EUROPEAN CENTRAL BANK
EUROSYSTEM

Explainer on CRDM terms and concepts for T2

Version	Publication date	Comment
1	14/04/2022	Initial Publication

Author ECB

Date 2022-04-14

Contents

1. Introduction 2
2. Users and privileges 2
3. Distinguished Names 2
4. Notifications and reports 3
5. Technical addresses 3
5.1. Definition 3
5.2. Configuration 4
6. Inbound Communication (to T2) 4
7. Routing of outbound communication (from T2) 4
7.1. Determination of the channel 4
7.2. Determination of DN 5

1. Introduction

This explainer gives an overview of how some key CRDM concepts interact with each other for RTGS and CLM purposes. Details may be found in the UDFS and UHB.

The scope of the explainer is T2; the statements below may not fully apply to T2S and TIPS.

2. Users and privileges

A person or an application interacting with T2 is identified by a **distinguished name (DN)**.

A DN can be linked to one or several **system users** through **user certificate distinguished name links**. The same DN should not be linked to two system users of the same party.

Each system user is attached to one **party** (central Bank, payment bank, ancillary system).

Each system user is granted one or more **roles**. A role is defined by grouping a set of **privileges.** A privilege authorises a user to perform different actions, to access different kinds of information or to make different requests

A system user can query/update data based on their **data scope**, which is determined by the party the user belongs to, plus any MCAs co-managed by the user´s party.

3. Distinguished Names

A DN is a sequence of attribute-value assertions separated by commas, e.g. <cn=meier,ou=RTGS,o=nkacct,o=nsp-nspname>. CRDM needs a precise syntax for the DNs, but it does not directly use the values themselves. The values are used by the NSPs.

Distinguished names are mainly used:

- To identify a U2A or A2A user as described in 2
- As a technical address as described in 5.1.1

4. Notifications and reports

Some notifications (e.g. error messages) are always received by the recipient and cannot be deactivated.

For other message types, an actor can configure which messages it will receive in A2A from T2 or a common component according to pre-defined rules. The **Message subscription** functionality allows to configure this.

It is also possible for an actor to request the daily reception of some reports generated by RTGS/CLM (statement of accounts) and CRDM (RTGS Directory). A **Report configuration** allows to specify the type of report to be received and whether a full report or only the information delta from the previous report should be received (applicable to the RTGS Directory only). It also allows to configure if the report should be received in in push mode via A2A or if the report should be generated and stored for later query in pull mode (applicable for statement of account).

5. Technical addresses

5.1. Definition

At the technical layer, each inbound or outbound communication with T2 or a common component involves:

- A Distinguished Name
- A Network Service Provider (NSP)
- A channel (message-based or file-based channel; real-time or store-and-forward)

5.1.1. Distinguished Name

In this context, a distinguished name is called “technical address” in the ESMIG and CRDM documentation, whereas the RTGS and CLM documentation refers to the triplet (Distinguished Name, NSP, Channel) as a technical address.

5.1.2. NSP

SIA-COLT or SWIFT.

5.1.3. Channel

The message-based channel can be used for any communication with size < 32 kB.

The file-based channel must be used for any communication > 32 kB.

No communication can exceed 32 MB. If a camt.006 or camt.053 exceeds this size, it is paginated.

The real-time channel must be used for queries and is used by RTGS/CLM for the related query responses[1].

The store-and-forward channel must be used for instructions and is used by RTGS/CLM for the related instruction responses as well as for push notifications and reports.

The allowed combinations of file/message-based vs real-time/store-and-forward are detailed in the UDFS (Table 2 in the RTGS and CLM UDFS).

5.2. Configuration

Channels and NSPs are combined in **Network Services**.

Network services and DNs/Technical Addresses are combined through **Technical Address Network Services Links**. This implements the triplet mentioned above.

Each party can have one or several **Party Technical Addresses** (in the sense of Distinguished Names).

6. Inbound Communication (to T2)

Each inbound communication to T2 comes from:

- A source DN, provided to TARGET Services by the NSP (and originally given by the participant): the **technical sender**
- An NSP
- A channel

T2 will check that the DN is declared in CRDM as a technical address of that party, and whether it is linked to a Network service corresponding to the NSP and Channel.

The message/file contains a system user reference, which belongs to a party.

The system further checks that the system user has the right privilege and data scope to perform the action/query described in the message, and that it is linked to the certificate DN derived from the signature sent with the message.

The **business sender** of a message is the BIC in the From element of the Business Application Header.

7. Routing of outbound communication (from T2)

T2 will derive a DN (technical address), an NSP and a channel from the nature of the communication (query response, notification, report, etc.), the size of the communication, and the party configuration.

7.1. Determination of the channel

Through the size and nature of communication:

- Message-based channel for communications < 32 kB
  - but only if message-based channel exists for the party
- File-based channel for communication between 32 kB and 32 MB
  - Or if only file-based channel exists even for messages < 32 kB

[1] In some scenarios, T2 sends an interim answer/acknowledgement in real-time and later the actual answer via store-and-forward. See UDFS for details.

- Store-and-forward versus real-time per table 2 of the RTGS and CLM UDFS.

7.2. Determination of DN

7.2.1. **Query and instruction response**

A query or instruction response will be sent back to the DN and network service which sent the query[2] or instruction respectively.

7.2.2. Push notifications and reports

Each Actor must configure a **Default routing** stating the DN and Network Service to communications from the relevant TARGET Service/component will be routed to.

An Actor can also configure exceptions to the Default routing for some types of messages. A **Conditional routing** must be configured in this case, indicating the Party Technical Address and network service where the communications should be routed to, the Service/component it applies to, and the type of message subject to this routing exception. It should be noted that only a subset of the messages submitted by each Service/component are subject to Conditional routing (the list of supported messages is specified in CRDM UDFS).

7.2.3. Messages forwarded by RTGS

The **DN-BIC routing** derives – from a BIC (in the TO element of a Business Application Header) – the Distinguished Name (technical address) to which RTGS should forward a message. Such forwarding applies to pacs.- and a subset of camt.-messages. A network service is then derived from this DN, which must be configured as PTA of the linked party.

A DN-BIC Routing needs to be configured for each BIC listed in the RTGS directory with participation type direct or multi-addressee. Each such BIC may only be linked to one DN through the DN-BIC routing.

[2] In case of timeout and/or oversize additional messages are sent using the store-and-forward message-based network channel or store-and-forward file-based network channel for the same technical receiver and the same network provider.