

Clarification note

CRDM Configuration Guidelines for Payment Banks and Ancillary Systems relevant in CLM/RTGS

|  |  |
| --- | --- |
| Author | Banca d’Italia |
| Version | 1.0 |
| Date | 03-2022 |
|  |  |
| All rights reserved. |  |

Table of contents

[1 Scope of the note 3](#_Toc99040001)

[2 Steps covered by the Central Bank 4](#_Toc99040002)

[2.1 Party data 4](#_Toc99040003)

[2.2 Technical Address Network Service Link 4](#_Toc99040004)

[2.3 Party Service Link 5](#_Toc99040005)

[2.4 Cash Account data 5](#_Toc99040006)

[3 Steps covered by the Participant 7](#_Toc99040007)

[3.1 Users and Certificates 7](#_Toc99040008)

[3.1.1 Users 7](#_Toc99040009)

[3.1.2 Certificate DNs 7](#_Toc99040010)

[3.1.3 User-Certificate DN Links 8](#_Toc99040011)

[3.2 Roles and Privileges 8](#_Toc99040012)

[3.3 Message Routing 8](#_Toc99040013)

[3.3.1 Default Routing 8](#_Toc99040014)

[3.3.2 DN-BIC Routing (RTGS only) 8](#_Toc99040015)

[3.4 Additional (non mandatory) configuration 10](#_Toc99040016)

# Scope of the note

This note provides a list of sequential steps to be followed in order to configure a Payment Bank or Ancillary System Participant in CRDM and enable them to autonomously operate within CLM, RTGS and in the related Common Components.

This guide is intended as providing a minimal set of steps that users should follow to be able to operate independently. Non-essential configurations, which may be dictated by the users’ specific business and requirements, will not be covered.

Detailed information on the screens and messages involved in the configuration is provided in the CRDM UDFS and UHB documents.

# Steps covered by the Central Bank

The Central Bank is responsible for configuring the following data for each of their Payment Bank and Ancillary System Participants, based also on information provided by the Participant in the related Registration Form.

## Party data

Screen: Party – New/Edit

Messages: reda.014, reda.016, reda.022

DMT: available

Party data includes the Party itself and related information, including the Party Technical Address (PTA).

The PTA is a Distinguished Name (DN) and it will have to exactly match the one that will be used as requestor (technical sender) in messages sent to the system.

|  |
| --- |
| The PTA is configured using lowercase qualifiers and without spaces, e.g.  *cn=user01,ou=example,ou=12345,o=t2,o=nsp* |

## Technical Address Network Service Link

Screen: Technical Addresses Network Service Link – New/Edit

Messages: n/a

DMT: available

The TANSL represents the link between the PTA and the related Network Service(s). Each PTA needs to be linked to all the Network Services required to interact with each specific Service and Component and for each communication channel (i.e. message/file and real-time/store-and-forward). For the T2 Service, this includes the following components:

* T2-specific components: CLM, RTGS
* Common components used in T2: CRDM, BILL, BDM

Each Network Service controls the routing of messages related to the individual component.

|  |
| --- |
| Network Services for T2 follow the naming convention below:  *ServiceComponent.NSP.Type of interaction*  Some examples follow:  T2CLM.SWIFT.FILESNF T2CLM.SWIFT.MSGRT T2CLM.SWIFT.MSGSNF  T2CLM.SIA-COLT.FILESNF T2CLM.SIA-COLT.MSGRT T2CLM.SIA-COLT.MSGSNF  T2RTGS.SWIFT.FILESNF T2RTGS.SWIFT.MSGRT T2RTGS.SWIFT.MSGSNF  T2CRDM.SWIFT.FILESNF T2CRDM.SWIFT.MSGSNF T2CRDM.SWIFT.MSGRT  T2BILL.SWIFT.FILESNF T2BILL.SWIFT.MSGSNF T2BILL.SWIFT.MSGRT |

## Party Service Link

Screen: Party Service Link – New/Edit

Messages: n/a

DMT: available

Party Service Links enable the Participant to operate in a specific Service/Component with a more specific Party Type. Separate Links for CLM and RTGS are required. Additional component-specific data (e.g. Minimum Reserve settings) is required for each Party Service Link.

At least one Cash Account of a specific type per Party Service Link is required to complete the configuration (see next section).

## Cash Account data

Screens: Cash Account – New/Edit, Authorised Account User – New/Edit

Messages: acmt.007, acmt.010, acmt.011, acmt.015, acmt.019

DMT: available for both Cash Account and Authorised Account User

Depending on the Participant’s business, different types of Cash Accounts may be opened by the CB.

In addition, Authorised Account User (AAU) data should be defined for the following account types in order to define the Cash Account BIC, which is required in order to identify the Cash Account in CLM/RTGS. The Participation Type should be set to “Direct”:

* For CLM
  + MCA
  + CLM CB account
  + CB ECB account
  + ECB mirror account
  + CLM dedicated Transit account for T2S
  + CLM dedicated Transit account for TIPS
  + CLM dedicated Transit account for RTGS
* For RTGS
  + RTGS DCA
  + RTGS CB account
  + RTGS dedicated Transit account
  + AS Technical account
  + Ancillary System Guarantee funds account

For the other T2 cash account types no account BIC is required.

Several AAU may be defined with different Participation Types (e.g. multi-addressee) but at least one with Participation Type “Direct” is required for this purpose.

Party Service Link, Cash Account and AAU represent an aggregate configuration of data that should be fully completed. For certain types of Party Service Link, at least one Cash Account (of a specific type) per Party Service Link is required to be open on the same business dates in order for the configuration to be usable in CLM/RTGS, as per table below.

|  |  |  |
| --- | --- | --- |
| **Owner Party**  **Party Type** | **Party Service Link**  **Service Party Type** | **Cash Account**  **Account Type** |
| Payment Bank | CLM Account Holder | Main Cash Account |
| Central Bank | CLM CB Account Holder | CLM CB Account |
| Central Bank | CLM CB Technical Account Holder | CB ECB Account |
| Central Bank | CLM Transit Account Holder | CLM Transit Account |
| Payment Bank | RTGS Account Holder | RTGS Dedicated Cash Account |
| Central Bank | RTGS Transit Account Holder | RTGS Transit Account |
| Central Bank | RTGS CB Account Holder |

RTGS CB Account

For the configuration of aspects related to Billing, refer to the dedicated BILL Configuration Guide.

# Steps covered by the Participant

Once the Central Bank has confirmed the setup described in the previous section, Participants are required to carry out the following configuration steps.

## Users and Certificates

### Users

Screens: User – New/Edit

Messages: n/a

DMT: available

Participants may define their own logical Users depending on the access channel (A2A or U2A).

If the Participant intends to operate using the A2A channel, at least one A2A User is required, representing the Participant’s back-office application. In this case the User’s System User Reference field should match the one foreseen to be used in the messages’ Business Application Header (BAH) field /Document/AppHdr/Fr/FIId/FinInstnId/ClrSysMmbId/MmbId.

U2A Users may be created to represent users interacting with the Graphical User Interfaces.

CRDM does not make a distinction between A2A and U2A Users. Proper configuration of Certificates is required to enable each channel, as described in the next sections.

### Certificate DNs

Screens: Certificate Distinguished Name – New/Edit

Messages: n/a

DMT: available

Certificate DNs are required for both A2A and U2A users.

A2A Certificates represent the DN linked to an A2A User. This Certificate DN should match the one used in the BAH for signing the message.

|  |
| --- |
| Certificate DNs for T2 in A2A mode should be defined with uppercase qualifiers and no spaces, e.g.  CN=user01,OU=example,OU=12345,O=t2,O=nsp |

U2A Certificates represent the DN used by a physical user to access the system or to sign the U2A instruction (through Non-Repudiation of Origin).

|  |
| --- |
| Certificate DNs for T2 in U2A mode should be defined with uppercase qualifiers and spaces after each comma, e.g.  CN=user01, OU=example, OU=12345, O=t2, O=nsp |

### User-Certificate DN Links

Screen: User-Certificate Distinguished Name Link – New

Messages: n/a

DMT: available

User-Certificate DN Links are required to link a Certificate DN to the respective User.

In A2A mode the DN used as Business Signing DN in messages sent to the system must be defined as a Certificate DN linked to the A2A User.

In U2A mode the DN used by each user to access the system should be configured as a Certificate DN and linked to the U2A User representing the individual system user.

## Roles and Privileges

Screens: User – New/Edit, Certificate Distinguished Name – New/Edit, User-Certificate Distinguished Name Link – New, Grant/Revoke Role – New/Edit

Messages: n/a

DMT: available *for User, Certificate Distinguished Name, User-Certificate Distinguished Name Link and Role granting*

The Participant’s Party Administrator(s) can propagate the Roles and Privileges received from the Central Bank by granting them to the appropriate Users.

The Roles and Privileges to be assigned depend on the business needs and access rights profile of the Participant and of each of their internal Users.

## Message Routing

### Default Routing

Screen: Routing – New/Edit

Messages: n/a

DMT: n/a

Participants must define a Default Routing configuration for each Network Service linked to their PTAs. The Routing configuration defines the default PTA for communication related to the relevant Network Service.

Default routing is necessary to receive messages and reports in A2A mode.

### DN-BIC Routing (RTGS only)

Screens: Distinguished Name-BIC Routing – New/Edit

Messages: n/a

DMT: available

The DN-BIC Routing links a Cash Account BIC (defined as Authorised Account User) to its related DN in order to receive payment orders, payment revocation and recall orders or payment recall responses. The DN should match the message recipient stated in the “To” field of the message’s Business Application Header (BAH).

For the usage in RTGS a A DN can be defined in CRDM in a DN-BIC Routing if it has previously been defined

* as PTA (see section 2.1) for the Party holding the Cash Account linked to the relevant AAU, and
* as Certificate DN with a User-Certificate DN Link to a User belonging to the same Party (see section 3.2).

In other words, CRDM validates DN-BIC Routing data against Certificate DNs and Party Technical Addresses. On T2 side the DN-BIC Routing data is validated against the list of Party Technical Addresses for the relevant Party. Possible differences in upper/lowercase characters between the DN referenced in DN-BIC Routing and the related PTA are expected and do not create an issue on T2 side.

The Participation Type for the DN-BIC Routing should be the same as the related AAU – i.e. for the Cash Account BIC it should be “Direct”[[1]](#footnote-2).

|  |
| --- |
| The DN in a DN-BIC Routing instance refers to the respective Certificate DN; therefore it will appear as for an A2A DN with uppercase qualifiers and no spaces after each comma, e.g.  *CN=user01,OU=example,OU=12345,O=t2,O=nsp*  Differences in upper/lowercase between DN-BIC Routing and PTA are not relevant. RTGS will use the data of the PTA related to the DN defined in the DN-BIC Routing, avoiding any possible discrepancy. |

Different DNs may be used as DN-BIC Routing and as User DNs to sign messages to the system; all DNs should be captured as Certificate DNs.

**Example 1: the participant uses only one DN:**

The participant wants to register DN cn=test,o=abcxxx,o=swift as DN-BIC routing.

In this scenario, the DN should be present in CRDM as:

* Party Technical Address (PTA), captured by the CB together with the relevant TANSL – see section 2.1
* Certificate DN of the A2A user – CN=test,O=abcxxx,O=swift – see section 3.2.2
* DN-BIC Routing - CN=test,O=bnbgbgsf,O=swift – same as certificate DN of the A2A user

The DN-BIC Routing points automatically to a Certificate DN instance, so differences in upper/lowercase characters compared to the PTA will occur for A2A users. These differences are expected and will have no impact on normal functionality in CLM/RTGS.

**Example 2: the participant uses more than one DN**

If the participant will use a different DN as technical sender and another one for signing the BAH, the DNs should be captured in CRDM as:

* Party Technical Address (PTA) – should include all the DNs used for incoming and outgoing messages – captured by the CB together with the relevant TANSL – see section 2.1
* Certificate DN of both the technical sender DN and the DN that signs the BAH: both are captured with upper case, without space - CN=test,O=abcxxx,O=swift – see section 3.2.2
* DN-BIC routing – for each BIC only one DN-BIC routing is allowed; the DN to be used for the DN-BIC Routing should match the DN used as Technical Sender

## Additional (non mandatory) configuration

Depending on the Participant’s specific business, the following objects may be additionally configured:

* Message Subscription Rule Sets and Rules to receive specific messages (e.g. pacs.002, camt.054, camt.077, etc.);
* Report Configuration to receive reports (e.g. Statement of Account, RTGS Directory, etc.);
* Conditional Routing configurations to define alternative PTAs to receive specific messages/reports;
* Additional AAU/DN-BIC Routing configuration for Multi-Addressee and Addressable BICs on each Cash Account.

1. For RTGS outbound communication, for both account BICs and multi-addressee BICs, each BIC must be linked to one single DN (technical address) but the same DN can be linked to multiple BICs. The DN is derived from the Business Receiver BIC used in the BAH of the inbound message. [↑](#footnote-ref-2)