Clarification note

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

Author Banca d'Italia

Version 1.0

Date 07-2022

Table of contents

1 Scope of the note

This note provides a list of sequential steps to be followed by Payment Bank or Ancillary System Participants in CRDM to enable them to autonomously operate within CLM, RTGS and in the related Common Components. The central bank must have performed an initial configuration as a prerequisite.

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, are not be covered.

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

2 Steps covered by the Participant

Once the Central Bank has confirmed its setup, Participants are required to carry out the following configuration steps.

2.1 Users and Certificates

2.1.1 Users

Screens: User – New/Edit
Messages: n/a

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.

2.1.2 Certificate DNs

Screens: Certificate Distinguished Name – New/Edit
Messages: n/a

Certificate DNs are *required* for:

a) A2A Users
b) U2A users.

Certificate DNs *may be required* for:

c) A2A Technical senders/receiver (technical address/PTA)

a)

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

b)

U2A Certificates represent the DN used by a person 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

c) Optional configuration needed if no A2A certificate matches[1] a PTA where RTGS payments need to be received: PTA Certificates represent the DN linked to a technical sender/receiver as a technical address. This configuration requires the setup of a DN-BIC Routing (see section 2.3.2) which in turn requires the definition of a Certificate DN. This type of Certificate DN is then different from the one used in the BAH for signing the message according to a) or the U2A instruction according to b) as it does not need to be linked to a user.

> Certificate DNs for T2 technical sender/receiver should be defined with lower qualifiers and no spaces, e.g.
>
> cn=user01,ou=example2,ou=12345,o=t2,o=nsp

2.1.3 User-Certificate DN Links

Screen: User-Certificate Distinguished Name Link – New
Messages: n/a

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 a person to access the system should be configured as a Certificate DN and linked to the U2A User representing the person.

2.2 Roles and Privileges

Screens: Grant/Revoke Role – New/Edit
Messages: n/a

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

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

It is not possible to grant the same Role in 4E and 2E to the same Party/User. If a Role 4E is granted to a A2A User, it will be used as a 2E role by the system when A2A messages are sent.

[1] Matching regardless of the uppercase/lowercase characters

2.3 Message Routing

2.3.1 Default Routing

Screen: Routing – New/Edit
Messages: 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. If no Default Routing is defined the Party will be treated as U2A-only: no messages will be generated.

2.3.2 DN-BIC Routing (RTGS only)

Screens: Distinguished Name-BIC Routing – New/Edit
Messages: n/a

The DN-BIC Routing links a Cash Account BIC (defined as Authorised Account User) to a DN in order to receive payment orders, payment revocation and recall orders or payment recall responses. The DN-BIC Routing therefore links a DN to the message business recipient stated in the "To" field of the message's Business Application Header (BAH).

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

- By the central bank as PTA for the Party holding the Cash Account linked to the relevant AAU, and
- as Certificate DN (see section 2.1.2 a) or c)).

In other words, CRDM validates DN-BIC Routing data against Certificate DNs and Party Technical Addresses. On the 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 the 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"[2].

> The DN in a DN-BIC Routing instance refers to a Certificate DN, which the user can select when inserting the DN-BIC routing; therefore the DN will appear as the Certificate DN was inserted:
>
> *CN=user01,OU=example,OU=12345,O=t2,O=nsp* if the Certificate DN was inserted per 2.1.2 a)

[2] 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.

cn=user01,ou=example,ou=12345,o=t2,o=nsp if the Certificate DN was inserted per 2.1.2 c)

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 in the DN-BIC Routing and as A2A User DNs to sign messages; all such 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=nsp as DN-BIC routing.

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

- Party Technical Address (PTA), captured by the CB: cn=test,o=abcxxx,o=nsp
- Certificate DN of the A2A user – CN=test,O=abcxxx,O=nsp – see section 2.1.2.a)
- DN-BIC Routing - CN=test,O=abcxxx,O=nsp – 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 when the Certificate is an A2A users certificate. 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 uses a different DN as technical sender/receiver (cn=test,o=abcxxx,o=nsp) and another one for signing the BAH (CN=test,O=abcdef,O=nsp), the DNs should be captured in CRDM as:

- Party Technical Address (PTA) – captured by the CB: cn=test,o=abcxxx,o=nsp
- Certificate DN of the A2A user CN=test,O=abcdef,O=nsp – see section 2.1.2.a)
- Certificate DN of the technical sender/receiver - cn=test,o=abcxxx,o=nsp – see section 2.1.2.c)

DN-BIC routing – the DN to be used for the DN-BIC Routing should be the Certificate DN used as Technical Sender/receiver: cn=test,o=abcxxx,o=nsp

2.4 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 on each Cash Account.

    - For a multi-addressee, the technical sender DN (the PTA) must be linked to the system user in the BAH of the payment message (through a user certificate DN link)
- Additional AAU/DN-BIC Routing configuration for Addressable BICs on each Cash Account