account Number	VARCHAR (34)	Unique number of the TIPS Cash Account		1..1	
4	D	Authorised Account User BIC	VARCHAR (11)	BIC code to authorise for the TIPS Cash Account		1..1	
5	E	Valid From	DATE	Starting validity date for the authorisation		1..1	
6	F	Valid To	DATE	Ending validity date for the authorisation		0..1	

3.5.3.15. Party Service Link

- Record Type: “Party Service Link”

The record is used to Link a Party to the Service TIPS.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.		1..1	
3	C	Parent BIC	CHAR (11)	Parent BIC of the party to link.		1..1	
4	D	Party BIC	CHAR (11)	Party BIC of the party to link.		1..1	
5	E	Service Name	Possible values: • TIPS	Classification of the Service Name: • TIPS: TIPS Settlement Service		1..1	
6	F	Valid From	DATE	Starting validity date for the link.		1..1	
7	G	Valid To	DATE	Ending validity date for the link		0..1	
8	H	Service Party Type	Possible values: • TPPT • TPRP	Classification of the Service Name: • TPPT: TIPS Participant • TPRP: Reachable Party		1..1	

3.5.3.16. DN-BIC Routing

- Record Type: “DN-BIC Routing”

The record is to define a Distinguished Name as Instructing Party for a specific BIC.

Flat file column	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.		1..1	
3	C	Distinguished Name	VARCHAR (256)	Distinguished Name to link to the BIC.	Interoperability character set restriction does not apply	1..1	
4	D	BIC	VARCHAR (11)	BIC to link to the Distinguished Name		1..1	
5	E	Inbound Flag	BOOLEAN	Classification of the type of link: • TRUE: Inbound • FALSE: Outbound		1..1	
6	F	Valid From	DATE	Starting validity date for		1..1	

				the link.			
7	G	Valid To	DATE	Ending validity date for the link		0..1	

3.6. Format of “Enriched Files”

The format of the enriched files is based on the format of the Excel and the flat files that have been submitted to TIPS DMT. The submitted data remains unchanged but is supplemented with “Further Notifications” and “Statistical Information”.

3.6.1. Further Notifications for Static Data records

This data appears in the first row of each Static Data record. It is located right to the migration data.

Flat file column	Excel Column	Field	Format	Description	Rules	Occurs per Record
last +1	last +1	Status	Possible values: • Migrated • Not migrated	Status of the migration.	n/a	1..1
last +2	last +2	Error Code	CHAR (4)	Code of the error.	Occurs when Status is ‘Not migrated’.	0..1
last +3	last +3	Error Description	VARCHAR (210)	Description of the error.	Occurs when Status is ‘Not migrated’.	0..1
last +4	last +4	Error Code 2	CHAR (4)	Code of the error.	Occurs when Status is ‘Not migrated’.	0..1
last +5	last +5	Error Description 2	VARCHAR (210)	Description of the error.	Occurs when Status is ‘Not migrated’.	0..1
last +6	last +6	Error Code 3	CHAR (4)	Code of the error.	Occurs when Status is ‘Not migrated’.	0..1
last +7	last +7	Error Description 3	VARCHAR (210)	Description of the error.	Occurs when Status is ‘Not migrated’.	0..1
last +8	last +8	Error Code 4	CHAR (4)	Code of the error.	Occurs when Status is ‘Not migrated’.	0..1
last +9	last +9	Error Description 4	VARCHAR (210)	Description of the error.	Occurs when Status is ‘Not migrated’.	0..1
last +10	last +10	Error Code 5	CHAR (4)	Code of the error.	Occurs when Status is ‘Not migrated’.	0..1
last	last	Error	VARCHAR (210)	Description of the error.	Occurs when Status is ‘Not	0..1

+11	+11	Description 5			migrated'.	

- "last" stands for the last column with migration data

3.6.2. Statistical Information

This data appears in the 2nd row of the spreadsheet. It is located right to the further notifications.

Flat file column	Excel Column	Field	Format	Description	Rules	Occurs per File
last +12	last +12	Submitted	NUMERIC (10)	Total number of records submitted.	n/a	1..1
last +13	last +13	Migrated	NUMERIC (10)	Total number of records that have been migrated successfully.	n/a	1..1
last +14	last + 14	Not Migrated	NUMERIC (10)	Total number or records that have not been migrated due to an error.	n/a	1..1

- "last" stands for the last column with migration data

4. Appendices

4.1. Business Rules

Due to the coexistence of CRDM and T2S SDMG, the business rules listed below may refer to certain concepts that are not applicable in CRDM-TIPS.

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DCC1001	When performing a Cash Account create request, the Party Type of the Requestor must be NCB or Payment Bank. Users belonging to NCBs can only create Cash Accounts for Parties that fall under their responsibility according to the Hierarchical Party Model, or TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility. Users belonging to Payment Banks can only create TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility. Exceptions to the above rules are represented by any user that is granted the appropriate privilege(s) on the specific Party to be linked to the account.	Create Cash Account	Requestor not allowed
DCC1024	When performing a Cash Account create request, the Restriction Type must refer to an existing Restriction Type with Object Restriction Type equal to Cash Account and belonging to the same system entity of the Cash Account or of the Service Operator.	Create Cash Account	Invalid restriction type

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DCC1025	When performing a Cash Account create request, the Valid From specified in the Cash Account Restriction section must be equal to or greater than the current timestamp.	Create Cash Account	“Valid From” invalid
DCC1100	When performing a Cash Account create request the Currency Code must refer to an existing instance in CRDM with Settlement Currency set to True or a Currency-Service Link in place with the relevant Service.	Create Cash Account	Currency Code not found
DCC1101	When performing a Cash Account create request the Floor Notification Amount specified must be less than the Ceiling Notification Amount.	Create Cash Account	Invalid Floor Notification Amount/Ceiling Notification Amount
DCC1103	When performing a Cash Account create request, the Cash Account Number must be compliant with ISO 20022 standards and it must not be already assigned to any other Cash Account in CRDM.	Create Cash Account	Cash Account Number already assigned
DCC1205	When performing a Cash Account create request the Opening Date must be equal to or greater than the current date and be equal or greater than the Account Holder Opening Date. Furthermore it must be equal to or less than the Account Holder Closing Date.	Create Cash Account	“Opening Date” invalid
DCC1206	When performing a Cash Account create request to create a T2S Dedicated Cash Account, RTGS Dedicated Transit Account or T2S Central Bank Account, the Linked Account must refer to an existing and open External RTGS Account instance in CRDM.	Create Cash Account	Invalid External RTGS account
DCC1207	When performing a Cash Account create request, if the Linked Account references an External RTGS Account it must have the same currency code of the Cash Account.	Create Cash Account	Invalid Currency code

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DCC1208	When performing a Cash Account create request, in case of request of creation of Cash Account Restriction, the Valid From of the Cash Account Restriction must be equal or greater than the Valid From of the Restriction Type entity.	Create Cash Account	“Valid From” invalid
DCC1209	When performing a Cash Account create request, in case of request of creation of Cash Account Restriction, the Valid To of the Cash Account Restriction must be equal or less than the Valid To of the Restriction Type entity.	Create Cash Account	“Valid To” invalid
DCC1210	When performing a Cash Account create request the Closing Date specified in the request must be equal to or greater than the Opening Date. Furthermore it must be equal to or less than the Account Holder Closing Date.	Create Cash Account	“Closing Date” invalid
DCC1212	When performing a Cash Account create request, the Valid To specified in the T2S Dedicated Cash Account Restriction section must be equal to or greater than the Valid From.	Create Cash Account	“Valid To” invalid
DCC1216	When performing a Cash Account create request to create a TIPS Credit Memorandum Balance the Linked Account must refer to an existing Cash Account instance in CRDM with type "TIPS Cash Account" which is open throughout the specified opening period of the TIPS CMB being created.	Create Cash Account	Invalid linked account
DCC1300	When performing a Cash Account Create request, in case of request for creation of a Cash Account Restriction, the created restriction must not overlap with any other Cash Account Restriction in input having the same Restriction Type.	Create Cash Account	Cash Account Restriction overlaps with existing instance
DCC1524	When performing a Cash Account create request, the account holding Party must refer to an existing active and open instance in CRDM with Party Type equal to NCB or Payment Bank.	Create Cash Account	Invalid Party Mnemonic
DCC1530	When performing a Cash Account create request, when creating an RTGS Dedicated Transit Account, no other	Create Cash	Transit account

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	account of the same type must be already associated to the relevant currency.	Account	already existing for this currency
DCC1531	When performing a Cash Account create request, when creating a T2S Dedicated Cash Account or a T2S central bank account, there must be an RTGS Dedicated Transit Account related to the relevant currency.	Create Cash Account	Transit account not found for this currency
DCC1532	When performing a Cash Account create request, when creating a TIPS Account, there must be a TIPS Transit Account related to the relevant currency.	Create Cash Account	Transit account not found for this currency
DCC1533	When performing a Cash Account create request, when creating a TIPS Transit Account, no other account of the same type must be already associated to the relevant currency.	Create Cash Account	Transit account already existing for this currency
DCC1555	When performing a Cash Account create request check the relation between the Account Type to be created and the Party Type of the account holder.	Create Cash Account	Invalid relations between account type and party type
DCC1800	When performing a Cash Account Create request, the number of decimals in the values provided for Floor Notification Amount and Ceiling Notification Amount must be compliant with the number of decimals foreseen for the relevant currency.	Create Cash Account	Invalid number of decimals
DCC2001	Authorised Account Users can be created only by the Service Operator, NCBs or Payment Banks. NCBs can create Authorised Account Users for Cash Accounts within their own System Entities. Payment Banks can create Authorised Account users for TIPS Accounts owned by them and for the TIPS CMBs	Create Authorised Account	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	linked to them.	User	
DCC2002	The Cash Account Identifier must refer to an existing, active and non-closed Cash Account with Account Type 'TIPS Account' or 'TIPS Credit Memorandum Balance'.	Create Authorised Account User	Unknown or invalid Cash Account
DCC2003	The BIC Mnemonic must refer to an existing and active BIC.	Create Authorised Account User	Unknown or invalid BIC
DCC2004	The Valid From must be equal to or greater than the current business date.	Create Authorised Account User	Valid From cannot be set to a past date
DCC2005	The Valid To must be equal to or greater than the current business date, and equal to or greater than the Valid From.	Create Authorised Account User	Valid To cannot be set to a past date or to a date before Valid From
DCC2006	At any given point in time, there cannot be more than one Authorised Account User for each BIC in any given Currency.	Create Authorised Account	Authorised Account user already defined for this BIC

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		User	in the related Cash Account Currency
DCC2007	At any given point in time, there cannot be more than one Authorised Account User for each TIPS Credit Memorandum Balance.	Create Authorised Account User	Authorised Account User already defined for this TIPS CMB
DCD1001	When performing a Cash Account delete or restore request, the Party Type of the Requestor must be NCB or Payment Bank. Users belonging to NCBs can only delete or restore Cash Accounts for Parties that fall under their responsibility according to the Hierarchical Party Model, or TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility. Users belonging to Payment Banks can only delete or restore TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility. Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the account or on the relevant Party holding the account.	Delete Cash Account	Requestor not allowed
DCD1003	The delete requests of Cash Accounts must refer to an existing and active instance. The account to be deleted must be already closed or must have Opening Date greater than the current date.	Delete Cash Account	Unknown Cash Account. The account must be

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
			closed or have Opening Date greater than the current date.
DCD1012	When performing a Cash Account restore request it must refer to an existing and deleted Cash Account. The account to be restored must have Closing date equal to or earlier than the Current Business date or Opening date equal to or later than the Current Business date; in addition, the Opening date must be equal to or later than the Account Holder Opening Date and the Closing Date must be equal to or earlier than the Account Holder Closing Date.	Delete Cash Account	Cash Account cannot be restored
DCD1013	When performing a Cash Account restore request, when restoring an RTGS Dedicated Transit Account or a TIPS Transit Account, no other Transit Account must be already associated to the relevant currency in the same validity period.	Delete Cash Account	Transit account already existing for this currency
DCD1014	When performing a Cash Account delete request, in case of deletion of a future RTGS Dedicated Transit Account or TIPS Transit Account, no active Cash Accounts with the same currency for T2S or TIPS respectively must exist in T2S.	Delete Cash Account	Deletion not allowed due to open Cash Accounts related to this Transit Account
DCD1030	A Cash Account cannot be deleted if there still are valid instances of the following entities linked to it: Liquidity Transfer Order, Liquidity Transfer Order Link Set, Credit Memorandum Balance, TIPS Credit Memorandum Balance-type Cash Account.	Delete Cash Account	The deletion/close is not allowed due to a deletion priority constraint

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DCD1082	When performing a Cash Account restore request the currency code of the Cash Account to be restored must refer to an existing currency code in CRDM with Settlement Currency set to True or a Currency-Service Link in place with the relevant Service.	Delete Cash Account	Unknown currency code
DCD1083	When performing a Cash Account restore request the account holder must be an existing and active Party in CRDM with Party Type equal to NCB or Payment Bank.	Delete Cash Account	Unknown Party
DCD1084	When performing a Cash Account restore request, all restrictions associated to the Cash Account to be restored must refer to existing Restriction Types whose Object Restriction Type is Cash Account.	Delete Cash Account	Invalid restriction type
DCD1085	When performing a Cash Account restore request the Linked Account of the T2S Dedicated Cash Account, T2S Central Bank Account or RTGS Dedicated Transit Account to be restored must refer to an existing External RTGS Account in T2S.	Delete Cash Account	Unknown External RTGS Account
DCD1086	When performing a Cash Account restore request the Linked Account of the TIPS Credit Memorandum Balance to be restored must refer to an existing and open TIPS Account in CRDM.	Delete Cash Account	Unknown linked Cash Account
DCD1207	When performing a Cash Account restore request, if the Cash Account to be restored is linked to an External RTGS Account, they must have the same currency code.	Delete Cash Account	Invalid External RTGS Account Currency Code
DCD1532	When performing a Cash Account restore request, the validity period of a TIPS Account, T2S Dedicated Cash Account or T2S Central Bank Account must be consistent with the validity period of the relevant Transit Account.	Delete Cash Account	Transit Account not found or not valid
DCD1555	When performing a Cash Account restore request the relation between the Account Type to be restored and the Party Type of the account holder is checked.	Delete Cash Account	Invalid relations between account

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
			type and party type
DCD2001	Authorised Account Users can be deleted or restored only by the Service Operator, NCBs or Payment Banks. NCBs can delete or restore Authorised Account Users within their own System Entities. Payment Banks can delete or restore Authorised Account Users for Cash Accounts owned by them.	Delete Authorised Account User	Requestor not allowed
DCD2002	Deletion requests must refer to existing, active and closed Authorised Account Users.	Delete Authorised Account User	Unknown, deleted or open Authorised Account User
DCD2003	Restore requests must refer to existing, deleted and non-open Authorised Account Users.	Delete Authorised Account User	Unknown, active or open Authorised Account User
DCD2004	In a restore request, the Cash Account Identifier must refer to an existing, active and non-closed Cash Account with Account Type 'TIPS Account' or 'TIPS Credit Memorandum Balance'.	Delete Authorised Account User	Unknown, deleted, closed or invalid Cash Account
DCD2005	In a restore request, the BIC Mnemonic must refer to an existing and active BIC.	Delete Authorised Account	Unknown or deleted BIC

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		User	
DCD2006	At any given point in time, there cannot be more than one Authorised Account User for each BIC in any given Currency.	Delete Authorised Account User	Authorised Account user already defined for this BIC
DCD2007	At any given point in time, there cannot be more than one Authorised Account User for each TIPS Credit Memorandum Balance.	Delete Authorised Account User	Authorised Account User already defined for this TIPS CMB
DCD2008	In a delete request, there cannot be any DN-BIC Routing instances referencing the same BIC as the Authorised Account User.	Delete Authorised Account User	Deletion not allowed due to a priority constraint
DCR1001	When performing a request to read a Cash Account, the requestor must be authorised to access the requested data according to the following: A Service Operator user can access all data An NCB user can access only data belonging to its own System Entity A Payment Bank user can access only its own data Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the account or on the specific Party linked to the account	Read Cash Account	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DCR1002	A request to read a Cash Account must refer to existing data in CRDM.	Read Cash Account	No data available
DCU1001	When performing a Cash Account update request the Party Type of the Requestor must be NCB or Payment Bank. Users belonging to NCBs can only update Cash Accounts for Parties that fall under their responsibility according to the Hierarchical Party Model, or TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility. Users belonging to Payment Banks can only update TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility. Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the account or on the relevant Party holding the account.	Update Cash Account	Requestor not allowed
DCU1003	The update requests of a Cash Account must refer to an existing and active account. Furthermore, the Closing Date must be equal to or greater than the current date.	Update Cash Account	Data to be updated not found
DCU1024	When performing a Cash Account update request, in case of request of creation of Cash Account Restriction, the Restriction Type must refer to an existing Restriction Type with Object Restriction Type equal to Cash Account and belonging to the same system entity of the Cash Account or of the Service Operator.	Update Cash Account	Invalid restriction type
DCU1030	A Cash Account cannot be closed if there still are valid instances of the following entities linked to it: Liquidity	Update Cash	The account cannot be closed due to a

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	Transfer Order, Liquidity Transfer Order Link Set.	Account	closure priority constraint
DCU1040	When performing a Cash Account update request, any update of the Opening Date and Closing Date must be consistent with the validity periods of other existing Cash Accounts with type 'TIPS Credit Memorandum Balance' linking to it.	Update Cash Account	Opening/Closing Date not consistent with linked TIPS CMB
DCU1101	When performing a Cash Account update request, the Floor Notification Amount must be less than the Ceiling Notification Amount	Update Cash Account	Invalid Floor Notification Amount/Ceiling Notification Amount
DCU1204	When performing a Cash Account update request, the Linked Account can be specified only for TIPS Credit Memorandum Balances, RTGS Dedicated Transit Accounts, T2S Central Bank Accounts and T2S Dedicated Cash Accounts.	Update Cash Account	Invalid use of Linked Account
DCU1206	When performing a Cash Account update request, the Linked Account, when it refers to an External RTGS Cash Account, must refer to an existing and open instance in T2S.	Update Cash Account	Invalid External RTGS account
DCU1207	When performing a Cash Account update request, if the Linked Account references an External RTGS Account it must have the same currency code of the Cash Account.	Update Cash Account	Invalid External RTGS account
DCU1210	When performing a Cash Account update request, the Closing Date must be equal to or greater than the current date and equal to or greater than the Cash Account Opening Date. Furthermore it must be equal to or less than the Account Holder Closing Date.	Update Cash Account	“Closing Date” Invalid

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DCU1211	When performing a Cash Account update request, in case of request of creation of Cash Account Restriction, the Valid From must be equal to or greater than the current timestamp.	Update Cash Account	“Valid From” invalid
DCU1212	When performing a Cash Account update request, in case of request of creation/update of Cash Account Restriction, the Valid To specified in the Cash Account Restriction section must be equal to or greater than the current timestamp and must be equal to or greater than the Valid From.	Update Cash Account	“Valid To” invalid
DCU1213	When performing a T2S Dedicated Cash Account update request, the Opening Date can be updated only if the existing one is greater than the current date and the new one must be equal to or greater than the current date. Furthermore it must be equal to or greater than the Account Holder Opening Date and equal to or less than the Account Holder Closing Date.	Update Cash Account	“Opening Date” Invalid
DCU1214	When performing a Cash Account update request on the Linked Account, Opening Date and/or Closing Date of a TIPS Credit Memorandum Balance, the Linked Account must refer to an existing Cash Account instance in CRDM with type "TIPS Cash Account" which is open throughout the specified validity period of the TIPS CMB being updated.	Update Cash Account	Invalid linked account
DCU1216	When performing a Cash Account update request, in case of request of deletion of Cash Account Restriction, the Valid From must be greater than the current timestamp or the Cash Account Restriction must be closed.	Update Cash Account	Restriction cannot be deleted
DCU1217	When performing a Cash Account update request, case of request of update of Cash Account Restriction, it must refer to an existing Cash Account Restriction with a non-past Valid To.	Update Cash Account	Account is not restricted
DCU1218	When performing a Cash Account update request, the specified Currency Code must refer to the one already linked to the existing Cash Account.	Update Cash Account	Invalid Currency Code

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DCU1219	When performing a Cash Account update request, in case of request of creation of Cash Account Restriction, the Valid From of the Cash Account Restriction must be equal or greater than the Valid From of the Restriction Type.	Update Cash Account	“Valid From” invalid
DCU1220	When performing a Cash Account update request, in case of request of creation of Cash Account Restriction, the Valid To of the Cash Account Restriction must be equal or less than the Valid To of the Restriction Type.	Update Cash Account	“Valid To” invalid
DCU1300	When performing a Cash Account Update request, in case of request for creation/update of Cash Account Restriction, the new or updated restriction must not overlap with any other Cash Account Restrictions having the same Restriction Type on the same Cash Account.	Update Cash Account	Cash Account Restriction overlaps with existing instance
DCU1313	When performing a Cash Account update request, in case of update of the Opening or Closing Date of an RTGS Dedicated Transit Account or TIPS Transit Account, no active Cash Account with the same currency for T2S and TIPS respectively must be open outside of the Transit Account validity period.	Update Cash Account	Open Cash Accounts exist related to this Transit Account
DCU1532	When performing a Cash Account Update request, the validity period of the TIPS Account, T2S Dedicated Cash Account or T2S Central Bank Account must be contained within the validity period of the relevant Transit Account.	Update Cash Account	No valid Transit Account found for the specified validity period
DCU1555	When performing a Cash Account Update request, Cash Accounts for TIPS require an existing and active Party-Service Link to be in place between the Owner Party and TIPS for the relevant validity period.	Update Cash Account	Party-Service Link for TIPS not found or not valid

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DCU1800	When performing a Cash Account Update request, the number of decimals in the values provided for Floor Notification Amount and Ceiling Notification Amount must be compliant with the number of decimals foreseen for the relevant currency.	Update Cash Account	Invalid number of decimals
DCU2001	Authorised Account Users can be updated only by the Service Operator, NCBs or Payment Banks. NCBs can update Authorised Account Users within their own System Entities. Payment Banks can update Authorised Account users for TIPS Accounts owned by them and for the TIPS CMBs linked to them.	Update Authorised Account User	Requestor not allowed
DCU2002	The Authorised Account User to be updated must refer to an existing, active and non-closed instance.	Update Authorised Account User	Unknown or invalid Authorised Account User
DCU2003	The Valid From can be updated only if the current value is later than the current business date.	Update Authorised Account User	Valid From cannot be modified
DCU2004	The modified Valid From must be equal to or later than the current business date and equal to or earlier than the Valid From of all DN-BIC Routing instances referencing the same BIC as the Authorised Account User.	Update Authorised Account User	Valid From cannot be set to a past date or later than existing DN-BIC Routing Valid From

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DCU2005	The Valid To must be equal to or later than the current business date, equal to or later than the Valid From and equal to or later than the Valid To of all DN-BIC Routing instances referencing the same BIC as the Authorised Account User.	Update Authorised Account User	Valid To cannot be set to a past date, to a date before Valid From or earlier than existing DN-BIC Routing Valid To
DCU2006	At any given point in time, there cannot be more than one Authorised Account User for each BIC in any given Currency.	Update Authorised Account User	Authorised Account user already defined for this BIC in the related Cash Account Currency
DCU2007	At any given point in time, there cannot be more than one Authorised Account User for each TIPS Credit Memorandum Balance.	Update Authorised Account User	Authorised Account User already defined for this TIPS CMB
DPC1001	A Party can be created only by Service Operator, CSD or NCB. A user belonging to a CSD or NCB can only create parties that fall under their responsibility according to the Hierarchical Party Model. Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the Party responsible for the Party to be created.	Create Party	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DPC1002	When performing a Party Create request, the 'System Entity' specified in input must refer to an existing instance in CRDM, and its type must be consistent with the 'Party Type' specified in input.	Create Party	Invalid System Entity Identifier
DPC1005	When performing a Party Create request, the Party Type cannot be 'CSD' or 'NCB' if there is already a CSD or NCB defined within the System Entity.	Create Party	Only one CSD/NCB per System Entity allowed
DPC1013	When performing a Party Create request, the 'Party Mnemonic' specified in the Party Code section must not be already assigned to another active Party belonging to the same System Entity and having the same Parent BIC.	Create Party	Party Mnemonic already used
DPC1021	When performing a Party Create request, the 'Country Code' specified in the Party Address section must refer to an existing Country Code in CRDM.	Create Party	Invalid country code
DPC1024	When performing a Party Create request, In case of request for creation of Party Restriction, the created restriction type must refer to an existing type in [Restriction Type] entity with Object Restriction Type 'Party'.	Create Party	Invalid restriction type
DPC1025	When performing a Party Create request, In case of request for creation of Party Restriction, the created restriction type must not overlap with any other Party Restriction in input having the same [Restriction Type].	Create Party	Party Restriction overlaps with existing instance
DPC1180	When performing a Party Create request, the 'Party Mnemonic' specified in the Party Code section (when its type is BIC) must exist in the BIC Directory.	Create Party	Party Mnemonic not found in BIC directory
DPC1205	When performing a Party Create request, the Party Opening Date specified in the request must be equal to or greater than the current date.	Create Party	"Opening Date" invalid

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DPC1206	When performing a Party Create request, the Party Closing Date, if specified, must be equal to or greater than the current date and greater than the Opening Date.	Create Party	“Closing Date” invalid
DPC1207	When performing a Party Create request, the Party Restriction ‘Valid To’, when specified, must be equal to or greater than the current timestamp, equal to or greater than the Party Restriction Valid From and equal to or less than the Valid To of the relevant Restriction Type entity.	Create Party	“Valid To” invalid
DPC1208	When performing a Party Create request, the Party Restriction ‘Valid From”, when specified, must be equal to or greater than the current timestamp and equal to or greater than the Valid From of the relevant Restriction Type entity and equal to or less than the Valid To of the relevant Restriction Type entity.	Create Party	“Valid From” invalid
DPC1252	When performing a Party Create request, in case of request for creation of Market-Specific Party Attribute Value, it must refer to an existing Market-Specific Attribute with Type “Party” and it must belong to the relevant System Entity.	Create Party	Invalid Market-Specific Party Attribute Value
DPC1254	When performing a Party Create request, in case of request for creation of Market-Specific Party Attribute Value, it must be unique within its System Entity in case it is defined as such in CRDM.	Create Party	The value for the Market-Specific attribute is already used (and it must be unique)
DPC1256	When performing a Party Create request, in case of request for creation of a Market-Specific Party Attribute, the Market-Specific Attribute Value must be present if the relevant Market-Specific Attribute is defined as mandatory.	Create Party	Missing mandatory Market-Specific attribute value

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DPC1257	When performing a Party create request the Market-Specific Party Attribute Value must be compliant with the values or rules defined in the relevant Attribute Domain.	Create Party	Invalid Market-Specific Party Attribute Value
DPC1300	When performing a Party Create request, the 'Valid From' specified in the Party Code section, must be equal to the current business date.	Create Party	"Valid From" invalid
DPC1301	When performing a Party Create request, the 'Valid From' specified in the Party Address section, must be equal to the current business date.	Create Party	"Valid From" invalid
DPC1302	When performing a Party Create request, the 'Valid From' specified in the Party Name section, must be equal to the current business date.	Create Party	"Valid From" invalid
DPC1303	When performing a Party Create request, the Maximum Credit Percentage and the Use of Maximum Credit Percentage specified in Autocollateralisation Rule section, must not be filled in in case the Party Type is not NCB.	Create Party	Use of Maximum Percentage is not allowed for Payment Bank
DPC1304	When performing a Party Create request, the Collateralisation Procedure specified in Autocollateralisation Rule section, must be equal to Repo in case the Party Type is not NCB.	Create Party	Collateralisation Procedure must be equal to Repo for Payment Bank
DPC1305	When performing a Party Create request, the Party Address section must not be filled in if the Party Type is CSD Participant.	Create Party	Party Address must not be defined for

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
			CSD Participant
DPC1306	When performing a Party Create request, the Autocollateralisation Rule section must not be filled in if the Party Type is not NCB or Payment Bank.	Create Party	Autocollateralisation Rule is allowed only for NCB or Payment Bank.
DPC3001	Technical Address Network Service Link can only be created by Service Operator, CSD or NCB. A user belonging to a CSD or NCB can only create Technical Address Network Service Links that fall under their responsibility according to the Hierarchical Party Model.	Create Technical Address Network Service Link	Requestor not allowed
DPC3002	When performing a Technical Address Network Service Link create request, the Party must refer to an existing and active Party in CRDM.	Create Technical Address Network Service Link	Unknown party
DPC3003	When performing a Technical Address Network Service Link create request, the Technical Address must refer to an existing, active Technical Address in CRDM belonging to the Party provided in input.	Create Technical Address Network Service Link	Unknown technical address

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DPC3004	When performing a Technical Address Network Service Link create request, the Network Service must refer to an existing, active Network Service in CRDM.	Create Technical Address Network Service Link	Unknown network service
DPC3005	When performing a Technical Address Network Service Link create request, the Technical Address Type provided in input must be compliant with the Technical Address Type of the Network Service provided.	Create Technical Address Network Service Link	Invalid Technical Address Type
DPC3006	When performing a Technical Address Network Service Link create request, each Party can have no more than one link to a Network Service for TIPS notifications and reports.	Create Technical Address Network Service Link	Technical Address Network Service Link for TIPS already defined for Party
DPC4001	Party-Service Links can be created only by the Service Operator, CSDs or NCBs. CSDs and NCBs can create Links for Parties within their own System Entities, but not for their own Party.	Create Party-Service Link	Requestor not allowed
DPC4002	The Party Identifier must refer to an existing, active and non-closed Party.	Create Party-Service Link	Unknown, deleted or closed Party
DPC4003	The Service Identifier must refer to an existing and active Service.	Create Party-	Unknown or deleted

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		Service Link	Service
DPC4004	The Valid From must be equal to or greater than the current business date.	Create Party-Service Link	Valid From cannot be set to a past date
DPC4005	The Valid To must be equal to or greater than the current business date, and equal to or greater than the Valid From.	Create Party-Service Link	Valid To cannot be set to a past date or to a date before Valid From
DPC4006	The Service Party Type must be consistent with the linked Party Type.	Create Party-Service Link	Service Party Type is not consistent with linked Party
DPC4007	The Service Party Type must be consistent with the linked Service.	Create Party-Service Link	Service Party Type is not consistent with linked Service
DPC4008	At any given point in time, there cannot be more than one Party-Service Link between a given Party-Service couple.	Create Party-Service Link	Validity period overlaps with duplicate Party-Service Link entry
DPC4009	At any given point in time, there cannot be more than one Party-Service Link for TIPS for multiple Payment Bank Parties with the same Party BIC.	Create Party-Service Link	TIPS Party-Service Link already

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
			defined for this Party BIC
DPD1001	Party can only be deleted or restored by the Service Operator, CSD or NCB. A user belonging to a CSD or NCB can only delete or restore parties that fall under their responsibility according to the Hierarchical Party Model. Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the specific Party to be maintained.	Delete Party	Requestor not allowed
DPD1003	When performing a Party Delete request, it must refer to an existing, active and closed Party or with a future Opening date.	Delete Party	Unknown party
DPD1004	When performing a Party Restore request, it must refer to an existing and deleted Party already closed or with an Opening date equal to or greater than the current business date.	Delete Party	Party is not deleted
DPD1005	When performing a Party Restore request, the Party Type cannot be ‘CSD’ or ‘NCB’ if there is already a CSD or NCB defined within the System Entity.	Delete Party	Only one CSD/NCB per System Entity allowed
DPD1013	When performing a Party Restore request, the ‘PartyMnemonic specified in the PartyCode section must not be already assigned to an active party having the same Party Type and belonging to the same System Entity and having the same Parent BIC in case the Party to be restored is not closed.	Delete Party	Party Mnemonic already used
DPD1021	When performing a Party Restore request, the ‘Country Code’ specified in the Party Address section must refer to an existing Country Code in CRDM.	Delete Party	Invalid country code
DPD1024	When performing a Party Restore request, the ‘Restriction Type’ specified in the Party Restriction section must	Delete Party	Invalid restriction

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	refer to an existing type in CRDM available for the relevant System Entity.		type
DPD1030	In case of request to delete a Party, all the linked instances in a higher position within the deletion hierarchy (i.e. Securities Account, Cash Account, External RTGS Account, Security CSD Link, CSD Account Link and Party) must be deleted.	Delete Party	The deletion is not allowed due to a deletion priority constraint
DPD1040	When performing a Party Restore request, the 'Technical Address' specified in the Party Technical Address section must exist in the BIC Directory, when its type is BIC.	Delete Party	Technical Address not found in BIC directory
DPD1180	When performing a Party Restore request, the 'Party Mnemonic' specified in the Party Code section (when its type is BIC) must exist in the BIC Directory.	Delete Party	Party Mnemonic not found in BIC directory
DPD1207	When performing a Party restore request, the Party Restriction 'Valid To', when specified, must be equal to or less than the Valid To of the relevant Restriction Type entity.	Delete Party	"Valid To" invalid
DPD1208	When performing a Party restore request, the Party Restriction 'Valid From", when specified, must be equal to or greater than the Valid From of the relevant Restriction Type entity and equal to or less than the Valid To of the relevant Restriction Type entity.	Delete Party	"Valid From" invalid
DPD1252	In case of restore of Market-Specific Party Attribute Value, it must refer to an existing Market-Specific Attribute with Type "Party" and it must belong to the relevant System Entity.	Delete Party	Invalid Market-Specific Party Attribute Value

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DPD1254	In case of request for restore of Market-Specific Party Attribute Value, the Value must be unique (within its System Entity) if it is defined as “unique” in [Market-Specific Attribute] entity.	Delete Party	Market-Specific Party Attribute Value already used
DPD1256	When performing a Party Restore request, the Market-Specific Attribute Value must be present if the relevant Market-Specific Attribute is defined as mandatory.	Delete Party	Missing mandatory Market-Specific attribute value
DPD1257	When performing a Party restore request the Market-Specific Party Attribute Value must be compliant with the values or rules defined in the relevant Attribute Domain.	Delete Party	Invalid Market-Specific Party Attribute Value
DPD3001	Technical Address Network Service Link can only be deleted/restored by Service Operator, CSD or NCB. A user belonging to a CSD or NCB can only delete/restore Technical Address Network Service Links that fall under their responsibility according to the Hierarchical Party Model.	Delete Technical Address Network Service Link	Requestor not allowed
DPD3003	When performing a Technical Address Network Service Link Delete request, it must refer to an existing and active instance.	Delete Technical Address Network Service Link	Unknown Technical Address Network Service Link
DPD3004	When performing a Technical Address Network Service Link restore request, it must refer to an existing and	Delete	Technical Address

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	deleted Technical Address Network Service Link.	Technical Address Network Service Link	Network Service Link is not deleted
DPD3005	When performing a Technical Address Network Service Link restore request, the 'Technical Address' linked must refer to an existing, active Technical Address in CRDM.	Delete Technical Address Network Service Link	Unknown Technical Address
DPD3006	When performing a Technical Address Network Service Link Restore request, the 'Party' linked must refer to an existing, active party in CRDM.	Delete Technical Address Network Service Link	Unknown Party
DPD3007	When performing a Technical Address Network Service Link restore request, the 'Network Service' linked must refer to an existing, active Network Service in CRDM.	Delete Technical Address Network Service Link	Unknown Network Service
DPD3008	When performing a Technical Address Network Service Link restore request, it must refer to a 'Technical Address' belonging to the same linked Party in CRDM.	Delete Technical	Technical Address not belongs to the

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		Address Network Service Link	linked party
DPD3009	When performing a Technical Address Network Service Link restore request, each Party can have no more than one link to a Network Service for TIPS notifications and reports.	Delete Technical Address Network Service Link	Technical Address Network Service Link for TIPS already defined for Party
DPD4001	Party-Service Links can be deleted or restored only by the Service Operator, CSDs or NCBs. CSDs and NCBs can delete or restore Links within their own System Entities, but not for their own Party.	Delete Party-Service Link	Requestor not allowed
DPD4002	Deletion requests must refer to existing, active and closed Party-Service Links.	Delete Party-Service Link	Unknown, deleted or open Party-Service Link
DPD4003	Restore requests must refer to existing, deleted and non-open Party-Service Links.	Delete Party-Service Link	Unknown, active or open Party-Service Link
DPD4004	In a restore request, the linked Party must be an existing, active and non-closed Party.	Delete Party-Service Link	Unknown, deleted or closed Party
DPD4005	In a restore request, the linked Service must be an existing and active Service.	Delete Party-Service Link	Unknown or deleted Service

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DPD4006	At any given point in time, there cannot be more than one Party-Service Link between a given Party-Service couple.	Delete Party-Service Link	Validity period overlaps with duplicate Party-Service Link entry
DPD4007	At any given point in time, there cannot be more than one Party-Service Link for TIPS for multiple Payment Bank Parties with the same Party BIC.	Delete Party-Service Link	TIPS Party-Service Link already defined for this Party BIC
DPR1001	When performing a request to read a Party, the requestor must be authorised to access the requested data according to the following: The Service Operator user can access all data A CSD or NCB user can access only data belonging to its own System Entity A CSD Participant or Payment Bank user can access only its own data Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) to read the specified Party or the Party responsible for it.	Read Party	Requestor not allowed
DPR1002	A request to read a Party must refer to existing data in CRDM.	Read Party	No data available
DPU1001	Party can only be updated by the Service Operator, CSD or NCB. A user belonging to a CSD or NCB can only update parties that fall under their responsibility according to the Hierarchical Party Model. Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the specific Party to be	Update Party	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	maintained.		
DPU1003	When performing a Party Update request, it must refer to an existing and active Party whose Closing Date is equal to or greater than the current business date.	Update Party	Unknown Party
DPU1005	When performing a Party Update request, the update request of a “minor” entity (such as Party Name, Party code, Party Address,Market-Specific Attribute, Party Restriction, AutoCollateralisation Rule) must refer to an existing and active instance with a non-past Valid To, where applicable.	Update Party	Unknown minor entity
DPU1006	Each party must have at least one party technical address.	Update Party	Missing mandatory section/field
DPU1007	When performing a Party Update request, in case of request for creation of Party Technical Address, the PTA specified cannot be identical to a PTA already linked to the relevant Party.	Update Party	Party Technical address already defined for Party
DPU1009	When performing a Party Update request, the create request of a historical (i.e. which has the validity date) “minor” entity (such as Party Name Party code, Party Address) cannot have a past validity date.	Update Party	“Opening Date” or “Close Date” invalid
DPU1010	When performing a Party Update request, the delete request of a historical (i.e. which has the validity date) “minor” entity (such as Party Name, Party Address) cannot refer to an entity having a past validity date. This does not apply to the Party Code, for which only the currently active entity cannot be deleted.	Update Party	Instance with past validity date cannot be deleted
DPU1013	When performing a Party Update request, the ‘Party Mnemonic’ specified in the Party Code section must not be	Update Party	Party Mnemonic

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	already assigned, as an active instance, to another active Party belonging to the same System Entity and having the same Parent BIC.		already used
DPU1021	When performing a Party Update request, the 'Country Code' specified in the Party Address section must refer to an existing Country Code in CRDM.	Update Party	Invalid country code
DPU1024	When performing a Party Update request, in case of request for creation of Party Restriction, the created restriction type must refer to an existing type in [Restriction Type] entity with Object Restriction Type 'Party'.	Update Party	Invalid restriction type
DPU1025	When performing a Party Update request, in case of request for deletion of Party Restriction, it must refer to a closed instance or its Valid From must be greater than the current timestamp.	Update Party	Invalid restriction type
DPU1030	When performing a Party Update request, in case of request to close a Party, all the linked instances in a higher position within the deletion hierarchy (i.e. Securities Account, Cash Account, External RTGS Account, Security CSD Link and CSD Account link, Party) must be closed or deleted.	Update Party	The deletion/close is not allowed due to a deletion priority constraint
DPU1180	When performing a Party Update request, the 'Party Mnemonic' specified in the Party Code section (when its type is BIC) must exist in the BIC Directory.	Update Party	Party Mnemonic not found in BIC directory
DPU1205	When performing a Party Update request, in case of Closing of [Party], the specified 'Closing Date' must be equal to or greater than the current business date.	Update Party	"Opening Date" or "Close Date" invalid
DPU1206	When performing a Party Update request, it is only possible to update the 'Opening Date' if it is greater than the current T2S date. The new specified value must be equal to or greater than the current T2S date and it must not	Update Party	"Opening Date" or "Close Date" invalid

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	be greater than the opening date of the DCA for which the party is the Account holder.		
DPU1207	When performing a Party Update request, the specified Party Restriction 'Valid To' must be equal to or greater than the current timestamp, greater than the relevant Valid From, equal to or greater than the Valid From of the relevant Restriction Type and equal to or less than the Valid To of the relevant Restriction Type.	Update Party	"Valid To" invalid
DPU1208	When performing a Party update request, the Valid From specified in a Party Restriction create request must be equal to or greater than the current timestamp, equal to or greater than the Valid From of the relevant Restriction Type and equal to or less than the Valid To of the relevant Restriction Type.	Update Party	"Valid From" invalid
DPU1252	When performing a Party Update request, in case of request for creation/update of Market-Specific Party Attribute Value, it must refer to an existing Market-Specific Attribute with Type "Party" and it must belong to the relevant System Entity.	Update Party	Invalid Market-Specific Party Attribute Name
DPU1254	When performing a Party Update request, in case of request for creation/update of Market-Specific Party Attribute Value, it must be unique within its System Entity in case it is defined as such in CRDM.	Update Party	The value for the Market-Specific attribute is already used (and it must be unique)
DPU1255	When performing a Party Update request, in case of request for deletion of a Market-Specific Party Attribute, the relevant [Market-Specific Attribute] entity must not be defined as "mandatory".	Update Party	Missing mandatory section/field

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DPU1256	When performing a Party Update request, in case of request for update of a Market-Specific Party Attribute, the Market-Specific Attribute Value must be present if the relevant [Market-Specific Attribute] is defined as mandatory.	Update Party	Missing mandatory Market-Specific attribute value
DPU1257	When performing a Party update request the Market-Specific Party Attribute Value must be compliant with the values or rules defined in the relevant Attribute Domain.	Update Party	Invalid Market-Specific Party Attribute Name
DPU1258	When performing a Party Update request, each Market-Specific Attribute can have no more than one value for a given Party.	Update Party	Market-Specific Attribute cannot have more than one value for this Party
DPU1300	When performing a Party Update request, in case of request for creation/update of Party Restriction, the new or updated restriction must not overlap with any other Party Restriction having the same Restriction Type on the same Party.	Update Party	Party Restriction overlaps with existing instance
DPU1303	When performing a Party update request, the Maximum Credit Percentage and the Use of Maximum Credit Percentage specified in Autocollateralisation Rule section, must not be filled in in case the Party Type is not NCB.	Update Party	Maximum Credit Percentage is not allowed for

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
			Payment Bank
DPU1304	When performing a Party update request, the Collateralisation Procedure specified in Autocollateralisation Rule section, must be equal to Repo in case the Party Type is not NCB.	Update Party	Collateralisation Procedure must be equal to Repo for Payment Bank
DPU1305	When performing a Party update request, the Party Address section must not be filled in if the Party Type is CSD Participant.	Update Party	Party Address must not be defined for CSD Participant
DPU1306	When performing a Party update request, the Autocollateralisation Rule section must not be filled in if the Party Type is not NCB or Payment Bank.	Update Party	Autocollateralisation Rule is allowed only for NCB or Payment Bank.
DPU1308	When performing a Party update request, the request of creation of the Autocollateralisation Rule is not allowed in case Rules have already been defined.	Update Party	Autocollateralisation Rule already exists for the specified Party
DPU1350	When performing a Party Update request to change the Party BIC, there cannot be more than one Party, besides the Central Bank, with the same BIC linked to the TIPS service.	Update Party	Party BIC already linked to the TIPS

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
			service
DPU1351	When performing a Party Update request to change the Party BIC, there cannot be more than one User flagged as Main User for the same Certificate DN and the same Party BIC.	Update Party	Main User already exists for this Party BIC
DPU1500	When performing a Party Update request, the update request of a historical “minor” entity (such as Party Name, Party Address) must refer to an instance currently in use or having a future validity.	Update Party	Minor entity is not the one currently in use or the future one
DPU1501	When performing a Party Update request, the update request of Party Code must refer to an instance having a future validity.	Update Party	Party Code to be updated must have a future validity
DPU4001	Party-Service Links can be updated only by the Service Operator, CSDs or NCBs. CSDs and NCBs can update Links within their own System Entities, but not for their own Party.	Update Party-Service Link	Requestor not allowed
DPU4002	Update requests must refer to existing, active and open Party-Service Links.	Update Party-Service Link	Unknown, deleted or closed Party-Service Link
DPU4003	The Valid From can only be modified if the current Valid From is later than the current business date.	Update Party-Service Link	Valid From cannot be modified

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DPU4004	The Valid From must be equal to or greater than the current business date.	Update Party-Service Link	Valid From cannot be set to a past date
DPU4005	The Valid To must be equal to or greater than the current business date and equal to or greater than the Valid From.	Update Party-Service Link	Valid To cannot be set to a past date or to a date before Valid From
DPU4006	At any given point in time, there cannot be more than one Party-Service Link between a given Party-Service couple.	Update Party-Service Link	Validity period overlaps with duplicate Party-Service Link entry
DPU4007	The Valid To must be equal to or greater than the Closing Date of every Cash Account owned by the linked Party for the relevant linked Service.	Update Party-Service Link	Party-Service Link cannot be closed due to a priority constraint
DPU4008	At any given point in time, there cannot be more than one Party-Service Link for TIPS for multiple Payment Bank Parties with the same Party BIC.	Update Party-Service Link	TIPS Party-Service Link already defined for this Party BIC
DRC0001	A Certificate DN can be created only by users with the correct privilege.	Create User-	Requestor not

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		Certificate DN Link	allowed
DRC0002	When performing a User Certificate DN creation request, the specified User must be within the System Entity of the requestor (if the requestor is a CSD or NCB) or within the Party of the requestor (if the requestor is a Payment Bank, External CSD or CSD Participant)	Create User-Certificate DN Link	Invalid User
DRC0003	When performing a User Certificate DN creation request, the specified User must be an existing and active instance in T2S.	Create User-Certificate DN Link	Unknown or not active User
DRC0004	When performing a User Certificate DN creation request, the specified Certificate DN must be an existing and active instance in T2S.	Create User-Certificate DN Link	Unknown or not active Certificate DN
DRC0005	When performing a User Certificate DN creation request, there cannot be more than one active link between the same User and Certificate DN.	Create User-Certificate DN Link	Link already exists
DRC0006	When performing a User Certificate DN creation request, there can only be one User Certificate DN with Default flag set to TRUE for any given Certificate.	Create User-Certificate DN Link	Default Link already exists
DRC0007	When performing a User Certificate DN creation request, there can only be one User Certificate DN with Main User flag set to TRUE for all the Users of any Party using the same BIC.	Create User-Certificate DN Link	Main User already exists for the same Party BIC

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRC6001	A Role can be created only by Service Operator, CSD or NCB.	Create Role	Requestor not allowed
DRC6006	When performing a Role creation request, the Role Name specified must not be already assigned within the same System Entity.	Create Role	Role Name already assigned
DRC7001	A User can be created by Service Operator, CSD, NCB, CSD Participant, External CSD or Payment Bank. Users belonging to CSDs, NCBs, CSD Participants, External CSDs and Payment Banks can only create users that fall under their responsibility according to the Hierarchical Party Model.	Create User	Requestor not allowed
DRC7005	When performing a User Create request, the specified Party Technical Identifier must refer to an existing, active and open or future Party in CRDM.	Create User	Unknown Party Technical Identifier
DRC7006	When performing a User Create request, the Login Name specified must not be already assigned to another User in CRDM.	Create User	User Name already assigned
DRC7007	When performing a User Create request, the System User Reference must not be already assigned to another User in CRDM.	Create User	Unknown Party Technical Identifier
DRC8001	DN-BIC Routing can be created only by the Service Operator, NCBs or Payment Banks. NCBs can create DN-BIC Routing acting on behalf of their TIPS Participants. Payment Banks can create DN-BIC Routing for the BIC which currently identifies their own Party.	Create DN-BIC Routing	Requestor not allowed
DRC8002	The Distinguished Name specified in input must refer to an existing and active Certificate DN which is linked to at least one User of the Requestor Party. If the Requestor Party is a Central Bank, it is sufficient for the User to be within the same System Entity.	Create DN-BIC Routing	Unknown or invalid Distinguished Name

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRC8003	The BIC Mnemonic must refer to an existing and active BIC which is linked in the same validity period to at least one Authorised Account User referencing an Account owned by the Requestor Party. If the Requestor Party is a Central Bank, it is sufficient for the Account to be within the same System Entity.	Create DN-BIC Routing	Unknown or invalid BIC
DRC8004	The Valid From must be equal to or greater than the current business date.	Create DN-BIC Routing	Valid From cannot be set to a past date
DRC8005	The Valid To must be equal to or greater than the current business date, and equal to or greater than the Valid From.	Create DN-BIC Routing	Valid To cannot be set to a past date or to a date before Valid From
DRC8006	At any given point in time, there cannot be more than one DN-BIC Routing for the same combination of BIC Mnemonic, Distinguished Name and Direction.	Create DN-BIC Routing	DN-BIC Routing already defined for this BIC, DN and Direction
DRC8007	At any given point in time, there cannot be more than one Outbound DN-BIC Routing for the same BIC Mnemonic.	Create DN-BIC Routing	Outbound DN-BIC Routing already defined for this BIC
DRC9001	When performing a request to create a Limit, the requestor must be authorised to create the requested data according to the following: A Service Operator user can create all data	Create Limit	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	A NCB user can create only Limits for CMBs (T2S CMBs and TIPS CMBs) belonging to its own System Entity A Payment Bank user can create only Limits for non-primary T2S CMBs and TIPS CMBs linked to its own Cash Account		
DRC9052	When performing a Limit create request, the Cash Account specified must refer to an existing and active instance in CRDM.	Create Limit	Unknown Cash Account Identifier
DRC9053	When performing an autocollateralisation, external guarantee or unsecured credit Limit create request, the BIC+BIC Branch Code specified must refer to an existing and active BIC+BIC Branch Code in BIC directory.	Create Limit	Unknown BIC
DRC9054	When performing an autocollateralisation, external guarantee or unsecured credit limit create request , the Limit Type must be Autocollateralisation if the relevant CMB is a primary one.	Create Limit	Invalid Limit Type
DRC9055	When performing an autocollateralisation, external guarantee or unsecured credit limit create request, the Limit Value must be set to zero for Primary CMB if the Regular Securities Account or the NCB Cash Account for the relevant CMB are not defined.	Create Limit	Limit Value must be zero
DRC9056	When performing an autocollateralisation, external guarantee or unsecured credit limit create request, the Limit Value must be set to zero if the Receiving Securities Account for the relevant CMB are not defined for Repo and Pledge countries.	Create Limit	Limit Value must be zero
DRC9057	When performing an autocollateralisation, external guarantee or unsecured credit limit create request, the BIC+BIC Branch Code specified must be authorised to use the Cash Account provided in input.	Create Limit	Invalid BIC: it cannot use the specified Cash Account

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRC9058	When performing a limit create request, if the limit type is TIPS CMB Limit then the Cash Account type must be TIPS CMB; if the limit type is autocollateralisation, external guarantee or unsecured credit the Cash Account type cannot be TIPS Account, TIPS Transit Account or TIPS CMB.	Create Limit	Invalid Cash Account type
DRC9100	When performing a Limit create request, it must be verified that no Limit has already been defined for the BIC+BIC Branch Code (if present), Cash Account, Valid From and Limit Type provided in input.	Create Limit	Limit already defined
DRC9205	When performing a Limit create request, the Valid From date must be equal to or greater than the current date.	Create Limit	Valid From invalid
DRC9800	When performing a Limit Create request, the number of decimals in the value provided for Limit Amount must be compliant with the number of decimals foreseen for the relevant currency.	Create Limit	Invalid number of decimals
DRCA001	A Certificate DN can be created only by users with the correct privilege.	Create Certificate DN	Requestor not allowed
DRCA002	When performing a Certificate DN Create request, the Distinguished Name must not be already used within active instances in CRDM.	Create Certificate DN	Distinguished Name already used
DRCE001	A Message Subscription Rule Sets can be created only by users belonging to Service Operator, CSD, NCB, CSD Participant, Payment Bank and External CSD with the correct privilege. CSD and NCB users can only create Message Subscription Rule Sets within their own system entity. CSD Participant, Payment Bank and External CSD users can only create Message Subscription Rule Sets for their own party.	Create Message Susbcription Rule Set	Requestor not allowed
DRCE002	When performing a Message Subscription Rule Set Party creation request, the Parties specified must exist and	Create	Unknown Party

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	be active in CRDM.	Message Susbcription Rule Set	
DRCE005	When performing a Message Subscription Rule Set Party creation request, the Party Id specified must belong to a Party in the default data scope of the requestor.	Create Message Susbcription Rule Set	Invalid Party
DRCE006	When performing a Message Subscription Rule Set Party creation request, the Creator Party specified must be the same Party as the Requestor or the CSD/NCB specified as System Entity by the Service Operator in case of act on behalf.	Create Message Susbcription Rule Set	Invalid Party
DRCE009	When performing a Message Subscription Rule Set creation request, the Valid From must be greater than the current date. The Service Operator can skip this check in contingency situations.	Create Message Susbcription Rule Set	“Valid From” invalid
DRCE010	When performing a Message Subscription Rule Set creation request, the Valid To must be greater than or equal to the Valid From.	Create Message Susbcription Rule Set	"Valid To" invalid
DRCE100	When performing a Message Subscription Rule Set create request, the specified System Entity must refer to an	Create	Invalid System

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	existing and active instance in CRDM.	Message Susbcription Rule Set	Entity
DRCE200	When performing a Message Subscription Rule Set create request, the specified Name must not be already assigned in CRDM under the same Party.	Create Message Susbcription Rule Set	Name already assigned
DRCF001	A Message Subscription Rule can be created only by users belonging to Service Operator, CSD, NCB, CSD Participant, Payment Bank and External CSD with the correct privilege. CSD and NCB users can only create Message Subscription Rules within their own system entity. CSD Participant, Payment Bank and External CSD users can only create Message Subscription Rules for their own party.	Create Message Susbcription Rule	Requestor not allowed
DRCF002	When performing a Message Subscription Rule creation request, the Message Subscription Rule Set Identifier specified must exist in CRDM and must belong to the data scope of the requestor.	Create Message Susbcription Rule	Unknown Message Subscription Rule Set Identifier
DRCF003	When performing a Message Subscription Rule creation request, the Rule Sequence specified must not be already existing for the same Message Subscription Rule Set Identifier	Create Message Susbcription Rule	Rule Sequence already inserted
DRCF004	When performing a Message Subscription Rule creation request, the Rule Parameters Type specified must	Create	Unknown Rule

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	refer, depending on the Parameter Type, to an existing Attribute Domain Name in Attribute Domain entity defined by the Service Operator or to an existing CRDM Reference Data entity.	Message Susbcription Rule	Parameters Type
DRCF005	When performing a Message Subscription Rule creation request, the Valid From must be greater than the current date. The Service Operator can skip this check in contingency situations.	Create Message Susbcription Rule	Relevant Message Subscription Rule Set must have future Valid From
DRCF006	When performing a Message Subscription Rule creation request, the Valid From must be equal to or greater than the Valid From of the related Message Subscription Rule Set. The Service Operator can skip this check in contingency situations.	Create Message Susbcription Rule	Invald "Valid From"
DRCF007	When performing a Message Subscription Rule creation request, the Valid To, if specified, must be equal to or greater than the Valid From, and equal to or less than the related Message Subscription Rule Set Valid To.	Create Message Susbcription Rule	Invalid "Valid To"
DRCF008	When performing a Message Subscription Rule creation request, certain parameter types are only applicable for a number of message types, as described below: - Instruction Type: only applicable for message types SettlementInstruction, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, BankToCustomerDebitCreditNotification	Create Message Susbcription Rule	Invalid combination of parameter types for the given message type

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	- Message Status: only applicable for AccountRequestAcknowledgement, PartyStatusAdvice, SecurityCreationStatusAdvice, SecurityMaintenanceStatusAdvice, SecurityDeletionStatusAdvice, SecuritiesAccountStatusAdvice, CollateralDataStatusAdvice, EligibleCounterpartCSDStatusAdvice, SecuritiesCSDLinkStatusAdvice, AccountLinkStatusAdvice, Receipt, IntraPositionMovementStatusAdvice, SecuritiesSettlementTransactionStatusAdvice, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementConditionsModificationStatusAdvice, IntraBalanceMovementStatusAdvice, IntraBalanceMovementModificationRequestStatusAdvice, IntraBalanceMovementCancellationRequestStatusAdvice. - Party: only applicable for SettlementInstruction, SettlementRestriction on securities, SettlementRestriction on cash, AccountRequestAcknowledgement, PartyStatusAdvice, SecuritiesCSDLinkStatusAdvice, IntraPositionMovementStatusAdvice, IntraPositionMovementConfirmation, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementTransactionAllegementNotification, SecuritiesMessageCancellationAdvice, SecuritiesSettlementAllegementRemovalAdvice, SecuritiesSettlementConditionsModificationStatusAdvice, IntraBalanceMovementStatusAdvice, IntraBalanceMovementConfirmation, SecuritiesSettlementTransactionGenerationNotification, IntraBalanceMovementModificationRequestStatusAdvice, IntraBalanceMovementCancellationRequestStatusAdvice, SecuritiesMessageCancellationAdvice. - Securities Account: only applicable for SettlementInstruction, SettlementRestriction on securities,		

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	SecuritiesAccountStatusAdvice, IntraPositionMovementStatusAdvice, IntraPositionMovementConfirmation, AccountLinkStatusAdvice, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementTransactionAllegementNotification, SecuritiesMessageCancellationAdvice, SecuritiesSettlementAllegementRemovalAdvice, SecuritiesSettlementConditionsModificationStatusAdvice, SecuritiesSettlementTransactionGenerationNotification, SecuritiesMessageCancellationAdvice. - ISIN: only applicable for SettlementInstruction, SettlementRestriction on securities, SecurityCreationStatusAdvice, SecurityMaintenanceStatusAdvice, SecurityDeletionStatusAdvice, SecuritiesCSDLinkStatusAdvice, IntraPositionMovementStatusAdvice, IntraPositionMovementConfirmation, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementTransactionAllegementNotification, SecuritiesSettlementAllegementRemovalAdvice, SecuritiesSettlementConditionsModificationStatusAdvice, SecuritiesSettlementTransactionGenerationNotification. - Cash Account: only applicable for SettlementInstruction, SettlementRestriction on cash,AccountRequestAcknowledgement, BankToCustomerDebitCreditNotification, AccountLinkStatusAdvice, SecuritiesSettlementTransactionConfirmation, IntraBalanceMovementStatusAdvice, IntraBalanceMovementConfirmation, SecuritiesSettlementTransactionGenerationNotification, IntraBalanceMovementModificationRequestStatusAdvice, IntraBalanceMovementCancellationRequestStatusAdvice.		

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	- Instruction Status: only applicable for IntraPositionMovementStatusAdvice, SecuritiesSettlementTransactionStatusAdvice, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementConditionsModificationStatusAdvice, IntraBalanceMovementStatusAdvice, IntraBalanceMovementModificationRequestStatusAdvice, IntraBalanceMovementCancellationRequestStatusAdvice. - Transaction Code: only applicable for SettlementInstruction, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesSettlementTransactionAllegementNotification, SecuritiesSettlementTransactionGenerationNotification. - Currency: only applicable for SettlementInstruction, SettlementRestriction on cash,BankToCustomerDebitCreditNotification, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementTransactionAllegementNotification, IntraBalanceMovementStatusAdvice, IntraBalanceMovementConfirmation, SecuritiesSettlementTransactionGenerationNotification, IntraBalanceMovementModificationRequestStatusAdvice, IntraBalanceMovementCancellationRequestStatusAdvice. - Already Matched Flag: only applicable for SettlementInstruction, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementConditionsModificationStatusAdvice - Settlement Transaction Condition Code: only applicable for SettlementInstruction,		

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesSettlementTransactionGenerationNotification. - Business Sending Party: only applicable for SettlementInstruction, SettlementRestriction on securities, SettlementRestriction on cash, IntraPositionMovementStatusAdvice, IntraPositionMovementConfirmation, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementConditionsModificationStatusAdvice, IntraBalanceMovementStatusAdvice, IntraBalanceMovementConfirmation, SecuritiesSettlementTransactionGenerationNotification,IntraBalanceMovementModificationRequestStatusAdvice IntraBalanceMovementCancellationRequestStatusAdvice, - Business Sending User: only applicable for SettlementInstruction, SettlementRestriction on securities, SettlementRestriction on cash - Instructing Party: only applicable for SettlementInstruction, SettlementRestriction on securities, SettlementRestriction on cash, IntraPositionMovementStatusAdvice, IntraPositionMovementConfirmation, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice SecuritiesSettlementConditionsModificationStatusAdvice, IntraBalanceMovementStatusAdvice, IntraBalanceMovementConfirmation, SecuritiesSettlementTransactionGenerationNotification,IntraBalanceMovementModificationRequestStatusAdvice IntraBalanceMovementCancellationRequestStatusAdvice,		

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	SecuritiesSettlementTransactionGenerationNotification		
DRCF050	When performing a Message Subscription Rule creation request involving a TIPS Account as Rule Parameter Value, the account must belong to the data scope of the requestor.	Create Message Susbcription Rule	Invalid TIPS Account
DRCF060	When performing a Message Subscription Rule Create request, the same set of Parameter Types must be used for Groups belonging to the same Rule.	Create Message Susbcription Rule	Invalid Parameter Types for the Specified Parameter Group
DRCF200	When performing a Message Subscription Rule create request, the Parameter Value must be compliant with the values or rules defined in the relevant Attribute Domain or Reference Data entity.	Create Message Susbcription Rule	Invalid Parameter Value
DRCF300	When performing a Message Subscription Rule create request, the overall number of group of parameters for the relevant CSD must be compliant with the configuration limit defined in CRDM.	Create Message Susbcription Rule	Number of maximum active Message Subscription Rule exceeded
DRCF310	When performing a Message Subscription Rule create request, the overall number of distinct Parameter Value defined for the same Parameter Type for the relevant CSD must be compliant with the configuration limit defined	Create Message	Number of maximum

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	in CRDM.	Susbcription Rule	Parameter Values exceeded
DRCV001	Report Configuration can be created only by Service Operator, CSD, NCB, CSD Participant or Payment Bank. A user belonging to a CSD or NCB can only create Report Configuration for parties that fall under their responsibility according to the Hierarchical Party Model. A user belonging to a CSD Participant or Payment Bank can only create Report Configuration for his own party.	Create Report Configuration	Requestor not allowed
DRCV004	When performing a Report Configuration creation request, the Owner Party Technical Identifier specified must refer to an existing and active Party in CRDM.	Create Report Configuration	Unknown Party Identifier
DRCV005	When performing a Report Configuration creation request, the Opting Party Technical Identifier specified in the Report Configuration Party Link section, must refer to an existing and active Party belonging to the System Entity Code specified.	Create Report Configuration	Unknown Party Identifier
DRCV006	When performing a Report Configuration creation request, the Event Type specified must belong to an existing instance in CRDM and its Event Type Category must be compliant with the Report Name.	Create Report Configuration	Unknown Event Type Identifier
DRCV008	The Configuration Name specified in the Report Configuration creation request must be unique with the same System Entity.	Create Report Configuration	Configuration Name already assigned
DRCV009	When performing a Report Configuration creation request, the Report Name specified must refer to an existing and active Attribute Value of the relevant Attribute Domain instance.	Create Report	Unknown Report Name

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		Configuration	
DRCV020	When performing a Report Configuration create request, the System Entity Code must be equal to the System Entity Code of the requestor or, in case the requestor is a T2S Operator, to an existing System Entity with System Entity type equal to CSD or NCB.	Create Report Configuration	“System Entity Code” invalid
DRCV030	When performing a Report Configuration creation request, the System Entity Wide Report must be set to FALSE in case the Owner Party Technical Identifier specified refers to a Party Type equal to CSD Participant or Payment Bank.	Create Report Configuration	“System Entity Wide Report” invalid
DRCV040	When performing a Report Configuration creation request, the Valid From specified in the Report Configuration Party Link section must be greater than the current business date.	Create Report Configuration	“Valid From” invalid
DRCV050	When performing a Report Configuration creation request, the Valid To specified in the Report Configuration Party Link section must be greater than the Valid From.	Create Report Configuration	“Valid To” invalid
DRCV070	When performing a Report Configuration create request, the specified Currency must refer to an existing Currency.	Create Report Configuration	Invalid currency
DRCV080	When performing a Report Configuration create request, the Currency field can only be used in combination with a currency-dependent event and one of the currency-related report types listed in the T2S documentation.	Create Report Configuration	Currency not relevant

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRCV100	When performing a Report Configuration creation request for a given CSD and report type, its validity period cannot overlap with the validity period of an already existing flat file report configuration defined for the same CSD and the same report type.	Create Report Configuration	Flat file configuration exists for the same CSD, report type and period.
DRCV110	When performing a Report Configuration creation request, if a TIPS Report is selected as Report Name, the Opting Party must be equal to the Owner Party. Furthermore the Party Type must be Payment Bank.	Create Report Configuration	Invalid Party for TIPS reports.
DRCV120	When performing a Report Configuration creation request, if a TIPS Report is selected as Report Name, the System Entity Wide flag must be set to FALSE and the Push flag to TRUE. Furthermore the Execution Time, Event Type and Currency fields must not be used.	Create Report Configuration	Invalid fields for TIPS reports.
DRCV130	When performing a Report Configuration creation request, if a TIPS Report is selected as Report Name and the Delta flag is set to TRUE, the report Frequency must be specified. If a non-TIPS Report is selected or if the Delta flag is set to FALSE, the report Frequency cannot be specified.	Create Report Configuration	Frequency must be specified for TIPS reports in Delta mode.
DRCV140	When performing a Report Configuration creation request, if a TIPS Report is selected as Report Name and the Delta flag is set to TRUE, the Report must be defined as available in Delta mode in the related Attribute Domain.	Create Report Configuration	Report not available in Delta mode
DRCW001	Routing can be created by Service Operator, CSD, NCB, CSD Participant, Payment Bank and Ancillary System. Users can only create Routing entity linked to the Party they belong to. Service Operator User can create	Create Routing	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	Routing entity linked to any Party.		
DRCW002	When performing a Routing Create request, the Network Service Identifier specified must refer to an existing and active instance in CRDM linked to the Party Technical Address specified in input.	Create Routing	Unknown Network Service Identifier
DRCW003	When performing a Routing Create request, the Party Technical Identifier must refer to an existing and active instance in CRDM.	Create Routing	Unknown Party Technical Identifier
DRCW004	When performing a Routing Create request, the Party Technical Address must refer to an existing and active instance in CRDM belonging to the Party specified in input.	Create Routing	Unknown Party Technical Address
DRCW007	When performing a Routing Create request, if the Default Routing is set to True, it has to be verified that no other Routing are defined as such for the Party specified in input and for the specified Network Service. Furthermore, for T2S, the Network Service must be a store-n-forward one.	Create Routing	Default Routing already defined for this Party and Service, or the Service is set to real time
DRCW012	When performing a Routing Create request, the Message Type must refer to an existing and active Message Type configured in CRDM for the relevant Service.	Create Routing	Invalid Message Type
DRD0001	A Certificate DN can be deleted/restored only by Users belonging to the Party responsible for the User, or to said Party's CSD/NCB.	Delete User-Certificate DN Link	Requestor not allowed
DRD0002	When performing a User Certificate DN delete request, it must refer to an existing and active instance.	Delete User-	Unknown or not

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		Certificate DN Link	active link
DRD0003	When performing a User Certificate DN restore request, the specified User must be an existing and active instance in T2S.	Delete User-Certificate DN Link	Unknown or not active User
DRD0004	When performing a User Certificate DN restore request, the specified Certificate DN must be an existing and active instance in T2S.	Delete User-Certificate DN Link	Unknown or not active Certificate DN
DRD0005	When performing a User Certificate DN restore request, there cannot be more than one link between the same User and Certificate DN.	Delete User-Certificate DN Link	Link already exists
DRD0006	When performing a User Certificate DN restore request, there can only be one User Certificate DN with Default flag set to TRUE for any given Certificate.	Delete User-Certificate DN Link	Default link already exists
DRD0007	When performing a User Certificate DN restore request, it must refer to an existing and deleted instance.	Delete User-Certificate DN Link	Unknown or not deleted link
DRD0008	When performing a User Certificate DN restore request, there can only be one User Certificate DN with Main User flag set to TRUE for all the Users of any Party using the same BIC.	Delete User-Certificate DN Link	Main User already exists for the same Party BIC

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRD6001	A Role can be deleted/restored only by Service Operator, CSD or NCB. A User is authorised to delete/restore only data belonging to its own System Entity.	Delete Role	Requestor not allowed
DRD6002	When performing a Role restore request, the Role Name must not be already assigned within the same System Entity.	Delete Role	Role Name already assigned
DRD6003	When performing a Role deletion request it must refer to an existing and active instance of Role.	Delete Role	Data to be deleted/restored not found
DRD6044	When performing a Role restore request it must refer to an existing and deleted instance of Role.	Delete Role	Data to be deleted/restored not found
DRD6050	A Role cannot be deleted if there still are valid instances of the following entities linked to it: Role Party, Role User.	Delete Role	The Role cannot be revoked due to a priority constraint.
DRD7001	A User can be deleted/restored by T2S Operator, CSD, NCB, CSD Participant, External CSD or Payment Bank. Users belonging to CSDs, NCBs, CSD Participants, External CSDs and Payment Banks can only delete/restore users that fall under their responsibility according to the Hierarchical Party Model.	Delete User	Requestor not allowed
DRD7002	When performing a User Restore request, the Login Name must not be already assigned to another User in T2S.	Delete User	Login Name already assigned
DRD7003	When performing a User Delete request, it must refer to an existing and active instance.	Delete User	Data to be

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
			deleted/restored not found
DRD7004	When performing a User Restore request, it must refer to an existing and deleted instance.	Delete User	Data to be deleted/restored not found
DRD7005	When performing a User Restore request, the System User Reference must not be already assigned to another User in CRDM.	Delete User	System User Reference already assigned
DRD7007	When performing a User Restore request, the specified Party Technical Identifier must refer to an existing, active and open or future Party in CRDM.	Delete User	Unknown Party Identifier
DRD7008	When performing a User Delete Request, there cannot be any existing and active instances of User Certificate DN linked to it.	Delete User	Deletion not allowed due to existing links to Certificate DN
DRD8001	DN-BIC Routing can be deleted or restored only by the Service Operator, NCBs or Payment Banks. NCBs can delete or restore DN-BIC Routings within their own System Entities. Payment Banks can delete or restore DN-BIC Routings that reference DNs linked to their own Users and BICs authorised to act on their own accounts.	Delete DN-BIC Routing	Requestor not allowed
DRD8002	Deletion requests must refer to existing, active and closed DN-BIC Routings.	Delete DN-BIC Routing	Unknown, deleted or open DN-BIC

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
			Routing
DRD8003	Restore requests must refer to existing, deleted and non-open DN-BIC Routings.	Delete DN-BIC Routing	Unknown, active or open DN-BIC Routing
DRD8004	In a restore request, the Distinguished Name Identifier must refer to an existing and active Certificate DN which is linked to at least one User of the Requestor Party. If the Requestor Party is a Central Bank, it is sufficient for the User to be within the same System Entity.	Delete DN-BIC Routing	Unknown, deleted or invalid Distinguished Name
DRD8005	In a restore request, the BIC Mnemonic must refer to an existing and active BIC which is linked to at least one Authorised Account User referencing an Account owned by the Requestor Party. If the Requestor Party is a Central Bank, it is sufficient for the Account to be within the same System Entity.	Delete DN-BIC Routing	Unknown, deleted or invalid BIC
DRD8006	At any given point in time, there cannot be more than one DN-BIC Routing for the same combination of BIC Mnemonic, Distinguished Name and Direction.	Delete DN-BIC Routing	DN-BIC Routing already defined for this BIC, DN and Direction
DRD8007	At any given point in time, there cannot be more than one Outbound DN-BIC Routing for the same BIC Mnemonic.	Delete DN-BIC Routing	Outbound DN-BIC Routing already defined for this BIC
DRD9001	When performing a request to delete a Limit, the requestor must be authorised to delete the requested data according to the following: A System Operator user can delete all data	Delete Limit	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	A NCB user can delete only Limits for CMBs (T2S CMBs and TIPS CMBs) belonging to its own System Entity A Payment Bank user can delete only Limits for non-primary T2S CMBs and TIPS CMBs linked to its own Cash Account		
DRD9003	The delete requests of an autocollateralisation, external guarantee or unsecured credit Limit must refer to an existing and active instance whose Limit Amount is equal to zero.	Delete Limit	Limit to be deleted not found
DRD9004	The restore requests of a Limit must refer to an existing and deleted instance.	Delete Limit	Limit to be restored not found
DRD9064	When performing an autocollateralisation, external guarantee or unsecured credit Limit restore request, the Credit Memorandum Balance Identifier must refer to an existing and active CMB instance in CRDM.	Delete Limit	Unknown Credit Memorandum Balance Identifier
DRD9065	When performing a TIPS CMB Limit restore request, the Credit Memorandum Balance Identifier must refer to an existing and active Cash Account instance in CRDM with Account Type equal to TIPS CMB.	Delete Limit	Unknown Credit Memorandum Balance Identifier
DRD9205	When performing a Limit restore request, the Valid From date must be equal to or greater than the current date.	Delete Limit	Valid From invalid
DRDA001	A Certificate DN can be deleted or restored only by users with the correct privilege.	Delete Certificate DN	Requestor not allowed
DRDA002	When performing a Certificate DN Restore request, the Distinguished Name must not be already used within active instances in CRDM.	Delete Certificate	Distinguished Name already used

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		DN	
DRDA003	When performing a Certificate DN Delete request, it must refer to an existing and active Certificate DN.	Delete Certificate DN	Unknown or not active Certificate DN
DRDA004	When performing a Certificate DN Restore request, it must refer to an existing and deleted Certificate DN.	Delete Certificate DN	Unknown or not deleted Certificate DN
DRDA010	When performing a Certificate DN Delete request, it must refer to a Certificate DN not actively linked to any User.	Delete Certificate DN	Certificate DN is linked to a User
DRDE001	A user can delete/restore only Message Subscription Rule Sets belonging to its own data scope.	Delete Message Susbcription Rule Set	Requestor not allowed
DRDE002	When performing a Message Subscription Rule Set restore request, the Message Subscription Rule Set Party must reference Parties that exist and are active in CRDM.	Delete Message Susbcription Rule Set	Unknown Party
DRDE003	When performing a Message Subscription Rule Set delete request it must refer to an existing and active instance of Message Subscription Rule Set with future Valid From or past Valid To.	Delete Message	Data to be deleted/restored not

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		Susbcription Rule Set	found
DRDE006	When performing a Message Subscription Rule Set restore request, either the Valid From must be greater than the current date, or the Valid To must be in the past. The Service Operator can skip this check in contingency situations.	Delete Message Susbcription Rule Set	Invalid validity dates
DRDE040	A Message Subscription Rule Set cannot be deleted if there still are valid instances of the following entity linked to it: Message Subscription Rule.	Delete Message Susbcription Rule Set	The deletion/close is not allowed due to a priority constraint
DRDE044	When performing a Message Subscription Rule Set restore request it must refer to an existing and deleted instance of Message Subscription Rule Set.	Delete Message Susbcription Rule Set	Data to be deleted/restored not found
DRDE200	When performing a Message Subscription Rule Set restore request, the specified Name must not be already assigned in CRDM under the same Party.	Delete Message Susbcription Rule Set	Name already assigned
DRDF001	A user can delete/restore only Message Subscription Rules belonging to its own data scope.	Delete Message	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		Susbcription Rule	
DRDF002	When performing a Message Subscription Rule restore request, the Message Subscription Rule Set Identifier to be restored must exist and be active in T2S.	Delete Message Susbcription Rule	Unknown Message Subscription Rule Set Identifier
DRDF003	When performing a Message Subscription Rule delete request, it must refer to an existing and active instance of Message Subscription Rule with future Valid From or past Valid To. The Service Operator can skip this check in contingency situations.	Delete Message Susbcription Rule	Data to be deleted/restored not found
DRDF005	When performing a Message Subscription Rule restore request, the Rule Sequence to be restored must not be already used for the same Message Subscription Rule Set Identifier	Delete Message Susbcription Rule	Rule Sequence already used
DRDF007	When performing a Message Subscription Rule restore request, the Valid From must be equal to or greater than the Valid From of the related Message Subscription Rule Set.	Delete Message Susbcription Rule	Invalid 'Valid From'
DRDF008	When performing a Message Subscription Rule restore request, the Valid To must be equal to or less than the Valid To of the related Message Subscription Rule Set.	Delete Message	Invalid 'Valid To'

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		Susbcription Rule	
DRDF044	When performing a Message Subscription Rule restore request it must refer to an existing and deleted instance of Message Subscription Rule.	Delete Message Susbcription Rule	Data to be deleted/restored not found
DRDF045	When performing a Message Subscription Rule restore request, the Rule Parameter Type to be restored must refer, depending on the Parameter Type, to an existing and active Attribute Domain Name in Attribute Domain entity defined by the Service Operator or to an existing CRDM Reference Data entity.	Delete Message Susbcription Rule	Unknown Rule Parameter Type
DRDF200	When performing a Message Subscription Rule restore request, the Parameter Value must be compliant with the values or rules defined in the relevant Attribute Domain or CRDM Reference Data entity.	Delete Message Susbcription Rule	Invalid Parameter Value
DRDF300	When performing a Message Subscription Rule restore request, the overall number of group of parameters for the relevant CSD must be compliant with the configuration limit defined in CRDM.	Delete Message Susbcription Rule	Number of maximum active Message Subscription Rule exceeded
DRDF310	When performing a Message Subscription Rule restore request, the overall number of distinct Parameter Value	Delete	Number of

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	defined for the same Parameter Type for the relevant CSD must be compliant with the configuration limit defined in CRDM.	Message Susbcription Rule	maximum Parameter Values exceeded
DRDV001	Report Configuration can be deleted/restored only by Service Operator, CSD, NCB, CSD Participant or Payment Bank. A user belonging to a CSD or NCB can only deleted/restored Report Configuration for parties that fall under their responsibility according to the Hierarchical Party Model. A user belonging to a CSD Participant or Payment Bank can only deleted/restored Report Configuration for his own party	Delete Report Configuration	Requestor not allowed
DRDV004	When performing a Report Configuration restore request, the Owner Party Technical Identifier to be restored must refer to an existing and active Party with the same System Entity of the Report Configuration.	Delete Report Configuration	Unknown Party Identifier
DRDV005	When performing a Report Configuration restore request, the Opting Party Technical Identifier specified in the Report Configuration Party Link section, must refer to an existing and active Party with the same System Entity of the Report Configuration.	Delete Report Configuration	Unknown Party Identifier
DRDV006	When performing a Report Configuration restore request, the Event Type Identifier to be restored must belong to an existing instance in CRDM and its Event Type Category must be compliant with the Report Name.	Delete Report Configuration	Unknown Event Type Identifier
DRDV007	When performing a Report Configuration restore request, the Report Name specified must refer to an existing and active Attribute Domain Name of an Attribute Domain instance.	Delete Report Configuration	Unknown Report Name
DRDV008	When performing a Report Configuration restore request, the Configuration Name specified must be unique	Delete	Configuration Name

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	within the same System Entity	Report Configuration	already assigned
DRDV020	The request to delete a Report Configuration must refer to an existing and active Report Configuration in CRDM.	Delete Report Configuration	Invalid Report Configuration to be deleted
DRDV030	The request to restore a Report Configuration must refer to an existing and deleted Report Configuration in CRDM.	Delete Report Configuration	Invalid Report Configuration to be restored
DRDV050	When performing a Report Configuration restore request, all the Report Configuration Party Link must be closed or must have a future Valid From.	Delete Report Configuration	Invalid Report Configuration to be restored
DRDV060	When performing a Report Configuration delete request, all the Report Configuration Party Link must be closed or must have a future Valid From.	Delete Report Configuration	Invalid Report Configuration to be deleted
DRDV070	When performing a Report Configuration restore request, the specified Currency must refer to an existing Currency.	Delete Report Configuration	Invalid currency
DRDV100	When performing a Report Configuration restore request for a given CSD and report type, its validity period cannot overlap with the validity period of an already existing flat file report configuration defined for the same CSD and the same report type.	Delete Report Configuration	Flat file configuration exists for the same CSD,

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
			report type and period.
DRDW001	Routing can be deleted/restored by Service Operator, CSD, NCB, CSD Participant, Payment Bank and Ancillary System. Users can only delete/restore Routing entity linked to Party they belong to. Service Operator User can delete/restore Routing entity linked to any Party.	Delete Routing	Requestor not allowed
DRDW002	When performing a Routing deletion request, it must refer to an existing and active instance in CRDM.	Delete Routing	Data to be updated not found
DRDW003	When performing a Routing restore request, the Network Service Identifier to be restored must refer to an existing instance in CRDM linked to the Party of the Routing entity.	Delete Routing	Unknown Network Service Identifier
DRDW004	When performing a Routing restore request, the Party Technical Address to be restored must refer to an existing instance in CRDM belonging to the same Party of the Routing entity.	Delete Routing	Unknown Technical Address
DRDW005	When performing a Routing restore request, the Party Technical Identifier to be restored must refer to an existing instance in CRDM.	Delete Routing	Unknown Party Technical Identifier
DRDW044	When performing a Routing restore request it must refer to an existing and deleted instance in CRDM.	Delete Routing	Data to be updated not found
DRGP001	A Grant Privilege request grants a system privilege and/or an object privilege on a secured element to a user, a role or a party. The grantor user must be granted with the relevant privilege beforehand in order to administer it. If the grantor user is a Party Administrator, the privilege must be granted to the Party the user belongs to. Otherwise, the privilege must be granted directly to the user.	Grant Privilege	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRGP002	When performing a Grant Privilege request the privilege to be granted must refer to an existing privilege. A System Privilege cannot be assigned to a Party if this would always result in an empty data scope for that Party type.	Grant Privilege	Invalid system privilege
DRGP004	When performing a Grant Privilege request, it is only possible to grant an object privilege if the grantee already has the related system privilege.	Grant Privilege	System Privilege missing, object privilege cannot be granted
DRGP005	When performing a Grant Privilege request to grant a system privilege to a Party, the grantee party must be an active one in the default data scope of the grantor.	Grant Privilege	Invalid grantee party
DRGP006	When performing a Grant Privilege request to grant an object privilege to a Party, only Service Operator, CSD and NCB users can grant privileges to Parties outside their System Entity. CSD and NCB users cannot grant privileges to the Service Operator. CSD Participants, Payment Banks and External CSDs can only grant privileges to other Parties within their System Entity.	Grant Privilege	Invalid grantee party
DRGP007	When performing a Grant Privilege request, the User to be granted with a privilege must refer to an existing one belonging to the same party as the grantor, with the following exceptions: - The Service Operator can grant any privilege to any User. - CSD/NCB Party Administrators can grant Party Administrator privileges to any User within their own System Entity. The Party Administrator privileges are ARM_AdministerParty, ARM_GrantPrivilege, ARM_GrantRole, ARQ_GrantedSysPrivilegesListQuery, ARQ_GrantObjectPrivilegesListQuery, ARQ_GrantedRolesListQuery.	Grant Privilege	Invalid grantee user
DRGP008	When performing a Grant Privilege request, the Role to be granted with a privilege must refer to an existing one	Grant	Invalid grantee role

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	in the data scope of the grantor.	Privilege	
DRGP009	When performing a Grant Privilege request, to grant an object privilege on a System Entity, it must be an existing one. The Service Operator can grant privileges on any System Entity, while CSD and NCB users can grant privileges on their System Entity only.	Grant Privilege	Invalid System Entity
DRGP010	When performing a Grant Privilege request, the reference data object to be secured may be a Party, a Securities, a Securities Account or a Cash Account and must refer to an existing one in the data scope of the requestor.	Grant Privilege	Invalid reference data object to be secured
DRGP011	When performing a Grant Privilege request, to grant an object privilege on a Secured Group, it must be an existing one belonging to the data scope of the requestor.	Grant Privilege	Invalid secured group
DRGP012	When performing a Grant Privilege request, the specified privilege type must be consistent with its use. System privileges can only be granted at system level.	Grant Privilege	Invalid privilege type
DRGP013	When performing a Grant Privilege request, in order to prevent the possibility to grant contradicting privileges to the same role, user or party: Each system privilege can be granted to a role, a user or a party only once. Each object privilege can be granted to a role, a user or a party on the same object only once.	Grant Privilege	Privilege already granted
DRGP014	When performing a Grant Privilege request, the valid from date can’t be less then the current business date.	Grant Privilege	Invalid valid from date
DRGP015	If the Grant Privilege request specifies both a System Privilege and an Object Privilege or the request is about an object privilege grant, the period of validity of the grant on the object must be consistent with that of the	Grant Privilege	Valid from of object privilege not

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	system privilege.		compliant with validity of system privilege
DRGP016	A Party Administrator can grant a Privilege to a Party only if the Privilege is already granted to their Party with Admin flag = TRUE. A Party Administrator can grant a Privilege to a User or Role only if the Privilege is already granted to their Party with Deny Flag = FALSE. Any other user can grant a privilege only to other users of its own Party or Roles and only if the Privilege is already granted to the grantor User with Admin Flag = TRUE.	Grant Privilege	User does not have Admin rights on the specified privilege
DRGP017	When performing a Grant Privilege request, it is not possible to set the Deny flag to TRUE when the grantee is a Party.	Grant Privilege	Deny flag cannot be set to TRUE when granting privilege to a Party
DRGP018	When performing a Grant Privilege request, if a Privilege is granted to a Party with Four-Eyes flag = TRUE, the responsible Party Administrator can only grant it with Four-Eyes flag = TRUE. If a Privilege is granted to a User with Four-Eyes flag = TRUE and Admin flag = TRUE, the User can only grant it with Four-Eyes flag = TRUE.	Grant Privilege	Four-Eyes flag must be set to TRUE
DRGP019	When performing a Grant Privilege request, Privileges linked to a certain Service cannot be granted to a Role if the Role already contains Privileges linked to a different Service.	Grant Privilege	A Role cannot contain privileges related to multiple Services

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRGP020	When performing a Grant Privilege request, privileges for the TIPS service can only be granted to Roles.	Grant Privilege	TIPS privileges can only be granted to Roles.
DRGR001	When performing a “Grant/Revoke Role” request, the role to be granted/revoked must be in the data scope of the requestor. This means that at least one of the following conditions has to be fulfilled: • The requestor is the Service Operator; • The requestor is a Party Administrator of a CSD/NCB and the Role to be granted is in the same System Entity as the requestor’s Party; • The requestor is a Party Administrator user and the Role is currently granted to their Party	Grant and Revoke Role	Requestor not allowed
DRGR002	When performing a “Grant/Revoke Role” request, a role can be granted to/revoked from a user only if the user belongs to the same Party as the requestor. The Service Operator can grant and revoke any Role to/from any User. As an exception to this rule, CSD/NCB Party Administrators can grant/revoke Roles directly to any User within their own System Entity provided the Role does not contain any privileges different from ARM_AdministerParty, ARM_GrantPrivilege, ARM_GrantRole, ARQ_GrantedSysPrivilegesListQuery, ARQ_GrantObjectPrivilegesListQuery, ARQ_GrantedRolesListQuery.	Grant and Revoke Role	Requestor not allowed
DRGR003	When performing a “Grant/Revoke Role” request to grant a role to a party or user, the request must refer to a role that is not already granted to the party or user.	Grant and Revoke Role	Invalid role
DRGR004	When performing a “Grant/Revoke Role” request to revoke a role to a party or user, the request must refer to a party or user the role to be revoked is granted to.	Grant and Revoke Role	Invalid role

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRGR005	When performing a “Grant/Revoke Role” request, the request must refer to an existing party or user.	Grant and Revoke Role	Invalid Grantee User/Party
DRGR007	When performing a “Grant/Revoke Role” request to grant a role to a party or user, the set of privileges connected to the role must not intersect with the set of privileges already granted to the party/user.	Grant and Revoke Role	Invalid role
DRGR008	When performing a “Grant/Revoke Role” request, the Role can be granted to/revoked from a Party as follows: • The Service Operator can grant and revoke any Role to/from any Party; • CSD/NCBs can grant and revoke the Role to/from any Party within their System Entity; • CSD Participants, External CSDs and Payment Banks cannot grant the Role to Parties.	Grant and Revoke Role	Requestor not allowed
DRRP001	A Revoke Privilege request revokes a system privilege from a user, a role or a party and/or revokes an object privilege on a secured element. The requestor user must be a Party Administrator of their own Party or a User granted with the relevant privilege with Admin flag = TRUE.	Revoke Privilege	Requestor not allowed
DRRP003	In case of request to revoke a system privilege, all the object privileges linked to it must be revoked beforehand.	Revoke Privilege	The revoke is not allowed due to a revoke constraint
DRRP004	In case of request to revoke a privilege from a party, the requestor user must be a Party Administrator and the privilege to be revoked must have been granted by a user belonging to the same party of the requestor. The Service Operator can revoke any privilege from any Party.	Revoke Privilege	Requestor not allowed
DRRP005	In case of request to revoke a privilege from a role, the requestor must belong to the Service Operator, or to a CSD, or to an NCB. The Service Operator can revoke any privilege from any Role. CSDs and NCBs can revoke	Revoke Privilege	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	privileges from Roles that have the same system entity as the requestor.		
DRRP006	In case of request to revoke a privilege from a user, the user must belong to the same party of the requestor, with the following exceptions: • The Service Operator can revoke any privilege from any user; • Party Administrator privileges can be revoked from any user in the requestor's system entity provided the requestor is a Party Administrator of a CSD or NCB Party. The Party Administrator privileges are ARM_AdministerParty, ARM_GrantPrivilege, ARM_GrantRole, ARQ_GrantedSysPrivilegesListQuery, ARQ_GrantObjectPrivilegesListQuery, ARQ_GrantedRolesListQuery.	Revoke Privilege	Requestor not allowed
DRU6001	A Role can be updated only by Service Operator, CSD or NCB. A User is authorised to update only data belonging to its own System Entity.	Update Role	Requestor not allowed
DRU6003	When performing a Role update request it must refer to an existing and active instance of Role.	Update Role	Data to be updated not found
DRU6006	When performing a Role update request, the Role Name, if specified, must not be already assigned within the same System Entity.	Update Role	Role Name already assigned
DRU7001	A User can be updated by Service Operator, CSD, NCB, CSD Participant, External CSD or Payment Bank. Users belonging to CSDs, NCBs, CSD Participants, External CSDs and Payment Banks can only update users that fall under their responsibility according to the Hierarchical Party Model.	Update User	Requestor not allowed
DRU7003	When performing a User Update request, it must refer to an existing and active instance.	Update User	Data to be updated not found

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRU7005	When performing a User Update request, the System User Reference must not be already assigned to another User in CRDM.	Update User	The specified System User Reference is already assigned
DRU7008	When performing a User Update request, the Login Name specified must not be already assigned to another User in CRDM.	Update User	The specified Login Name is already assigned
DRU8001	DN-BIC Routings can be updated only by the Service Operator, NCBs or Payment Banks. NCBs can update DN-BIC Routings within their own System Entities. Payment Banks can update DN-BIC Routings that reference DNs linked to their own Users and BICs authorised to act on their own accounts.	Update DN-BIC Routing	Requestor not allowed
DRU8002	The DN-BIC Routing to be updated must refer to an existing, active and non-closed instance.	Update DN-BIC Routing	Unknown or invalid DN-BIC Routing
DRU8003	The Valid From can be updated only if the current value is greater than the current business date.	Update DN-BIC Routing	Valid From cannot be modified
DRU8004	The modified Valid From must be equal to or later than the current business date and equal to or later than the Valid From of the Authorised Account User referencing the BIC.	Update DN-BIC Routing	Valid From cannot be set to a past date or earlier than the related Authorised Account

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
			User
DRU8005	The Valid To must be equal to or later than the current business date, equal to or later than the Valid From, and equal to or earlier than the Valid To of the Authorised Account User referencing the BIC.	Update DN-BIC Routing	Valid To cannot be set to a past date, to a date before Valid From or later than the related Authorised Account User
DRU8006	At any given point in time, there cannot be more than one DN-BIC Routing for the same combination of BIC Mnemonic, Distinguished Name and Direction.	Update DN-BIC Routing	DN-BIC Routing already defined for this BIC, DN and Direction
DRU8007	At any given point in time, there cannot be more than one Outbound DN-BIC Routing for the same BIC Mnemonic.	Update DN-BIC Routing	Outbound DN-BIC Routing already defined for this BIC
DRU9001	When performing a request to update a Limit, the requestor must be authorised to update the requested data according to the following: A Service Operator user can update all data A NCB user can update only Limits for CMBs (T2S CMBs and TIPS CMBs) belonging to its own System Entity A Payment Bank user can update only Limits for non-primary T2S CMBs and TIPS CMBs linked to its own Cash Account	Update Limit	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRU9003	The update requests of a Limit must refer to an existing and active instance.	Update Limit	Data to be updated not found
DRU9055	When performing an autocollateralisation, external guarantee or unsecured credit Limit update request, the Limit Value must be set to zero for Primary CMB if the Regular Securities Account or the NCB Cash Account for the relevant CMB are not defined.	Update Limit	Limit Amount must be zero
DRU9056	When performing an autocollateralisation, external guarantee or unsecured credit Limit update request, the Limit Value must be set to zero if the Receiving Securities Account for the relevant CMB are not defined for Repo and Pledge countries.	Update Limit	Limit Amount must be zero
DRU9800	When performing a Limit Update request, the number of decimals in the value provided for Limit Amount must be compliant with the number of decimals foreseen for the relevant currency.	Update Limit	Invalid number of decimals
DRUE001	A Message Subscription Rule Sets can be updated only by users belonging to Service Operator, CSD, NCB, CSD Participant, Payment Bank and External CSD with the correct privilege. CSD and NCB users can only update Message Subscription Rule Sets within their own system entity. CSD Participant, Payment Bank and External CSD users can only update Message Subscription Rule Sets for their own party.	Update Message Susbcription Rule Set	Requestor not allowed
DRUE003	When performing a Message Subscription Rule Set update request it must refer to an existing and active instance of Message Subscription Rule Set. If the Valid To is in the past, only the Valid From can be updated (The Service Operator can skip this check in contingency situations).	Update Message Susbcription Rule Set	Data to be updated not found
DRUE004	When performing a Message Subscription Rule Set Party create request, the same Party Id cannot be specified	Update Message	Party Id already

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	twice.	Susbcription Rule Set	specified
DRUE005	When performing a Message Subscription Rule Set Party create request, the Party Id specified must belong to a Party in the default data scope of the requestor.	Update Message Susbcription Rule Set	Invalid Party Id
DRUE006	When performing a Message Subscription Rule Set Party create request, the Creator Party specified must be the same party as the requestor or the CSD/NCB specified as System Entity by the Service Operator in case of act on behalf.	Update Message Susbcription Rule Set	Invalid Creator Party
DRUE007	When performing a Message Subscription Rule Set Party delete request, the Party Id specified must refer to an existing Message Subscription Rule Set Party instance.	Update Message Susbcription Rule Set	Invalid Party Id
DRUE008	When performing a Message Subscription Rule Set update request if the Valid From is in the past, only a future Valid To can be updated (The Service Operator can skip this check in contingency situations).	Update Message Susbcription Rule Set	Only "Valid To" can be updated
DRUE010	When performing a Message Subscription Rule Set update request, the Party Id and Creator Party specified must exist and be active in CRDM.	Update Message	Unknown Party

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		Susbcription Rule Set	
DRUE200	When performing a Message Subscription Rule Set update request, the specified Name must not be already assigned in CRDM under the same Party.	Update Message Susbcription Rule Set	Name already assigned
DRUE205	When performing a Message Subscription Rule Set update request, the Valid From must be greater than the current date. The Service Operator can skip this check in contingency situations.	Update Message Susbcription Rule Set	“Valid From” invalid
DRUE206	When performing a Message Subscription Rule Set update request, the Valid To must be greater than or equal to the current date and greater than or equal to the Valid From.	Update Message Susbcription Rule Set	"Valid To" invalid
DRUE207	When performing a Message Subscription Rule Set update request, the Valid To must be greater than or equal to all the Valid To of the related Message Subscription Rules. The Valid From must be equal to or less than the Valid From of the related Message Subscription Rules.	Update Message Susbcription Rule Set	Validity dates not compliant with Message Subscription Rules
DRUF001	A user can only update Message Subscription Rules within its own data scope.	Update Message	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
		Susbcription Rule	
DRUF003	When performing a Message Subscription Rule update request it must refer to an existing and active instance of Message Subscription Rule.	Update Message Susbcription Rule	Data to be updated not found
DRUF004	When performing a Message Subscription Rule update request, if the existing Valid From is equal to or less than the current business date, it is only possible to modify the Valid To field.	Update Message Susbcription Rule	Only 'Valid To' can be updated
DRUF005	When performing a Message Subscription Rule update request, the Rule Sequence, when specified, must not be already used for the same Message Subscription Rule Set Identifier	Update Message Susbcription Rule	Rule Sequence already inserted
DRUF006	When performing a Message Subscription Rule update request, the specified Valid From must be equal to or greater than the related Message Subscription Rule Set Valid From and greater to the current business date. The Service Operator can skip this check in contingency situations.	Update Message Susbcription Rule	Invalid 'Valid From'
DRUF007	When performing a Message Subscription Rule update request, the specified Valid To must be equal to or less than the related Message Subscription Rule Set Valid To and equal to or greater than the Valid From specified	Update Message	Invalid 'Valid To'

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	in input, if present.	Susbcription Rule	
DRUF008	When performing a Message Subscription Rule update request, certain parameter types are only applicable for a number of message types, as described below: - Instruction Type: only applicable for message types SettlementInstruction, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, BankToCustomerDebitCreditNotification - Message Status: only applicable for AccountRequestAcknowledgement, PartyStatusAdvice, SecurityCreationStatusAdvice, SecurityMaintenanceStatusAdvice, SecurityDeletionStatusAdvice, SecuritiesAccountStatusAdvice, CollateralDataStatusAdvice, EligibleCounterpartCSDStatusAdvice, SecuritiesCSDLinkStatusAdvice, AccountLinkStatusAdvice, Receipt, IntraPositionMovementStatusAdvice, SecuritiesSettlementTransactionStatusAdvice, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementConditionsModificationStatusAdvice, IntraBalanceMovementStatusAdvice, IntraBalanceMovementModificationRequestStatusAdvice, IntraBalanceMovementCancellationRequestStatusAdvice. - Party: only applicable for SettlementInstruction, SettlementRestriction on securities, SettlementRestriction on cash, AccountRequestAcknowledgement, PartyStatusAdvice, SecuritiesCSDLinkStatusAdvice, IntraPositionMovementStatusAdvice, IntraPositionMovementConfirmation, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation,	Update Message Susbcription Rule	Invalid combination of parameter types for the given message type

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementTransactionAllegementNotification, SecuritiesMessageCancellationAdvice, SecuritiesSettlementAllegementRemovalAdvice, SecuritiesSettlementConditionsModificationStatusAdvice, IntraBalanceMovementStatusAdvice, IntraBalanceMovementConfirmation, SecuritiesSettlementTransactionGenerationNotification, IntraBalanceMovementModificationRequestStatusAdvice, IntraBalanceMovementCancellationRequestStatusAdvice, SecuritiesMessageCancellationAdvice. - Securities Account: only applicable for SettlementInstruction, SettlementRestriction on securities, SecuritiesAccountStatusAdvice, IntraPositionMovementStatusAdvice, IntraPositionMovementConfirmation, AccountLinkStatusAdvice, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementTransactionAllegementNotification, SecuritiesMessageCancellationAdvice, SecuritiesSettlementAllegementRemovalAdvice, SecuritiesSettlementConditionsModificationStatusAdvice, SecuritiesSettlementTransactionGenerationNotification, SecuritiesMessageCancellationAdvice. - ISIN: only applicable for SettlementInstruction, SettlementRestriction on securities, SecurityCreationStatusAdvice, SecurityMaintenanceStatusAdvice, SecurityDeletionStatusAdvice, SecuritiesCSDLinkStatusAdvice, IntraPositionMovementStatusAdvice, IntraPositionMovementConfirmation, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementTransactionAllegementNotification, SecuritiesSettlementAllegementRemovalAdvice, SecuritiesSettlementConditionsModificationStatusAdvice,		

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	SecuritiesSettlementTransactionGenerationNotification. - Cash Account: only applicable for SettlementInstruction, SettlementRestriction on cash,AccountRequestAcknowledgement, BankToCustomerDebitCreditNotification, AccountLinkStatusAdvice, SecuritiesSettlementTransactionConfirmation, IntraBalanceMovementStatusAdvice, IntraBalanceMovementConfirmation, SecuritiesSettlementTransactionGenerationNotification, IntraBalanceMovementModificationRequestStatusAdvice, IntraBalanceMovementCancellationRequestStatusAdvice. - Instruction Status: only applicable for IntraPositionMovementStatusAdvice, SecuritiesSettlementTransactionStatusAdvice, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementConditionsModificationStatusAdvice, IntraBalanceMovementStatusAdvice, IntraBalanceMovementModificationRequestStatusAdvice, IntraBalanceMovementCancellationRequestStatusAdvice. - Transaction Code: only applicable for SettlementInstruction, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesSettlementTransactionAllegementNotification, SecuritiesSettlementTransactionGenerationNotification. - Currency: only applicable for SettlementInstruction, SettlementRestriction on cash,BankToCustomerDebitCreditNotification, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementTransactionAllegementNotification, IntraBalanceMovementStatusAdvice,		

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	IntraBalanceMovementConfirmation, SecuritiesSettlementTransactionGenerationNotification, IntraBalanceMovementModificationRequestStatusAdvice, IntraBalanceMovementCancellationRequestStatusAdvice. - Already Matched Flag: only applicable for SettlementInstruction, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementConditionsModificationStatusAdvice - Settlement Transaction Condition Code: only applicable for SettlementInstruction, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesSettlementTransactionGenerationNotification. - Business Sending Party: only applicable for SettlementInstruction, SettlementRestriction on securities, SettlementRestriction on cash, IntraPositionMovementStatusAdvice, IntraPositionMovementConfirmation, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice, SecuritiesSettlementConditionsModificationStatusAdvice, IntraBalanceMovementStatusAdvice, IntraBalanceMovementConfirmation, SecuritiesSettlementTransactionGenerationNotification,IntraBalanceMovementModificationRequestStatusAdvice IntraBalanceMovementCancellationRequestStatusAdvice,		

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	- Business Sending User: only applicable for SettlementInstruction, SettlementRestriction on securities, SettlementRestriction on cash - Instructing Party: only applicable for SettlementInstruction, SettlementRestriction on securities, SettlementRestriction on cash, IntraPositionMovementStatusAdvice, IntraPositionMovementConfirmation, SecuritiesSettlementTransactionStatusAdvice, SecuritiesSettlementTransactionConfirmation, SecuritiesTransactionCancellationRequestStatusAdvice SecuritiesSettlementConditionsModificationStatusAdvice, IntraBalanceMovementStatusAdvice, IntraBalanceMovementConfirmation, SecuritiesSettlementTransactionGenerationNotification,IntraBalanceMovementModificationRequestStatusAdvice IntraBalanceMovementCancellationRequestStatusAdvice, SecuritiesSettlementTransactionGenerationNotification		
DRUF044	When performing a Message Subscription Rule update request, the Rule Parameter Type specified must refer, depending on the Parameter Type, to an existing and active Attribute Domain Name in Attribute Domain defined by the Service Operator or to an existing CRDM Reference Data entity.	Update Message Susbcription Rule	Unknown Rule Parameter Type Identifier
DRUF050	When performing a Message Subscription Rule update request involving a TIPS Account as Rule Parameter Value, the account must belong to the data scope of the requestor.	Update Message Susbcription Rule	Invalid TIPS Account

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRUF200	When performing a Message Subscription Rule update request, in case of creation/update of Message Subscription Rule Parameter, the Parameter Value must be compliant with the values or rules defined in the relevant Attribute Domain or CRDM Reference Data entity.	Update Message Susbcription Rule	Invalid Parameter Value
DRUF300	When performing a Message Subscription Rule update request, in case of creation of Message Subscription Rule Parameter, the overall number of group of parameters for the relevant CSD must be compliant with the configuration limit defined in CRDM.	Update Message Susbcription Rule	Number of maximum active Message Subscription Rules exceeded
DRUF310	When performing a Message Subscription Rule update request, in case of creation/update of Message Subscription Rule Parameter, the overall number of distinct Parameter Value defined for the same Parameter Type for the relevant CSD must be compliant with the configuration limit defined in CRDM.	Update Message Susbcription Rule	Number of maximum Parameter Values exceeded
DRUF600	When performing a Message Subscription Rule update request, in case of creation/deletion of a parameter type it has to be ensured that the same set of parameters is used into the different groups of the specified rule.	Update Message Susbcription Rule	Invalid Parameter Types for the Specified Parameter Group
DRUV001	Report Configuration can be updated only by Service Operator, CSD, NCB, CSD Participant or Payment Bank. A user belonging to a CSD or NCB can only update Report Configuration for parties that fall under their responsibility according to the Hierarchical Party Model. A user belonging to a CSD Participant or Payment Bank	Update Report Configuration	Requestor not allowed

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
	can only update Report Configuration for his own party		
DRUV003	When performing a Report Configuration update request, it must refer to an existing and active instance of Report Configuration.	Update Report Configuration	Data to be updated not found
DRUV005	When performing a Report Configuration update request, the Opting Party Technical Identifier specified in the Report Configuration Party Link section, must refer to an existing and active Party with the same System Entity of the Report Configuration.	Update Report Configuration	Unknown Opting Party Identifier
DRUV006	When performing a Report Configuration update request, the Event Type specified must belong to an existing instance in CRDM and its Event Type Category must be compliant with the Report Name.	Update Report Configuration	Invalid Event Type
DRUV010	When performing a Report Configuration update request, in case of request to update a Report Configuration Party Link, it must refer to an existing and active minor entity.	Update Report Configuration	Unknown Report Configuration Party Link
DRUV020	When performing a Report Configuration update request, in case of request to delete a Report Configuration Party Link, it must refer to an existing and active minor entity with a future Valid From or already Closed.	Update Report Configuration	Unknown Report Configuration Party Link
DRUV030	When performing a Report Configuration update request, in case of request to create a Report Configuration Party Link, the Valid From must be greater than the current date.	Update Report Configuration	Invalid Valid From

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRUV040	When performing a Report Configuration update request, in case of request to create/update a Report Configuration Party Link, the Valid To must be greater than the current date and greater than the relevant Valid From.	Update Report Configuration	Invalid Valid To
DRUV070	When performing a Report Configuration update request, the specified Currency must refer to an existing Currency.	Update Report Configuration	Invalid currency
DRUV080	When performing a Report Configuration update request, the Currency field can only be used in combination with a currency-dependent event and one of the currency-related report types listed in the T2S documentation.	Update Report Configuration	Currency not relevant
DRUV100	When performing a Report Configuration update request for a given CSD and report type, its validity period cannot overlap with the validity period of an already existing flat file report configuration defined for the same CSD and the same report type.	Update Report Configuration	Flat file configuration exists for the same CSD, report type and period.
DRUV110	When performing a Report Configuration update request, if it refers to a TIPS Report, the Opting Party must be equal to the Owner Party. Furthermore the Party Type must be Payment Bank.	Update Report Configuration	Invalid Party for TIPS reports.
DRUV120	When performing a Report Configuration update request, if it refers to a TIPS Report, the Push Mode flag must be set to TRUE. Furthermore the Execution Time, Event Type and Currency fields must not be used.	Update Report Configuration	Invalid fields for TIPS reports.

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRUV130	When performing a Report Configuration update request, the Frequency field can only be specified for TIPS Reports that are available in Delta mode.	Update Report Configuration	Frequency can only be specified for TIPS reports in Delta mode.
DRUW001	Routing can be updated by Service Operator, CSD, NCB, CSD Participant, Payment Bank and Ancillary System. Users can only update Routing entity linked to Party they belong to. Service Operator User can update Routing entity linked to any Party.	Update Routing	Requestor not allowed
DRUW003	When performing a Routing update request, it must refer to an existing and active instance in CRDM.	Update Routing	Data to be updated not found
DRUW004	When performing a Routing update request, the Network Service Identifier specified must refer to an existing and active instance in CRDM linked to the Party of the Routing entity.	Update Routing	Unknown Network Service Identifier
DRUW006	When performing a Routing update request, the Party Technical Address specified must exist in CRDM belonging to the same Party of the existing Routing.	Update Routing	Unknown Party Technical Address
DRUW007	When performing a Routing update request, if it refers to a Routing with the Default Routing set to True, the Conditional Routing Group must not be specified in input. Furthermore, for T2S in case a Network Service is specified in input, it must be a store-n-forward one and no other default routing is defined for this store-n-forward service.	Update Routing	Invalid combination of values: Default Routing already defined for this Party and Service, or the Service is set to real time

BR NAME	DESCRIPTION	USER FUNCTION	ERROR TEXT
DRUW012	When performing a Routing update request, the Message Type must refer to an existing and active Message Type configured in CRDM for the relevant Service.	Update Routing	Invalid Message Type