Common Reference Data Management for TIPS

User Detailed Functional Specifications

V0.2.0

Author	4CB
Version	0.2.0
Date	12/03/2018

Introduction

[…]

Reader’s guide

[…]

1. General features of CRDM

The present chapter, after a short introduction of the Common Reference Data Management shareable 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 shareable component, has with other services and shareable 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 1.2.3).

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

[…]

1.2.2. Authentication and authorisation

[…]

1.2.3. Access rights

This section provides information on access rights management in the CRDM. More into detail, section 1.2.3.1 presents some basic concepts (e.g. user, privilege, role and data scope) related to access rights management. On this basis, section 1.2.3.2 illustrates all the available options for the configuration of access rights. Finally, section 1.2.3.3 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.

1.2.3.1. Access rights concepts

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

1.2.3.1.1. User function

XML messages and GUI functions are the atomic elements users can trigger in A2A mode and in U2A mode respectively to interact with CRDM and TIPS. Based on these set of XML messages 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 A2A mode or in U2A mode.

1.2.3.1.2. 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.

See section 1.2.3.2.2. for information on the configuration of privileges.

1.2.3.1.3. Role

A role is a set of privileges. See section 1.2.3.2.3. for information on the configuration of roles.

1.2.3.1.4. User

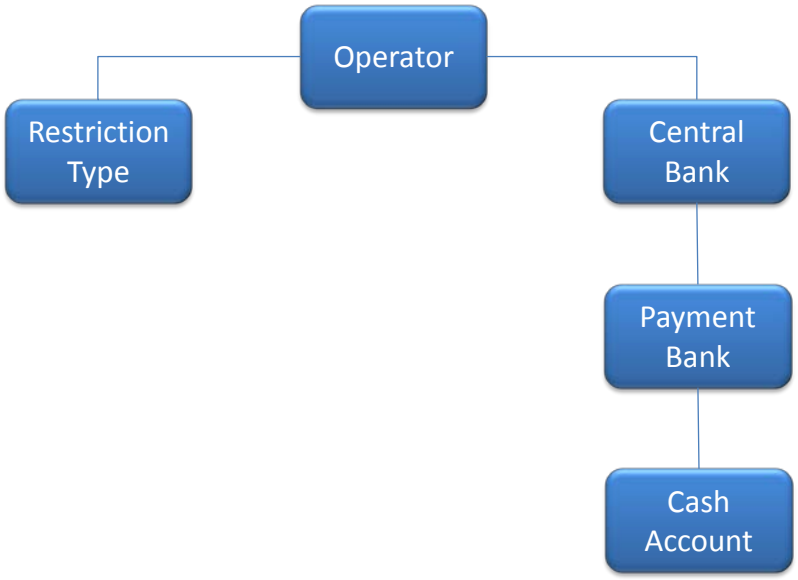
See section 1.2.3.2.1.

1.2.3.1.5. 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. 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



1.2.3.1.6. 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;[2]
- 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.[3]

2 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.

3 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

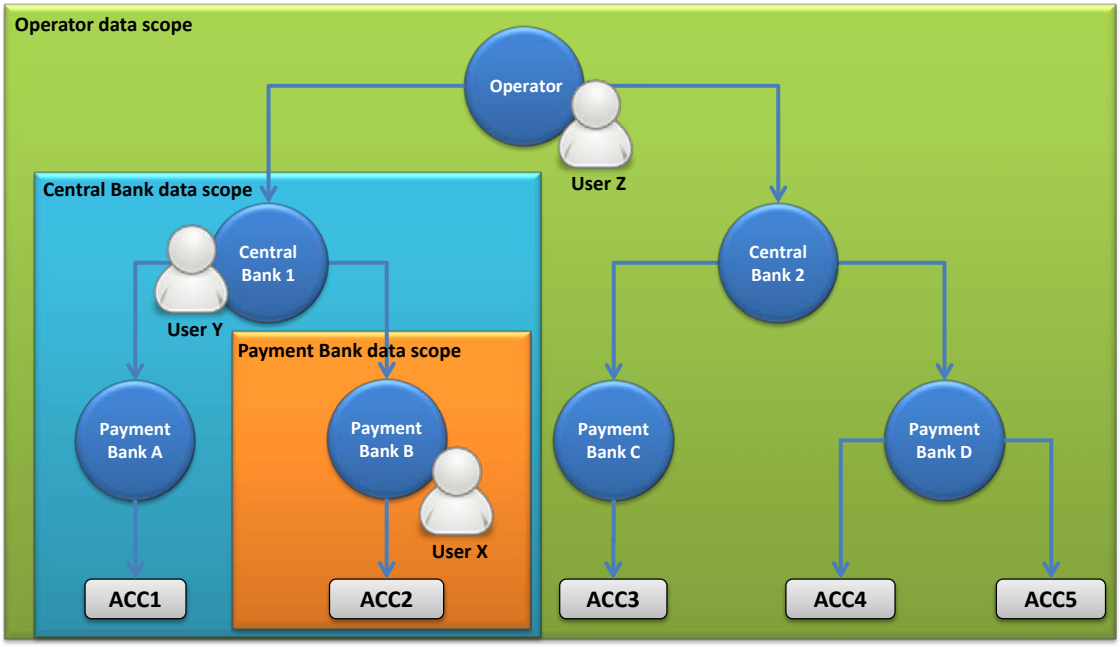
Three users, X, Y and Z, belonging to a Payment Bank, to a Central Bank and to the Operator respectively, are granted with the same privilege to query cash accounts:

TABLE 1 - 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.

1.2.3.2. 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.

1.2.3.2.1. 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 1.2.3.1.6.).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.

1.2.3.2.2. 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.

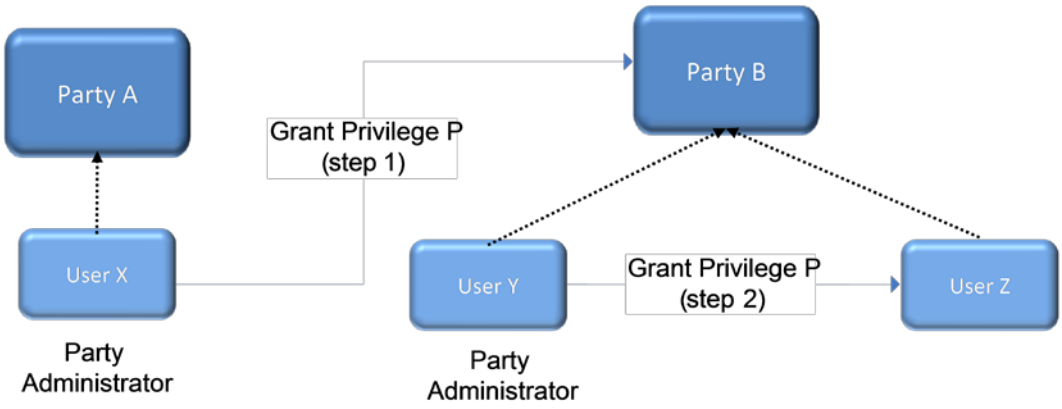
A privilege becomes available to a party administrator of a party different from the CRDM Operator only after this privilege has been granted to this party. From this moment on, the party administrator can grant this privilege, according to the rules defined in the following sections.

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.[4]

4 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.

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 granted to Parties and Users. For details on the configuration of Roles see section 1.2.3.2.3.

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 2 - 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)

OPTION	DESCRIPTION
	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 3 - 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 [5];
- 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:

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

- Without Deny, 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 4 - 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 5 - 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.

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 cascade process is automatically triggered in a deferred mode one time per 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.

1.2.3.2.3. Configuration of roles

Links between roles

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

Granting roles

Roles can be granted to users and parties.

When granting a role to a user, the grantee user 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 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 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 loses all the privileges of the revoked role, i.e. all the privileges linked to the revoked role.

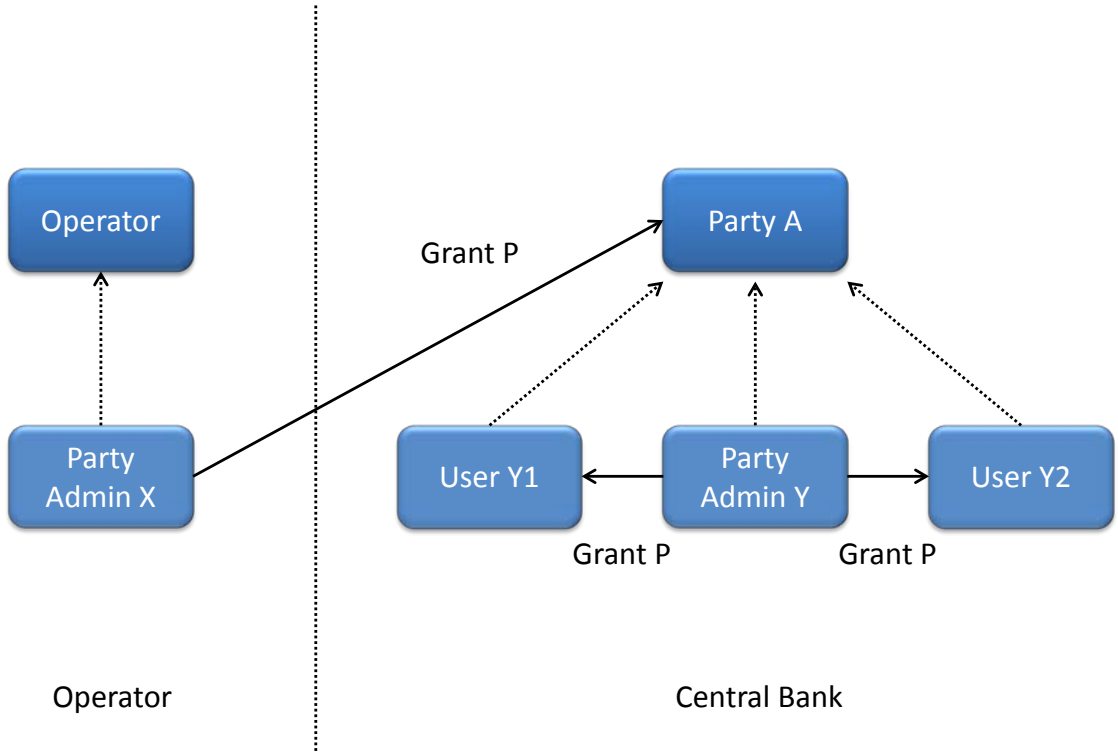
Both when revoking roles from users and from parties, CRDM does not apply a cascade effect.

1.2.3.3. Access rights configuration process

As described in section 1.2.3.2.2. , 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)

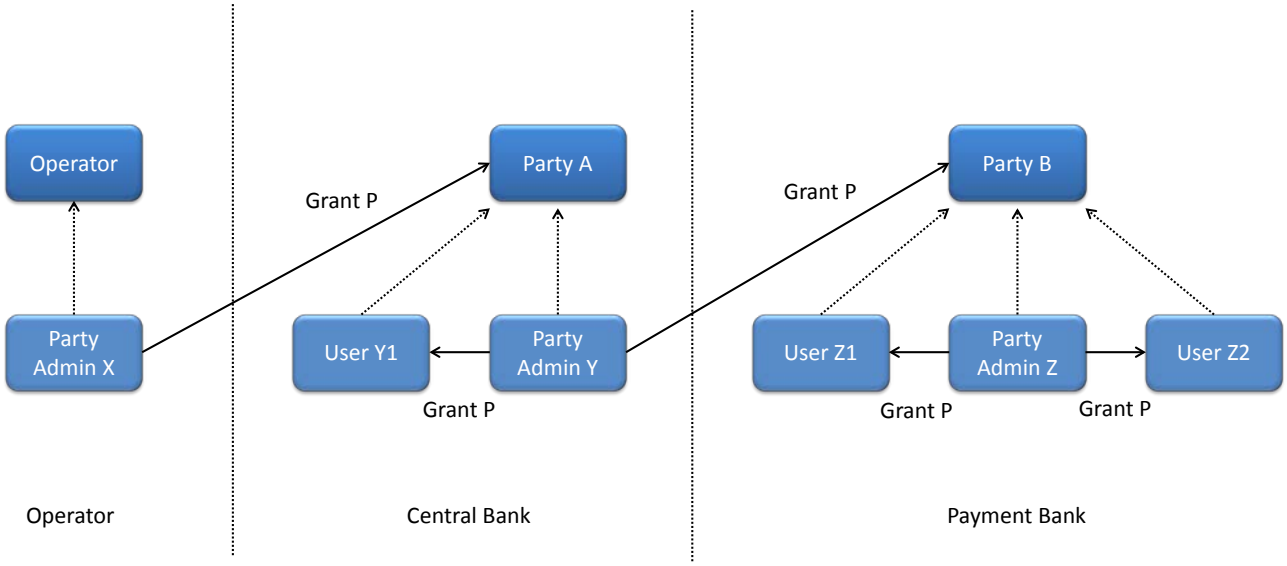


The diagram shows that the two required steps are as follows:

- 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:

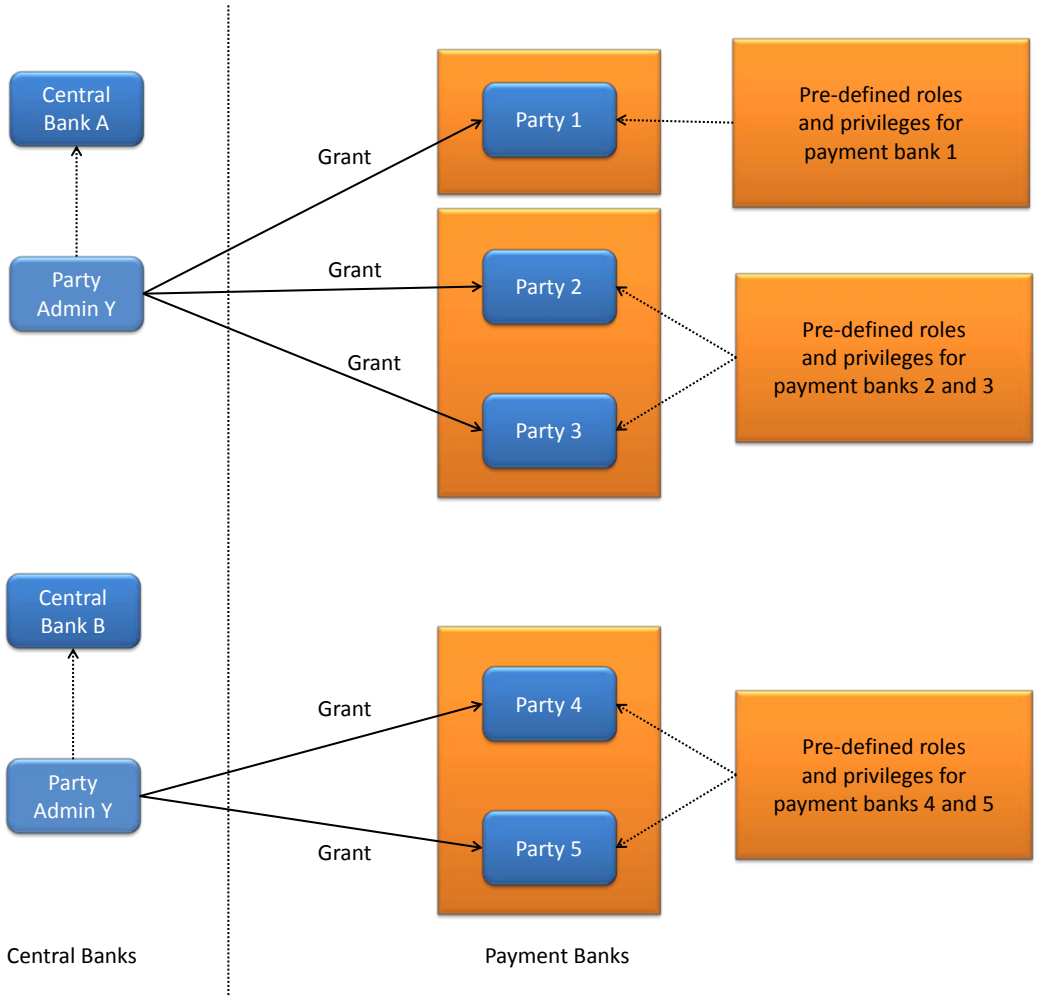
- Configuration of access rights at party level
- Configuration of access rights at user level

1.2.3.3.1. 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

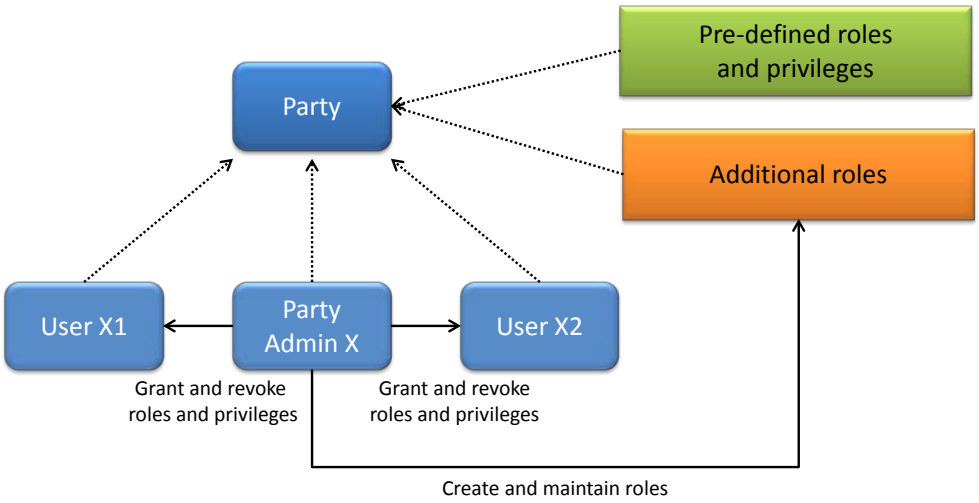


A party administrator of each Central Bank assigns the relevant set of roles and privileges to all its payment banks. In this example the party administrator of a Central Bank A configures the relevant access rights for three payment banks Party 1, Party 2 and Party 3. This results in two different set 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 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.

1.2.3.3.2. 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[6] additional roles, besides the ones previously granted at party level[7]
- By granting (and revoking) the (default and additional) roles and the (default) privileges to the users of the same party.

1.2.4. Message subscription

1.2.4.1. 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.
- 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.

6 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.

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

- 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.

1.2.4.2. 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 6 - 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.

1.2.4.3. 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.

These 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 7 - 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
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 8 - 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

1.2.5. 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 9 – CRDM U2A FUNCTIONS

Function	Actor[8]
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[9]
Update Cash Account	CRDM Operator, Central Bank, Payment Bank[9]
Delete/Restore Cash Account	CRDM Operator, Central Bank, Payment Bank[9]
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

[8] 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 that are described in the MOP.

[9] 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.

Function	Actor[8]
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
Update Message Subscription Rule	Central Bank
Delete/Restore Message Subscription Rule	Central Bank

Function	Actor[8]
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
Update Message Subscription Rule Set	Central Bank
Delete/Restore Message Subscription Rule Set	Central 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

Via U2A mode, CRDM offers to CRDM Actors a dual authorisation concept, the Four-Eyes-Principle (See section 1.2.6).

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

1.2.6. 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.

1.2.6.1. 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 1.2.3. In conjunction with mechanisms of authentication[10] and authorisation applying to all requests received by CRDM in both A2A 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 in order to ensure a strict separation of their respective data in CRDM.

1.2.6.2. 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 A2A 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.

1.2.6.3. 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.

1.2.6.4. Availability

The overall availability of the CRDM services 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.

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

1.2.6.5. 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.

In order to ensure sustainability, CRDM archives all data by storing for a harmonised period of ten years all inbound and outbound messages (except queries) in their original format.

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 10 – 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. 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 11 – VALIDITY PERIOD ATTRIBUTES

Attribute	Description
Valid From[11]	It specifies the date (inclusive) from which the reference data item is valid.
Valid To[12]	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 12 – 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 13 – BEFORE THE PROCESSING

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

[11] Opening Date for certain items.

[12] Closing Data 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. 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.

TABLE 14 – 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 15 – 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 16 – 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 17 – 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 18 – 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.

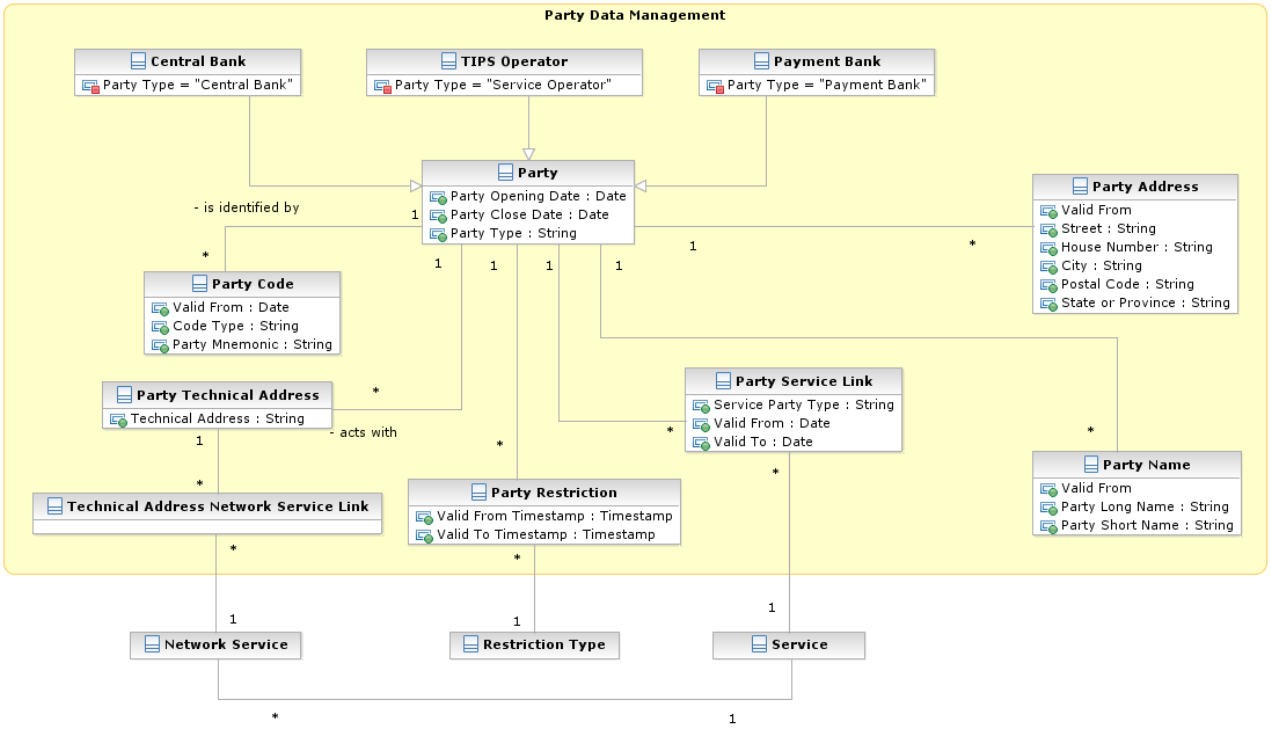
TABLE 19 – AFTER THE PROCESSING

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

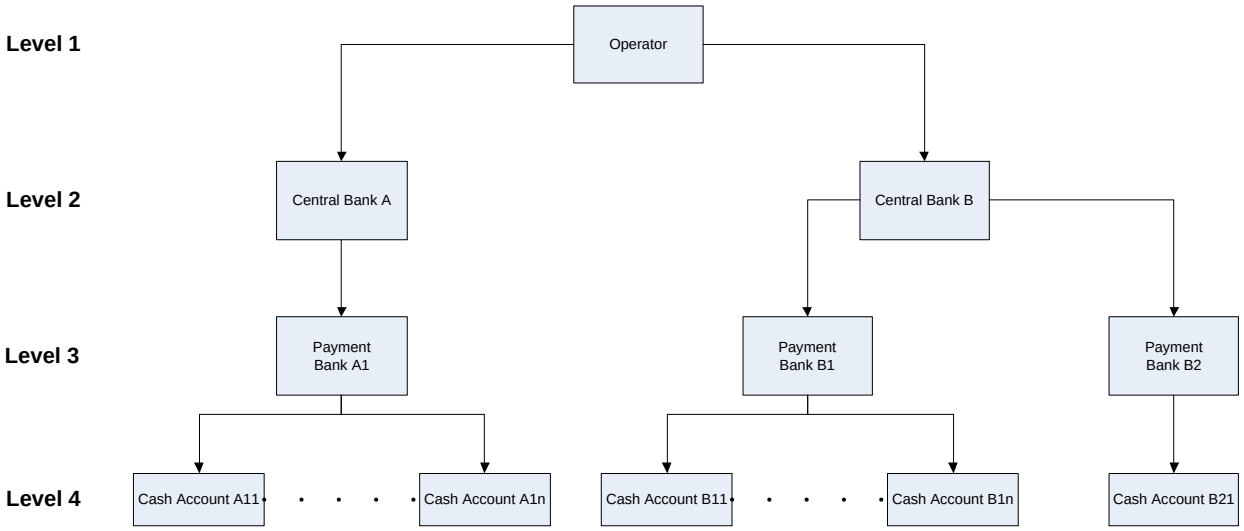
1.3.2.1. Data Model of the component

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*[13].

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*.

[13] 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*.

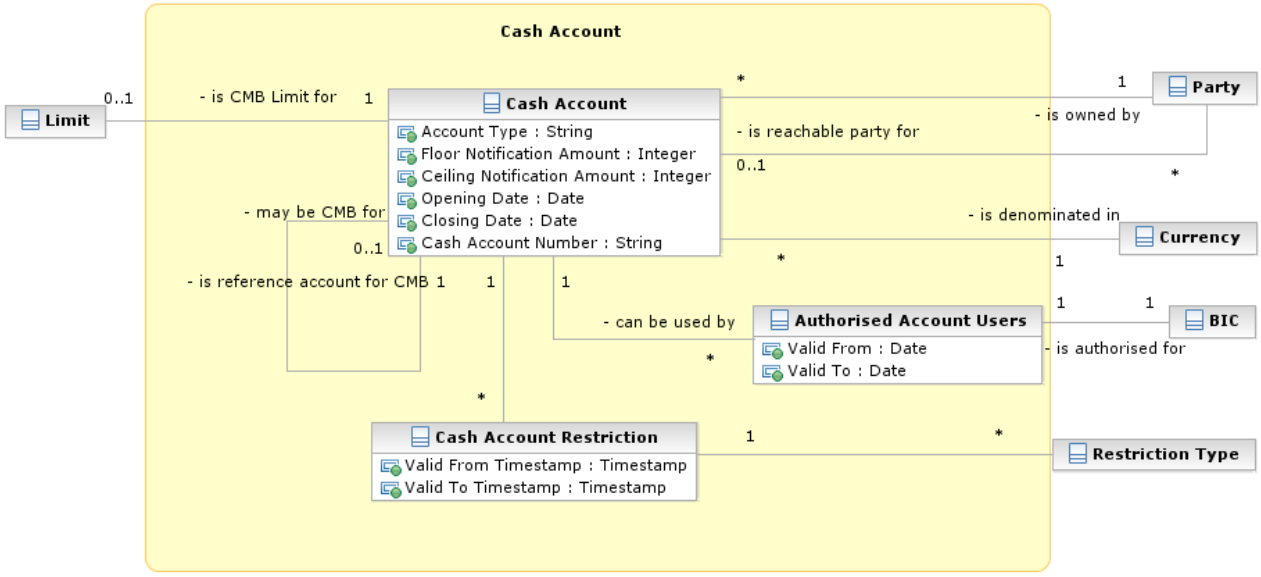
ATTRIBUTE	DESCRIPTION
Service Party Type	Service-specific classification for the Party. Certain values may be used only in conjunction with specific Services and specific Party Types defined at Party level. The exhaustive list of possible values for the TIPS Service is as follows: - TIPS Operator - TIPS 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 Central Bank Accounts may have a negative 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*[14]. *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"[15]. Each TIPS Credit Memorandum Balance may be linked to only one "Authorised Account User".

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

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

2. Limit

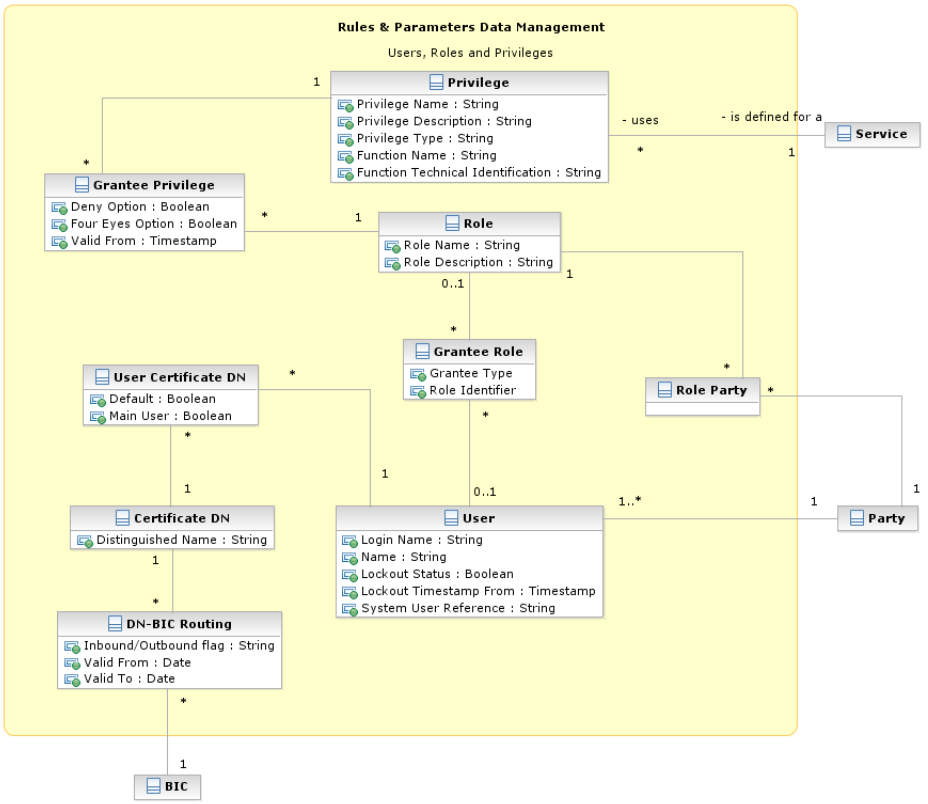
This entity includes all reference data related to *Limits* defined on TIPS Credit Memorandum Balances. Common Reference Data Management shall allow a Payment Bank (linked to the TIPS *Service* as a TIPS Participant) to define and maintain credit limits for their individual customers related to the usage 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 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 Paymebt 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* 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, 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 applications connecting in A2A mode and using functions via XML messages.

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*[16].

2. Certificate DN

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

ATTRIBUTE	DESCRIPTION
Distinguished Name	It specifies the distinguished name.

[16] 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.

Each *Certificate DN* can be linked to one or many *Users*[17].

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* and is linked to a single *Service*. When granting a *Privilege* to a *Role*, 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*.

[17] 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

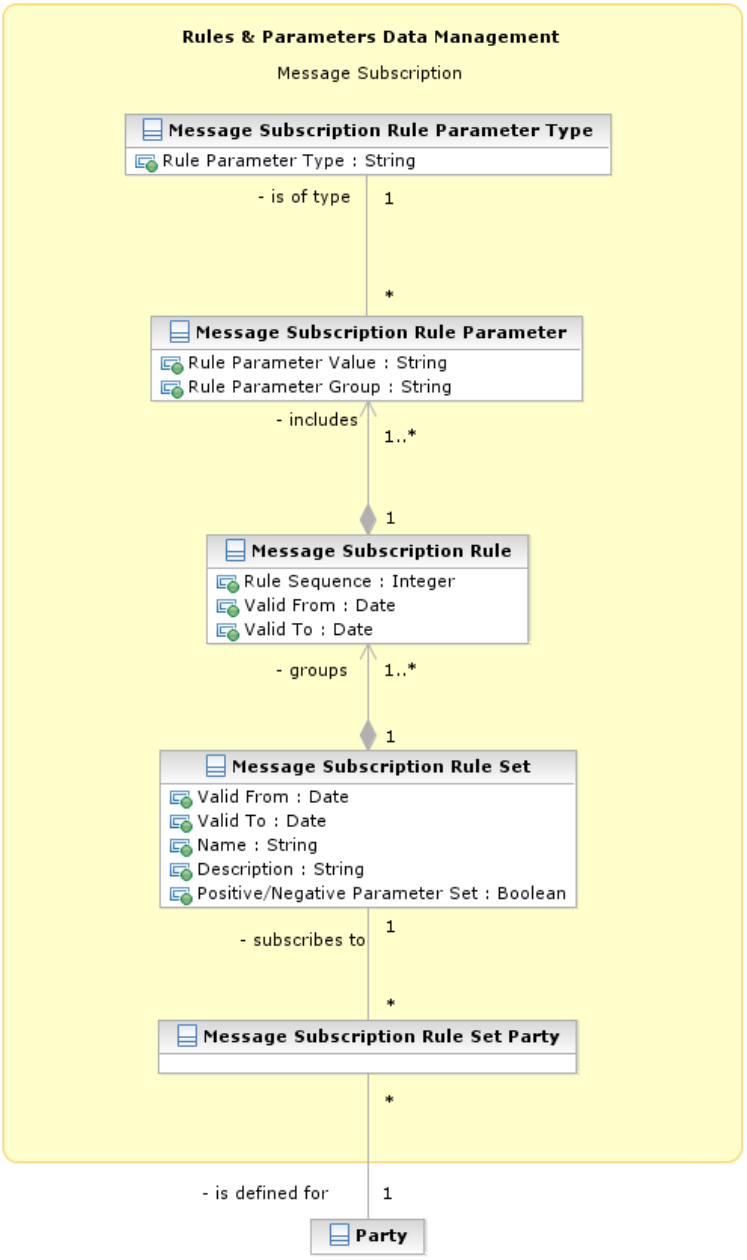
This entity includes all reference data for DN-BIC Routing, for inbound and outbound communication. In the former case, different DNs can be linked to different BICs and vice versa. In the outbound case, the same DN can only be linked to a single BIC. However different DNs can still be linked to the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

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*.

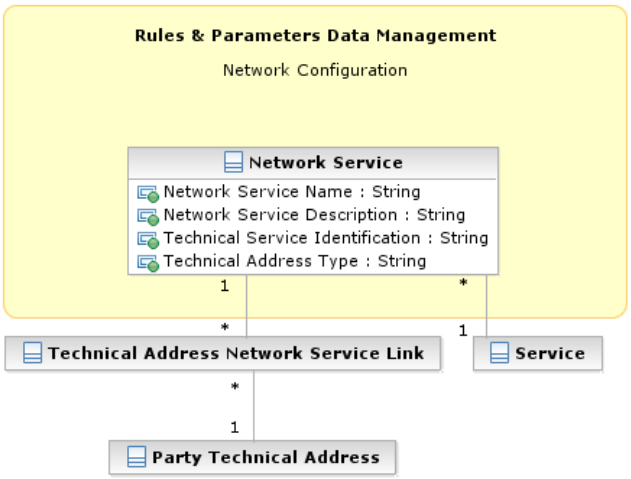
4. Message Subscription Rule Parameter Type

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*.

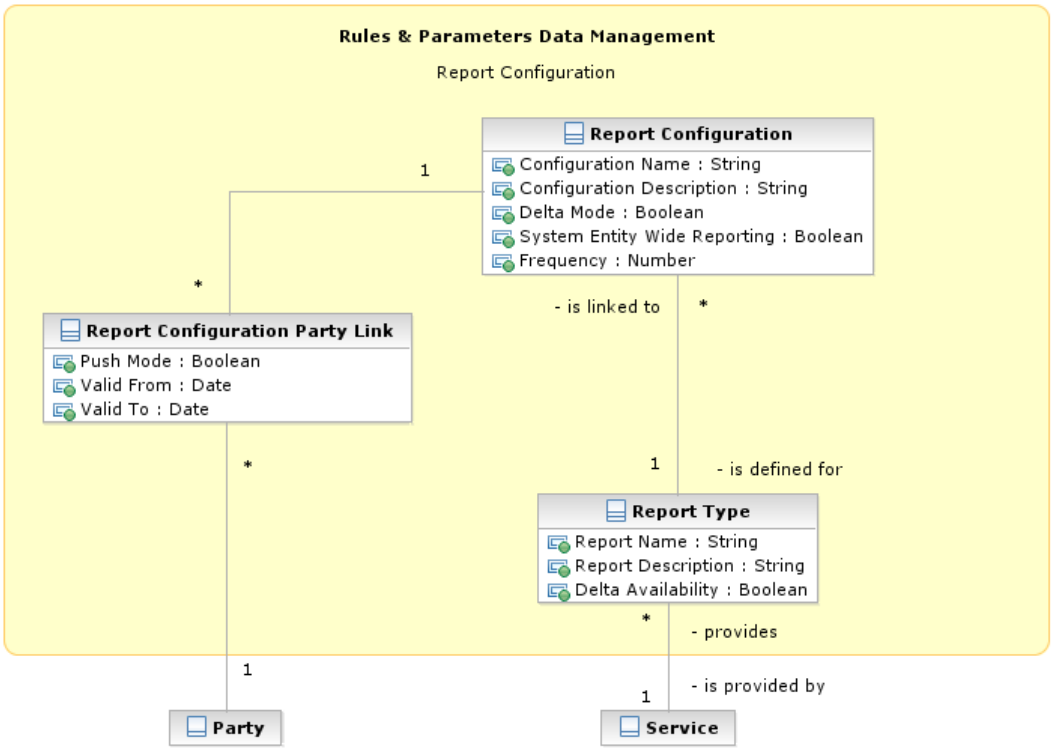
ATTRIBUTE	DESCRIPTION
Network Service Name	Name of the network service.
Network Service Description	Description of the network service.
Technical Service Identification	It specifies all the data needed in order to identify and to use a network service[18].
Technical Address Type	It specifies the type of technical address for the network service (e.g. BIC, Distinguished Name, IP address).

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

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

1.3.7. Report configuration

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



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

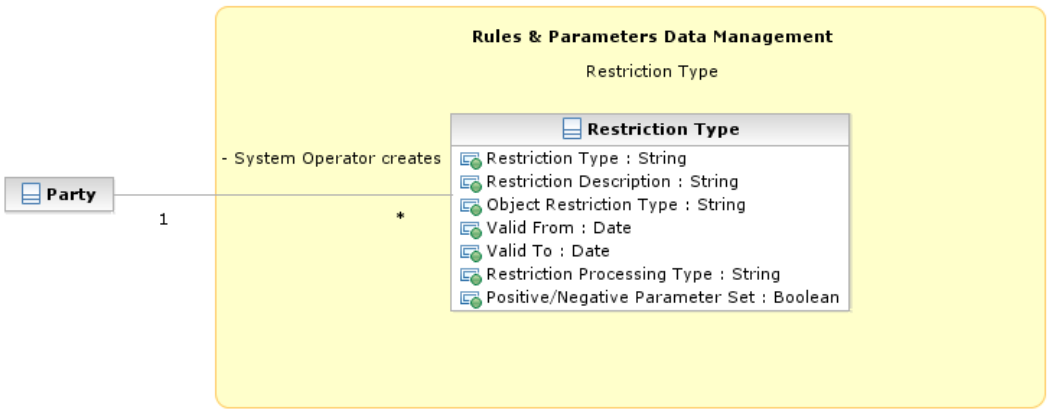
This entity stores all reference data for report configurations. Each *Report Configuration* specifies a type of report, its data scope (i.e. full or delta report), the set of parties entitled to get said type of report and the mode they get it (i.e. push or pull).

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. 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*[19].

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*.

19 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.

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.

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.

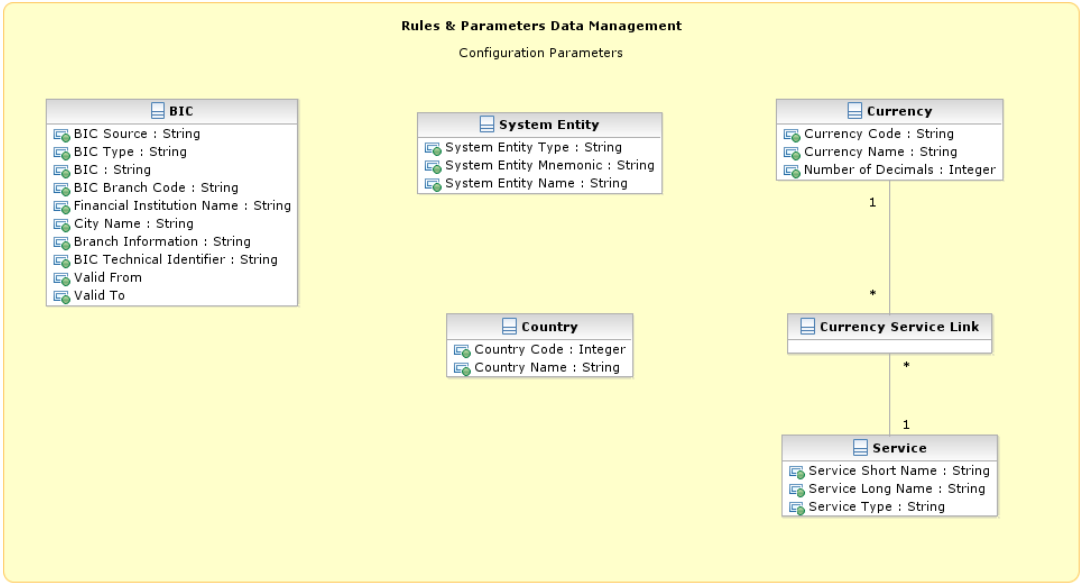
Each *Restriction Type* is linked to the specifying *Party* (i.e. the CRDM Operator).

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 service 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 service 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 service 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 service 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 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 in A2A mode (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 1.2.3).

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 service and the CRDM Actors that are responsible for their management, i.e. for creating and maintaining them:

TABLE 20 - COMMON REFERENCE DATA OBJECTS

AREA	OBJECT	RESPONSIBLE CRDM ACTORS [20, 21]
Party	Party	CRDM Operator, Central Bank
	Party Service Link	CRDM Operator, Central Bank
Cash account	Cash account	All[22]
	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 Link[23]	All
	Role Party Link[24]	CRDM Operator, Central Bank
	Privilege Role Link[25]	CRDM Operator, Central Bank
Message subscription configuration	Message subscription rule	Central Bank
	Message subscription rule set	Central Bank
Network configuration	DN BIC Routing	Payment Bank
	Network service	CRDM Operator
	Technical address Network service link	CRDM Operator, Central Bank
Report configuration	Report configuration	Payment Bank
Restriction type management	Restriction type	CRDM Operator
Configuration parameters	Country	CRDM Operator

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

21 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 that are described in the MOP.

22 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.

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

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

25 This object is related to the granting/revoking of Privileges to/from Roles.

AREA	OBJECT	RESPONSIBLE CRDM ACTORS [20, 21]
	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 service 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 service 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 service 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 service when performing the purge process following the archiving process (See section 1.4.3.4).
- Restore [26]. 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 service provides some specific types of reference data maintenance operations for the configuration of access rights (See section 1.2.3 for a detailed description of these operations).

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 service 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 21 - COMMON REFERENCE DATA OBJECTS WITH UNLIMITED VALIDITY PERIOD

AREA	OBJECT
Cash account	Authorized Account User

26 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
Access rights management	User
	Role
	Privilege
	Certificate DN
	User-Certificate DN Link
	Role User Link
	Role Party Link
	Privilege Role Link
Network configuration	DN BIC Routing
	Network service
	Technical Address Network Service Link
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 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 service 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 22 - COMMON REFERENCE DATA OBJECTS WITH LIMITED VALIDITY PERIOD [27]

AREA	OBJECT	CREATION	UPDATE	DELETION
Party	Party	Validity date may take the value of the current date.	May take effect on the current date [28].	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.
	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.
	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.

27 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.

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

AREA	OBJECT	CREATION	UPDATE	DELETION
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.
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.

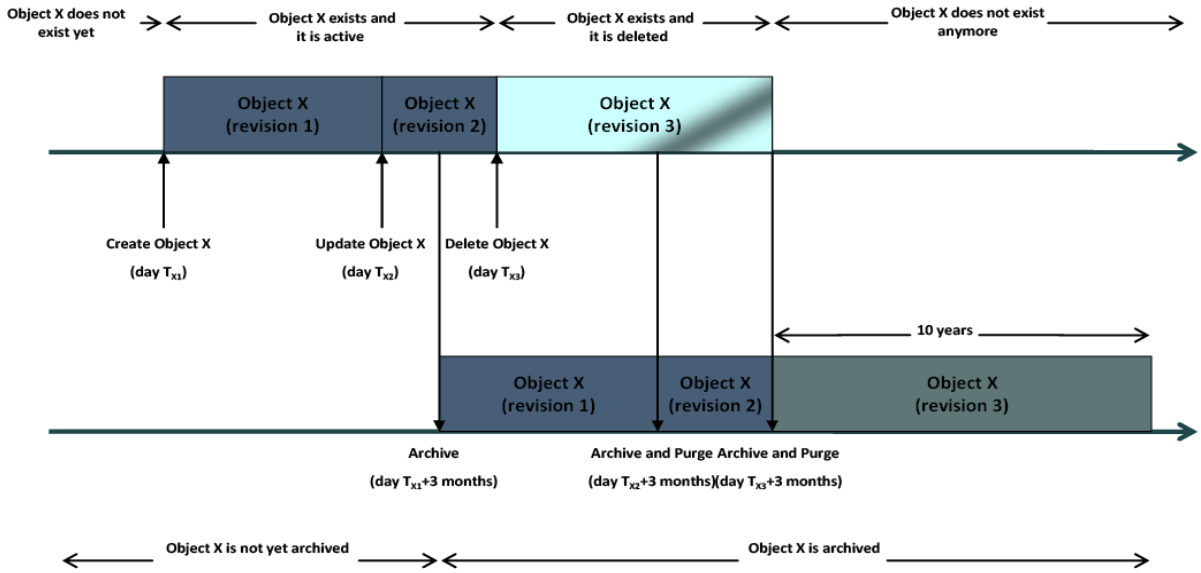
For parties and cash accounts the validity period is defined by an Opening Date and a Closing Date attribute. Between these two dates the common reference data object, i.e. the party or the cash account, is valid, meaning that TIPS can use it for processing (e.g. for settlement purpose). Outside this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

1.4.3.4. Common reference data archiving and purging

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

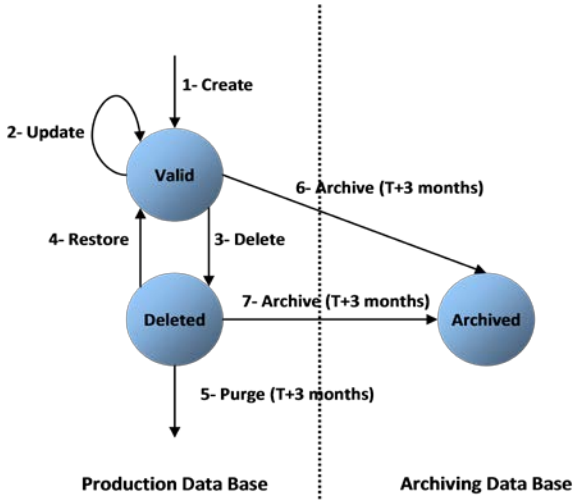
1.4.3.5. Lifecycle of common reference data objects

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 service a reference data maintenance instruction to create a common reference data object with unlimited validity period, the Common Reference Data Management service 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 service one or many reference data maintenance instructions to update the common reference data object. Regardless of the result of the Common Reference Data Management service 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 service a reference data maintenance instruction to delete a common reference data object, the Common Reference Data Management service 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 service a reference data maintenance instruction to restore a previously deleted common reference data object, the Common Reference Data Management service processes it and, in case of successful processing, it restores the relevant object. As a result, the object becomes valid again (transition 4).

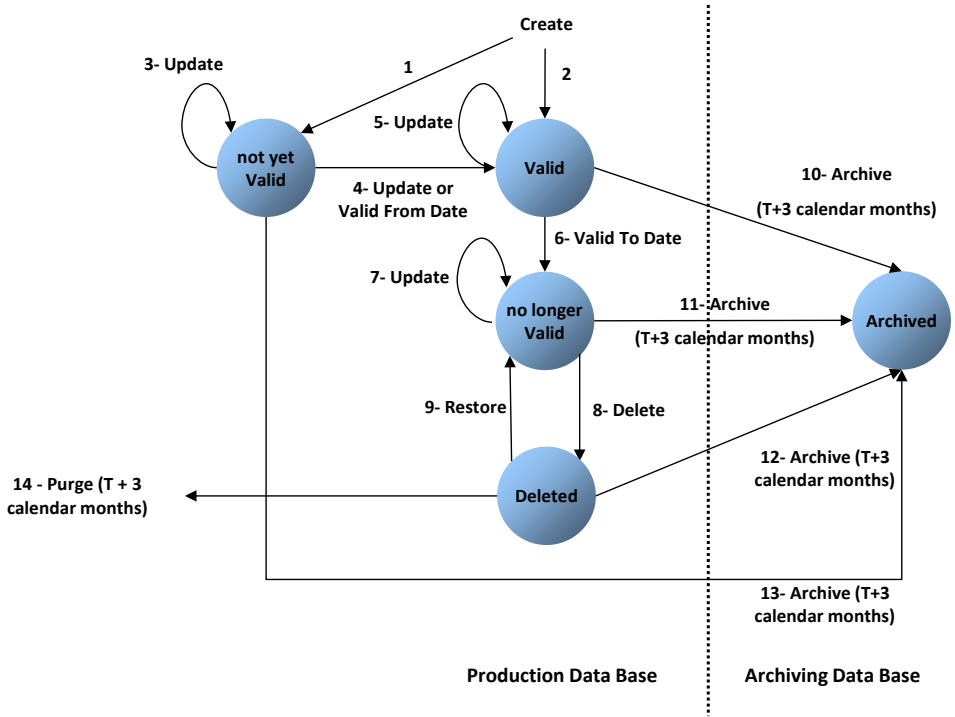
Three calendar months after a common reference data object has been deleted, the Common Reference Data Management service physically deletes it from the production data base. This results in the object being purged by the production data base (transition 5), i.e. it exists only in the archiving data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

Three calendar months after a common reference data object has been either created, updated or deleted, the Common Reference Data Management service 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 service a reference data maintenance instruction to create a common reference data object with limited validity

period, the Common Reference Data Management service 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 service 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 (transitions 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 service a reference data maintenance instruction to delete a common reference data object, the Common Reference Data Management service 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 service a reference data maintenance instruction to restore a previously deleted common reference data object, the Common Reference Data Management service 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 service 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 are 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

The structure of the TIPS Directory is as follows:

TABLE 23 – TIPS DIRECTORY STRUCTURE

O/M	FIELD No.	FIELD NAME	FORMAT	DESCRIPTION
M	1	User BIC	CHAR(11)	BIC of the TIPS Participant or Reachable Party configured as Authorised Account User in TIPS. This BIC identifies 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 if 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	Type of Change	CHAR(1)	Exhaustive list of possible values: A – Added M – Modified D – Deleted U – Unchanged
M	5	Valid From	DATE(YYYYMMDD)	Date from which the entry is valid.
M	6	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.

O/M	FIELD No.	FIELD NAME	FORMAT	DESCRIPTION
M	7	Participation Type	CHAR(2)	Exhaustive list of possible values: 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 24 – 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 day at 17:00 CET. The full version includes all BICs of TIPS Participants and Reachable Parties that are addressable within TIPS, wheras the delta version only includes changes 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.

1.5. Interactions with other services

[…]

1.5.1. TARGET2-Securities

[…]

1.5.2. TARGET2

[…]

1.5.3. TARGET Instant Payment Service

[…]

1.6. Operations and support

1.6.1. Service 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 modify the access rights of their users independently, without resorting to the CRDM Operator. For details on access rights management, see section 1.2.3 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 service 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 service 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.

1.6.3. Archiving management

[...]

2. Dialogue between CRDM and CRDM Actors

[…]

3. Catalogue of messages

[...]

3.1. Introduction

[...]

3.2. General information

[...]

3.2.1. Message signing

[...]

3.2.2. Technical validation

[...]

3.2.3. Supported Character Set

[...]

3.3. Messages usage

3.3.1. List of messages

[...]

3.3.2. Messages description

[...]

4. Appendices

4.1. Business Rules

[…]

4.2. List of ISO Error codes

[…]

4.3. Index of figures

[...]

4.4. Index of tables

[…]

4.5. List of acronyms

[…]

4.6. List of referenced documents

[…]