EUROPEAN CENTRAL BANK

EUROSYSTEM

Eurosystem Collateral Management System

Information pack

ECMS access and connectivity

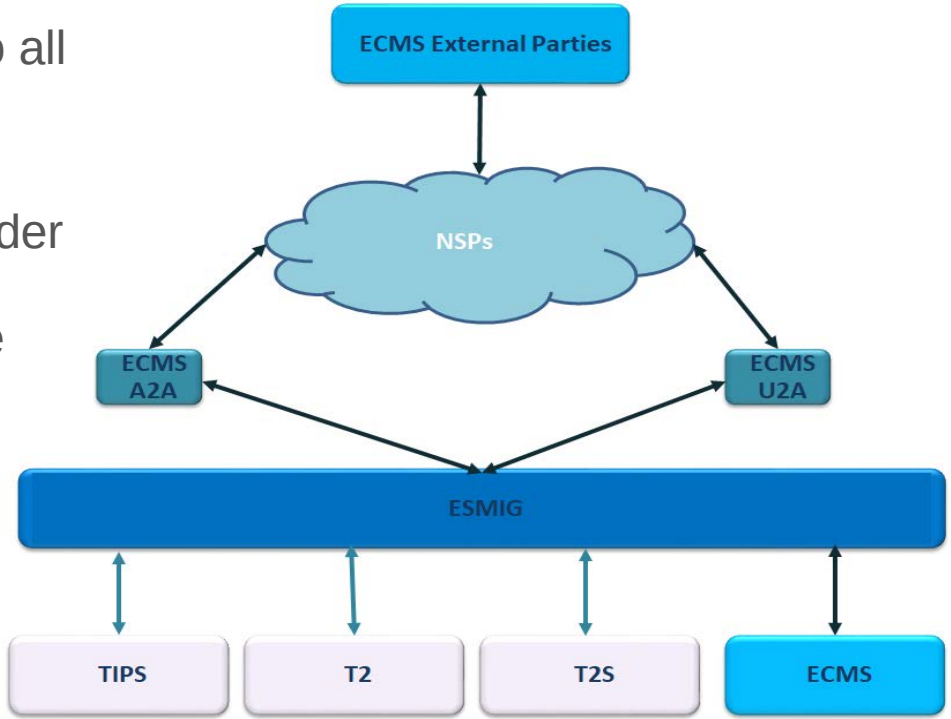
January 2020

target services | ECMS

Eurosystem Single Market Infrastructure Gateway

ESMIG provides a **single entry point** to all TARGET services, including the ECMS

- free choice of Network Service Provider
- single sign on and a single certificate
- **A2A** communication via ISO 20022 messages
- **U2A** connection **via a GUI**



Modes of connectivity – A2A and U2A

A2A mode

Communication with the ECMS via ISO 20022 messages, files which are compliant with the ISO 20022 format or XML messages. A file may contain several messages.

All ECMS actors interacting in A2A are expected to be ISO20022 compliant.

All communication between CSDs, TPAs and the ECMS is in A2A mode.

U2A mode

Online screen-based activities performed by ECMS actors via a GUI – graphical user interface. Counterparties can fully manage their pool in U2A mode only, and do not need an A2A connection.

Network service providers (NSP)

- SWIFT and SIA Colt, as licensed NSPs, will provide client specific solutions for the connection between ECMS external actors' interface and ESMIG.
- They will provide an easy access solution in U2A mode, designed especially for participants with only a low volume of transactions.
- Individual users can log on to all TARGET Services with a single sign-on and a single certificate.
- If an ECMS actor uses more than one connectivity provider to connect to the ECMS, then a separate certificate needs to be assigned to each user and application for each connectivity provider.

Connectivity Guide – description of functionality

NSP functionalities

- Technical sender authentication
- Closed group of users (CGU)
- ……

Information on U2A mode

- https protocol
- NSP provides CGU and public key infrastructure (PKI) services

Information on A2A mode

- Transfer mode in which messages and files can be exchanged
- Message/file compression and message size
- Message/file signature

Technical envelope
digital signature with certificates issued by NSP PKI

Business layer signature authenticates the business sender and guarantee the integrity of the business message/content.

Stored in the business application header (BAH) for individual messages. Stored in the file header (BFH) for files.

Connectivity Guide – how to register

Checklist

Providing a summary of steps

- from how to connect to the ECMS
- via the selection of the NSP
- to the setting up of parties and users

Registration process is defined by NSP

The NSP specifies the connectivity services and communication channels. The ECMS Connectivity Guide provides information on the following topics:

- Closed group of users
- Approval cycle of the registration request
- Request for digital certificates

Authentication and authorisation (1)

Each ECMS user needs a **unique login name** and a **certificate** to access the ECMS.

which includes the Distinguished Name (DN) defined by the NSP

assigned by the NSP to ECMS users (persons or applications)

The **technical sender** is the ECMS actor submitting the request to the ECMS.

- Each technical sender is identified by means of a certificate issued by the connectivity provider. The NSP authenticates the technical sender on the basis of its certificate.
- The certificate DN of the technical sender represents the technical address used by the technical sender to connect to the ECMS.

The **business sender** is the ECMS actor responsible for the business content of a message. The two roles can be performed by different entities.

Authentication and authorisation (2)

- Once ESMIG has authenticated the user and checked that the user is authorised to address the ECMS, the ECMS checks the rights of the user to carry out a specific function in the ECMS.
- Authorisation is granted based on the user's privileges (embedded in pre-defined roles) which are stored in the ECMS reference data.

Instructing scenarios

- The ECMS manages three instructing scenarios:

Direct submission of messages	Indirect submission of messages: case 1	Indirect submission of messages: case 2

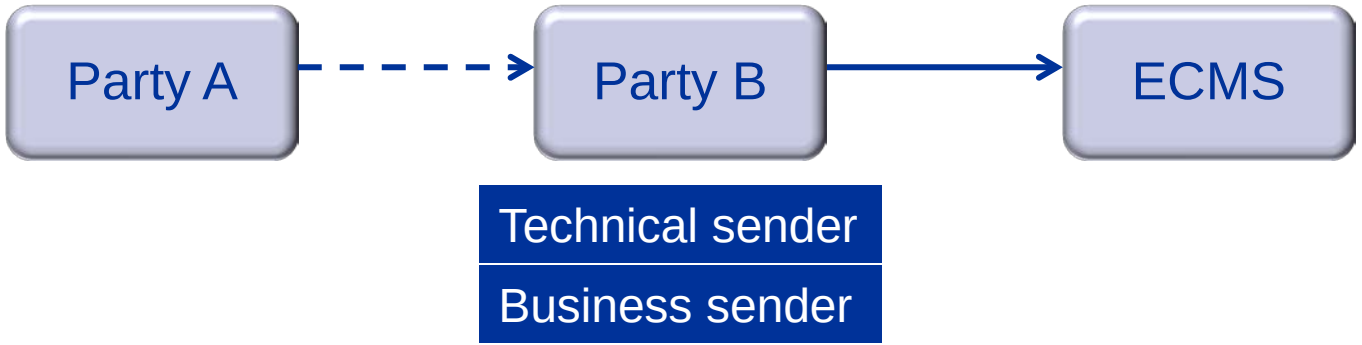
- Information on the instructing party and the business sender can be found in the business application header, which is combined with an ISO 20022 message to form a business message.

Instructing scenario – direct submission

- The ECMS party sends and signs its own instructions, and receives notifications regarding the status of the instructions.
- This means that this party acts both as technical and business sender.

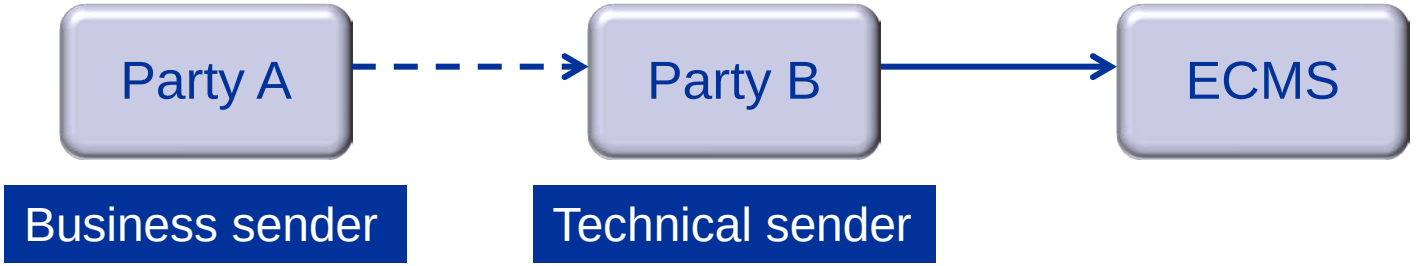
Instructing scenario – indirect submission case 1

- ECMS party A fully relies on another entity, ECMS party B for signing and sending the instructions party A wants to submit to the ECMS for processing.
- ECMS party B therefore acts both as technical and business sender on behalf of ECMS party A.



Instructing scenario – indirect submission case 2

- ECMS party A wishes to maintain responsibility for signing the instructions it wants to submit to the ECMS for processing. ECMS party A is therefore the business sender.
- However, ECMS party A relies on ECMS party B to actually send the instructions to the ECMS. ECMS party B is the technical sender.



Access rights and privileges in the ECMS

- Each user is assigned one or more **pre-defined roles** encompassing a set of **pre-defined privileges** by the party administrator in each entity.
- Privileges specify the ECMS functionalities that a user is allowed to perform.
- While an ECMS actor may allow its users to access the ECMS in either U2A or A2A mode, each individual user must choose which mode to use. In U2A mode, the ECMS may be configured to require four-eye verification.
- Users have access to the data objects of the party they belong to. An NCB can extend the data scope of one ECMS actor (for specific activities) to allow it to operate on behalf of a different ECMS actor.

Configuration of access rights