T2S-0701-SYS

Annex: General Functional Specifications (GFS)

Draft sections provided for CR-701 – ESMIG impact on T2S

1.1 ESMIG

1.1.1 Introduction

The Eurosystem Single Market Infrastructure Gateway (ESMIG) is a common component whose introduction aims at serving various TARGET Services. The component is composed by two different sub-components, which focus respectively on (i) Application-to-Application flows and (ii) User-to-Application interaction by means of a dedicated portal.

In T2S respect, the component performs validation checks on inbound communications before routing them to the relevant business interface. Similarly, ESMIG takes care of the routing of outbound communications towards the Network Service Provider (NSP).

The ESMIG component shall:

- Authenticate the message sender;
- Check that the sender belongs to the Closed Group of Users (CGU) entitled to send messages to the relevant TARGET Services, common components and applications;
- Execute the technical validation of the received messages (well-formedness of the XML) at transport level;
- Perform the schema validation, in case the backend component requires it (compliance of the incoming A2A message with the referenced XML schema definition - e.g. it checks that the message contains all the mandatory fields, that the value of each field is consistent with the data type of the field, etc.);
- Provide digital signature services;
- Forward the message to TARGET Services, common components and applications along with the technical sender's Distinguished Name (DN);
- For what concerns A2A traffic, data for Archiving will be provided by ESMIG whereas, for U2A traffic, each web application is in charge of feeding the Archiving module with the required information.

For some of these validations, ESMIG shall make use of services offered by the NSPs according to the connectivity dossier requirements.

1.1.2 Flat-file management

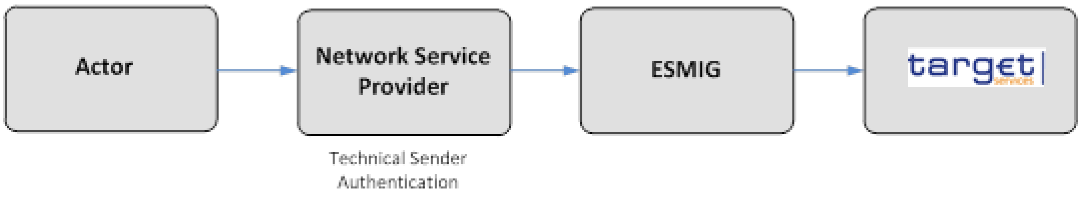
T2S benefits from the usage of different communication via flat-file for several purposes, e.g. for Penalty Mechanism reports, Penalty Data loading, Securities Valuations and Reporting for Dynamic Data.

For these communications, either in inbound or outbound direction, a deviation is implemented compared to the standard flow in which each business interface intermediates its backend function. For flat-file processing a direct queue is implemented between the ESMIG and each responsible back-end for the purpose of receiving/sending flat-files.

1.1.3 A2A authentication/authorisation

The authentication of the technical sender is performed at network infrastructure level and is based on the certificate used by the Actor to establish the technical connection with the network infrastructure itself. This authentication process is under the responsibility of the NSP selected by the Actor to connect to the TARGET Services, common components and applications.

Figure X – Technical sender authentication



In case of successful authentication of the technical sender, the TARGET Services, common components or applications get the certificate DN of the technical sender. The TARGET Services, specific/common components or applications may use this certificate DN later on, during the authorisation process.

The authorisation process refers to the authorisation of the technical sender for which ESMIG checks whether the technical sender is allowed to access the service / component, making use of the Closed Group of Users feature provided at NSP level.

1.1.4 Portal and U2A authentication/authorisation

Users of TARGET Services and applications belonging to the appropriate closed group of users, defined and enforced at NSP level, can communicate in U2A mode via a web-based GUI.

Those users are directed to an initial page, namely the *ESMIG Portal*, that ensures proper routing to the web applications according to the user access rights profiles.

In particular, the ESMIG Portal shows to the user all the applications the user is authorised to access. These applications are linked one-to-one to special system privileges (stored in CRDM) the user has been previously granted with and that are specifically dedicated to those web applications.

When accessing the ESMIG Portal without any authentication, the user is redirected to the IAM page that asks user to authenticate the access validating the user’s distinguished name (DN). Thus, the authentication process, at IAM level, securely associates the DN to the person accessing the system

1.1.5 A2A Real-Time: Timeout/oversize management

ESMIG is in charge for handling the timeout and oversize management.

In the scenarios where the timeout condition is reached for inbound communication, ESMIG shall respond with inform the sender the relevant query reached the timeout limit and the communication will switch to file store-and-forward.

For communications that trigger a reply from T2S which cannot fit within the expected size limitation of a realtime network service, ESMIG shall inform the sender that the communication will switch to file store-and-forward.

1.1.6 Digital signature verification

The purpose of the signature verification for A2A mode is to authenticate the business sender and guarantee the integrity of the business payload delivered to T2S. ESMIG will take care of executing (i) the technical validation of the inbound communications at transport protocol level, (ii) check the signature at transport protocol level and (iii) verify the digital signature at business level, prior to the delivery of the relevant payload to the interested business interfaces.

As for the U2A mode, ESMIG provides APIs or signature verifications that will be invoked by each application for the appropriate check in the GUI screens.