Eurosystem Market Infrastructure Single Gateway for TIPS

User Detailed Functional Specifications

V0.1.0

Author	4CB
Version	0.1.0
Date	01/03/2018

Introduction

The description of the Eurosystem Single Market Infrastructure Gateway included in this document is related to the network connectivity services provided by ESMIG for TIPS. The ESMIG as a whole provides different and additional services based on the needs of the others market infrastructure services (TARGET2, T2S, TIPS, ECMS).

When possible, synergies between the ESMIG provided features across the different market infrastructure services have to be put in place. The ESMIG offers scalability to cope with the different Eurosystem Market Infrastructure Service throughputs and it ensures that the traffic of one backend service may not impact the processing time of messages from or to other services. The ESMIG provides the single access point for the external communication to TIPS. This means it is in charge of A2A and U2A traffic management providing authentication of all inbound traffic (U2A and A2A) as well as sender (i.e. external party sending communication) authentication and identification.

Due to high message volumes estimated for the TIPS service, a specific A2A protocol used to exchange messages with the Network Service Provider (NSP) is used. It is based on the MQ protocol as transport layer.

Messages managed by ESMIG for TIPS are not persistent; it means no guarantee of delivery is in place for messages received/sent by the NSP.

The ESMIG provides business continuity measures (e.g. multiple sites, path diversification, etc.) and PKI Services. Moreover the ESMIG provides operational/monitoring tools to ensure the monitoring of the system's functioning by the Operator Service Desk.

The ESMIG opening hours are aligned with the opening hours of the respective market infrastructure services, e.g. for TIPS it is 24/7/365.

From a TIPS perspective, the ESMIG is expected to perform basic checks on inbound messages and then route them to the TIPS application. Similarly, ESMIG takes care of the routing of outbound messages from TIPS application to the related NSP.

The ESMIG, in some cases making use of services offered by the NSPs, is expected to:

- authenticate the message sender;
- check that the sender belongs to the Closed Group of Users (CGU) entitled to send messages to TIPS;
- execute the technical validation of the received messages (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.);
- forward the message to TIPS along with the originator's Distinguished Name (DN).

1. General features of ESMIG

1.1. ESMIG Features Overview

The ESMIG infrastructure provides a set of features shared among all the market infrastructure services beyond representing a single point of contact with the external networks.

These features, detailed below, belong to two main areas and can be provided by both the NSPs and the market infrastructure services:

- security, for example authentication of the sender and authorisation against a Closed Group of Users.
- message management, for example message technical validation and forwarding.

1.1.1. Authentication of the message sender

The authentication of the message sender is performed by the NSP both at the entry point of the network (by providing to the TIPS Actors digital certificates needed to access the A2A and U2A messaging services) and at the interface with the TIPS service through the relevant services provided by the NSP.

The NSP identifies the TIPS Actor and the TIPS service every time they open a new session with the NSP's Network Gateway for A2A traffic. There is no end-to-end session. The NSP transfers the identity of the sender to the receiver, including this information in the network envelope provided to the receiver together with the message. Moreover, the NSP authenticates the TIPS Actor and the TIPS service as local message partner every time they open a new session with the NSP's Network Gateway for A2A traffic exchange.

1.1.2. Participation to the Closed Group of Users

Each NSP defines a CGU for each TIPS environment and checks the authorisation of the TIPS Actors to access the TIPS service based on enforced rules at NSP level, supporting segregation of traffic flows between participants. CGUs are defined for both A2A and U2A messaging services.

The subscription to a group of users, and any subsequent modification to such subscription, is arranged through an electronic workflow on the Internet.

1.1.3. Technical validation of the received messages

Technical validation of the received messages at transport level for the inbound channel is run to verify that the mandatory transport protocol information provided by NSP is present and no required field is missing.

In the TIPS context ESMIG carries out the schema validation of the received business message.

Additional information on the technical validation of the received messages is available in section 1.5.3 and on the schema validation in section 1.5.4.

1.1.4. Message forwarding

ESMIG is responsible to forward inbound/outbound communication to the right service/NSP. For the inbound path all the messages are passed to the TIPS application since a unique “Message Router” process is in charge to manage inbound messages. For the outbound path, ESMIG addresses the correct NSP interface among the available ones based on the information available in the Common Reference Data Management (CRDM) database. The reader can refer to the CRDM UDFS (see CRDM User Detailed Functional Specification) for any related additional information.

1.2. Access to ESMIG

1.2.1. Single access point for the external communication

The ESMIG represents the single access point for the external communication to all market infrastructure services. It offers scalability to cope with the different market infrastructure service throughputs and it ensures that the traffic of one backend service may not impact the processing time of messages from or to other services. The ESMIG is the access portal for U2A users to all underlying business applications.

After the logon to ESMIG a landing page is displayed offering all market infrastructure services according to the access rights of the user. It is designed following a concept allowing an easy adoption of further services to be accessed by the ESMIG.

The ESMIG provides Business Continuity measures (e.g. multiple sites, path diversification, persistent information, etc.).

1.2.2. Network agnostic communication

The ESMIG ensures a network agnostic communication with the users, where network agnostic means multiple network providers are allowed. All network providers have to comply with the same communication interface specification towards ESMIG, but they are free to use their own features internally in terms of network and messaging.

1.2.3. Connectivity

1.2.3.1. Introduction

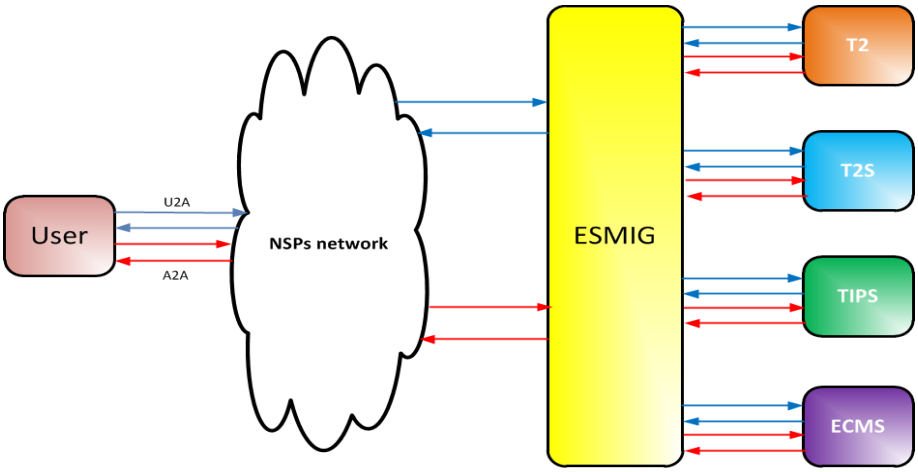
The purpose of this section is to introduce the basic connectivity to ESMIG. It does not aim to describe in details the technical connection with ESMIG.

1.2.3.2. Modes of connectivity

ESMIG supports the connectivity of ESMIG Actors as follows:

- Communication between software applications via XML messages or files (A2A mode);
- Online screen-based activities performed by ESMIG Actors (U2A mode).

Figure 1 - Modes of connectivity



All messages exchanged between ESMIG and ESMIG Actors are based on XML technology and comply with the ISO 20022 standards, when applicable. They can be sent to ESMIG as individual messages.

U2A and A2A communication patterns are managed separately at technical level. Different software stack components are used to handle them in the most effective way.

TIPS A2A, due to very specific needs in terms of message latency, uses dedicated gateways provided by the NSP to manage the inbound/outbound traffic and provide digital signature, authentication and CGU related services.

U2A is based on Web applications; ESMIG provides Identity and Access Management (IAM) and Reverse Proxy services. Based on the type of request received from the network, either the U2A or the A2A communication mode is invoked.

1.2.3.3. Technical connectivity and connectivity services providers

ESMIG does neither provide technical connectivity nor network services to ESMIG Actors. ESMIG Actors directly connected to ESMIG use a network provided by an accredited connectivity services provider. ESMIG only defines the technical and operational requirements for the connectivity services providers.

Detailed information as to the usage of network services is provided in the "TIPS Connectivity Guide" (see TIPS Connectivity Guide).

1.2.3.4 Common rules for message and file transfer services

This section describes the rules of the transfer services envisaged in ESMIG for messages and files that are relevant for TIPS. The configuration of the routing is described in details in the UDFS of the CRDM (see CRDM User Detailed Functional Specification).

In A2A mode, ESMIG Actors and ESMIG can exchange messages and files by means of two types of transfer services:

- The instant messaging, which requires that both parties, i.e. the sender and the receiver, are available at the same time to exchange the relevant data. In case of unavailability of the receiver, no retry mechanism is foreseen.
- The file-based store-and-forward transfer, which enables the sender to transmit files even when the receiver is not available. In case of temporary unavailability of the receiver, the NSP stores the files and delivers them as soon as the receiver becomes available again.

The following table shows how the main types of ESMIG business data exchanges are mapped against the two above mentioned transfer services for inbound and outbound communication.

Table 1 - ESMIG business data exchanges and network services features

TIPS BUSINESS DATA EXCHANGES	INBOUND COMMUNICATION	OUTBOUND COMMUNICATION
Settlement-related messages[1]	Instant messaging	Instant messaging
Reference data update (LRDM only[2])	Instant messaging	Instant messaging
Queries	Instant messaging	Instant messaging
Reports (push)	n/a	File-based, store-n-forward

This table shows that, as far as the inbound communication is concerned, ESMIG Actors can submit:

- all settlement related messages (i.e., in TIPS, Instant Payment transactions, Recall, and Investigation) and LRDM updates using a message-based network service. In both cases the transfer service is instant messaging;
- all queries using an instant messaging network service.

As to the outbound communication, the same table shows that ESMIG sends:

- all settlement related messages (i.e., in TIPS, Instant Payment transactions, Recall and Investigation) and LRDM updates using a message-based network service. In both cases the transfer service is instant messaging;
- all queries using an instant messaging network service;
- all reports in push mode using a file-based network service transferred via store and forward service.

[1] The settlement-related messages refer to Instant Payment transactions, recall processing and Liquidity Transfers.

[2] Local Reference Data Management (LRDM) is the local repository in TIPS which is fed by the data propagated from the CRDM on a daily basis. A subset of LRDM entities can be modified directly in TIPS on 24/7/365 basis, as specified in the TIPS URD (see TIPS User Detailed Functional Specifications). The usage of Instant messaging communication is limited to those entities.

1.2.4. Authentication and authorisation

[…]

1.2.4.1. Authentication and authorisation concepts

[…]

1.2.4.1.1 User

[…]

1.2.4.1.2 Certificate

[…]

1.2.4.1.3 Distinguished Name

[…]

1.2.4.1.4 Technical sender

[…]

1.2.4.1.5 Business sender

[…]

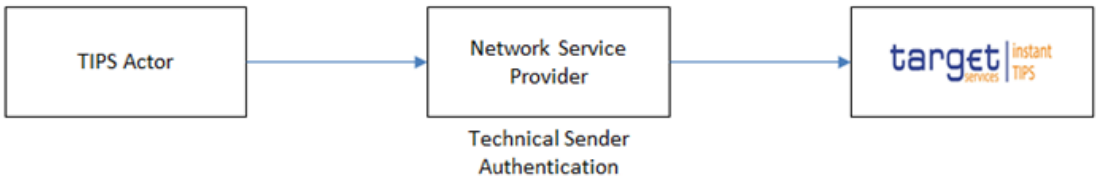
1.2.4.2. Authentication process

The authentication process refers in TIPS to the authentication of the technical sender.

1.2.4.2.1 Authentication of the technical sender

The authentication of the technical sender is performed at network infrastructure level and it is based on the certificate used by the TIPS Actor to establish the technical connection with the network infrastructure itself. This authentication process is under the responsibility of the technical connectivity provider selected by the TIPS Actor to connect to the TIPS service.

Figure 2 - Technical sender authentication



In case of successful authentication of the technical sender, the TIPS application gets the certificate DN of the technical sender. The TIPS application uses this certificate DN later on, during the authorisation process (see section 1.2.4.3.1 “Authorisation of the technical sender”).

1.2.4.3. Authorisation process

The authorisation process refers in TIPS to the authorisation of the technical sender.

1.2.4.3.1 Authorisation of the technical sender

The authorisation of the technical sender is performed at application level. The TIPS application authorises the technical sender for a given request only if the certificate DN (i.e. the technical address) of the same technical sender is in the list of the party technical addresses of the business sender (i.e. the Originator BIC, the Beneficiary BIC, the responsible Central Bank) which are linked to the NSP used to submit the request.

1.2.5. ESMIG Portal

[…]

1.2.6. Security

This section aims at describing the main processes performed by ESMIG in terms of security principles applied to ensure to TIPS users that they can securely exchange information with the TIPS application.

“Secure exchange” means that the following requirements are met:

- Confidentiality: Ensuring that information is accessible only to authorised TIPS Actors;
- Integrity: Safeguarding information against tampering attempts;
- Monitoring: Detecting technical problems and recording appropriate information for crisis management scenarios and future investigations;
- Availability: Ensuring that authorised users have access to the service whenever required;
- Auditability: Ensuring the possibility to establish whether a system is functioning properly and that it has worked properly.

1.2.6.1. Confidentiality

The confidentiality of data between the TIPS Actor and the ESMIG is guaranteed by the NSP. In fact, as stated in the Connectivity Requirements TIPS.UC.TC.20165 and TIPS.UC.TC.42040 (see Connectivity - Technical Requirements), the NSP takes appropriate measures and installs sufficient networking facilities to protect all the data in transit (i) between the TIPS sites and the NSP sites and (ii) between the NSP sites and the TIPS Actor's sites. An example of an "appropriate measure" is an IPSec VPN tunnel; IPSec VPN tunnels start in the TIPS Actor’s site and end in the TIPS sites. All traffic is encrypted and authenticated. Only authenticated parties can access the TIPS service. The

links between the NSP and the TIPS sites are closed to traffic from other sources or to other destinations than authenticated parties.

The NSP ensures that its staff and other parties cannot access or copy data exchanged over its network except when subject to controlled access, under secure logging and reported to TIPS Operator.

1.2.6.2. Integrity

According to the Connectivity Requirements TIPS.UC.TC.20165 and TIPS.UC.TC.43070 (see Connectivity - Technical Requirements), the NSP providing the connectivity between the TIPS Actors and the TIPS service guarantees the integrity of data exchanged.

1.2.6.3. Monitoring

TIPS operational monitoring provides the TIPS Operator with tools for the detection in real-time of operational problems.

Moreover, the NSPs deliver to the TIPS Operator the facilities to monitor their network components which provide security features from an operational and a configuration point of view. In particular, the NSP delivers features to monitor the configuration of the security providing components. Each NSP implements mechanisms to monitor its infrastructure for security vulnerabilities, breaches and attacks and shall ensure quick updates of all devices whenever security patches are available. The NSP must report immediately any issues to the TIPS Operator using collaboration tools (such as e-mail, instant messages, smartphones). In particular cases also automated alerts can be triggered.

1.2.6.4. Availability

The overall availability of the ESMIG infrastructure is ensured by the innovative architectural design and is pursued through node redundancy and self-recovery capability (built at application level). In the event of unavailability of some local nodes of the application cluster or unavailability of an entire site, TIPS adapts its behaviour as far as possible to continue operating. Also the infrastructure and the connectivity model provided by each NSP are highly available to meet the requirement to be operational 24/7/365.

1.2.6.5. Auditability

ESMIG components (e.g. servers, devices, etc.) provide an audit logs with which it is possible to reconstruct user activities, exceptions and security events.

1.3. Possible actions of ESMIG Operator

[…]

1.3.1. Business and operations monitoring

[…]

1.4. ESMIG configuration

[…]

1.4.1. Compression

[…]

1.4.2. Instant messaging

[…]

1.4.3. File-Based Store and Forward

[…].

1.5. Communication processing

[…]

1.5.1. Introduction

[…]

1.5.2. Inbound and Outbound messages

[…]

1.5.2.1. Inbound messages

[…]

1.5.2.2. Outbound Messages

[…]

1.5.3. Technical validation

[…]

1.5.4. Schema validation

[…]

1.6. Index of figures

1.7. Index of tables

1.8. List of acronyms

Item	Description
24/7/365	24-hour and seven-day around the year
A2A	Application-to-Application
BIC	Business Identifier Code
CGU	Closed Group of Users
CRDM	Common Reference Data Management
DN	Distinguished Name
ECB	European Central Bank
ECMS	Eurosystem Collateral Management System
ESMIG	Eurosystem Single Market Infrastructure Gateway
GUI	Graphical User Interface (see U2A)
IAM	Identity and Access Management
IPSec	IP Security
LRDM	Local Reference Data Management
MQ	Message Queue
NSP	Network Service Provider
PKI	Public Key Infrastructure
T2S	TARGET2-Securities
TIPS	TARGET Instant Payments Settlement
U2A	User-to-Application
UDFS	User Detailed Functional Specifications
UHB	User Handbook
URD	User Requirements Document
XML	Extensible Mark-up Language

1.9. List of referenced documents

	Title	Source
[1]	Connectivity - Technical Requirements	4CB
[2]	TIPS Connectivity Guide	4CB
[3]	TIPS User Handbook	4CB
[4]	T2-T2S Consolidation - User Requirements Document - Shared Services SHRD	ECB
[5]	TIPS User Requirements	ECB
[6]	CRDM User Detailed Functional Specifications	4CB
[7]	TIPS User Detailed Functional Specifications	4CB