EUROPEAN CENTRAL BANK
EUROSYSTEM

7 July 2021

ECMS Project

Explainer on authentication and authorisation of instructions in the ECMS

1 Introduction

This document describes how ESMIG and the ECMS verify that an A2A message sender is entitled to perform the instruction described by the message, i.e. how ESMIG and the ECMS prevent the processing of a message/file built and sent by an actor not allowed to perform the action. It is based on the T2 document ‘’Explainer on Distinguised Name and Authentication”, which has been updated for ECMS stakeholders.

2 NSP Checks for inbound messages

The Network Service Provider (“NSP”) receives a message from an actor, directed to a TARGET service component, in this case the ECMS. As this communication takes place between the actor and the NSP, it does not directly involve TARGET services components and is not described in the TARGET or ECMS 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 Distinguished Name (“DN”)
- A business message made up of a Business Application Header (“BAH”; head.001) and a payload (pacs.009, sese.023, 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 an ECMS system user in element /Document/AppHdr/Fr/FIId/FinInstnId/ClrSysMmbId/MmbId, which will be used in subsequent ECMS checks.
- A destination component related to a TARGET Service (for example RTGS/T2, CLM/T2, ECMS, etc.)

The NSP identifies the sender and checks whether the Technical Sender DN is in the Closed Group of Users of the destination TARGET service (ECMS). The NSP then conveys all three items (Technical Sender DN, business message, destination component related to a TARGET Service) to ESMIG through the Data Exchange

[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) or they can be different, depending on the instructing scenario.

Protocol (“DEP”), 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 for inbound messages

Upon reception in ESMIG the following signature checks (in addition to the 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 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 level: ESMIG verifies that the inbound message is signed correctly, extracts the DN and passes it to the ECMS.

More specifically, the following parameters are passed to the ECMS, along with the BAH 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) and NSP used (SIA-Colt, SWIFT)
- Unique ID assigned by ESMIG
- Entry Timestamp

These parameters are used in the ECMS validations detailed below: for example, the DN must be linked to the system user in the BAH.

4 ECMS Checks for inbound messages

The ECMS business interface derives the following information from the system user stored in the BAH:

- The party/parties in the data scope of the user

- The roles of the user

It checks whether the instruction described in the payload is allowed by the roles and data scope of the user.

The ECMS also checks cross-dependencies between:

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

For more details see “Business rules in the ECMS” (AARR001, AARR002, INTF002, INTF007, and the example in Section 6.4 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, 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 the ECMS. In other words, a BIC in a DN is independent from the ECMS configuration.

5 Outbound Messages

The ECMS business interface, in the same way as described above, passes the technical receiver DN to ESMIG for its outbound communications to the NSP (and use the ECMS Business Sender DN to sign the outbound message).

- For the ECMS and ESMIG, the technical receiver DN is again just an identifier which is not used by the ECMS or ESMIG, but is only sent to be used downstream by the NSP itself.
- This technical receiver DN is derived by the ECMS.
  - (a) For ReceiptAcknowledgement (admi.007) messages the technical receiver DN is the Technical sender DN of the inbound message.
  - (b) For notifications and reports the technical receiver DN is a DN set up as “party technical address” in the message/report message subscription configuration.
- A DN could be used
  - only for outbound messages: if configured as a party technical address in the message/report message subscription configuration but not used by the party for inbound messages; or

- for both inbound and outbound messages.

A DN used for inbound messages must always be used in the related admi.007 message, so there are no DNs which are used “only for inbound”.

6 Example

Counterparty A uses an external Service Provider[3] B to connect to the ECMS via NSP C.

Counterparty A is defined as Party A in the ECMS and has defined A2AUserCollateralManager as a user in Party A.

Counterparty A has an internal collateral management application called CollateralManager.

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

- CollateralManager 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 the ECMS, A2AUserCollateralManager is linked to DN XYZ.

1. Counterparty A steps

Counterparty A wants to mobilise collateral through a sese.023 message.

Counterparty A builds a head.001 BAH. The BAH includes A2AUserCollateralManager in element /Document/AppHdr/Fr/FIId/FinInstnId/ClrSysMmbId/MmbId.

Counterparty A computes the signature of the message (head.001 and sese.023) using the private key of certificate ABC. It stores the signature in the head.001.

[3] The use of an external service provider to connect to the ECMS is optional.

2. Service Provider steps

Service provider B wraps the message in a technical header and sends it to the NSP, with destination ECMS, 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 the ECMS.

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

NSP C computes the signature of the message with its certificate GHI and transmits the signed message to the ESMIG instance serving the ECMS.

4. ESMIG and ECMS 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 and extracts DN XYZ.

After a successful signature check, ESMIG transmits the message to the ECMS.

The ECMS checks that A2AUserCollateralManager has the role to send a sese.023 message.

The ECMS checks that the instruction is consistent with the data scope of A2AUserCollateralManager.The ECMS verifies that DN XYZ is linked to user A2AUserCollateral Manager stored in the BAH, and that A2AUserCollateralManager is under Party A.

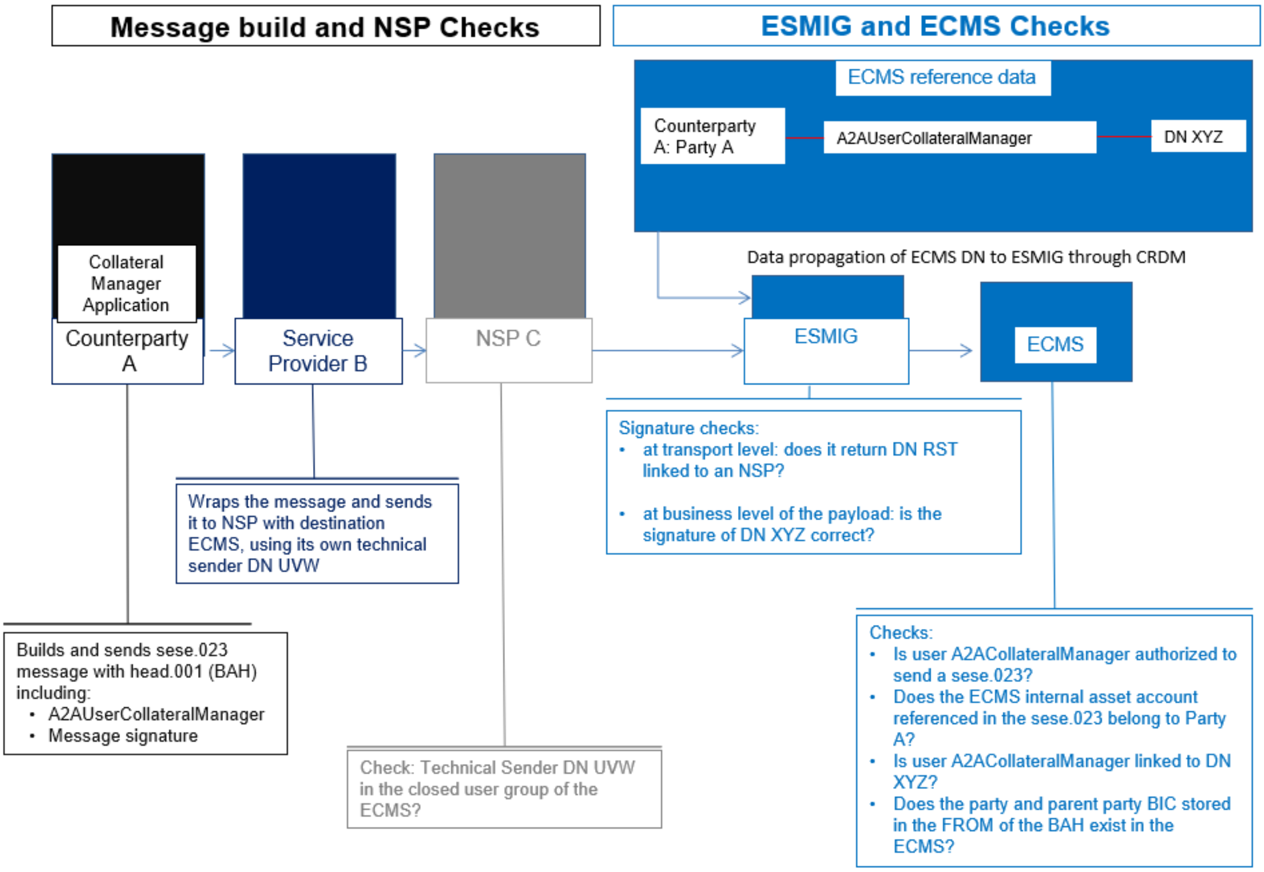
In practice those checks are implemented through the following business rules:

- AARR001: The user must be authorized to send the message type. Is user A2ACollateralManager authorized to send a sese.023?
- AARR002: The relevant data (e.g. Internal Asset account, pool reference) must belong to the party data scope. Does the ECMS internal asset account referenced in the sese.023 belong to Party A?
- INTF002: The specified system user must be authorized for the specified business sender distinguished name. Is user A2ACollateralManager linked to DN XYZ?

- INTF007: The party BIC and the parent party BIC specified in the business application header must exist in the ECMS reference data. Do the party and parent party BIC stored in the FROM of the BAH exist in the ECMS?

7 Annex

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



Signature checks:
- at transport level: does it return DN RST linked to an NSP?
- at business level of the payload: is the signature of DN XYZ correct?

Wraps the message and sends it to NSP with destination ECMS, using its own technical sender DN UVW

Builds and sends sese.023 message with head.001 (BAH) including:
- A2AUserCollateralManager
- Message signature

Check: Technical Sender DN UVW in the closed user group of the ECMS?

Checks:
- Is user A2ACollateralManager authorized to send a sese.023?
- Does the ECMS internal asset account referenced in the sese.023 belong to Party A?
- Is user A2ACollateralManager linked to DN XYZ?
- Does the party and parent party BIC stored in the FROM of the BAH exist in the ECMS?