EUROPEAN CENTRAL BANK
EUROSYSTEM

10 September 2020

T2-T2S Consolidation Project

Explainer on authentication of queries and instructions in T2

1 Introduction

This document describes how T2 components (specific components like CLM and RTGS or common components like BILL and CRDM) verify that an A2A message/file sender is entitled to perform the instruction/query described by the message, i.e. how T2 components prevent the processing of a message/file built and sent by an actor not allowed to perform the action.

Note: This verification is not done on the basis of the "DN-BIC Routing". The DN-BIC routing has a fully different purpose, namely to derive from a BIC in the TO of a Business Application Header ("BAH") the Distinguished Name ("DN") to which RTGS should forward a message (which applies to only a subset of messages).

2 NSP Checks

The Network Service Provider ("NSP") receives a message or a file from an actor, directed to a TARGET service component. As this communication takes places between the actor and the NSP, it does not directly involve TARGET services components and is not described in the TARGET documentation. For the purpose of understanding the overall framework, in the message scenario, we only need to know that the NSP receives from the actor:

- A Technical Sender DN
- A business message made up of a BAH (head.001) and a payload (pacs.009, camt.050, etc.)
    - The BAH contains a signature which was built using the private key of the unique certificate[1] linked to the Business Sender[2] DN.
    - The BAH contains a system user in element /Document/AppHdr/Fr/FIId/FinInstnId/ClrSysMmbId/MmbId, which will be used in subsequent T2 checks.
- A destination component related to a TARGET Service (for example RTGS/T2, CRDM/T2, BILL/T2S, etc.)

[1] Each identity bound to a digital certificate is assigned a unique distinguished name (certificate DN).

[2] The Business Sender DN and the Technical Sender DN may be the same (i.e. they may have the same value).

The NSP identifies the sender and checks whether the Technical Sender DN is in the Closed Group of Users of the destination TARGET service. The NSP then conveys all three items (Technical Sender DN, business message, destination component related to a TARGET Service) to ESMIG through the DEP protocol, i.e. the message will be wrapped in a DEP technical header containing the destination component related to a TARGET Service and the Technical Sender DN, and be signed by the NSP.

The entity which has signed the message (the business sender) may be different from the entity which has technically submitted the message to ESMIG (the technical sender).

3 ESMIG Checks

Upon reception in ESMIG the following signature checks (in addition to the Data Exchange Protocol ("DEP") checks, i.e. unique IDs, correct channel and queue used, etc.) are executed:

1 – Signature verification at DEP level to check the message is signed by the trusted NSPs (the signature verification returns a DN. The DEP protocol checks that this DN was assigned to the NSP. That NSP DN is different from the business sender and technical sender DNs mentioned above). ESMIG does not directly validate the Technical Sender DN ; instead, it validates the NSP signature and relies on the NSP validation of the technical sender DN described in 2..

2 – Signature verification at BAH/BFH (Business File Header) level: returns the DN used to sign the BAH/BFH (i.e. the DN of the business sender). This is compared with the DNs linked to the user stored in the BAH (such link is stored in the CRDM entity "User Certificate DN Link", which links a system user configured under a party to a DN). If there is no match, the verification is not successful and the message is rejected.

The following parameters are then passed to the TARGET Service Component Business Interface, along with BAH/BFH and the business payload:

- Technical Sender DN (used by the service to build the answer messages in some cases)
- Business sender DN (the DN used to sign the message)
- Network channel (MSG/FILE SnF or MSG RT) and NSP used (SIA-Colt, SWIFT)
- Unique ID assigned by ESMIG
- Entry Timestamp

Those parameters are used in some validations detailed below: as an example, the DN must be linked to the system user in the BAH (by means of the “User-Certificate DN link” CRDM entity).

Note: This link between a system user (as defined in 1.3.4.1 of the CRDM UDFS) and a DN is part of the reference data and is maintained by each responsible party in CRDM; this is a many-to-many link since (i) a system user modelled in a CRDM party can be linked to multiple DNs, each provided by an NSP and (ii) a DN may be linked to multiple system users under different parties.

4 TARGET Service Checks

The TARGET service component business interface will derive from the system user stored in the BAH/BFH:

- The party/parties and accounts in the data scope of the user
- The privileges of the user

It will check whether the query/instruction described in the payload is allowed by the privileges and data scope of the user.

RTGS/CLM will also check cross-dependencies between:

- technical sender DN ;
- user (system user reference in BAH, element /Document/AppHdr/Fr/FIId/FinInstnId/ClrSysMmbId/MmbId);
- business sender DN;
- business sender BIC(From BIC in BAH).

For more details see validation rules VR00080, VR00090, VR00091, VR00100, VR00110 and VR00960 (in the project documentation, and in the example at the end of this document).

Note: The process above does not read the contents of the DN (the list of attribute/values). It only uses the DN as a unique string pointing to a certificate and linked to a user. To the process above, and more generally to CRDM and T2, the DN is “just an identifier”. The contents of the DN are used by the NSP for routing purposes. If an NSP requires BICs in the contents of the DN, these BICs can be different from the BICs set up in CRDM as party BICs, authorized account user, etc. In other words, a BIC in a DN is independent from the CRDM and T2 configuration.

5 Outbound Messages

In the same way the DNs (Technical Sender DN and Business Sender DN) are passed from the NSP through ESMIG to the TARGET service component business interface for inbound messages/files as described above, the TARGET service component business interface will pass to ESMIG the technical receiver DN for its outbound communications to the NSP (and use the platform Business Sender DN to sign the outbound message).

- For the TARGET service component and ESMIG, this is again just an identifier which it does not use. It is only used downstream by the NSP itself.
- This technical receiver DN is derived by the service/component. In cases (a), (b) and (d) below, only one technical receiver DN is derived.

  (a) For response messages (on queries or instructions), the technical receiver DN is the Technical sender DN of the inbound message.

  (b) For push notifications, the technical receiver DN is a DN set up as “party technical address” with the related routing configuration.

  (c) For reports, the technical receiver DN is a DN set up as part of the routing configuration for the Party’s report configuration. This configuration may result in the report being sent to multiple DNs, as parties can use both a default routing and a conditional routing.

  (d) For forwarded messages, the technical receiver DN is derived from the “DN BIC Routing”.
- The technical receiver DNs sent with outbound messages are taken from the same list as the DNs used in inbound messages in the authentication process described above. A DN could be used

  - only for outbound messages: if configured as a party technical address/report routing but not used by the party for inbound messages; or
  - for both inbound and outbound: for example DNs which are used to submit queries.

A DN used for inbound messages may always be used in the related response/error message, so there are no DNs which are used “only for inbound”.

6 Example

Bank A uses an external service provider B to connect to T2 via NSP C.

Bank A is defined as Party A in CRDM, and has defined TechnicalUserCashManager as a system user.

Bank A has an internal cash management application called CashManager.

The following certificates are granted, each containing a public and a private encryption key.

- CashManager is granted certificate ABC, uniquely linked to DN XYZ
- Service Provider B is granted certificate DEF, uniquely linked to DN UVW
- NSP C is granted certificate GHI, uniquely linked to DN RST

In CRDM, TechnicalUserCashManager is linked to DN XYZ.

1. Bank A steps

Bank A wants to query an RTGS transaction through a camt.005 message

Bank A builds a head.001 BAH. The BAH includes TechnicalUserCashManager in element

/Document/AppHdr/Fr/FIId/FinInstnId/ClrSysMmbId/MmbId.

Bank A computes the signature of the message (head.001 and camt.005) using the private key of the certificate ABC. It stores the signature in the head.001.

2. Service Provider Steps

Service provider B wraps the message in a technical header and sends it to the NSP, with destination T2 RTGS, including its DN UVW in the communication.

There are other encryption/communication details between the service provider and the NSP, which are out of scope of this document.

3. NSP Steps

NSP C checks that DN UVW is in the closed user group of T2.

There are other encryption/communication details between the service provider and the NSP, which are out of scope of this document.

NSP C transmits the message to the ESMIG instance serving the T2 service, having signed it with its certificate GHI.

4. TARGET Steps

ESMIG verifies the signature of NSP C: the signature check at transport level on the message returns DN RST; ESMIG checks that DN RST is one of the accredited NSP (i.e. NSP C).

ESMIG verifies the signature at business level of the payload. The signature check returns DN XYZ.

After successful signature check, ESMIG transmits the message to T2 RTGS.

T2 RTGS checks that TechnicalUserCashManager has the roles/privileges to perform a camt.005 query.

T2 RTGS verifies that DN XYZ is linked to user TechnicalUserCashManager stored in the BAH, and that TechnicalUserCashManager is under Party A.

T2 RTGS checks that the query is consistent with the data scope of TechnicalUserCashManager.

In practice those checks are implemented through the following T2 business rules:

- VR00080: The technical sender DN must be authorised to send messages for the party of the business sender: is DN UVW authorized to send messages for Party A? (Is UVW registered as a Party technical address for Party A?)
- VR00090: The business sending user (system user reference) must be authorised to send messages for the party of the business sender: is TechnicalUserCashManager authorized for Party A?
- VR00091: The certificate DN (business signature) must be linked to the business sending user of the message/file: is certificate XYZ linked to TechnicalUserCashManager?
- VR00100: validation of the BIC in the FROM of the BAH vs the content of the payload. In the case of a camt.005, the FROM BIC should be the BIC of Party A.
- VR00110: The business sending user (system user reference) must have the privilege to perform this business function: does TechnicalUserCashManager have the rights to query transactions?

7 Annex

This is a non-exhaustive illustration of the example described in chapter 6: