Eurosystem Single Market Infrastructure Gateway for TIPS

User Detailed Functional Specifications

~~V1~~V2.~~1~~0.0

Author	4CB
Version	~~1~~2.~~1~~0.0
Date	~~31~~14/~~08~~06/~~2018~~2019

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. In the context of the Market Infrastructure Services' consolidation, the ESMIG will also provide differentiated and additional services based on the needs of the others Eurosystem Market Infrastructure services.

When possible, synergies between the ESMIG provided features across the different Eurosystem Market Infrastructure Services have to be put in place. 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. In the context of the current document, the ESMIG provides to TIPS Actors 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).

Due to high message volumes estimated for the TIPS service, a specific A2A protocol is used to exchange messages with the Network Service Provider (NSP) which 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, for some validations 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 technical sender'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 either the NSPs or by the ESMIG component:

- 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 CGU, and any subsequent modification to such subscription, is arranged through an electronic workflow on the Internet.

1.1.3. Validation of the received messages

ESMIG validates the incoming messages in order to ensure they are well-formed from both technical and schema viewpoint before routing them to the TIPS application.

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 mandatory field is missing.

In the TIPS context ESMIG carries out the schema validation of the received business message. Additionally, as part of the technical checks, ESMIG enforces the compliance of the messages to the cross-field validation.

Additional information on the schema validation at business level is provided with section 1.5.2 - Schema validation whereas the reader can find additional details on the message validation in section 1.5.3 - Technical message validation.

1.1.4. Message forwarding

ESMIG is responsible for forwarding inbound/outbound communication to the right service/NSP. For the inbound path all the messages are passed to the TIPS application process 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 Specifications) 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, 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

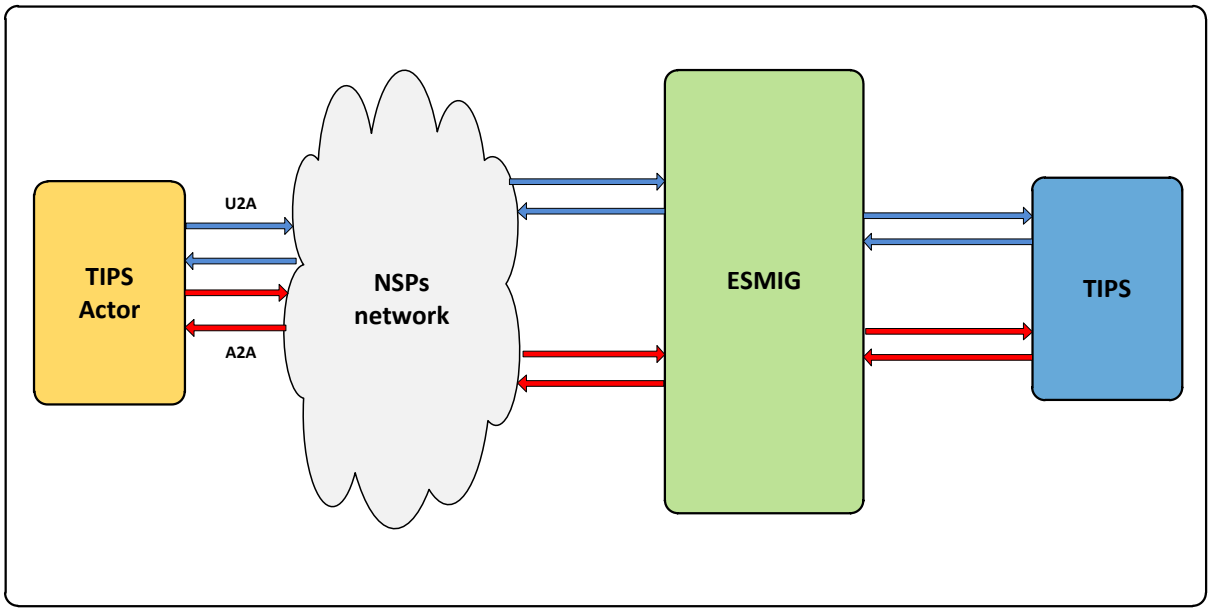
The purpose of this section is to introduce the basic connectivity to ESMIG. It does not aim to describe in details the technical connection with ESMIG.

1.2.3.2. Modes of connectivity

ESMIG supports the connectivity of TIPS Actors as follows:

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

Figure 1 – Modes of connectivity



All messages exchanged between ESMIG and TIPS Actors are based on XML technology and comply with the ISO 20022 standards, when applicable. They have to 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 network service providers

ESMIG does neither provide technical connectivity nor network services to Market Infrastructure Service Actors (e.g. TIPS Actors). Fr instance, TIPS Actors shall use a network provided by an NSP who successfully passed the compliance check, i.e. it means that the NSP gave evidence of meeting the technical and operational requirements defined in the TIPS Connectivity Technical requirements.

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 Specifications).

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

- The real-time transfer, 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. In the context of the ESMIG for TIPS, this service will be named as instant messaging to avoid any confusion with the real-time protocol supported by other Market Infrastructure Services.
- 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
Non-Settlement related messages[2]	Instant messaging	Instant messaging
Reference data update (LRDM only[3])	Instant messaging	Instant messaging
Queries	Instant messaging	Instant messaging
Investigations	Instant messaging	Instant messaging
Notifications	n/a	Instant messaging
Reports (push)	n/a	File-based, store-and-forward

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

- All settlement related messages (i.e., in TIPS, Instant Payment transactions, positive Recall answers and Liquidity Transfers[4]), non-settlement related message and LRDM updates using a message-based network service. In all cases the transfer service is instant messaging;
- All queries and investigation 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, positive recall answer and Liquidity Transfers), non-settlement related message and LRDM updates using a message-based network service. In all cases the transfer service is instant messaging;
- All queries, investigations and notifications using an instant messaging network service;
- All reports in push mode using a file-based network service transferred via store-and-forward service.

1.2.4. Authentication and authorisation

This section provides information on the authentication and authorisation processes in ESMIG. More into detail, section 1.2.4.1 – Authentication and authorisation concepts presents some basic notions

[1] The settlement-related messages refer to Instant Payment transactions, Positive Recall Answer and Liquidity Transfers.

[2] All the remaining EPC scheme-related messages, e.g. Recalls, Negative Recall Answers, Beneficary Replies.

[3] 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 UDFS (see TIPS User Detailed Functional Specifications). The usage of real.time communication is limited to those entities.

[4] Inbound Liquidity Transfers received by TARGET2 do not need to pass through the ESMIG.

(e.g. user, certificate, distinguished name, technical sender) related to access rights management in the Eurosystem Market Infrastructure Services. On this basis, sections 1.2.4.2 – Authentication process and 1.2.4.3 – Authorisation process show respectively how and where the authentication and the authorisation processes take place.

1.2.4.1. Authentication and authorisation concepts

This section presents the main concepts related to authentication and authorisation processes in ESMIG.

1.2.4.1.1 User

A user is an individual or application that interacts with ESMIG triggering the available Eurosystem Market Infrastructure Service user functions. E.g. the set of available TIPS user functions stems from the set of privileges for which the user is grantee. Each user defined in TIPS corresponds to an individual, i.e. an employee of a given TIPS Actor using the TIPS GUI, or to an application, i.e. a software component of a given TIPS Actor interacting with TIPS in A2A mode.

1.2.4.1.2 Certificate

A digital certificate is an electronic document binding an identity to a pair of electronic keys, a private key (used to sign digital information to be sent to a counterpart or to decrypt digital information received from a counterpart) and a public key (used to encrypt digital information to be sent to a counterpart or to perform the authentication and to ensure the integrity of digital information received from a counterpart). TIPS Actors assign certificates to their individuals (interacting with ESMIG in U2A mode) and applications (interacting with ESMIG in A2A mode). If a TIPS Actor uses multiple connectivity providers to connect to a Eurosystem Market Infrastructure Service, then it has to assign one certificate to each of its individuals and applications for each of these connectivity providers.

1.2.4.1.3 Distinguished Name

A Distinguished Name is a sequence of attribute-value assertions (e.g. “cn=smith”) separated by commas, e.g.:

<cn=smith,ou=tips-ops,o=bnkacct,o=nsp-1>

Each identity bound to a digital certificate is assigned a unique distinguished name (certificate DN). This applies both to individuals and applications. If a TIPS Actor uses multiple connectivity providers, each of its individuals and applications is assigned one certificate per connectivity provider and hence one certificate DN per connectivity provider.

1.2.4.1.4 Technical sender

The technical sender is the TIPS Actor submitting an A2A or an U2A request to TIPS. Each technical sender is identified by means of a certificate issued by one of the compliant NSP. The network infrastructure of the NSP authenticates the technical sender on the basis of its certificate, both in A2A mode and in U2A mode. The certificate DN of the technical sender represents the technical address used by the technical sender to connect to the TIPS application.

1.2.4.1.5 Business sender

The business sender is the TIPS Actor creating the business payload of an A2A or an U2A request to be submitted to and processed by TIPS. In some instructing scenarios, the business sender and the technical sender can be different TIPS Actors, e.g. the business sender is represented by the Originator BIC of a Reachable Party whereas the technical sender can be the Distinguished Name of the Instructing Party acting on Reachable Party’s behalf.

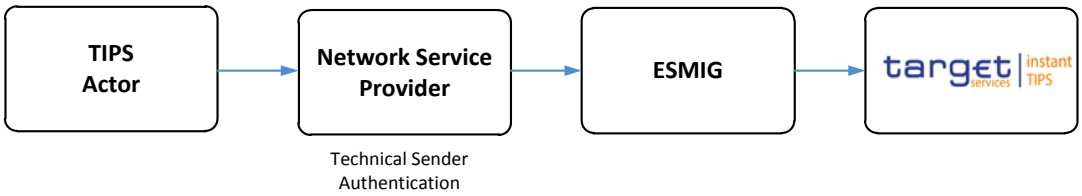
1.2.4.2. Authentication process

The authentication process refers 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 NSP 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 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

Users of TIPS Actors belonging to the appropriate Closed Group of Users, defined and enforced at NSP level, can communicate with TIPS and CRDM^{TIPS} in U2A mode via a web-based graphical user interface (GUI).

Those users are directed to an initial page named ESMIG portal that ensures proper routing to the web applications (e.g. currently: TIPS, CRDM^{TIPS}, DMT) according to the access rights profiles.

In particular, the ESMIG portal shows to the user all the applications he is authorised to access. These applications are linked one-to-one to special system privileges (stored in CRDM^{TIPS}) the user has been previously granted to 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 his distinguished name (DN). Thus, the authentication process, at IAM level, securely associates the DN to the person accessing the system.

After authentication, the person must choose the logical “user” he wants to impersonate, selecting it among a set of User-IDs that have been previously linked to his DN. This selection is done in the ESMIG portal.

So, the ESMIG portal allows and guides the person accessing the system to:

- **Choose the application** among the authorised applications accessible by at least one User-ID linked to the DN of the user;

- **Choose the user** to impersonate when accessing such an application.

After this process, the ESMIG portal redirects to the homepage of the application selected (e.g. TIPS, CRDM[TIPS], DMT).

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 Operator Service Desk.

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 and authenticity of data exchanged.

1.2.6.3. Monitoring

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

Moreover, the NSPs deliver to the Operator Service Desk 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 updates of all devices whenever security patches are available. The NSP must report immediately any technical and security issues to the Operator Service Desk 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 must be 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 audit logs with which it is possible to reconstruct user activities, exceptions and security events.

1.3. Possible actions of Operator Service Desk

1.3.1. Technical monitoring

The Operator Service Desk is provided with technical monitoring tools to check the status of the ESMIG components involved in the A2A/U2A services.

In this context for A2A services the monitoring of the queue depth and queue age is in place to be sure that the traffic is correctly flowing at the ESMIG level without having any slow down or blocking in the workflow.

1.4. ESMIG data exchange information

1.4.1. Compression

In the TIPS context the compression is only used for file-based transfer.

1.4.2. Instant messaging

For the A2A instant messaging mode, the TIPS service communicates with the participants only using “stateless” messages and with no support of "store-and-forward". This implies that in the case of unavailability of the receiver no retry mechanism is in place.

The maximum size of exchanged instant messages is set to 10KiB (1 KiB = 1.024 bytes). The maximum length refers to the business content of the transferred message, without taking into account the communication protocol overheads.

1.4.3. File-Based Store-and-Forward

The file transfer operates in store-and-forward mode and, as such, enables a sender to transmit files even when a receiver is unavailable. In the case of temporary unavailability of the receiver, the NSP stores files for 14 calendar days (for PROD environment) and delivers them as soon as the receiver becomes available again.

The maximum size for exchanged files is set to 1 GB.

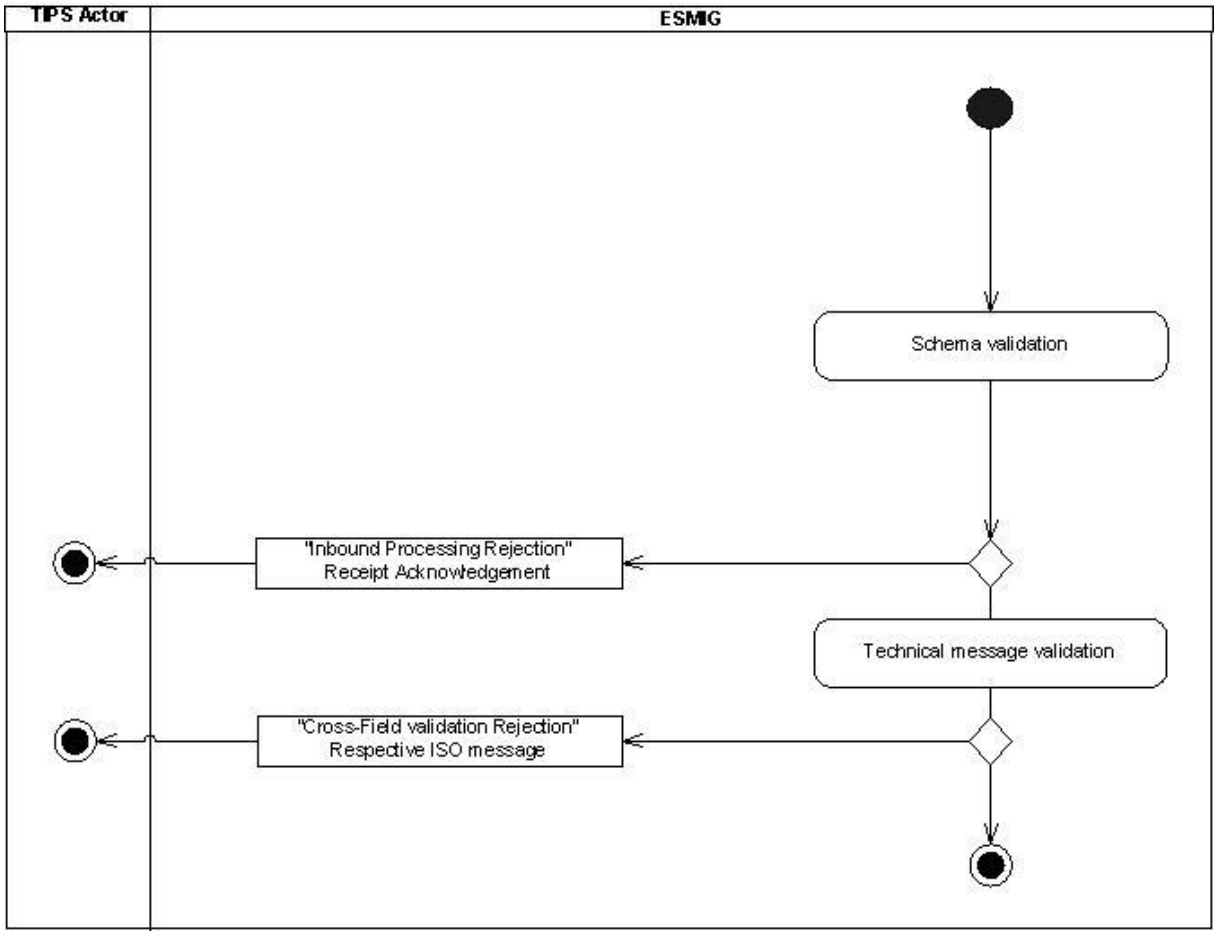
File transfer mode is used by the TIPS service only for outgoing exchange; there is no business case for using it for inbound communication from the TIPS actor to the TIPS application.

1.5. Communication processing

1.5.1. Introduction

The activity diagram shown in Figure 3 describes the generic technical entry check and covers the general aspects of the inbound communication between a TIPS Actor (via technical sender) and TIPS, where the TIPS Actor (via technical sender) sends a communication to TIPS via A2A. The network infrastructure authenticates the technical sender and authorises the technical sender to connect to TIPS. All A2A communication has to be encrypted and can be compressed. However, encryption and compression is handled on transport level by the NSP.

Figure 3 – Activity diagram



1.5.2. Schema validation

All ISO 20022 messages which reach ESMIG for further processing are subject to validation rules related to the syntax and structure of the message itself. In this context one can distinguish between well-formedness and validity of the message sent to ESMIG.

An ISO 20022 message is well-formed if it satisfies the general syntactical rules foreseen for XML, i.e. the major aspects to be respected are the following:

- The message only contains properly encoded Unicode characters;
- The specific syntax characters (e.g. “<” and “&”) are not used in the message except in their function as mark-up delineation;
- The element-delimiting tags (i.e. start, end and empty-element tags) are correctly nested and paired and none of them is missing or overlapping;
- The start and end tags match exactly and are case-sensitive;
- The message has one root element which contains all the other elements.

In contrast to other forms of representation the definition of XML documents is rather strict. XML processors cannot produce reasonable results if they encounter even slight violations against the principle of well-formedness. Any violation of this well-formedness automatically entails an interruption of the message pro-cessing and an error notification to the sender.

Every well-formed ISO 20022 message reaching ESMIG undergoes a validity check according to the rules contained in the enriched ESMIG schema files. These ESMIG enriched schemas make the structure of the message visible to the user and provide all necessary explanations on the validations the message undergoes.

The ESMIG enriched schema files serve different purposes:

- They provide a definition of all the elements and attributes in the message;
- They provide a definition on what elements are child elements and on their specific order and number;
- They provide a definition of the data types applicable to a specific element or attribute;
- They provide a definition of the possible values applicable to a specific element or attribute.

ESMIG provides the TIPS enriched schema file description in XSD format.

Based on the relevant ESMIG enriched schema, ESMIG performs the following validations for each incoming message instance:

- Validation of the XML structure (starting from the root element);
- Validation of the element sequencing (i.e. their prescribed order);
- Validation of the correctness of parent-child and sibling relations between the various elements;
- Validation of the cardinality of message elements (e.g. if all mandatory elements are present or if the overall number of occurrences is allowed);
- Validation of the choice options between the message elements;
- Validation of the correctness of the used character set;
- Validation of the correctness of the code list values and their format.

Regarding the use of namespace prefixes, the messages used for TIPS do not support the use of namespace prefixes which are hence not needed in the Eurosystem Market Infrastructure Services. However, messages received by ESMIG including namespace prefixes are processed properly (i.e. there is no validation performed at ESMIG level to check if namespace prefixes are included in messages received).

1.5.3. Technical message validation

Besides the schema validation, the messages received by ESMIG may require some additional technical checks before they can be successfully forwarded to the TIPS application. These additional

checks are required to detect potential inconsistencies in the format of the message, e.g. due to cross-field validation.

As soon as the first cross-field validation is unsuccessful, ESMIG prevents the forwarding of the incoming message to the TIPS application and replies to the sender (see Table 2 and 1.5.4.3 - ReceiptAcknowledgement (admi.007.001.01)) containing a proper error code, depending on the specific violation hit.

The table below describes, for each incoming message where the cross-field validation applies, the technical checks performed by ESMIG and the relevant error code issued.

Table 2 - Cross-field validations

ISO Code	Field/Group	Check to be performed	X-Path	ERROR Code	Output message
pacs.002.001.03	Group Status Transaction Status	Neither group status nor transaction status has been specified	FIToFIPmtStsRpt/OrgnlGrpInfAndSts/GrpSts FIToFIPmtStsRpt/TxInfAndSts/TxSts	MS01	pacs.002.001.03
pacs.002.001.03	Group Status Transaction Status	Both group status and transaction status have been specified	FIToFIPmtStsRpt/OrgnlGrpInfAndSts/GrpSts FIToFIPmtStsRpt/TxInfAndSts/TxSts	MS01	pacs.002.001.03
pacs.002.001.03	Reason	The relevant StsRsnInf tag for a negative reply (RJCT) should have been specified	FIToFIPmtStsRpt/OrgnlGrpInfAndSts/StsRsnInf/Rsn/Cd	MS01	pacs.002.001.03
pacs.002.001.03	Reason	The relevant StsRsnInf tag for a negative reply (RJCT) should have been specified	FIToFIPmtStsRpt/TxInfAndSts/StsRsnInf/Rsn/Cd	MS01	pacs.002.001.03
pacs.004.001.02	Number Of Transactions	TIPS supports only one transaction per message. NbOfTxs (attribute tag) = 1	PmtRtr/GrpHdr/NbOfTxs	MS01	pacs.002.001.03
pacs.004.001.02	Original Group Information	The OrgnlGrpInf has not been specified neither at group nor at transaction level	PmtRtr/OrgnlGrpInf PmtRtr/TxInf/OrgnlGrpInf	MS01	pacs.002.001.03
pacs.004.001.02	Original Group Information	The OrgnlGrpInf has been specified both at group and at transaction level	PmtRtr/OrgnlGrpInf PmtRtr/TxInf/OrgnlGrpInf	MS01	pacs.002.001.03
pacs.004.001.02	Transaction Information	The xml message should contain exactly one TxInf tag	PmtRtr/TxInf	MS01	pacs.002.001.03

ISO Code	Field/Group	Check to be performed	X-Path	ERROR Code	Output message
pacs.008.001.02	Remittance Information	Either Unstructured or Structured may be present. If both components are included, the message will be rejected	FIToFICstmrCdtTrf/CdtTrfTxInf/RmtInf/Ustrd FIToFICstmrCdtTrf/CdtTrfTxInf/RmtInf/Strd	MS01	pacs.002.001.03
pacs.028.001.01	Original Message Name Identification Original Instruction Identification	Original Message Name Identification = "camt.056.001.01" and Original Instruction Identification not specified.	FIToFIPmtStsReq/OrgnlGrpInf/OrgnlMsgNmId FIToFIPmtStsReq/TxInf/OrgnlInstrId	MS01	pacs.002.001.03
pacs.028.001.01	Original Message Name Identification Creditor Agent	Original Message Name Identification = "camt.056.001.01" and Creditor Agent not specified.	FIToFIPmtStsReq/OrgnlGrpInf/OrgnlMsgNmId FIToFIPmtStsReq/TxInf/OrgnlTxRef/CdtrAgt/FinInstnId/BICFI	MS01	pacs.002.001.03
camt.050.001.04	Creditor Account Type	This field must not be included in the request. The message will be rejected in that case.	LqdtyCdtTrf/LqdtyCdtTrf/CdtrAcct/Tp	L099	camt.025.001.04
camt.050.001.04	Debtor Account Type	This field must not be included in the request. The message will be rejected in that case.	LqdtyCdtTrf/LqdtyCdtTrf/DbtrAcct/Tp	L099	camt.025.001.04
camt.050.001.04	Settlement Date	This must be included in outgoing Credit Transfer. It must be filled with the stored RTGS business date.	LqdtyCdtTrf/LqdtyCdtTrf/SttlmDt	L099	camt.025.001.04

1.5.4. Inbound and Outbound messages

1.5.4.1. Inbound messages

No inbound message is directly addressed to the ESMIG for TIPS. All the successfully validated business messages are routed to the TIPS application.

1.5.4.2. Outbound Messages

Currently, three outbound messages are generated by the ESMIG for TIPS. The reason for the rejection is either due to schema validation or message validation as described in the previous sections.

The message elements for the latter two messages in Table 3 are currently being described in the TIPS UDFS.

Table 3 - Outbound messages generated by ESMIG

ISO Message / Message Usage	ISO Code
ReceiptAcknowledgement / "Inbound Processing Rejections"	admi.007.001.01
FIToFIPaymentStatusReport / "cross field validation rejection"	pacs.002.001.03
Receipt / "cross field validation rejection"	camt.025.001.04

1.5.4.3. ReceiptAcknowledgement (admi.007.001.01)

The ReceiptAcknowledgement message is sent by ESMIG to the sender of the message to reject the reception of an A2A-message. Within the ESMIG for TIPS this message is generated after an inbound processing rejection.

The table below describes the message elements filled by ESMIG.

Table 4 - ReceiptAcknowledgement

Field Name	Description	XML path	Mandatory	TIPS Usage
Message Identifier	Identification of the message assigned by ESMIG.	RctAck/MsgId/MsgId	Yes	
Related Reference	Reference of the original message generating the ReceiptAcknowledgment.	RctAck/Rpt/RltdRef/Ref	Yes	
Status Code	Status of the processing of the original message.	RctAck/Rpt/ReqHdlg/StsCd	Yes	Status Code specifiing the error. For schema validation the error code is 'X001'
Description	Description of the status	RctAck/Rpt/ReqHdlg/Desc	No	For schema validation the description is 'Parsing error'

1.6. Index of figures

1.7. Index of tables

1.8. List of acronyms

Item	Description
24/7/365	24 hours a day/ 7 days a week/ 365 days a 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
ESMIG	Eurosystem Single Market Infrastructure Gateway
GUI	Graphical User Interface (see U2A)
IAM	Identity and Access Management
IPSec	Internet Protocol Security
LRDM	Local Reference Data Management
MQ	Message Queuing
NSP	Network Service Provider
PKI	Public Key Infrastructure
PROD	Production (Environment)
TIPS	TARGET Instant Payment Settlement
U2A	User-to-Application
UDFS	User Detailed Functional Specifications
URD	User Requirements Document
XML	Extensible Mark-up Language
XSD	XML Schema Definition

1.9. List of referenced documents

	Title	Source
[1]	Connectivity - Technical Requirements	4CB
[2]	TIPS Connectivity Guide	4CB
[3]	TIPS User Requirements Document	ECB
[4]	CRDM User Detailed Functional Specifications	4CB
[5]	TIPS User Detailed Functional Specifications	4CB