BANCA D'ITALIA EUROSISTEMA BANCO DE ESPAÑA Eurosistema
BANQUE DE FRANCE EUROSYSTÈME DEUTSCHE BUNDESBANK EUROSYSTEM

target services

Eurosystem Single Market Infrastructure Gateway

User Detailed Functional Specifications

Author	4CB
Version	R2026.NOV
Identifier	ESMIG UDFS
Date	13~~0~~ ~~July~~ September 2026

Table of Contents

1 Introduction 5

2 Reader's guide 6

3 General features of ESMIG 8

3.1 ESMIG Features Overview 8
3.1.1 Authentication of the message sender 8
3.1.2 Participation to the Closed Group of Users 8
3.1.3 Validation of the received messages 8
3.1.4 Message forwarding 9
3.2 Access to ESMIG 9
3.2.1 Single access point for the external communication 9
3.2.2 Network agnostic communication 9
3.2.3 Connectivity 10
3.2.4 Authentication and authorisation 13
3.2.5 ESMIG Portal ..... 17~~16~~
3.2.6 Security 18
3.3 Possible actions of Operator Service Desk 20
3.3.1 Technical monitoring 20
3.4 ESMIG data exchange information 20
3.4.1 Compression 20
3.4.2 Instant messaging 20
3.4.3 Message-Based and File-Based Real-Time 21
3.4.4 Message-Based and File-Based Store-and-Forward 22
3.5 Communication processing 22
3.5.1 Introduction 22
3.5.2 Schema validation 23
3.5.3 Technical message validation 25
3.5.4 Inbound and Outbound messages 30
3.5.5 Digital Signature managed within the business layer 36
3.5.6 Routing 36

4 Annexes 40

4.1 Digital Signature on Business Layer 40
4.1.1 Mechanism and Introduction for signature constructions 40
4.1.2 Use of XML and canonicalization algorithm 40
4.1.3 Message Type 1: File with multiple ISO 20022 messages 40
4.1.4 Message Type 2: single ISO 20022 message 45
4.1.5 ESMIG digital signature services 50

All Rights reserved

4.2 List of business rules and error codes 52
4.3 Index of figures 53
4.4 Index of tables 54
4.5 List of acronyms 55
4.6 List of referenced documents 57
4.7 U2A Qualified configuration 58
4.7.1 Introduction 58
4.7.2 Ascertia GSD Single User Client (SU) 59
4.7.3 Ascertia GSD Multi User Client (MU) 70
4.7.4 GoSign Desktop client - Support and release policy 85
4.7.5 Annex 87

All Rights reserved

Disclaimer

All rights reserved.

Reproduction for educational and non-commercial purposes is permitted provided that the source is acknowledged

1 Introduction

The description of the Eurosystem Single Market Infrastructure Gateway included in this document is related to the network connectivity services provided by ESMIG to all the TARGET Services, common components and applications. 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 TARGET Services, common components and applications have to be put in place. ESMIG offers scalability to cope with the different TARGET Services, common components and applications 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 Actors the single access point for the external communication to TARGET Services, common components and applications. This means it is in charge of A2A and U2A traffic management providing authentication of all inbound traffic (U2A and A2A).

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.

The ESMIG is expected to perform basic checks on inbound messages and then route them to the relevant TARGET Services, common components and applications. Similarly, ESMIG takes care of the routing of outbound messages from TARGET Services, common components and applications 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 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.

All Rights reserved

2 Reader's guide

The UDFS document is available for the whole community of TARGET Services' Actors: in order to ensure the same level of information for participants directly connected to any TARGET Service is contained in one single book of UDFS.

Nevertheless, different readers may have different needs and priorities. For instance, "T2-T2S CSLD only" readers are interested to some sections (e.g. the Digital signature at business level) whereas they may not wish to enter into the full details of the TIPS specificities, whereas the opposite can apply to "TIPS-only" readers.

Due to the nature of ESMIG as a Common Component used as gateway to access multiple Services, most of the information presented in this document is applicable to all such Services, while some of it is specifically relevant only to individual Services. Readers that aim to use ESMIG for accessing all Services will find the entire document relevant for their purpose. On the other hand, readers who are only interested in the access to a specific Service or component may find the following sections particularly relevant.

Table 1 - UDFS sections containing service-specific information

SECTION	RELEVANT SERVICE/COMPONENT	NOTES
3.2.6.4.1 ESMIG availability for TARGET Services (excluding TIPS)~~ESMIG availability for TARGET Services (excluding TIPS)~~	CLM, RTGS, CRDM, ECONS II, ECMS	General availability aspects applicable to any Service/Component excluding TIPS.
3.2.6.4.2 ESMIG availability for TIPS~~ESMIG availability for TIPS~~	TIPS	The chapter outlines the specificity of TIPS with regards the availability requirement.
3.4.2 Instant messaging ~~Instant messaging~~	TIPS	Instant messaging mode is only used for the TIPS service.
3.4.3 Message-Based and File-Based Real-Time ~~Message-Based and File-Based Real-Time~~	CLM, RTGS, CRDM, ECONS II, ECMS	This section does not apply to TIPS
3.5.1 Introduction ~~Introduction~~	CLM, RTGS, CRDM, ECONS II, ECMS, TIPS	The activity diagram at Figure 3~~Figure 3~~ is only relevant for TIPS.

All Rights reserved

SECTION	RELEVANT SERVICE/COMPONENT	NOTES
3.5.2.1 Schema validation for TARGET Services (excluding TIPS)~~Schema validation for TARGET Services (excluding TIPS)~~	CLM, RTGS, CRDM, ECONS II, ECMS	For all the TARGET Services excluding TIPS the schema validation at business level is delegated to the Business Interface of the corresponding Service/Component.
3.5.2.2 Schema validation for TIPS~~Schema validation for TIPS~~	TIPS	ESMIG for TIPS is responsible of executing the message schema validation.
3.5.3.1 Technical message validation for TARGET Services (excluding TIPS)~~Technical message validation for TARGET Services (excluding TIPS)~~	CLM, RTGS, CRDM, ECONS II, ECMS	For all the TARGET Services excluding TIPS, the additional technical validation at business level is delegated to the Business Interface of the corresponding Service/Component.
3.5.3.2 Technical message validation for TIPS~~Technical message validation for TIPS~~	TIPS	Section only relevant for TIPS
3.5.4.2.1 Outbound Messages for TARGET Services (excluding TIPS)~~Outbound Messages for TARGET Services (excluding TIPS)~~	CLM, RTGS, CRDM, ECONS II, ECMS	Scenarios applicable for each Service/Component excluding TIPS.
3.5.4.2.4 Outbound Messages for TIPS~~Outbound Messages for TIPS~~	TIPS	Section only relevant for TIPS
3.5.4.3 ReceiptAcknowledgement (admi.007.001.01) ~~ReceiptAcknowledgement (admi.007.001.01)~~	CLM, RTGS, CRDM, ECONS II, ECMS, TIPS	The subsection "*Usage Case: Timeout Management and Oversized Data Management*" is valid for any Service/Component excluding TIPS. The subsection "*Usage Case: TIPS ReceiptAcknowledgement*" is only valid for TIPS.
4.1 Digital Signature on Business Layer ~~Digital Signature on Business Layer~~	CLM, RTGS, CRDM, ECONS II, ECMS	Digital signature aspects are applicable to any Service/Component excluding TIPS.
4.2 List of business rules and error codes ~~List of business rules and error codes~~	CLM, RTGS, CRDM, ECONS II, ECMS	The list of business rule is applicable to any Service/Component excluding TIPS.

All Rights reserved

3 General features of ESMIG

3.1 ESMIG Features Overview

The ESMIG infrastructure provides a set of features shared among all the TARGET Services, common components and applications beyond representing a single point of contact with the external networks.

These features, detailed below, belong to two main areas and can be provided either by the NSPs or by the ESMIG component:

- Security, for example authentication of the sender and authorisation against a Closed Group of Users (CGU).
- Message management, for example message technical validation and forwarding.

3.1.1 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 Actors digital certificates needed to access the A2A and U2A messaging services) and at the interface with the TARGET Services, common components and applications through the relevant services provided by the NSP.

The NSP identifies the Actor and the TARGET Services, common components and applications 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 Actor and the TARGET Services, common components and applications as local message partner every time they open a new session with the NSP's Network Gateway for A2A traffic exchange.

3.1.2 Participation to the Closed Group of Users

Each NSP defines a CGU for each TARGET Service environment (test and production) and checks the authorisation of the TARGET Services' Actors to access the TARGET Services 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.

3.1.3 Validation of the received messages

ESMIG validates the incoming messages in order to ensure they are well-formed at technical viewpoint before routing them to the TARGET Services. Additionally, the ESMIG for TIPS verifies also the incoming messages from a schema validation viewpoint.

All Rights reserved

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 3.5.2 – Schema validation~~Schema validation~~ whereas the reader can find additional details on the message validation in section 3.5.3 – Technical message validation~~Technical message validation~~.

3.1.4 Message forwarding

ESMIG is responsible for forwarding inbound/outbound communication to the right service/NSP. For the inbound path all the messages/files are passed to the TARGET Services[1], common components and applications in charge to manage inbound messages/files. For the outbound path, ESMIG addresses the correct NSP interface among the available ones based on the information provided by the sender TARGET Service and retrieved from the Common Reference Data Management (CRDM) database. The reader can refer to the CRDM UDFS (see CRDM User Detailed Functional Specification~~CRDM User Detailed Functional Specifications~~) for any related additional information.

3.2 Access to ESMIG

3.2.1 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 ESMIG login, 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.).

3.2.2 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] For TIPS only messages are envisioned in the inbound direction.

3.2.3 Connectivity

3.2.3.1 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.

3.2.3.2 Modes of connectivity

ESMIG supports the connectivity of TARGET Services' Actors as follows:

- Communication between software applications via XML messages or files and for the specific non-standard case of securities valuation or specific reports via flat files (A2A mode);
- Online screen-based activities performed by ESMIG users (U2A mode).

All messages exchanged between ESMIG and ESMIG Actors are based on XML technology and comply with the ISO 20022 standards, when applicable. However, for TIPS the messages have to be sent to ESMIG as individual messages, while for T2S they can be sent either individually or in a file containing one or several messages. However, for T2S the upload of securities valuations is handled via flat files. Additionally CSDs may decide to receive some specific reports via flat file instead of XML, while ECMS necessarily receives all its reports in flat file format.

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. A2A is based on message/file exchange; ESMIG manages the inbound/outbound traffic, provides digital signature services and routing functionalities. 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 to provide digital signature, authentication and CGU related services.

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

3.2.3.3 Technical connectivity and network service providers

ESMIG does not provide technical connectivity or network services to the TARGET Services connected actors. TARGET Services' Actors shall use network services and related technical connectivity provided by an NSP awarded in the relevant concession procedure for connectivity to the ESMIG, i.e. it means that the NSP gave evidence of meeting the technical and operational requirements defined in the Connectivity Technical requirements. Each TARGET Service and application provides the users with a dedicated Connectivity Guide. As for TIPS, detailed information related to the usage of network services is provided in the "TIPS Connectivity Guide" (see TIPS Connectivity Guide~~TIPS Connectivity Guide~~). For T2S, detailed information as to the usage of network services is provided in the "T2S Connectivity Guide".

3.2.3.4 Common rules for message and file transfer services

This section describes the rules of the transfer services envisaged in ESMIG for A2A messages and files exchange. The configuration of the routing is described in details in the UDFS of the CRDM (see CRDM User Detailed Functional Specifications).

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. Moreover, 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 A2A interaction is achieved through two different protocols: Data Exchange Protocol (DEP), used by the TARGET Services (excluding TIPS), and the Message Exchange Processing for TIPS (MEPT).

In A2A mode, ESMIG 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 particular:
  - DEP: this service is named as *real-time*;
  - MEPT: this service is named as *instant messaging* to avoid any confusion with the real-time protocol supported by DEP.
- The store-and-forward message and file transfer, which enables the sender to transmit messages or 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. In particular:
  - DEP: this service is named as *store-and-forward*;
  - MEPT: this service is named as *store-and-forward* and it is used in TIPS only for outbound communication (TIPS platform to user).

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

Table 2 - ESMIG business data exchanges and network services features[2]

[2] The one shown in table 1 is not the exhaustive list of Services, components and applications.

BUSINESS DATA EXCHANGES	SERVICE / COMPONENT	INBOUND COMMUNICATION	OUTBOUND COMMUNICATION
Settlement-related messages[3]	TIPS	Instant messaging	Instant messaging
Settlement-related messages	CLM/RTGS/ECONS II	Message-based, store-and-forward File-based, store-and-forward	Message-based, store-and-forward File-based, store-and-forward
Non-Settlement related messages[4]	TIPS	Instant messaging	Instant messaging
Reference data update (LRDM only[5])	TIPS	Instant messaging	Instant messaging
Reference data updates	CRDM	Message-based, store-and-forward File-based, store-and-forward	Message-based, store-and-forward File-based, store-and-forward
Queries	TIPS	Instant messaging	Instant messaging
Queries / Reports (pull)	CRDM/CLM/RTGS/ ECONS II	Message-based, real-time	Message-based, real-time Message-based, store-and-forward File-based, store-and-forward
Investigations	TIPS	Instant messaging	Instant messaging
Notifications	TIPS	n/a	Instant messaging
Reports (push)	TIPS	n/a	File-based, store-and-forward
Reports (push)	CRDM/CLM/RTGS	n/a	Message-based, store-and-forward File-based, store-and-forward
Reports (push)	DWH	n/a	File-based, store-and-forward
General Ledger	ECONS II	n/a	Message-based, real-time File-based, store-and-forward
Broadcast	TIPS	n/a	Instant messaging

The

Table **2**

~~Table 2~~ shows that, as far as the inbound communication is concerned, TARGET Services' Actors can submit:

- All settlement related messages for TIPS (i.e., Instant Payment transactions, positive Recall answers and Liquidity Transfers), non-settlement related message and LRDM updates for TIPS using a message-based network service. In all cases the transfer service is instant messaging;
- All settlement-related messages for CLM/RTGS/ECONS II (e.g. liquidity transfers) and reference data updates either using a message-based network service or via a file-based network service. In both cases, the transfer service is store-and-forward;
- All queries,investigation broadcasts and notifications for TIPS using an instant messaging network service;
- All queries and pull reports either using a message-based network service or via a file-based network service. In both cases, the transfer service is real-time.

As to the outbound communication,

Table 2

~~**Table** 2~~ shows that ESMIG sends:

- All settlement related messages for TIPS (i.e., Instant Payment transactions, positive Recall answers and Liquidity Transfers), non-settlement related message and LRDM updates for TIPS using a message-based network service. In all cases the transfer service is instant messaging;
- All outgoing settlement-related messages (i.e., status advices, notifications, etc.) for CLM/RTGS/ECONS II and responses related to reference data updates for CRDM using either a message-based or a file-based network service. In both cases, the transfer service is store-and-forward;
- All queries, investigations and notifications for TIPS using an instant messaging network service;
- All query responses and pull reports either using a message-based network service or via a file-based network service. The transfer service can be either real-time or store-and-forward for messages whereas it is store-and-forward for files. An exception takes place for responses exceeding a pre-defined size or time limit; in this case ESMIG sends these responses using either a message-based network service or a file-based network service. In both cases, the transfer service is store-and-forward;
- All reports in push mode for TIPS and DWH using a file-based network service transferred via store-and-forward service;
- All reports in push mode for CRDM/CLM/RTGS, including the General Ledger for ECONS II, either using either a message-based network service or a file-based network service. In both cases, the transfer service is store-and-forward.

3.2.4 Authentication and authorisation

This section provides information on the authentication and authorisation processes in ESMIG. In more detail, section 3.2.4.1 – Authentication and authorisation ~~Authentication and authorisation concepts~~ presents some basic notions (e.g. user, certificate, distinguished name, technical sender) related to access rights management in the TARGET Services, common components and applications.

On this basis, sections 3.2.4.2 – Authentication processAuthentication process and 3.2.4.3 – Authorisation processAuthorisation process show respectively how and where the authentication and the authorisation processes take place.

3.2.4.1 Authentication and authorisation concepts

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

3.2.4.1.1 User

A user is an individual or application that interacts with ESMIG triggering the available user functions of TARGET Services, common components and applications. E.g., the set of available user functions stems from the set of privileges of TARGET Services, common components and applications for which the user is grantee. Each user defined in TARGET Services, common components and applications corresponds to an individual or to an application.

3.2.4.1.2 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). Each Actor assigns certificates to their individuals (interacting with ESMIG in U2A mode) and applications (interacting with ESMIG in A2A mode). If an Actor uses multiple connectivity providers to connect to TARGET Services, common components or applications, then it has to assign one certificate to each of its individuals and applications for each of these connectivity providers.

3.2.4.1.3 Distinguished Name

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

<cn=smith,ou=serv-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 to applications. If an 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.

3.2.4.1.4 System User Reference

The System User Reference (SUR) is a unique reference that ESMIG uses to identify one user in TARGET Services, common components and applications. ESMIG allows Actors linking one certificate

DN to many system user references. As one system user reference identifies one user in TARGET Services[6], common components and applications, this means that each Actor can link one certificate DN to many users defined in TARGET Services, common components and applications.

3.2.4.1.5 Technical sender

The technical sender is the Actor submitting an A2A or an U2A request to TARGET Services, common components and applications. 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 based on 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 TARGET Services, common components or applications.

3.2.4.1.6 Business sender

The business sender is the Actor creating the business payload of an A2A or an U2A request to be submitted to and processed by TARGET Services, common components and applications. When allowed by the relevant TARGET Service or Application. The business sender and the technical sender can be different Actors. E.g., in some TIPS instructing scenarios 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.

3.2.4.1.7 Business sending user

The business sending user is the user creating the business payload of the request. This user corresponds to an individual or to an application of the business sender Actor. Each business sending user is identified by ESMIG through the signature verification process of the Business Application Header or Business File Header.

More precisely:

- For single messages the relevant information is included in the Business Application Header;
- For files (i.e. group of messages) it is included in the Business File Header and is not included in the Business Application Headers of the single messages belonging to the file.

From a business perspective, the business sending user signs only once the business payload, both in case this payload includes only one request (in this case the business sending user signs the Business Application Header of this request) or a set of requests (in this case the business sending user signs the Business File Header of the file including these requests). Consequently, one file cannot include requests referring to different business sending users, i.e. the business sender must send requests related to different business sending users into separate files.

[6] With the exception of the TIPS Service where the System User Reference is only configured in CRDM but not used in A2A communication. For Common Component traffic related to TIPS, the System User Reference is relevant.

3.2.4.2 Authentication process

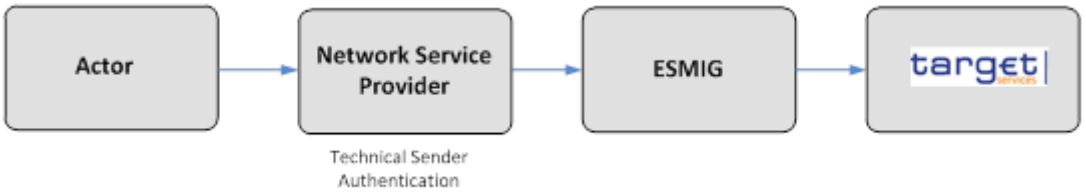
The authentication process refers to:

- The authentication of the technical sender and
- The authentication of the business sending user.

3.2.4.2.1 Authentication of the technical sender

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 1 – 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 (see section 3.2.4.3.1 – Authorisation of the technical sender~~Authorisation of the technical sender~~).

3.2.4.3 Authorisation process

The authorisation process refers to:

The authorisation of the technical sender.

3.2.4.3.1 Authorisation of the technical sender

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.

The authorisation of the technical sender is performed at application level, when required by the component. The TARGET Services, common components or applications authorise 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 (e.g., in TIPS, the Originator BIC, the Beneficiary BIC, the responsible Central Bank or the Business Sending Party in T2S) which are linked to the NSP used to submit the request.

3.2.5 ESMIG Portal

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 named 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 to special system privileges (stored in CRDM) the user has been previously granted with and that are specifically dedicated to those web applications. Access to applications is allowed by granting the proper privilege for the application itself combined with the type of Party to which the DN belongs to. In case the DN is linked only to user(s) belonging to Party(s) of party Type CSD or CSD Participant, then only the T2S Service is available. Otherwise all Services are present.

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.

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.

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

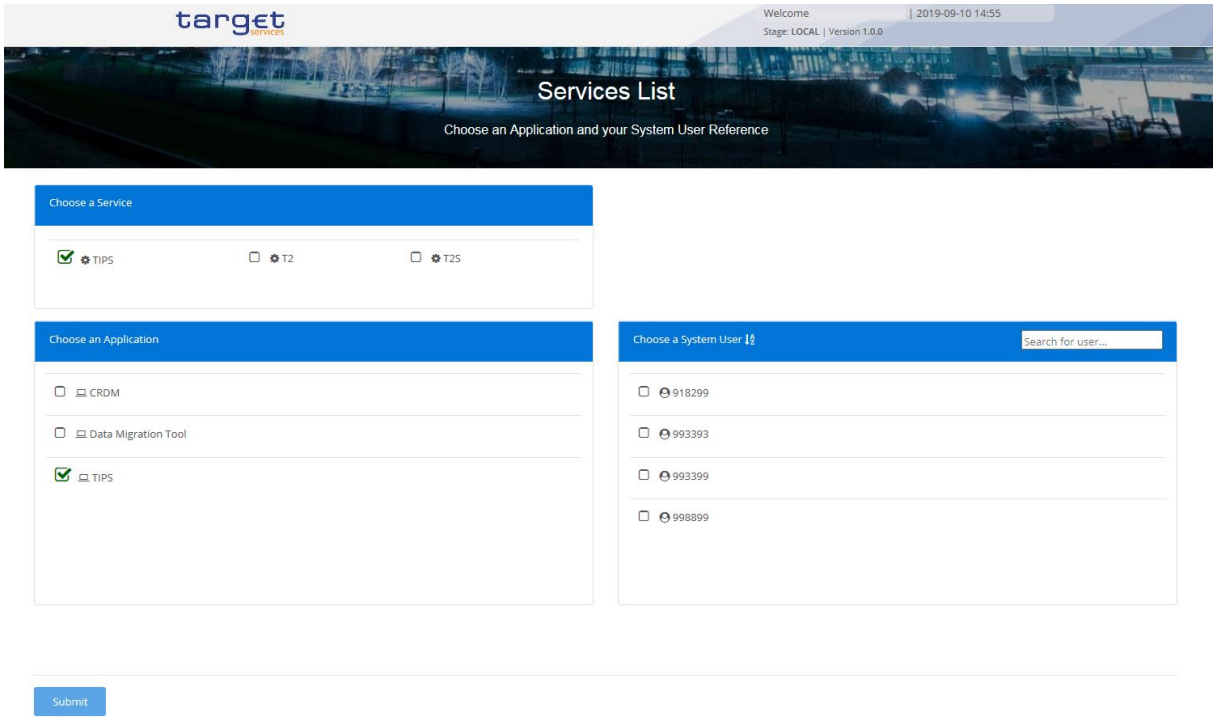
- **choose the service** among the authorised services accessible by at least one user-ID linked to the DN of the user;
- **choose the component/application** among the authorised components and applications accessible by at least one user-ID linked to the DN of the user;
- **choose the user** to impersonate when accessing such an application.

After this process, the ESMIG Portal redirects the user to the homepage of the application selected (e.g. CRDM, DMT, TIPS, etc.).

An example of how the ESMIG Portal GUI will look like is shown in the following picture.

All Rights reserved

Figure 2 – ESMIG Portal Graphical User Interface



3.2.6 Security

This section aims at describing the main processes performed by ESMIG in terms of security principles applied to ensure to TARGET Services' users that they can securely exchange information with the related service, component or application.

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

- Confidentiality: Ensuring that information is accessible only to authorised 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.

3.2.6.1 Confidentiality

The confidentiality of data between each Actor and the ESMIG is guaranteed by the NSP. In fact, the NSP takes appropriate measures and installs sufficient networking facilities to protect all the data in transit (i) between the TARGET Services’ sites and the NSP sites and (ii) between the NSP sites and the Actor's sites. An example of an "appropriate measure" is an IPsec VPN tunnel; IPsec VPN tunnels start in the Actor’s site and end in the TARGET Service sites. All traffic is encrypted and authenticated. Only authenticated parties can access the TARGET Service, components or application. The links between the NSP and the TARGET Service sites are closed to traffic from other sources or to other destinations than authenticated parties.

All Rights reserved

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.

3.2.6.2 Integrity

The NSP providing the connectivity between the Actors and the TARGET Services guarantees the integrity and authenticity of data exchanged.

3.2.6.3 Monitoring

TARGET Services 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.

3.2.6.4 Availability

3.2.6.4.1 ESMIG availability for TARGET Services (excluding TIPS)

The overall availability of the ESMIG for all TARGET Services is ensured by the infrastructure design. The technical environment follows a “two regions/four sites” approach to ensure availability throughout the widest possible range of system failures. For T2S further information regarding this architecture is available into the T2S General Technical Design published on the ECB website.

3.2.6.4.2 ESMIG availability for TIPS

The overall availability of the ESMIG infrastructure for TIPS 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. In addition, the infrastructure and the connectivity model provided by each NSP must be highly available to meet the requirement to be operational 24/7/365.

3.2.6.5 Auditability

ESMIG components (e.g. servers, devices, etc.) provide audit logs with which it is possible to reconstruct user activities, exceptions and security events. . All this data is available to authorised users via queries.

In order to ensure sustainability, ESMIG archives all data by storing for a harmonised period of ten years all inbound and outbound messages (except queries) in their original format.

All Rights reserved

3.3 Possible actions of Operator Service Desk

3.3.1 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.

ESMIG complies with the requirement of logging inbound/outbound communication based on the specific A2A/U2A features. The access to this information is provided with the Operator only, via the ESMIG console.

3.4 ESMIG data exchange information

3.4.1 Compression

A global compression size limit of 2 kb is defined valid over all networks. Only the messages sent by any business interface which exceed this limit can be compressed, upon request of the relevant business interface, due to the overhead for the compression of small messages.

All the XML business data has to be compressed including the Business Application Header (BAH) or the File Header (FH). Data belonging to the network protocol (DEP ExchangeHeader) is not compressed. That is valid for messages sent by a TARGET Services' actor.

The compression algorithm supported by TARGET Services' is the ZIP algorithm (i.e. ZIP deflate and the BASE64 RFC 7 2045).

If the decompression of inbound communication is not successful, the TARGET Service sends an error information on network layer to the TARGET Service actor indicating the decompression failure. The correlation to the original inbound message has to be identified on network layer

In the TIPS context the compression is always used for file-based transfer (i.e. for the TIPS reports).

When using DEP protocol message/file compressed cannot exceed, after the uncompress operation, the size limit of 99MB.

3.4.2 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.

All Rights reserved

3.4.3 Message-Based and File-Based Real-Time

	MINIMUM LENGTH	MAXIMUM LENGTH
Message channel	1	32 KB (KB=2^{10})
File channel	1	32 MB (MB=2^{20})

The channel for query responses and the communication mode depends on the size of the response and the channel that was used for the query request. The behaviour described in this section applies to any TARGET Service excluding TIPS.

Table 3 - Query response and communication mode depending on the size of the response

REQUEST	RESPONSE SIZE < 32 KB	RESPONSE 32 MB > SIZE > 32 KB	RESPONSE SIZE > 32 MB
Message channel Real-time	Message channel Real-time	File channel Store and forward	No transmission
File channel Real-time	File channel[7] Real-time	File channel[7] Real-time	No transmission

When the size[8] of the response is suitable the same channel that was used for the query request is used.

- The query response is sent in real-time mode.

When the request is sent via the message channel and the size of the response is too large for a transfer via the message channel the file Store and forward channel is used.

- ESMIG sends an “Oversize and timeout” ReceiptAcknowledgement in real-time mode to the TARGET Service actor (sender) indicating the change of the transfer mode. The related reference indicates the Business Message Identifier of the request.
- The query response is sent in store and forward mode according to the default routing rule for the file Store and forward channel.

In general, if the size of the response is too large for a transfer via the file channel the transmission is aborted.

- ESMIG sends an “Oversize and timeout” ReceiptAcknowledgement in real-time mode to the TARGET Service actor (sender) indicating the abortion. The related reference indicates the Business Message Identifier of the request.

[7] For the real-time mode, although incoming/outgoing messages and files exchange are part of the DEP protocol, for the time being usage of real-time mode is limited to incoming messages only.

[8] The size of the business content is whatever has to be encapsulated into the DEP envelope. In that respect the business data can be either:

- [BAH+Message payload] or,
- [BFH+File Data]

All Rights reserved

- The query response is not sent.

In case a certain response exceeds the maximum size of 32 MB for a transfer via the file channel, this TARGET Service outbound message may be split into several parts.

The size limitation refers to the allowed size range for messages and files in the transport channel, (i) without taking into account the communication protocols overheads and (ii) regardless of whether the business data is compressed or not.

3.4.4 Message-Based and File-Based Store-and-Forward

The message and file transfer operate in store-and-forward mode and, as such, enable 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.

For TIPS 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.

For exchange based on DEP protocol the following size limit applies.

	MINIMUM LENGTH	MAXIMUM LENGTH
Message channel	1	32 KB (KB=2^{10})
File channel	1	32 MB (MB=2^{20})

3.5 Communication processing

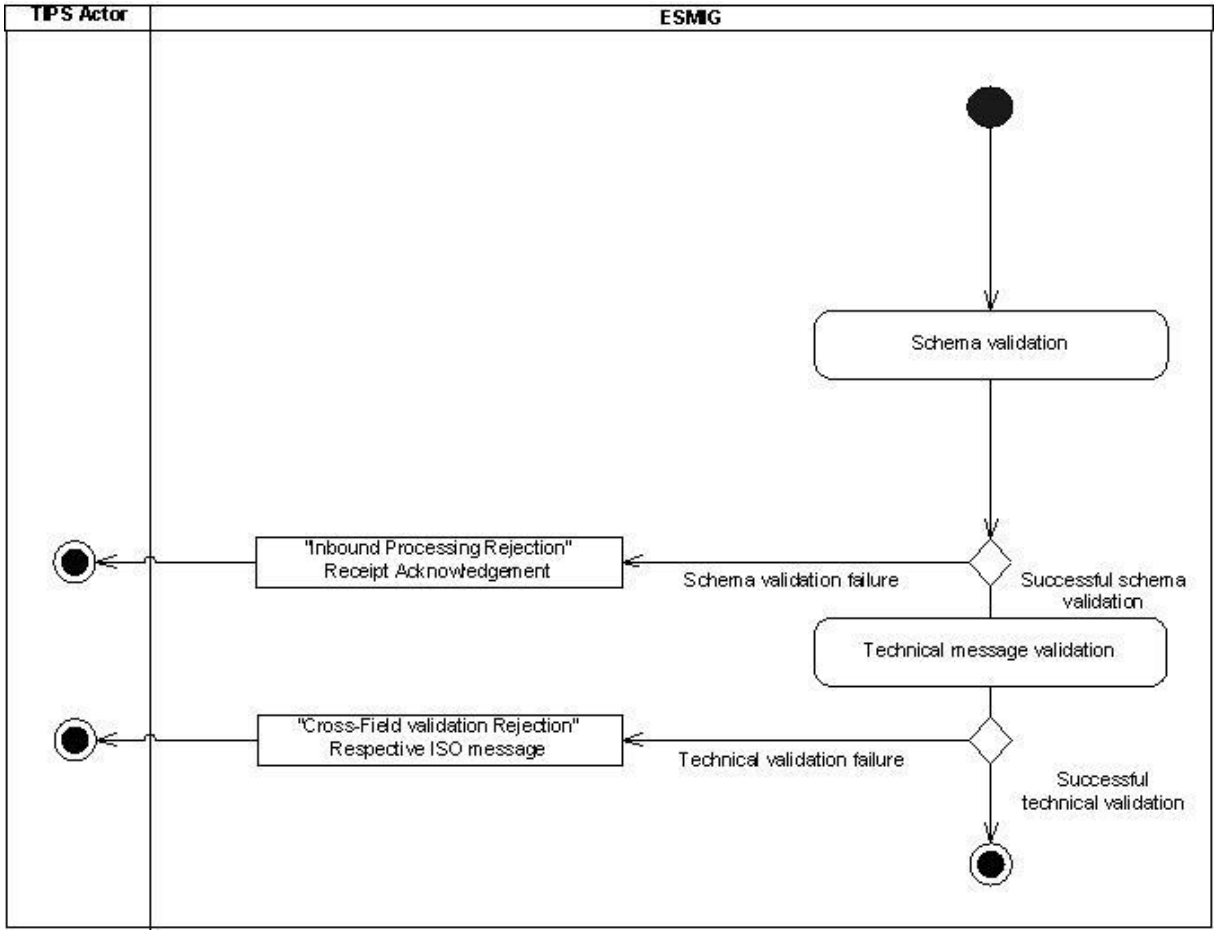
3.5.1 Introduction

The network infrastructure authenticates the technical sender and authorises the technical sender to connect to the relevant TARGET Service. Each A2A communication has to be encrypted and can be compressed. However, encryption and compression is handled on transport level by the NSP.

The activity diagram shown in Figure 3~~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.

All Rights reserved

Figure 3 – Activity diagram for TIPS



3.5.2 Schema validation

3.5.2.1 Schema validation for TARGET Services (excluding TIPS)

All ISO 20022 messages which reach ESMIG for further processing in any TARGET Services, excluding TIPS, (e.g. RTGS, CLM, etc.) are not subject to schema validation rules. This check is enforced by the Business Interface of the relevant Service/Component.

3.5.2.2 Schema validation for TIPS

All ISO 20022 messages which reach ESMIG for further processing in TIPS 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).

All Rights reserved

3.5.3 Technical message validation

3.5.3.1 Technical message validation for TARGET Services (excluding TIPS)

Besides the schema validation, the messages received by ESMIG may require some additional technical checks before they can be successfully forwarded to the TARGET service back-end. In the context of TARGET Service (excluding TIPS), these additional checks are enforced by the business interface of the relevant Service/Component. The aim of this check is the detection of potential inconsistencies in the format of the message, e.g. due to cross-field validation. Always with regards to all the TARGET services excluding TIPS, for non-registered ISO20022 messages (for which a DRAFT prefix is present in the XML namespace declaration) there is no need to specify the DRAFT prefix inside the BAH as well. For instance, whether the payload contains a DRAFT4camt.xyz message, the XML BAH field <MsgDefIdr> has to be filled in truncated, as camt.xyz.

3.5.3.2 Technical message validation for TIPS

3.5.3.2.1 Technical message validation for SCTInst scheme

In the business context of the EPC SCT^{Inst} scheme the additional technical message validation are executed by ESMIG and they 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 4~~Table 4~~ and 3.5.4.3 – ReceiptAcknowledgement (admi.007.001.01)

~~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 4 - Cross-field validations for SCT^{Inst} scheme

ISO Code	Field/Group	Check to be performed	X-Path	ERROR Code	Output message
pacs.002.001.10	Group Status Transaction Status	Neither group status nor transaction status has been specified	FIToFIPmtStsRpt/OrgnlGrpInfAndSts/GrpSts FIToFIPmtStsRpt/TxInfAndSts/TxSts	MS01	pacs.002.001.10
pacs.002.001.10	Group Status Transaction Status	Both group status and transaction status have been specified	FIToFIPmtStsRpt/OrgnlGrpInfAndSts/GrpSts FIToFIPmtStsRpt/TxInfAndSts/TxSts	MS01	pacs.002.001.10
pacs.002.001.10	Reason	The relevant StsRsnInf tag for a negative reply (RJCT) should have been specified	FIToFIPmtStsRpt/OrgnlGrpInfAndSts/StsRsnInf/Rsn/Cd	MS01	pacs.002.001.10
pacs.002.001.10	Reason	The relevant StsRsnInf tag for a negative reply (RJCT) should have been specified	FIToFIPmtStsRpt/TxInfAndSts/StsRsnInf/Rsn/Cd	MS01	pacs.002.001.10
pacs.004.001.09	Number Of Transactions	TIPS supports only one transaction per message. NbOfTxs (attribute tag) = 1	PmtRtr/GrpHdr/NbOfTxs	MS01	pacs.002.001.10
pacs.004.001.09	Original Group Information	The OrgnlGrpInf has not been specified neither at group nor at transaction level	PmtRtr/OrgnlGrpInf PmtRtr/TxInf/OrgnlGrpInf	MS01	pacs.002.001.10
pacs.004.001.09	Original Group Information	The OrgnlGrpInf has been specified both at group and at transaction level	PmtRtr/OrgnlGrpInf PmtRtr/TxInf/OrgnlGrpInf	MS01	pacs.002.001.10
pacs.004.001.09	Transaction Information	The xml message should contain exactly one TxInf tag	PmtRtr/TxInf	MS01	pacs.002.001.10
pacs.008.001.08	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.002.001.10
pacs.028.001.03	Original Message Name Identification Original Instruction Identification	Original Message Name Identification = "camt.056.001.01" or "camt.056.001.08", and Original Instruction Identification not specified.	FIToFIPmtStsReq/OrgnlGrpInf/OrgnlMsgNmId FIToFIPmtStsReq/TxInf/OrgnlInstrId	MS01	pacs.002.001.10

All Rights reserved

ISO CODE	Field/Group	Check to be performed	X-PATH	ERROR Code	Output message
pacs.028.001.03	Original Message Name Identification Creditor Agent	Original Message Name Identification = "camt.056.001.01" or "camt.056.001.08", and Creditor Agent not specified.	FIToFIPmtStsReq/OrgnlGrpInf/OrgnlMsgNmId FIToFIPmtStsReq/TxInf/OrgnlTxRef/CdtrAgt/FinInstnId/BICFI	MS01	pacs.002.001.10
pacs.028.001.03	Original Message Name Identification Creditor Agent	Original Message Name Identification = "camt.056.001.01" or "camt.056.001.08". Multiple instances of Transaction Information must have the same BIC as Creditor Agent.	FIToFIPmtStsReq/OrgnlGrpInf/OrgnlMsgNmId FIToFIPmtStsReq/TxInf/OrgnlTxRef/CdtrAgt/FinInstnId/BICFI	MS01	pacs.002.001.10
camt.050.001.07	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.025.001.0~~97~~
camt.050.001.07	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.025.001.0~~97~~
camt.050.001.07	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.025.001.0~~97~~ **{TIPS CR0097}**

3.5.3.2.2 Technical message validation for non-Euro currencies scheme

In the business context of non-Euro currencies scheme, the additional technical message validation are executed by ESMIG and they 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 5~~Table 5~~ and 3.5.4.3 – ReceiptAcknowledgement (admi.007.001.01)

~~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 5 - Cross Field validation for non-Euro currencies scheme

ISO Code	Field/Group	Check to be performed	X-Path	ERROR Code	Output message
pacs.002.001.10	Group Status Transaction Status	Neither group status nor transaction status has been specified	FIToFIPmtStsRpt/OrgnlGrpInfAndSts/GrpSts FIToFIPmtStsRpt/TxInfAndSts/TxSts	MS01	pacs.002.001.10
pacs.002.001.10	Group Status Transaction Status	Both group status and transaction status have been specified	FIToFIPmtStsRpt/OrgnlGrpInfAndSts/GrpSts FIToFIPmtStsRpt/TxInfAndSts/TxSts	MS01	pacs.002.001.10
pacs.002.001.10	Reason	The relevant StsRsnInf tag for a negative reply (RJCT) should have been specified	FIToFIPmtStsRpt/OrgnlGrpInfAndSts/StsRsnInf/Rsn/Cd	MS01	pacs.002.001.10
pacs.002.001.10	Reason	The relevant StsRsnInf tag for a negative reply (RJCT) should have been specified	FIToFIPmtStsRpt/TxInfAndSts/StsRsnInf/Rsn/Cd	MS01	pacs.002.001.10
pacs.004.001.09	Number Of Transactions	TIPS supports only one transaction per message. NbOfTxs (attribute tag) = 1	PmtRtr/GrpHdr/NbOfTxs	MS01	pacs.002.001.10
pacs.004.001.09	Original Group Information	The OrgnlGrpInf has not been specified neither at group nor at transaction level	PmtRtr/OrgnlGrpInf PmtRtr/TxInf/OrgnlGrpInf	MS01	pacs.002.001.10
pacs.004.001.09	Original Group Information	The OrgnlGrpInf has been specified both at group and at transaction level	PmtRtr/OrgnlGrpInf PmtRtr/TxInf/OrgnlGrpInf	MS01	pacs.002.001.10
pacs.004.001.09	Transaction Information	The xml message should contain exactly one TxInf tag	PmtRtr/TxInf	MS01	pacs.002.001.10
pacs.008.001.08	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.002.001.10

All Rights reserved

ISO Code	Field/Group	Check to be performed	X-Path	ERROR Code	Output message
pacs.028.001.03	Original Message Name Identification Original Instruction Identification	Original Message Name Identification = "camt.056.001.08" and Original Instruction Identification not specified.	FIToFIPmtStsReq/OrgnlGrpInf/OrgnlMsgNmId FIToFIPmtStsReq/TxInf/OrgnlInstrId	MS01	pacs.002.001.10
pacs.028.001.03	Original Message Name Identification Creditor Agent	Original Message Name Identification = "camt.056.001.08" and Creditor Agent not specified.	FIToFIPmtStsReq/OrgnlGrpInf/OrgnlMsgNmId FIToFIPmtStsReq/TxInf/OrgnlTxRef/CdtrAgt/FinInstnId/BICFI	MS01	pacs.002.001.10
pacs.028.001.03	Settlement Amount	The message should contain the IntrBkSttlmAmt	FIToFIPmtStsReq/TxInf/OrgnlTxRef/IntrBkSttlmAmt	MS01	pacs.002.001.10
camt.029.001.09	Interbank Settlement Amount	The message should contain the IntrBkSttlmAmt	RsltnOfInvstgtn/CxlDtls/TxInfAndSts/OrgnlTxRef/IntrBkSttlmAmt	MS01	pacs.002.001.10
camt.050.001.07	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.025.001.0~~97~~
camt.050.001.07	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.025.001.0~~97~~
camt.050.001.07	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.025.001.0~~97~~ **{TIPS CR0097}**

All Rights reserved

3.5.4 Inbound and Outbound messages

3.5.4.1 Inbound messages

No inbound message from any TARGET Service Actor is directly addressed to the ESMIG. All the successfully messages validated at transport level are routed to the related TARGET Service, common component or application.

3.5.4.2 Outbound Messages

3.5.4.2.1 Outbound Messages for TARGET Services (excluding TIPS)

Currently, one outbound message is generated by the ESMIG for all TARGET Services, excluding TIPS. The reasons for the rejection are due to:

- Invalid digital signature;
- Timeout management;
- Oversized management.

Table 6 - Outbound messages generated by ESMIG for TARGET Services (excluding TIPS)

ISO Message / Message Usage	ISO Code
ReceiptAcknowledgement / "Inbound Processing Rejections"	admi.007.001.01

Examples of the aforementioned use cases will be provided within the following two sub-sections.

3.5.4.2.2 Invalid digital signature

In the example 1 a ReceiptAcknowledgement referring to an incoming message with the ID INCOMINGMSG02 with "Invalid Digital Signature" is sent to the corresponding party.

Example 1:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Digital signature check of an incoming message was not successful-->
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:admi.007.001.01">
	<RctAck>
		<MsgId>
			<MsgId>NONREF</MsgId>
		</MsgId>
		<Rpt>
			<RltdRef>
				<Ref>INCOMINGMSG02</Ref>
			</RltdRef>
			<ReqHdlg>
```

```
                        <StsCd>I071</StsCd>
                        <Desc>ICSA010-Digital signature is not valid.</Desc>
                    </ReqHdlg>
                </Rpt>
        </RctAck>
</Document>
```

3.5.4.2.3 Timeout and oversized management

The ReceiptAcknowledgement message for TARGET Services is generated by ESMIG also in the two scenarios of (i) timeout management and (ii) oversized management.

In the example 2 a ReceiptAcknowledgement referring to an incoming message is sent to the corresponding party falling under the scope of “Timeout management”.

Example 2:

```
<?xml version="1.0" encoding="UTF-8"?>
<!–TARGET Service cannot respond to the query request within the timeout limit.-->
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:admi.007.001.01">
      <RctAck>
            <MsgId>
                  <MsgId>NONREF</MsgId>
            </MsgId>
            <Rpt>
                  <RltdRef>
                        <Ref>NONREF</Ref>
                  </RltdRef>
                  <ReqHdlg>
                  <StsCd>I074</StsCd>
                  <Desc>ICAA001 - The service cannot reply to the query request
                  within the timeout limit. Store and forward network service will
                  be used.
                  </Desc>
                  </ReqHdlg>
            </Rpt>
      </RctAck>
</Document>
```

In the example 3 a ReceiptAcknowledgement referring to an incoming message is sent to the corresponding party falling under the scope of “oversized management”.

Example 3:

```
<?xml version="1.0" encoding="UTF-8"?>
<!–TARGET Service cannot respond via message based network service due to size
restriction-->
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:admi.007.001.01">
      <RctAck>
            <MsgId>
                  <MsgId>NONREF</MsgId>
```

```
            </MsgId>
            <Rpt>
                  <RltdRef>
                        <Ref>NONREF</Ref>
                  </RltdRef>
                  <ReqHdlg>
                  <StsCd>I076</StsCd>
                  <Desc>ICAA002 - The service cannot reply via message network
                  service due to size restriction. File store and forward network
                  service will be used.
                  </Desc>
                  </ReqHdlg>
            </Rpt>
      </RctAck>
</Document>
```

3.5.4.2.4 Outbound Messages for TIPS

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 (i.e. pacs.002 and camt.025) in Table 7~~Table 7~~ are currently being described in the TIPS UDFS whereas the use case for Inbound Processing Rejections is described in section 3.5.4.3.2 (*Usage Case: TIPS ReceiptAcknowledgement*).

Table 7 - Outbound messages generated by ESMIG for TIPS

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.025.001.0~~97~~ **{TIPS CR0097}**

3.5.4.3 ReceiptAcknowledgement (admi.007.001.01)

This chapter illustrates the ReceiptAcknowledgement message.

The ReceiptAcknowledgement message (without BAH) is sent by ESMIG to the sender of a previous inbound. It is used to inform the sender that their previously sent message has been rejected and is not processed further. Within the ESMIG for TIPS this message is generated after an inbound processing rejection.

3.5.4.3.1 Schema

Outline of the schema

The ReceiptAcknowledgement message is composed of the following message building blocks:

MessageIdentification

This building block is mandatory and it contains the message identification generated by TIPS..

RelatedReference

This building block is mandatory and non-repetitive. It provides a reference of the request message to which this ReceiptAcknowledgement message is responding.

Report

This building block is mandatory and repetitive. Each block contains the Message identification of the request message and information related to a single validation issue.

RequestHandling

This building block is mandatory. It gives the status of the request. It may contain:

- status code;
- description.

References/links

The schema and the related documentation in XSD/EXCEL/PDF format as well as the message examples are provided within the MyStandards repository under the following link:

https://www.swift.com/mystandards/CoCo/admi.007.001.01

Business rules applicable to the schema

No business rules are applicable to a ReceiptAcknowledgement message

3.5.4.3.2 The message in business context

Usage Case: Timeout Management and Oversized Data Management

This usage case describes the case oversize and timeout scenario.

Specific message content

MESSAGE ITEM	UTILISATION
Related Reference Document/RctAck/Rpt/RltdRef/Ref	Reference of the incoming message. In case it cannot be identified: NONREF.
Status Code Document/RctAck/Rpt/ReqHdlg/StsCd	Status Code indicating the error. Possible values: - I074; - I076; - I077
Description Document/RctAck/Rpt/ReqHdlg/Desc	Description of the status

Usage case example: *admi.007OversizedAndTimeout_example.xml*

In this example a ReceiptAcknowledgement "Oversized limit" message to the corresponding party is sent, because the component cannot respond via message based network service due to size restriction.

Usage Case: TIPS ReceiptAcknowledgement

This usage case describes the case of admi.007 sent in the TIPS context.

Specific message content

MESSAGE ITEM	UTILISATION
Related Reference Document/RctAck/Rpt/RltdRef/Ref	If MEPT parameter MsgBizIdentifier of the incoming request is not empty, its value will be reported in this field. If the MsgBizIdentifier length exceeds the format of the field (i.e. greater than 35x), the string will be adapted to comply with the length defined at message level. Otherwise NONREF value will be used.
Status Code Document/RctAck/Rpt/ReqHdlg/StsCd	Status Code indicating the error. Possible values: 'X001' for schema validation error.
Description Document/RctAck/Rpt/ReqHdlg/Desc	For schema validation the description is 'Parsing error'

The ReceiptAcknowledgement message is sent by ESMIG to inform the sender that an incoming message has contained an error and resulted in a rejection, e.g. for missing authentication due to invalid signature.

The table below describes the message elements filled by ESMIG.

The ReceiptAcknowledgement message is used in this scenario to report that ESMIG is not able to process incoming message because of a failed authentication of the sending party due to invalid signature. For details on the error codes the reader can refer to section 4.2 - List of business rules and error codes

~~List of business rules and error codes~~

.

Specific message requirements

MESSAGE ITEM	DATA TYPE / CODE	UTILISATION
Reference Document/RctAck/Rpt/RltdRef/Ref	RestrictedFINXMax35Text	Related reference of the incoming message this ReceiptAcknowledgement is sent for
StatusCode Document/RctAck/Rpt/ReqHdlg/StsCd	Max4AlphaNumericText	Status Code indicating the error which occurred during the technical validation.
Description Document/RctAck/Rpt/ReqHdlg/Desc	RestrictedFINXMax140Text	Textual description of the technical validation error specified in the status code field.

The message examples for TIPS ReceiptAcknowledgement usage case are provided below. It is worth mentioning that the MsgId of the admi.007 is always generated by TIPS and it will have no connection with the MsgId of the incoming message, whose schema validation ended up with an error.

1) Scenario where the MEPT property value complies with the 35x length of the *Ref* field, e.g. MsgBizIdentifier= MsgBizID12345.

```
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:admi.007.001.01"
xmlns:xs="http://www.w3.org/2001/XMLSchema>
 <RctAck>
  <MsgId>
   <MsgId>MsgIDGeneratedByTIPS123</MsgId>
  </MsgId>
  <Rpt>
   <RltdRef>
    <Ref>MsgBizID12345</Ref>
   </RltdRef>
   <ReqHdlg>
    <StsCd>X001</StsCd>
    <Desc>Parsing error</Desc>
   </ReqHdlg>
  </Rpt>
 </RctAck>
</Document>
```

2) Scenario where the MEPT property value exceeds the 35x length of the *Ref* field, e.g. MsgBizIdentifier=MsgIDGeneratedByTheClient123456789ABCDEFGHILMNOPQRST.

In this scenario the *Ref* field will report only the first 35 characters of the related reference.

```
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:admi.007.001.01"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<RctAck>
  <MsgId>
   <MsgId>MsgIDGeneratedByTIPS123</MsgId>
  </MsgId>
  <Rpt>
   <RltdRef>
    <Ref>MsgIDGeneratedByTheClient123456789A</Ref>
   </RltdRef>
   <ReqHdlg>
    <StsCd>X001</StsCd>
    <Desc>Parsing error</Desc>
   </ReqHdlg>
  </Rpt>
</RctAck>
</Document>
```

All Rights reserved

3.5.5 Digital Signature managed within the business layer

The purpose of this signature is to authenticate the business sender and guarantee the integrity of the business payload. This business signature should be compliant with the W3C XAdES[9] standard.

The (NRO)[10] signature is stored in the BAH in case of individual messages or in the file header in case of messages grouped into a file. In case messages are grouped into a file, the BAH of the individual messages will not include a signature[11].

File (meaning multi-message):

The signature is part of the file header. It is over the list of BAH's and ISO 20022 messages and covers the whole <XChg> element of the Business File header (head.002), except for the signature itself.

Single message:

The signature is over the ISO 20022 message and takes into account the business processing relevant information specified within the BAH (e. g. pair of BICs for definition of the instructing party), except for the signature itself. The digital signature grouped in the BAH itself is not part of this signature calculation.

Further details referring the Digital Signature construction on Business Layer can be retrieved from the Annex 4.1 - Digital Signature on Business Layer

~~Digital Signature on Business Layer~~

.

3.5.6 Routing

The ESMIG routing functions are related to both inbound and outbound traffic. In this context ESMIG is able to route messages/files (i) to the addressed service/component for inbound traffic and (ii) to NSPs and network channel for outbound traffic.

3.5.6.1 Inbound Routing

ESMIG is in charge of managing the provision of messages and files received from the NSPs to each different TARGET service (excluding TIPS), component or application.

The ESMIG identifies and selects the appropriated TARGET service (excluding TIPS), component or application on the basis of information provided as part of the communication. In this respect, an enhancement of the Data Exchange Protocol (DEP) is required to transport supplementary information to infer whether the target of the inbound communication is a market infrastructure service, a common component or a specific component.

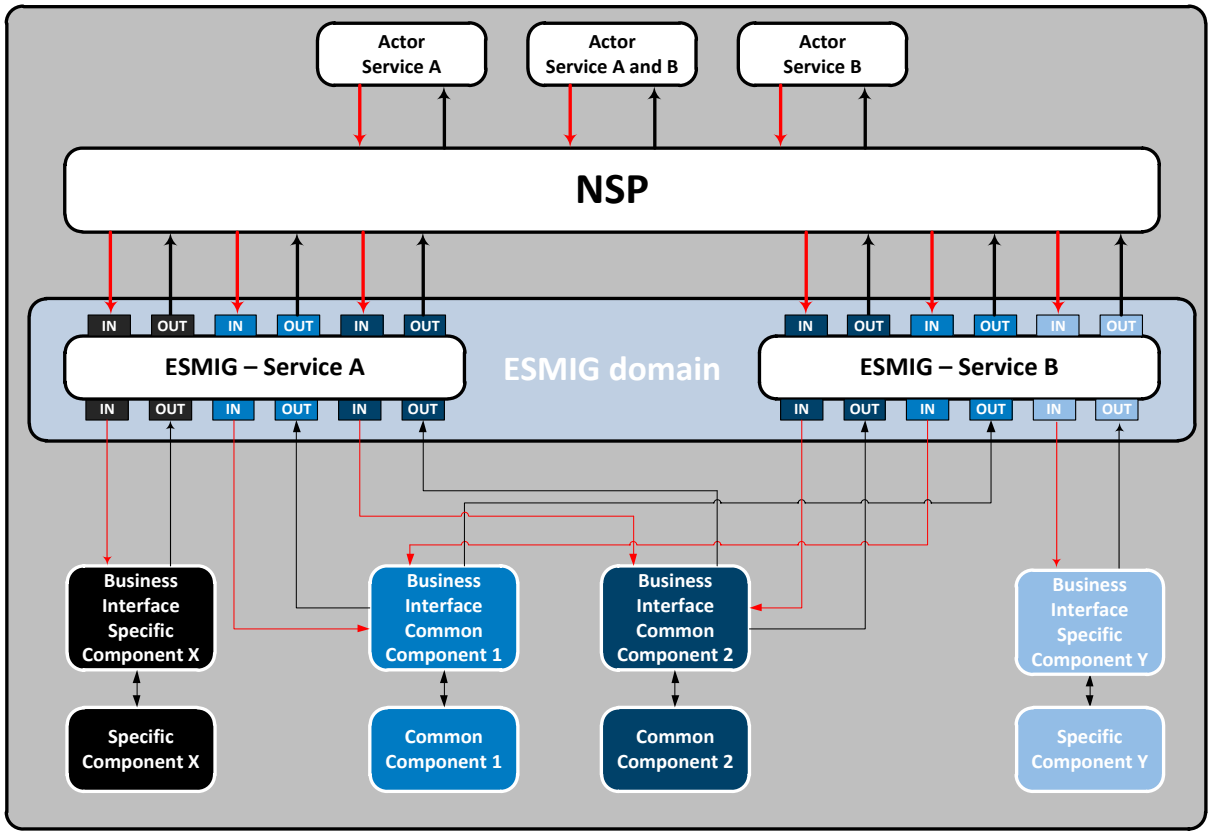
[9] The XML Advanced Electronic Signatures is a W3C note which extends the [XMLDSIG] specification into the domain of non-repudiation by defining XML formats for advanced electronic signatures that remain valid over long periods and are compliant with the European "Directive 1999/93/EC of the European Parliament.

[10] Non-repudiation of origin is intended to protect against the originator's false denial of having sent the message.

[11] For TARGET services making use of DEP and BAH, BAH and payload shall be included into the DEP envelope following the indications provided to their customers by each NSP

Furthermore, ESMIG passes to the business interface of the relevant TARGET service (excluding TIPS), component or application, the distinguished name (DN) of the sender (as result of the authentication process) and a predefined list of parameters.

Figure 4 – Inbound Routing



The interface between Eurosystem Market Infrastructure counterparties and the NSP is defined by the relevant NSP protocol documentation (DEP protocol is used only between NSP and the ESMIG). In this context, the NSP interface shall ensure that at least a minimum set of information is provided by the counterparties to be compliant with the DEP protocol.

Table 8 - TARGET Services, components and applications[12]

Business Service	Component	Communication mode and protocol
T2	CLM	**A2A**: MSGSNF, MSGRT, FILESNF, FILERT **U2A**
T2	RTGS	**A2A**: MSGSNF, MSGRT, FILESNF, FILERT **U2A**
T2	CRDM	**A2A**: MSGSNF, MSGRT, FILESNF, FILERT **U2A**

[12] The table shows a non-exhaustive list of components addressable via ESMIG.

Business Service	Component	Communication mode and protocol
T2	ECONS II	**A2A**: MSGSNF, FILESNF **U2A**
T2	DWH	**A2A**: FILESNF **U2A**
ECMS	ECMS	**A2A**: MSGSNF, MSGRT, FILESNF, FILERT **U2A**
T2S	T2S	**A2A**: MSGSNF, MSGRT, FILESNF, FILERT **U2A**
T2S	CRDM	**A2A**: MSGSNF, MSGRT, FILESNF, FILERT **U2A**
TIPS	TIPS	**A2A**: Instant messaging **U2A**
TIPS	CRDM	**A2A**[13]: MSGSNF, MSGRT, FILESNF, FILERT **U2A**

3.5.6.2 Outbound Routing

The ESMIG routes messages and files to the external party using:

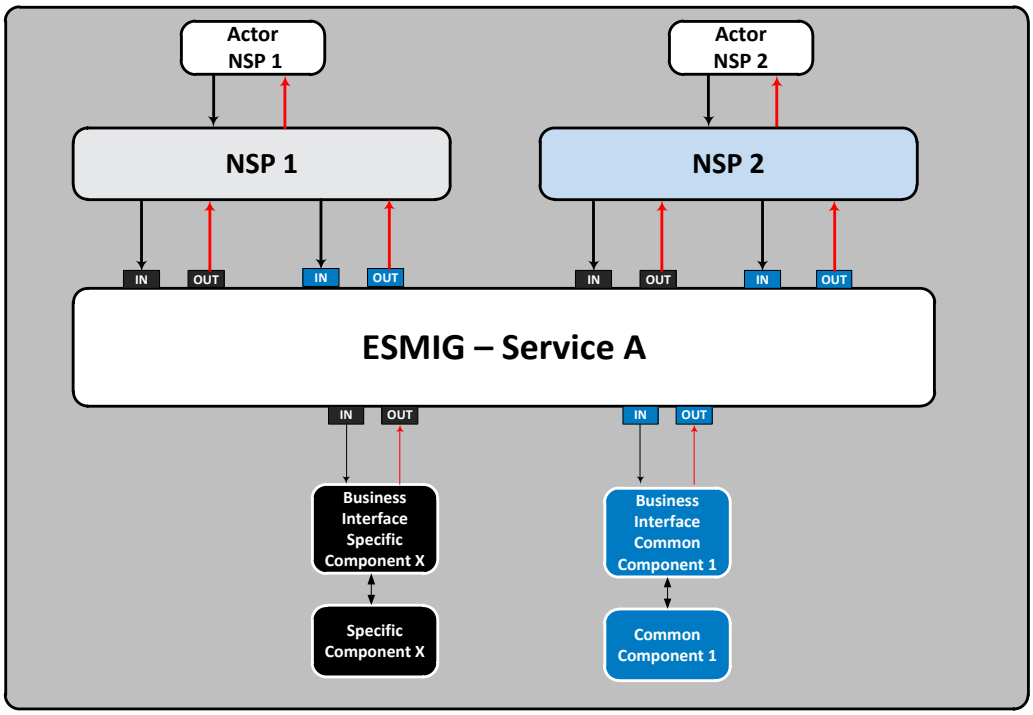
- the network provider,
- the address used by the NSP to identify the external party,
- the communication mode,
- the protocol.

The above mentioned information is provided by the TARGET service (excluding TIPS), component or application (i.e. right external user address) to the ESMIG.

[13] The technical connectivity solution provided by ESMIG at the TIPS go-live did not cover the full scope of connectivity services foreseen for the go-live of T2-T2S Consolidation. In particular, A2A connectivity towards the fully-fledged CRDM will only be available as of 2022.

All Rights reserved

Figure 5 – Outbound Routing



4 Annexes

4.1 Digital Signature on Business Layer

4.1.1 Mechanism and Introduction for signature constructions

This Annex outlines how signatures are constructed for the Business messages. The following business message types have been identified:

- Message Type 1: File with multiple ISO 20022 messages;
- Message Type 2: Single ISO20022 Business Application Header and message.

The design goal for the proposed construction of signatures in the following sections is that as much as possible is handled by standard XML Digital Signature processing specifications and as little as possible by specific processing. This makes it less likely that errors and/or discrepancies occur in the different implementations, and therefore improve the overall security of the solution.

This annex does not apply to the TIPS service.

4.1.2 Use of XML and canonicalization algorithm

Exclusive XML canonicalization[14] has to be performed for above mentioned business messages on extracted data. It is important to ensure a context free extraction otherwise the signatures will be broken if either the message or the signature itself is modified due to inherited namespaces.

This implies that the canonicalization algorithm specified in the SignedInfo element and in all the references should be in line with following information:

http://www.w3.org/2001/10/xml-exc-c14n#

4.1.3 Message Type 1: File with multiple ISO 20022 messages

For message type 1) the requirement in the UDFS section 3.5.5 – "Digital Signature managed within the business layer" states:

> *"The NRO[15] signature is stored in the BAH in case of individual messages or in the file header in case of messages grouped into a file. In case messages are grouped into a file, the BAH of the individual messages will not include a signature.*
>
> *File (meaning multi-message):*
>
> *The signature is part of the file header. It is over the list of BAH's and ISO 20022 messages and covers the whole <XChg> element of the Business File (head.002), except for the signature itself."*

[14] Exclusive XML Canonicalization http://www.w3.org/TR/xml-exc-c14n/

[15] Non-repudiation of origin is intended to protect against the originator's false denial of having sent the message.

The signature, in particular, covers the whole BusinessFileHeader <XChg> element, except for the signature itself. So consequently, the following field will be not taken into account for Signature calculation:

Xchg/PyldDesc/ApplSpcfcInf/Sgntr/ds:Signature[16]

Hence, a signature will then be constructed as follows:

- One reference (in blue below) points out the XChg itself. This is done using the same document reference URI = "", which means the entire document. To leave the signature element itself out of the digest calculation, the transform "#enveloped-signature" is used.
- One reference (in yellow below) points to the KeyInfo element of the signature itself. This is a XAdES[17] requirement.

[16] Due to the XAdES requirement the ds:KeyInfo element inside the ds:Signature is covered/protected by the signature.

[17] ETSI TS 101 903 V1.4.2 (2010-12) XML Advanced Electronic Signatures

1) A Message Type 1[18] signature example is reported in the below picture:

```
<ds:Signature Id="_8aaee938-014d-489e-a385-b72155000474" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <ds:Reference URI="">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>GUTJy22YxtDXe7yEvdYfJ/GYM+pGH4h5dgWe7c+2gXU=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#_4eaf74f7-086b-410e-b214-45136a615bac">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>8GepFqO0h78WgVHh23B16RFQRWhdfM6AjY+b0texoSk=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>QzvbmDLi8Q1PnsfKz...HNgew=</ds:SignatureValue>
  <ds:KeyInfo Id="_4eaf74f7-086b-410e-b214-45136a615bac">
    <ds:X509Data>
      <ds:X509Certificate>MIIEXTCCA8ag...IY5uXkO3IGZ3XUsw=</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
```

Reference to the whole document, less the signature

Reference to KeyInfo (a XAdES requirement)

Reference to the message (head.002):

```
<Xchg xmlns="urn:iso:std:iso:20022:tech:xsd:head.002.001.01">
      <PyldDesc>
            <PyldDtls>
                  <PyldIdr>FILEREF1</PyldIdr>
                  <CreDtAndTm>2014-12-17T09:30:47Z</CreDtAndTm>
            </PyldDtls>
            <ApplSpcfcInf>
                  <SysUsr>SystemUserX1</SysUsr>
                  <Sgntr>...</Sgntr>
                  <TtlNbOfDocs>1</TtlNbOfDocs>
            </ApplSpcfcInf>
            <PyldTpDtls>
                  <Tp>ISO20022</Tp>
            </PyldTpDtls>
            <MnfstDtls>
                  <DocTp>camt.003.001.05</DocTp>
                  <NbOfDocs>1</NbOfDocs>
            </MnfstDtls>
      </PyldDesc>
      <Pyld>
            <BizData xmlns="urn:iso:std:iso:20022:tech:xsd:head.003.001.01">
                  <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">...</AppHdr>
                  <Document xmlns="urn:swift:xsd:DRAFT7camt.003.001.05">...</Document>
            </BizData>
      </Pyld>
</Xchg>
```

2) A Message Type 1 structure example (including signature) is provided in XML format as described below:

```
<?xml version="1.0" encoding="UTF-8"?>
 <Xchg xmlns="urn:iso:std:iso:20022:tech:xsd:head.002.001.01">
  <PyldDesc>
   <PyldDtls>
    <PyldIdr>FILEREF1</PyldIdr>
     <CreDtAndTm>2014-12-17T09:30:47Z</CreDtAndTm>
   </PyldDtls>
   <ApplSpcfcInf>
    <SysUsr> SystemUserX1</SysUsr>
```

[18] ESMIG digital signature services are configured to produce and generate rsa-sha256 signatures, and use sha256 digest.

```
    <Sgntr>
     <ds:Signature Id="_8af629dd-bb2c-4207-b0b4-c3edb7d17444"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
       <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
         <ds:Reference URI="#_f6fa91c7-ee9f-4702-8f08-820bd7a86ac2">
          <ds:Transforms>
           <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>wFOmYpRxS6RAOxOdrlZKfmV3Tza4jVWW8Afg0efdogU=</ds:DigestValue>
         </ds:Reference>
         <ds:Reference URI="">
          <ds:Transforms>
           <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
           <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
         <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>LQSkT1Mksb6iSiyqwCmAAs/ZKd9NkwI068Kukx9JP/U=</ds:DigestValue>
         </ds:Reference>
       </ds:SignedInfo>
<ds:SignatureValue>rLCX6pUzTEYGAHMNu/NczFwbXVgncgVsjmhCNNNsXjbU8CqJeytFM3XJFvPocqq
TX2ZsPg+GAE89xFBb2xe7j8Z1mgTwEEuU3uvofKjN7Lo4ZnIaUQxPUBStY6cp7K+YtAwQ31bfq2a/mWPQb
b0C5fUsCwrn/Nxf/6q6PpO+MiMWbWOj4mgFnkqv3pFvhmFPPWC1AuReS/RMLjZrGYVSBiBgxkv71D7ijTb
bbZJzWfwlHK0z7fdzIA1OwUzi+9mst858kIEcVX7QhbBdK8PxBSvRGau1lbMIGlRHWEE9fgN6y15rSvpfR
ODewUS1GU+LgV9SuL3g+GxpWhYT5+MJ/A==</ds:SignatureValue>
       <ds:KeyInfo Id="_f6fa91c7-ee9f-4702-8f08-820bd7a86ac2">
        <ds:X509Data>
<ds:X509Certificate>MIID0DCCArigAwIBAgIBBTANBgkqhkiG9w0BAQsFADBMMQswCQYDVQQGEwJGUj
EcMBoGA1UECgwTS2V5bmVjdGlzLU9wZW5UcnVzdDEfMB0GA1UEAwwWT3BlblRydXN0IFRlc3QgQ0EgU0hB
MjAeFw0xMjExMTUwMDU3MzVaFw0xNDExMTUwMDU3MzVaMFgxCzAJBgNVBAYTAklUMQ8wDQYDVQQKDAZPIF
RFU1QxEjAQBgNVBAsMCU9VIFRFU1QgMjESMBAGA1UECwwJT1UgVEVTVCAxMRAwDgYDVQQDDAdUZXN0IENO
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtnB/1lzFO5cVqDIlzQJRsZZh9TK7AhlnxxnR2E
P1hRnP7GRnnksqyYMJECiL/4NnTEhftQe7AGSaWeX7xOsGHJGd72NwmFQazVjHyaT8XSxaxUoG4kclF5Qa
DOvvxUAHTtM2qYNjpqFyKkTGbA5D7IqS36zTBYawCE40k9hU2/pvInG3jiKA60U4of9oqEQe4+hW2IxkN0
1mRmxPunKYoZWVn3ggL/QQlH/yggkBdpLG2qmIUmO9cvyVdycABW+5R56NyR42xVRcb56rvI5Qcbnbsrvk
cbmslGdo/qnKvxcthXstt3TqGq+kZ1CIHDoJsF8ZDQKuIjXMEgsurt/OHQIDAQABo4GwMIGtMB0GA1UdDg
QWBBRsJehOf8/tO6YtFO4hEYcc1C0zoTAfBgNVHSMEGDAWgBRRcv9bAGffzbqlTCZ0MpE7ji+fpTARBglg
hkgBhvhCAQEEBAMCB4AwDgYDVR0PAQH/BAQDAgbAMEgGA1UdHwRBMD8wPaA7oDmGN2h0dHA6Ly9wa2l0ZX
N0Lm9wZW50cnVzdC5jb20vT3BlblRydXN0X1Rlc3RfQ0FfU0hBMi5jcmwwDQYJKoZIhvcNAQELBQADggEB
AGMAu3Yo2Z9Ff1FLX/DHVcw8T5otZlaYtJiHdYcEtvhjY24vcXJzwBuHbfopVu91XZFuxXjG12SSyksK4s
RHfUVPQdryAMGzMUW+OgjVFjupV54jr6vkaELq2t6oyE52CHqvvlHyLJz5CIW6jDEmAzGNJZ2wdRr4fu9z
M2lm4X5JITsZGxY/JHO2fll55QJuVn7NSfFx8PxRsIKYNZ+Z7kczNTSL9zDwYXob5PUBv6OfXMhWPJtngz
8OI8NGqDVQIjtnbgcsSgDchRMVy4JOUb8UK7RAJpG4aR/5RKaMk06DLHXJteXfmsKfLyDq3H8B+eHgfJJW
CeYMnvqk755EVNE=</ds:X509Certificate>
        </ds:X509Data>
       </ds:KeyInfo>
      </ds:Signature>
     </Sgntr>
     <TtlNbOfDocs>1</TtlNbOfDocs>
    </ApplSpcfcInf>
    <PyldTpDtls>
```

```
    <Tp>ISO20022</Tp>
   </PyldTpDtls>
   <MnfstDtls>
    <DocTp>camt.003.001.05</DocTp>
    <NbOfDocs>1</NbOfDocs>
   </MnfstDtls>
   </PyldDesc>
  <Pyld>
  <BizData xmlns="urn:iso:std:iso:20022:tech:xsd:head.003.001.01">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.04">
    <Fr>
     <FIId>
      <FinInstnId>
       <BICFI>CSDPARTCPNT</BICFI>
       <Othr>
        <Id>CSDBICIDXXX</Id>
       </Othr>
      </FinInstnId>
     </FIId>
    </Fr>
    <To>
     <FIId>
      <FinInstnId>
       <BICFI>SYSTEMIDT2S</BICFI>
       <Othr>
        <Id>CSDBICIDXXX</Id>
       </Othr>
      </FinInstnId>
     </FIId>
    </To>
    <BizMsgIdr>REF3 </BizMsgIdr>
    <MsgDefIdr>camt.003.001.08</MsgDefIdr>
    <CreDt>2014-12-17T09:30:47Z</CreDt>
   </AppHdr>
   <Document xmlns="urn:swift:xsd:camt.003.001.08">
    <GetAcct>
     <MsgHdr>
      <MsgId>REF3</MsgId>
      <ReqTp>
       <Prtry>
        <Id>CASB</Id>
       </Prtry>
      </ReqTp>
     </MsgHdr>
     <AcctQryDef>
      <AcctCrit>
       <NewCrit>
        <SchCrit>
        <AcctId>
          <EQ>
           <Othr>
            <Id>T2SDEDICATEDCASHACCOUNT1</Id>
           </Othr>
          </EQ>
         </AcctId>
         <Ccy>EUR</Ccy>
         <AcctOwnr>
          <FinInstnId>
```

```
            <BIC>ACCTOWNRXXX</BIC>
           </FinInstnId>
          </AcctOwnr>
          <AcctSvcr>
           <FinInstnId>
            <BIC>ACCTSVCRXXX</BIC>
           </FinInstnId>
          </AcctSvcr>
         </SchCrit>
        </NewCrit>
       </AcctCrit>
      </AcctQryDef>
     </GetAcct>
    </Document>
   </BizData>
  </Pyld>
</Xchg>
```

4.1.4 Message Type 2: single ISO 20022 message19

For message type 2) the requirement in UDFS section 3.5.5 – "Digital Signature managed within the business layer~~Digital Signature managed within the business layer~~" states:

> *"Single message: The signature is over the ISO 20022 message and takes into account the business processing relevant information specified within the BAH (e. g. pair of BICs for definition of the instructing party), except for the signature itself. The digital signature grouped in the BAH itself is not part of this signature calculation."*

So consequently, the following field will be not taken into account for Signature calculation:

AppHdr/Sgntr/ds:Signature[20]

In this case the BAH and the ISO 20022 message are considered not to be in the same document.

> *"Technically speaking, the Application Header is a separate XML document standing apart from the XML documents which represent the business message instance itself."*

Since the documents that are referenced do not carry an ID attribute[21] that could be used for identifying the specific document, it has been decided to use a specific reference for the business message, ESMIG ensures that the BAH and the corresponding ISO message are always stored together.

TARGET Service Specific Reference for document signature

In the XML Digital Signature standard there is the possibility to use a reference with no URI i.e. omitting the URI attribute entirely. However, there can be at most one such reference in a signature, and handling of it is specific, and not covered by the XML Digital Signature standard[22]. Hence, the reference to the message must be given by the context and known by the application.

The signature will then be constructed as follows:

[19] See also MUG (Message user guide) for BAH; http://www.iso20022.org/bah.page

[20] Due to the XAdES requirement the ds:KeyInfo element inside the ds:Signature is covered/protected by the signature.

[21] ISO20022 do not support and specify an ID attribute, that can be used to uniquely identify BAH and ISO message.

[22] XML Signature Syntax and Processing (Second Edition), W3C Recommendation 10 June 2008, "http://www.w3.org/TR/xmldsig-core/"

- One reference (in blue below) points out the BAH (AppHdr) itself. This is done using the same document reference URI = "", which means the entire document. To leave the signature element itself out of the digest calculation, the transform"#enveloped-signature" is used;
- One reference (in green below) is application specific and refers to the business message (no URI). The application will provide the signature API with the relevant message. The signature API is customized to resolve the no URI reference to this message;
- One reference (in yellow below) points to the KeyInfo element of the signature itself (XAdes requirements).

1) A message type 2[23] signature example (with application specific reference) is reported in the below picture:

```
<ds:Signature Id="_003adca5-654a-473d-b1cf-3e826cd5d3f7" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <ds:Reference URI="">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>Ffg8hActTHIR9tyj8BOP2/7FMyECb9wb7CKQvhG5z/A=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference>
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>hEXN3t4KgQt2fkJf7WH4xgg/21cKPaAUnfDII7vIdoQ=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#_05dda060-fd01-4538-9db0-56c8e5d3dfc1">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>bcF4Ty77sjsGLXSd5YbSQqJijbwy4RRbJxh8zPEFbco=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>FtlF0n3hzk5Y78Tm/...newuw=</ds:SignatureValue>
  <ds:KeyInfo Id="_05dda060-fd01-4538-9db0-56c8e5d3dfc1">
    <ds:X509Data>
      <ds:X509Certificate>MIIEXTCCA8ag...IY5uXkO3IGZ3XUsw=</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
```

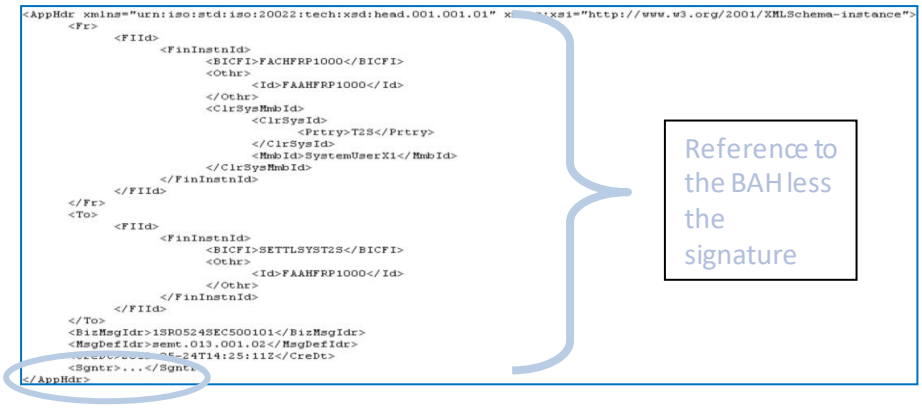
Reference to the BAH, less the signature

Application specific Reference (to the message)

Reference to KeyInfo (a XAdES requirement)

General remark: The signature is over the ISO 20022 message and takes into account the business processing relevant information specified within the Message Header (BAH), except the signature itself. The Digital Signature in the BAH itself is NOT part of this signature calculation.

Reference to the BAH (AppHdr):



[23] ESMIG digital signature services are configured to produce and generate rsa-sha256 signatures, and use sha256 digest.

Reference to the message (e.g. semt.013):



2) A Message Type 2 structure example[24] (including signature) is provided in XML format as described below:

```
<?xml version="1.0" encoding="UTF-8"?>
<AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.04">
 <Fr>
  <FIId>
   <FinInstnId>
    <BICFI>CSDPARTCPNT</BICFI>
    <ClrSysMmbId>
     <ClrSysId>
      <Prtry>T2S</Prtry>
     </ClrSysId>
     <MmbId>SystemUserX1</MmbId>
    </ClrSysMmbId>
    <Othr>
     <Id>CSDBICIDXXX</Id>
    </Othr>
   </FinInstnId>
  </FIId>
 </Fr>
 <To>
  <FIId>
   <FinInstnId>
    <BICFI>SETTLSYST2S</BICFI>
    <Othr>
     <Id>CSDBICIDXXX</Id>
    </Othr>
   </FinInstnId>
  </FIId>
 </To>
 <BizMsgIdr>SENDERSREFERENCE</BizMsgIdr>
 <MsgDefIdr>sese.023.001.11</MsgDefIdr>
 <CreDt>2015-01-02T09:30:47Z</CreDt>
 <Sgntr>
  <ds:Signature Id="_be4dd7de-c63a-43a6-9b62-f69290939eb6"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

[24] BAH and payload are not encapsulated in an xml envelope at T2/Common component level. Each NSP will inform their customers how to group them.

```
   <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
    <ds:Reference URI="#_98742d60-2afc-4fa7-a731-828756ce47b1">
     <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     </ds:Transforms>
     <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
     <ds:DigestValue>vB/xxu+qkEVUH5i9uVdBHOXOp6+XDsAn/iHxH+UiMGo=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="">
     <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     </ds:Transforms>
     <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
     <ds:DigestValue>hWGkHPu5IMYxe4KFYyaMOFWYq0w2pi+BYnYvHEwm/Z8=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference>
     <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     </ds:Transforms>
     <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
     <ds:DigestValue>10eHeNdJM1v177M0HzFsmP0IBMYvdPXVuRcR77hAgUg=</ds:DigestValue>
    </ds:Reference>
   </ds:SignedInfo>
<ds:SignatureValue>HllitYLicuu5drRrzu5CFxk5GZ3LD00nEPCrXkfWiu54y0zA3P2r6AIe1cYIdue
Y8nioLEvcZcvKVS4zt6bbHv8RRaWmU+Jfl3x4vTH5g8W6RY10LPErRbTNcn9r3Nb/hxeBj6Rztv3vR+gW+
JY2ly3pkTIAb8OJhQ9kcauarcwqG6MAWM3UjK31j796Ldi7ddvHohgW1qHXzdidBfcONatYnIXZrw/77DU
nBecimz4yqJvCo1Sri1asC0LHFdbeudgBivJtQ/CDl/So9Mkrw6VNUXohv5L3i3J3fNI9gmM1oC/ZJGL1H
LfOsyJ7GokRsypdlYWFQvNNhu1OupanRA==</ds:SignatureValue>
   <ds:KeyInfo Id="_98742d60-2afc-4fa7-a731-828756ce47b1">
    <ds:X509Data>
<ds:X509Certificate>MIID0DCCArigAwIBAgIBBTANBgkqhkiG9w0BAQsFADBMMQswCQYDVQQGEwJGUj
EcMBoGA1UECgwTS2V5bmVjdGlzLU9wZW5UcnVzdDEfMB0GA1UEAwwWT3BlblRydXN0IFRlc3QgQ0EgU0hB
MjAeFw0xMjExMTUwMDU3MzVaFw0xNDExMTUwMDU3MzVaMFgxCzAJBgNVBAYTAklUMQ8wDQYDVQQKDAZPIF
RFU1QxEjAQBgNVBAsMCU9VIFRFU1QgMjESMBAGA1UECwwJT1UgVEVTVCAxMRAwDgYDVQQDDAdUZXN0IENO
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtnB/1lzFO5cVqDIlzQJRsZZh9TK7AhlnxxnR2E
P1hRnP7GRnnksqyYMJECiL/4NnTEhftQe7AGSaWeX7xOsGHJGd72NwmFQazVjHyaT8XSxaxUoG4kclF5Qa
DOvvxUAHTtM2qYNjpqFyKkTGbA5D7IqS36zTBYawCE40k9hU2/pvInG3jiKA60U4of9oqEQe4+hW2IxkN0
1mRmxPunKYoZWVn3ggL/QQlH/yggkBdpLG2qmIUmO9cvyVdycABW+5R56NyR42xVRcb56rvI5Qcbnbsrvk
cbmslGdo/qnKvxcthXstt3TqGq+kZ1CIHDoJsF8ZDQKuIjXMEgsurt/OHQIDAQABo4GwMIGtMB0GA1UdDg
QWBBRsJehOf8/tO6YtFO4hEYcc1C0zoTAfBgNVHSMEGDAWgBRRcv9bAGffzbqlTCZ0MpE7ji+fpTARBglg
hkgBhvhCAQEEBAMCB4AwDgYDVR0PAQH/BAQDAgbAMEgGA1UdHwRBMD8wPaA7oDmGN2h0dHA6Ly9wa2l0ZX
N0Lm9wZW50cnVzdC5jb20vT3BlblRydXN0X1Rlc3RfQ0FfU0hBMi5jcmwwDQYJKoZIhvcNAQELBQADggEB
AGMAu3Yo2Z9Ff1FLX/DHVcw8T5otZlaYtJiHdYcEtvhjY24vcXJzwBuHbfopVu91XZFuxXjG12SSyksK4s
RHfUVPQdryAMGzMUW+OgjVFjupV54jr6vkaELq2t6oyE52CHqvvlHyLJz5CIW6jDEmAzGNJZ2wdRr4fu9z
M2lm4X5JITsZGxY/JHO2fll55QJuVn7NSfFx8PxRsIKYNZ+Z7kczNTSL9zDwYXob5PUBv6OfXMhWPJtngz
8OI8NGqDVQIjtnbgcsSgDchRMVy4JOUb8UK7RAJpG4aR/5RKaMk06DLHXJteXfmsKfLyDq3H8B+eHgfJJW
CeYMnvqk755EVNE=</ds:X509Certificate>
    </ds:X509Data>
   </ds:KeyInfo>
  </ds:Signature>
 </Sgntr>
</AppHdr>
```

```
<Document xmlns:xs="http://www.w3.org/2001/XMLSchema"
          xmlns="urn:iso:std:iso:20022:tech:xsd:sese.023.001.11">
  <SctiesSttlmTxInstr>
   <TxId>REFABCD</TxId>
   <SttlmTpAndAddtlParams>
    <SctiesMvmntTp>DELI</SctiesMvmntTp>
    <Pmt>APMT</Pmt>
   </SttlmTpAndAddtlParams>
   <TradDtls>
    <TradDt>
     <Dt>
      <Dt>2015-01-02</Dt>
     </Dt>
    </TradDt>
    <SttlmDt>
     <Dt>
      <Dt>2015-01-03</Dt>
     </Dt>
    </SttlmDt>
   </TradDtls>
   <FinInstrmId>
    <ISIN>ISIN00000001</ISIN>
   </FinInstrmId>
   <QtyAndAcctDtls>
    <SttlmQty>
     <Qty>
      <Unit>100000</Unit>
     </Qty>
    </SttlmQty>
    <SfkpgAcct>
     <Id>1000000123</Id>
    </SfkpgAcct>
    <CshAcct>
     <Prtry>9000000123</Prtry>
    </CshAcct>
   </QtyAndAcctDtls>
   <SttlmParams>
    <Prty>
     <Nmrc>0003</Nmrc>
    </Prty>
    <SctiesTxTp>
     <Cd>TRAD</Cd>
    </SctiesTxTp>
    <PrtlSttlmInd>PART</PrtlSttlmInd>
    <ModCxlAllwd>
     <Ind>true</Ind>
    </ModCxlAllwd>
   </SttlmParams>
   <RcvgSttlmPties>
    <Dpstry>
     <Id>
      <AnyBIC>CSDBICIDXXX</AnyBIC>
     </Id>
    </Dpstry>
    <Pty1>
     <Id>
      <AnyBIC>CSDBICIDXXX</AnyBIC>
     </Id>
```

```
    </Pty1>
   </RcvgSttlmPties>
   <SttlmAmt>
    <Amt Ccy="EUR">575000</Amt>
    <CdtDbtInd>CRDT</CdtDbtInd>
   </SttlmAmt>
  </SctiesSttlmTxInstr>
</Document>
```

4.1.5 ESMIG digital signature services

Usage of block “Object”:

In message type 1 and 2 the ds:Object element is not used when constructing the signature. The ESMIG digital signature API (Application Programming Interface) follows standard XML Signature Processing which defines what happens when a ds:Object element is encountered:

- If the ds:Object (or its content) is referenced in ds:SignedInfo, then the API will verify this reference as part of the signature verification;
- If the ds:Object is not referenced in ds:SignedInfo, then the API will ignore it, when performing the cryptographic check of the signature.

However if the ds:Object contains e.g. XAdES Qualifying properties, these will be examined in order to determine the signature format, I.e. is the signature a XAdES-BES or XAdES-T or XAdES-C.

ESMIG recommendation is to not use in message type 1 and 2 the ds:Object element.

Usage of Attribute ID of the block “Signature”:

ESMIG will generate the ID attribute of the Signature element when building a signature to be sent to counterparts. The ID attribute is optional for signatures sent to ESMIG. If present the value of the ID attribute must be an underscore (”_”) followed by a universally unique identifier (UUID), that is either time-based (UUID version 1) or random (UUID version 4). The UUID generating system is responsible for ensuring that all the UUID's in a single document are unique.

Usage of block “KeyInfo”:

The XAdES standard allows two different methods to comply with the XAdES-BES requirement. In ESMIG signature services implementation it has been decided to use the one that includes the signer certificate in the KeyInfo element:

- Element KeyInfo must be present and must include the ds:X509Data/ds:X509Certificate containing the signing certificate.
- The ID attribute on the KeyInfo element is mandatory and the value of the ID attribute must be a underscore (”_”) followed by a universally unique identifier (UUID), that is either time-based (UUID version 1) or random (UUID version 4).
- The SignedInfo element must reference the KeyInfo element using the ID attribute.

Usage of the alternative

ds:Object/QualifyingProperties/SignedProperties/SignedSignatureProperties/SigningCertificate element is not allowed.

Anchor of trust

It is necessary that the parties have enough information to validate the signatures. This is ensured by having the same anchor of trust in both ends and providing certificates in KeyInfo. Depending on the Certificate Authority (CA) structure and the chosen anchor of trust, the number of certificates included in the KeyInfo element may vary:

- In case of a root CA that issues intermediate CA certificates that in turn issue the signer certificates, the chain in the KeyInfo element depends on the chosen anchor of trust:
  - If the anchor of trust is the intermediate CA, then the chain in the KeyInfo element need only to contain the signer certificate;
  - If the anchor of trust is the root CA, the chain in the KeyInfo element must include both the signer certificate and the intermediate CA certificate.
- In case of a root CA that issues signer certificates directly, the root CA is the anchor of trust: The chain in the KeyInfo element needs only to contain the signer certificate.

The parties communicating must use the same certificates as anchor of trust. It is up to ESMIG signature services for each CA to choose the certificate (root or intermediate) that constitutes the anchor of trust.

4.2 List of business rules and error codes

BR NAME	DESCRIPTION	INBOUND MESSAGE	REPLY MESSAGE	REASON CODE	ERROR TEXT
ICSA010	The digital signature has to be valid.	head.001	admi.007	I071	Digital signature is not valid.
ICSA010	The digital signature has to be valid.	head.002	admi.007	I071	Digital signature is not valid.
ICAA001	The invoked TARGET service responds to the query request within the timeout limit. Message based or file based store and forward network service will be used.	any query message	admi.007	I074	The service cannot reply to the query request within the timeout limit. Store and forward network service will be used.
ICAA002	The invoked TARGET service responds to the query request via file store and forward network service as the query response exceeds the real time message based network service size (oversize handling).	any query message	admi.007	I076	The service cannot reply via message network service due to size restriction. File store and forward network service will be used.
ICAA003	The invoked TARGET service responds to the query request as the query response exceeds the file store and forward network service size limit.	any query message	admi.007	I077	The service cannot respond to the query due to size restriction.

The abovementioned list of Business Rules does not apply to the TIPS Service.

4.3 Index of figures

Figure 1 – Technical sender authentication 16
Figure 2 – ESMIG Portal Graphical User Interface 18
Figure 3 – Activity diagram for TIPS 23
Figure 4 – Inbound Routing 37
Figure 5 – Outbound Routing 39

4.4 Index of tables

Table 1 - UDFS sections containing service-specific information 6
Table 2 - ESMIG business data exchanges and network services features 11
Table 3 - Query response and communication mode depending on the size of the response 21
Table 4 - Cross-field validations for SCT^{Inst} scheme 26
Table 5 - Cross Field validation for non-Euro currencies scheme 28
Table 6 - Outbound messages generated by ESMIG for TARGET Services (excluding TIPS) . 30
Table 7 - Outbound messages generated by ESMIG for TIPS 32
Table 8 - TARGET Services, components and applications 37

All Rights reserved

4.5 List of acronyms

Item	Description
24/7/365	24 hours a day/ 7 days a week/ 365 days a year
A2A	Application-to-Application
API	Application Programming Interface
BAH	Business Application Header
BIC	Business Identifier Code
CA	Certification Authority
CGU	Closed Group of Users
CLM	Central Liquidity Management
CONT	Contingency Component (i.e. ECONS II)
CRDM	Common Reference Data Management
DEP	Data Exchange Protocol
DN	Distinguished Name
ECB	European Central Bank
ECMS	Eurosystem Collateral Management System
ESMIG	Eurosystem Single Market Infrastructure Gateway
FH	File Header
FILERT	File Real-Time
FILESNF	File Store-and-Forward
GUI	Graphical User Interface (see U2A)
IAM	Identity and Access Management
IPsec	Internet Protocol Security
LRDM	Local Reference Data Management
MEPT	Message Exchange Processing for TIPS
MQ	Message Queuing
MSGRT	Message Real-Time
MSGSNF	Message Store-and-Forward
NRO	Non Repudiation of Origin
NSP	Network Service Provider
PKI	Public Key Infrastructure
PROD	Production (Environment)
RTGS	Real Time Gross Settlement
SCTInst	SEPA Credit Transfer Instant
T2S	TARGET2 Securities

All Rights reserved

Item	Description
TIPS	TARGET Instant Payment Settlement
U2A	User-to-Application
UDFS	User Detailed Functional Specifications
URD	User Requirements Document
URI	Universal Resource Identifier
XAdES	XML Advanced Electronic Signatures
XML	Extensible Mark-up Language
XSD	XML Schema Definition

All Rights reserved

4.6 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
[6]	T2S Connectivity Guide	4CB
[7]	T2S General Technical Design	4CB

All Rights reserved

4.7 U2A Qualified configuration

4.7.1 Introduction

4.7.1.1 Purpose and Objectives

This section describes the general configuration that ESMIG users shall be complaint with in order to access TIPS, T2S, ECMS, RTGS, CLM and CRDM GUI via the ESMIG web portal.

A specific section is devoted to describe the technical framework needed to fully implement the non-repudiation of origin functionality (NRO). The Ascertia solution is the NRO solution designed for all TARGET services.

4.7.1.2 Background remarks

The aim of the ESMIG qualified configurations is to provide ESMIG users with a specific configuration that is proved to be fully working.

As already mentioned, the NRO solution, based on the Ascertia Go>Sign Desktop application, will be the unique U2A NRO solution to be adopted for TARGET services, therefore only one version of the Go>Sign Desktop client will be used and distributed across the different services.

All Rights reserved

4.7.1.3 GSD Versions, Build No

	delivered	Build No	
Ascertia standard Release (SU+MU) version 8.3.6	Q4 2024	836.836.060924.202409061918	outdated
GoSign version 8.3.6. (SU+MU), security hotfix	Q1 2025	836.836.131124.202411131845	outdated
GoSign version 8.3.6. (SU+MU), security hotfix	Q2 2025	836.836.230525.202505231938	current version

4.7.2 Ascertia GSD Single User Client (SU)

4.7.2.1 Qualified configuration

As already mentioned, the 4CB has qualified a specific subset of the NSPs / Ascertia compatibility matrix. These configurations have been tested and support on them is guaranteed as specified in the "Support and Release policy" paragraph.

Go>Sign DESKTOP CLIENT (version will be regularly updated by the 4CB)		
NSP	SWIFT	NEXI
OS	Windows 11	
Browser	Microsoft Edge 136 Edge browser has been successfully tested within 4CB and is supported by 4CB LLS. If other browsers (Chrome and Firefox) are used, support is done by external provider Ascertia.	
Go>Sign Desktop SU	**6.9.0.20 or 8.3.6 (security hotfix)**.	6.9.0.20 or 8.3.6 (security hotfix)

Required software stack

SWIFT HSM Certificate	SWIFT USB Certificate
ESMIG U2A SWIFT Login Application 2.2.2.1 as Standard (version 2.2.0.8 deprecated, version 2.1.4.6 not supported anymore)	will no longer be supported by 4CB LLS starting from QI 2025, support is done by external provider SWIFT

NEXI HSM Certificate	NEXI USB Certificate
SIAVAL SafeCert 3.2.0.7993	YubiKey Manager 1.2.4 YubiKey-Minidriver 4.1.1.210

BDI Smartcard Certificate	BDI USB Certificate

All Rights reserved

IDProtect Manager 6.47.04	Bit4id PKI Manager 1.4.10.715 SwitchService_Installer

These above are the minimum certified requirements for GSD 4CB certified versions.

The 4CB will ask customers running a software version lower than the certified one to upgrade it to a certified version in order to proceed with problem investigation.

The 4CB will investigate issues experienced by customers while running a software version higher than that certified: if the root cause is linked to the specific software version, then the 4CB will attempt to find a workaround (which may involve customers downgrading their software to a certified version). The 4CB will evaluate whether a fix for the issue can be included in a future relevant TARGET Service GUI release.

Customers using totally or partially different system components or versions than those mentioned are then responsible for verifying the full compatibility with the relevant TARGET Service GUI in the test environments and the system. The 4CB will in any case, provide support to the maximum extent possible for checking / testing alternative configurations in order to support troubleshooting process.

The local customer system set-up, i.e. adaptation of the local firewall and security policies in order to enable the client installation, HTTPS transfer communication, access to the certificates on the USB tokens/HSM from the client machines (either physical or remote workstations) is under the sole responsibility of the end users (that may also need to involve their internal IT Dept. as well as external providers, in case of product specific issues).

These cryptographic key stores, used to access the signing keys, are supported:

- PKCS#11 for hardware-based tokens, SWIFT HSM based certificates
- MSCAPI only for NEXI hardware-based tokens, NEXI HSM based certificates

4.7.2.2 Technical requirements and recommendations

4.7.2.2.1 Single user download URLs

The client is available for download on the ESMIG portal (after log-in) at the following URLs. The software is the same for each environment, only access urls are different.

SHA256 hash:
21c02e846566721538ac1552a7347a0b99e1168cc6008fdd960ff99323d699b0

EAC PORTAL

https://esmig-eac-portal.u2a.sianet.sia.eu/gosign/download/64bit_client_SU

https://esmig-eac-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client_SU

UTEST PORTAL

https://esmig-cert-portal.u2a.sianet.sia.eu/gosign/download/64bit_client_SU

https://esmig-cert-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client_SU

PROD PORTAL

https://esmig-portal.u2a.sianet.sia.eu/gosign/download/64bit_client_SU

https://esmig-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client_SU

The full installation guide provided by Ascertia can be provided upon request and it can be used as reference for specific needs (e.g. automated installations). Downloading and installing the Go>Sign Desktop client is a mandatory step to sign/verify U2A requests. Installation requires administrative privileges; local IT support must be involved to make sure the installation correctly ends.

4CB entered into a license agreement with Ascertia and costs will be managed accordingly by 4CB ; disclaimer accepted by the user at installation phase should not be taken into consideration. Customer should open support request to 4CB only and NOT to Ascertia directly. 4CB will involve Ascertia as appropriate.

4.7.2.2.2 Removing previous Go>Sign Desktop client

In case a previous version of the Go>Sign Desktop client is already installed on a workstation, users or IT Admin should uninstall this version first (e.g. 6.9.0.20). After the deinstallation make sure that no “gosign” certificate will be installed for a user (certmgr.msc, Trusted Root Certification Authorities). Afterwards the new GSD version can be installed. Please make sure that after the installation only one “gosign” certificate will be installed for a user. If there is more than one “client.go-sign-desktop.com” certificate please explicitily delete the older ones.

When you observe the following error message: “Failed to start Go>Sign Desktop” and at the same time the log entry: “…java.io.IOException: Keystore was tampered with, or password was incorrect…”

Most likely the issue is that the keystore password between GSD 8.3.6 and the formerly installed GSD has changed. Therefore the password stored in the keystore file for the user does not match anymore.

Please check below instructions:

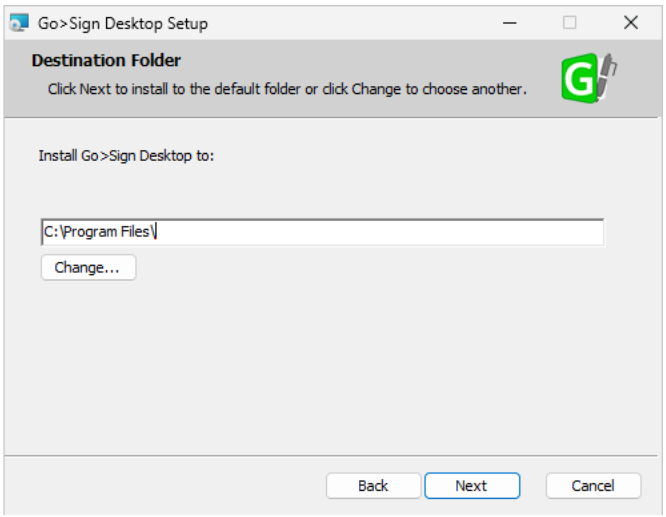
To resolve the issue please stop GoSign desktop and delete the content of the %AppData%\Ascertia\Go-Sign-Desktop folder of the user. Afterwards restart GSD again. User will be asked to confirm the installation of the self signed certificate again (might also been asked to delete the former certificate). Anyway, the certificate related security prompts need to be confirmed. In parallel a new keystore file will be created in the corresponding %AppData%\Ascertia\Go-Sign-Desktop and from this time on and signing should be possible. Please also note, that in case a user has adjusted e. g. the

All Rights reserved

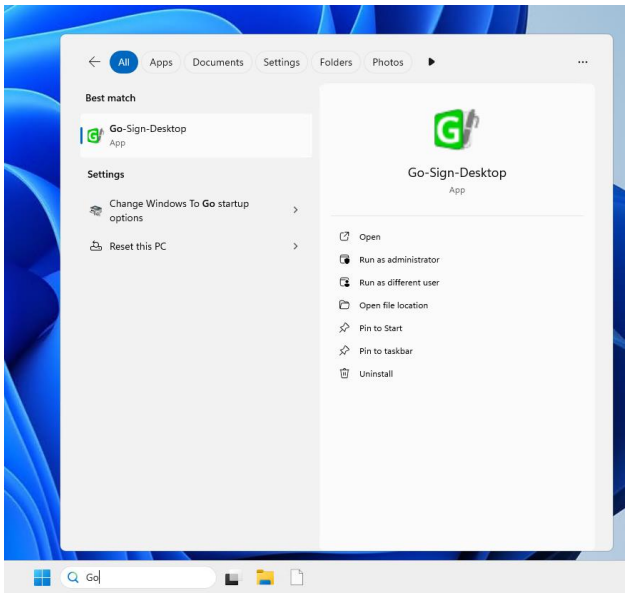
log level in the "go-sign-desktop.properties" file, that this setting will be gone as well and needs to be reapplied after GSD was started for the first time.

4.7.2.2.3 Go>Sign Desktop Client Requirements and post-installation remarks

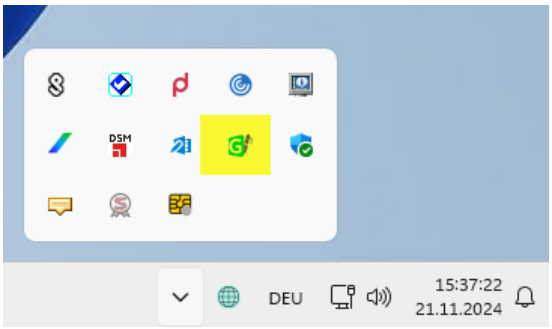
While installing this new functionality is available, please leave the default setting:



After installation, ADSS Go>Sign Desktop will start automatically at the user logon therefore user is not expected to manually start the client. Due to specific security settings, this might not happen, resulting signature attempts to end with a similar error "Go>Sign desktop not running/installed". In this case, it is necessary to start the client manually before initiating a browsing session. It is possible to lookup for the Go>Sign via the Windows Search bar:



- If the icon is not found, this can be probably linked to problems occurred during the installation. The local IT support needs to be involved in this case.
- Ensure that the Go>Sign icon is featured in the system tray:



If the icon is not found, this can be probably linked to problems occurred during the installation. The local IT support needs to be involved in this case.

ADSS Go>Sign Desktop relies on TLS communication with the web application (on port 8782). This communication is secured using a TLS server certificate having hostname:

client.go-sign-desktop.com.

Therefore, the local client machine must be able to resolve this FQDN (Fully Qualified Domain Name name for a specific computer, or host, on the internet) to itself. In order to achieve this, the standard installation procedure foresees that the Go>Sign Desktop Installer automatically adds the entry :

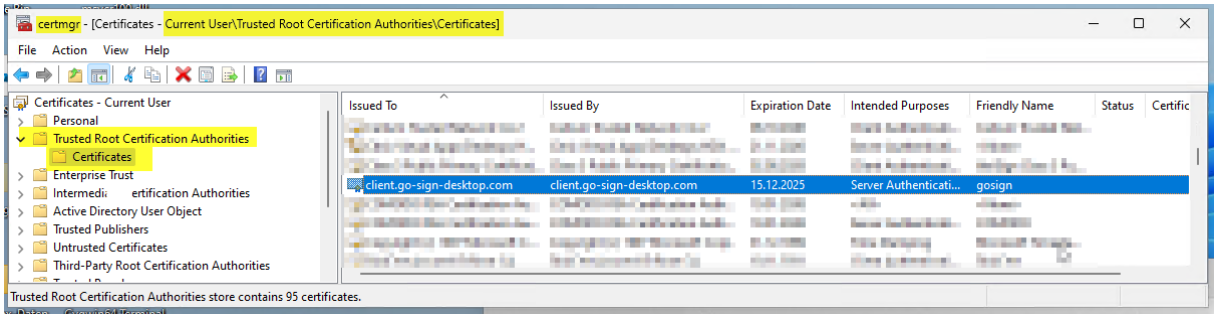
127.0.0.1 client.go-sign-desktop.com

in the Operating System host file in order to register the client.go-sign-desktop.com as a local domain (Windows OS: C:\Windows\System32\Drivers\etc\hosts). This will add the FQDN client.go-sign-desktop.com to resolve to IP address 127.0.0.1.

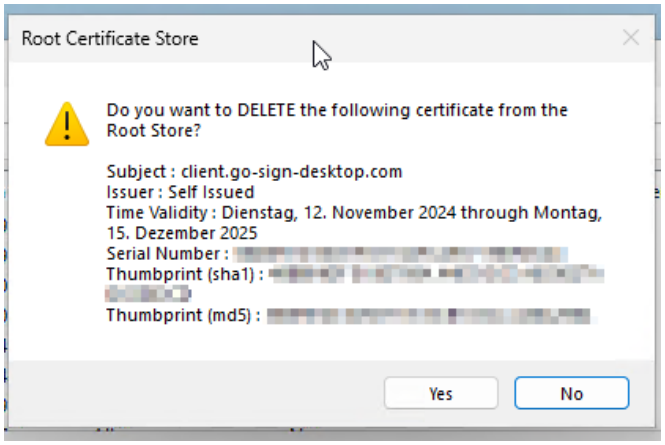
The default value client.go-sign-desktop.com must not be changed.

The TLS server certificate will be self-signed and different for each workstation where the client will be installed.

Open Command prompt and use “certmgr.msc”

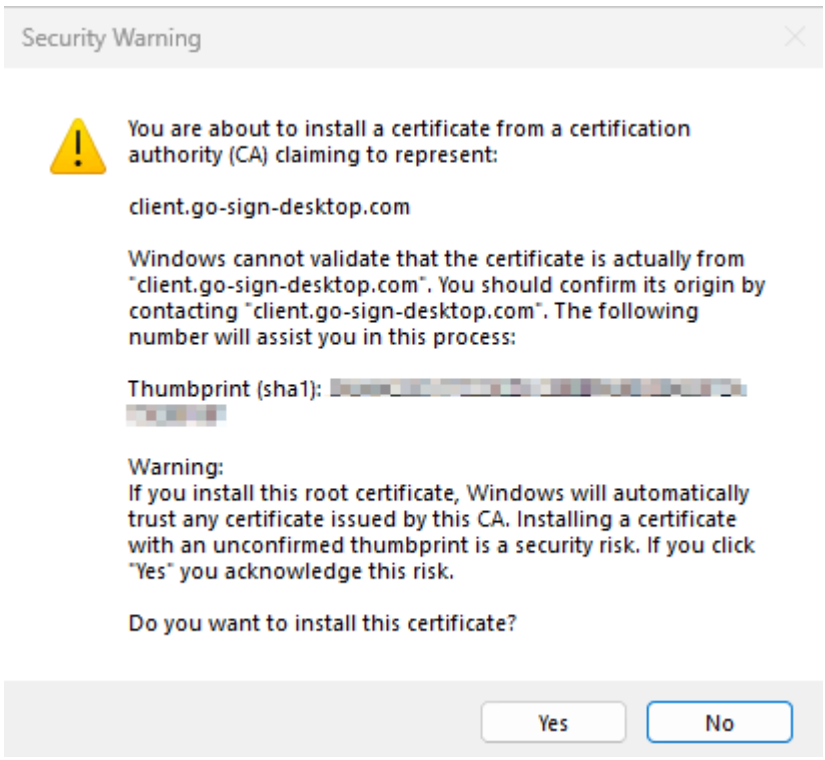


If user are asked during the single user GoSign installation: "Do you want to DELETE the following certificate from the Root Store?"



please confirm with “YES”

and afterwards next dialogue "You are about to install a certificate from a certification authority (CA) claiming to represent: …”



please confirm again with "YES".

Please note hat this dialogue may also appear when the GoSign application will start for the first time, e.g. in case workstation is shared by multiple users .

The end users have to ensure that the security settings of their institutions, i.e. firewalls, allow for installation of the desktop client, if not generally disabled. By default, User Account Control Settings (UAC) are enabled in windows. ADSS Go>Sign Desktop needs user permissions to make changes on the installing device. Windows always prompt a dialog to get the user permissions if user granted the permissions then ADSS Go>Sign Desktop would be installed on the device.

In order to check the correct version Go>Sign desktop is installed, users can right click on the go sign icon and choose "about".

In order to check that ADSS Go>Sign Desktop is running properly, user should access the test URL https://client.go-sign-desktop.com:8782/gosign-desktop.

Port 8782 must not be changed into gosign-desktop.properties file otherwise the overall NRO setup will not work.

All Rights reserved

4.7.2.2.4 Additional requirements

Here following a list of items to be checked before starting the test sessions or in case of exceptions that may block the testing. Internal IT support may be needed to perform these checks because of security restrictions that may be in place preventing the end users to complete them autonomously:

- As a general remark, please make sure that the configurations listed in the relevant NSPs documentation are applied (as a not exhaustive example, the mandatory changes on the pac file). For further details please refer to the "SWIFT's Solution for ESMIG U2A Setup Guide Step-by-Step" document and the " SIAnet.XS Connectivity Services for ESMIG U2A User Guide"

- In case of local network exceptions in the browser (i.e. **TUNNEL CONNECTION FAILED, NAME NOT RESOLVED**) during first interaction with Ascertia backend infrastructure: add DSS host certificates in browsers keyring . Host names following for information:

SIA-NEXI TST	esmig-tst-dss.u2a.sianet.sia.eu
SIA-NEXI CRT	esmig-cert-dss.u2a.sianet.sia.eu
SIA-NEXI PRD	esmig-dss.u2a.sianet.sia.eu
SWIFT TST	esmig-tst-dss.emip.swiftnet.sipn.swift.com
SWIFT CRT	esmig-cert-dss.emip.swiftnet.sipn.swift.com
SWIFT PRD	esmig-dss.emip.swiftnet.sipn.swift.com

The same above URL may need to be added to the browsers trusted sites.

- In case of Cross-Origin Resource Sharing (CORS) issue during first interaction with new Ascertia infrastructure, please temporarily disable CORS checks both in Chrome and/or FF

a. FF --> https://addons.mozilla.org/es/firefox/addon/access-control-allow-origin/ + Toggle ON

b. Chrome --> "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-web-security --user data-dir="C:\.....\Chrome" (for single user environment)

c. Chrome --> "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-web-security (for multi user environment)

- In case of proxy.pac file being used on a workstation/desktop, the following rule should be included in order to add the appropriate exception:

```
if (dnsDomainIs(host, "client.go-sign-desktop.com")){
return "DIRECT";
}
```

- Check installation / install "client.go-sign-desktop.com" certificate in web browser explicitly (or check first if it is in all browsers keyring after GSD client installation). As already stated above, one and only one GoSign certificate has to be present in user trust store; in case two or more GoSign certificates present, client may not start or may start with exceptions.
- No need to check the certificate of the go sign desktop against any CRL as it is self-signed.
- It is finally suggested to ensure that only one token/smartcard at time is connected to a workstation during signing operation.

4.7.2.2.5 How to act in case of GSD package needs to be integrated into some inhouse Software Integration process

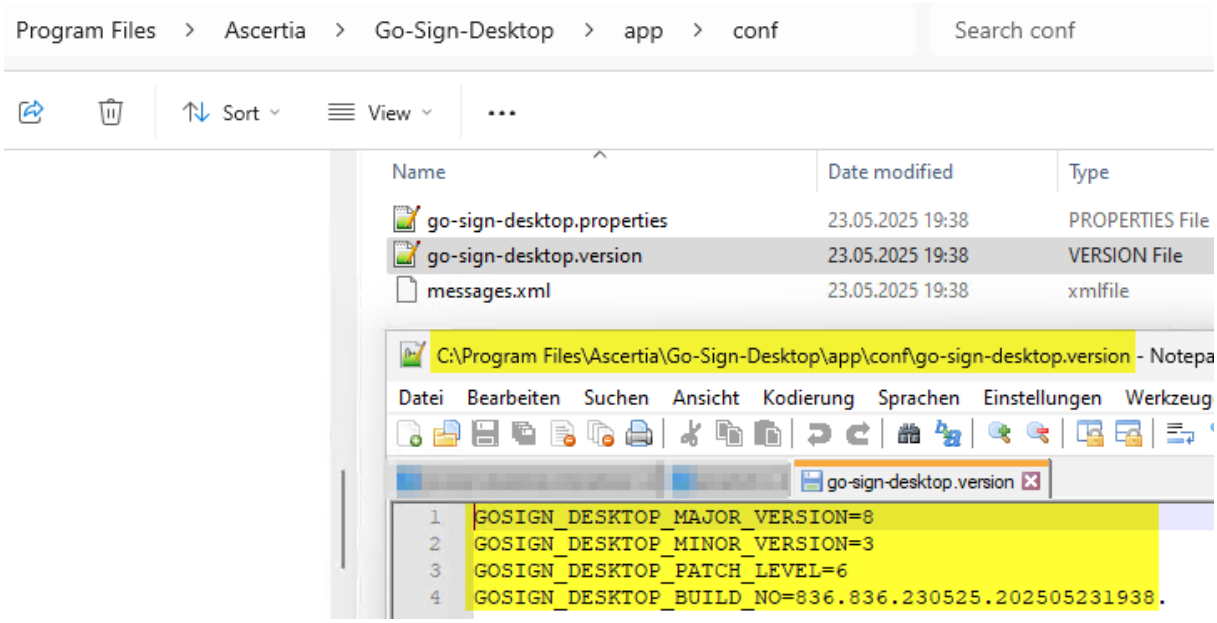
When installation is done as System/Admin user with privileges (on behalf of a regular business user / Windows standard user)

- Then self signed certificate is being created for this System User and also User AppData folder is being created only for the System user
- but GSD is running afterwards (as process of System User) and cannot be started again in the context of the current user as the port is blocked
- business user folder is not created, if GSD is stopped and started again there might be problems if previously an older version of GSD was installed as the hardcoded password of the keystore file in the user folder and in jar file of the installation folder might not match
  - in this case GSD must be stopped
  - user folder needs to be deleted
  - afterwards restarted GSD
    - new self signed certificate is being created
    - certificate imported into certmgr.msc "Trusted Root Certificates"

4.7.2.3 Mandatory troubleshooting information

When opening the incident to 4CB Service Desk, users must provide the following:

- OS and browser in use plus type of installation (SU) and its version (“About” panel or information from the following file):



- "go-sign-desktop.log" (DEBUG level, see next section)
- Copy of %userprofile%\AppData\Roaming\Ascertia\Go-Sign-Desktop\logs\go-sign-desktop.properties (if any changes applied from default values)
- Browser console log file (F12 button)
- Browers network trace file (F12 button) – only in case of network-related issue and if explicility required
- Relevant screenshots reporting any useful exception

It is higly suggested to check any expcetion first with the internal IT/Network support for a preliminary analysis and then with 4CB. NSP may be involved as well in case of network-related issues.

4.7.2.3.1 Client logging information and changing log level

ADSS Go>Sign Desktop application has two log levels. First informational, which is for normal use, and second, debug, which should only be used when investigating performance issues, functionality problems, etc. For Windows OS and go>sign client configuration, users can view ADSS Go>Sign Desktop application logs at:

C:\Users\[User_Name]\AppData\Roaming\Ascertia\Go-Sign-Desktop\logs\

By default, ADSS Go>Sign Desktop logging level is set to INFO. To enable detailed debug logging, follow these instructions:

1. Go to ADSS Go>Sign Desktop user installation path

C:\Users\[User_Name]\AppData\Roaming\Ascertia\Go-Sign-Desktop

2. Edit the go-sign-desktop.properties file using a suitable text editor.
3. Change the value of the property GOSIGN_DESKTOP_LOG_MODE from INFO to DEBUG and save the file.
4. Stop ADSS Go>Sign Desktop application → right click ADSS Go>Sign Desktop application icon and select the option Quit.
5. Start ADSS Go>Sign Desktop application → Start Menu

Please note that go-sign-desktop.log and go-sign-desktop.properties have been moved to new location compared to old GoSign 6.9.0.1.

4.7.3 Ascertia GSD Multi User Client (MU)

The Multi User Client is intended to be used on Window Terminal Server operating systems, e. g. Windows Server 2022.

4.7.3.1 Qualified configuration

As already mentioned, the 4CB has qualified a specific subset of the NSPs/Ascertia compatibility matrix. These configurations have been tested and support on them is guaranteed as specified in the "Support and Release policy" paragraph.

Go>Sign DESKTOP CLIENT (version will be regularly updated by the 4CB)		
NSP	SWIFT	NEXI
OS	Windows Server 2019/2022	
Browser	Google Chrome 132 Microsoft Edge 132 Edge and Chrome browsers have been successfully tested within 4CB and are supported by 4CB LLS. If Firefox is used, support is done by external provider Ascertia.	
Go>Sign Desktop MU	**6.9.0.20 or 8.3.6 (security hotfix)**	**6.9.0.20 or 8.3.6 (security hotfix)**

Required software stack

SWIFT HSM Certificate	SWIFT USB Certificate
ESMIG U2A SWIFT Login Application 2.2.2.1 as Standard (version 2.2.0.8 deprecated, version 2.1.4.6 not supported anymore)	SafeNet Authentication Client 10.9 R1

NEXI HSM Certificate	NEXI USB Certificate
SIAVAL SafeCert 3.2.0.7993	YubiKey Manager 1.2.4 YubiKey-Minidriver 4.1.1.210

BDI Smartcard Certificate	BDI USB Certificate
IDProtect Manager 6.47.04	Bit4id PKI Manager 1.4.10.715 SwitchService_Installer

These above are the minimum certified requirements for GSD 4CB certified versions.

The 4CB will ask customers running a software version lower than the certified one to upgrade it to a certified version in order to proceed with problem investigation.

The 4CB will investigate issues experienced by customers while running a software version higher than that certified: if the root cause is linked to the specific software version, then the 4CB will attempt to find a workaround (which may involve customers downgrading their software to a certified

version). The 4CB will evaluate whether a fix for the issue can be included in a future relevant TARGET Service GUI release.

Customers using totally or partially different system components or versions than those mentioned are then responsible for verifying the full compatibility with the relevant TARGET Service GUI in the test environments and the system. The 4CB will in any case, provide support to the maximum extent possible for checking / testing alternative configurations in order to support troubleshooting process.

The local customer system set-up, i.e. adaptation of the local firewall and security policies in order to enable the client installation, HTTPS transfer communication, access to the certificates on the USB tokens/HSM from the client machines (either physical or remote workstations) is under the sole responsibility of the end users (that may also need to involve their internal IT Dept. as well as external providers, in case of product specific issues).

These cryptographic key stores, used to access the signing keys, are supported:

- PKCS#11 for hardware-based tokens, SWIFT HSM based certificates
- MSCAPI only for NEXI hardware-based tokens, NEXI HSM based certificates

4.7.3.2 Technical requirements and recommendations

4.7.3.2.1 Multi user download URLs

ESMIG customers can download the client from the following URLs (after log-in to ESMIG portal):
SHA256 hash: **407864a82a3fc7c880ed772c7c8c6916d02c0a982c7e96fcb1bf3275b63d0e02**

EAC PORTAL

https://esmig-eac-portal.u2a.sianet.sia.eu/gosign/download/64bit_client_MU

https://esmig-eac-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client_MU

UTEST PORTAL

https://esmig-cert-portal.u2a.sianet.sia.eu/gosign/download/64bit_client_MU

https://esmig-cert-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client_MU

PROD PORTAL

https://esmig-portal.u2a.sianet.sia.eu/gosign/download/64bit_client_MU

https://esmig-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client_MU

All Rights reserved

Downloading and installing the Go>Sign Desktop client is a mandatory step to sign/verify U2A requests. Installation requires administrative privileges; local IT support must be involved to make sure the installation correctly ends.

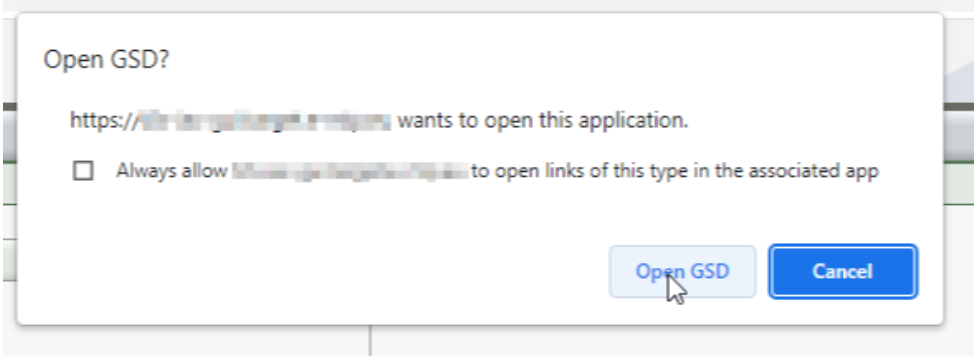
4CB entered into a license agreement with Ascertia and costs will be managed accordingly by 4CB ; disclaimer accepted by the admin at installation phase should not be taken into consideration. Customer should open support request to 4CB only and NOT to Ascertia directly. 4CB will involve Ascertia as appropriate.

4.7.3.2.2 Suggested upgrade procedure for 8.3.6 MU25

If a previous MU client installation is present on server environment, please follow the below checklist in order to correctly upgrade to the new release:

1. Stop the parent/service instance and any other child/user instance (mandatory to ensure proper clean up of all folders)
2. Client de-installation from control panel
3. Clean up the "GoSign" certificate from the Trusted Root CA stores of both the Current User (certmgr.msc) AND the local Computer (certlm.msc)
4. Check service deleted + check all Ascertia folders/subfolders deleted
5. Please check that no GoSign entry is present in Registry otherwise please delete the entry: Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
6. New client installation (as per section 3.2.3) + additional steps (as per section 3.2.4)::

The client invocation on user side will be triggered by the web application (via Javascript) with the first attempt to sign an instruction (and each time the user needs to sign one) and is transparent to users.

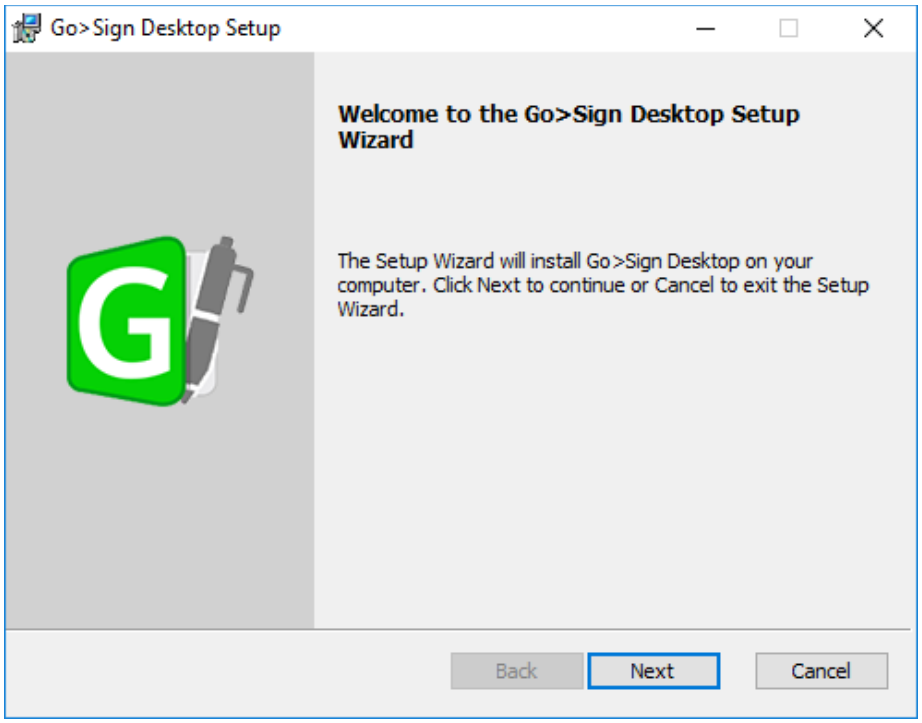


(Attention: please note that there may be individual company settings that do not allow the user to launch an application. If this is the case, please check with your local IT support/IT security! This function must be enabled.)

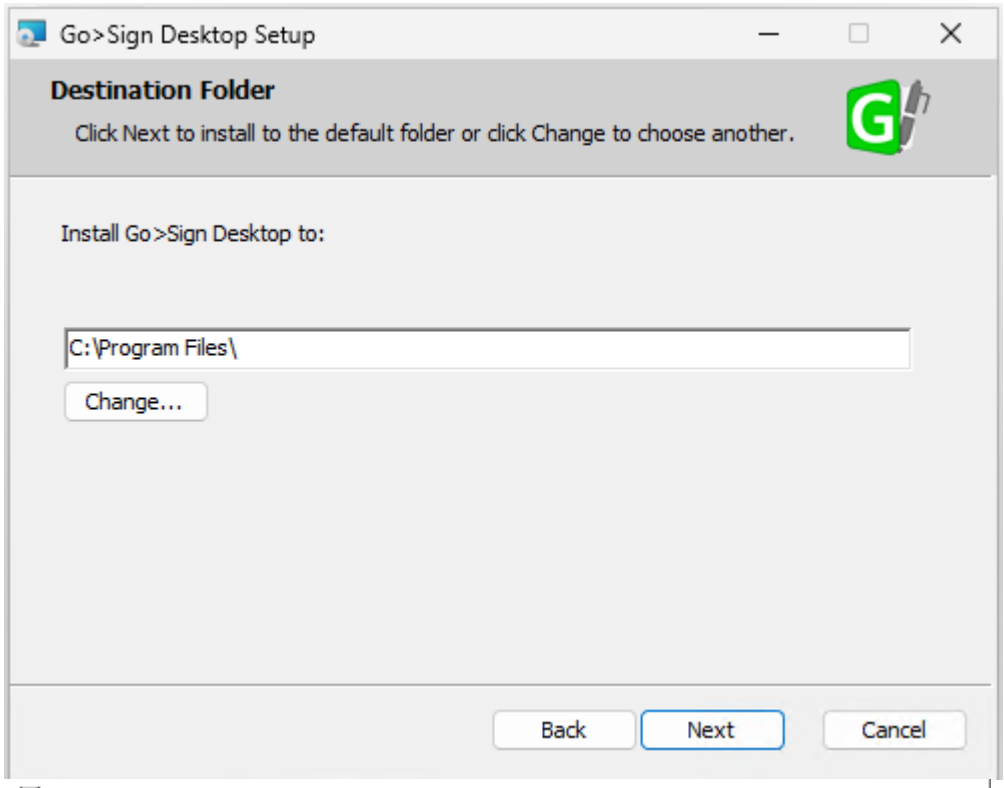
[25] For version 6.9.0.9 MU refer to previous version of this document.

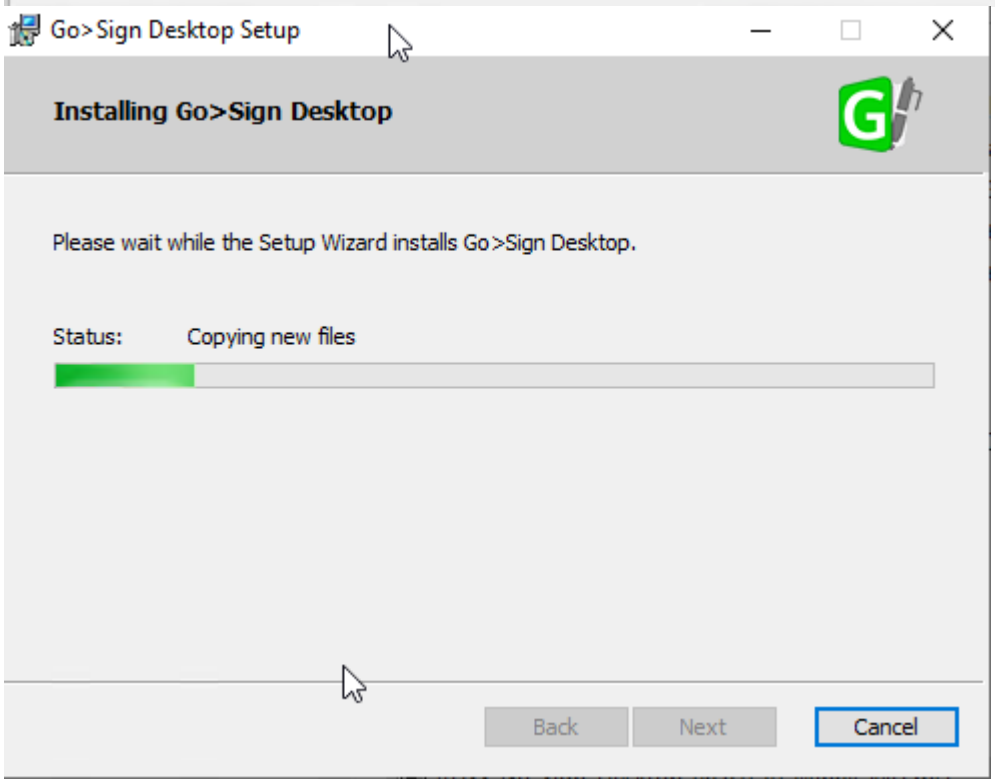
4.7.3.2.3 First installation of GSD multi user client

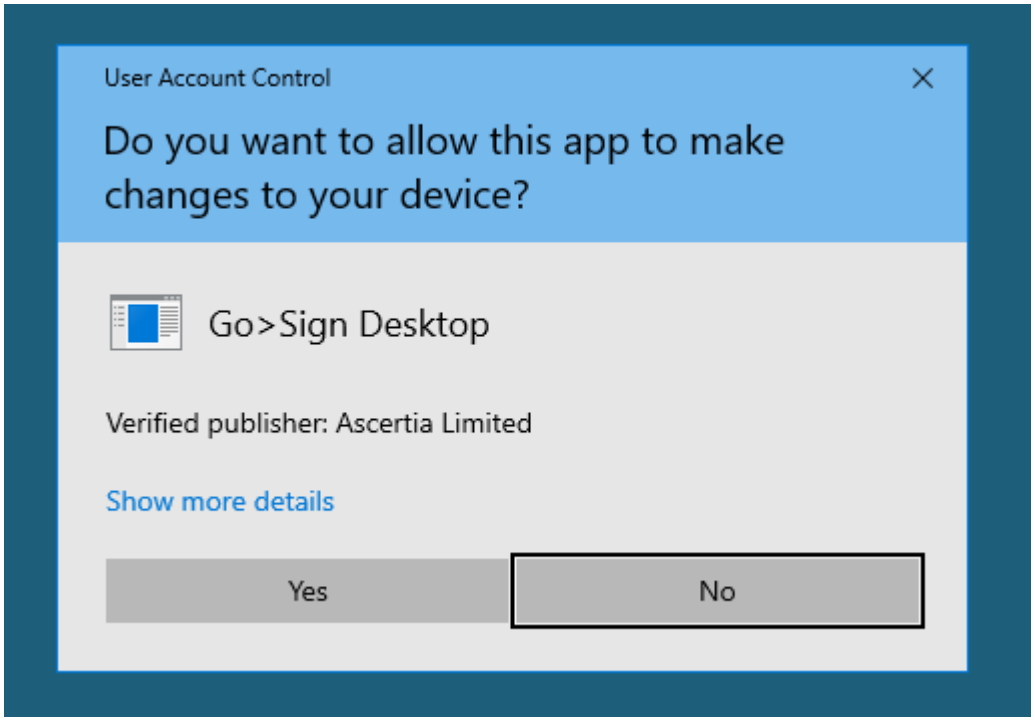
- Open Command prompt as Administrator
- Execute command: chgusr /install
- then run ADSS-Go-Sign-Desktop-v6.9.0.20-Win64-MU.msi installation package

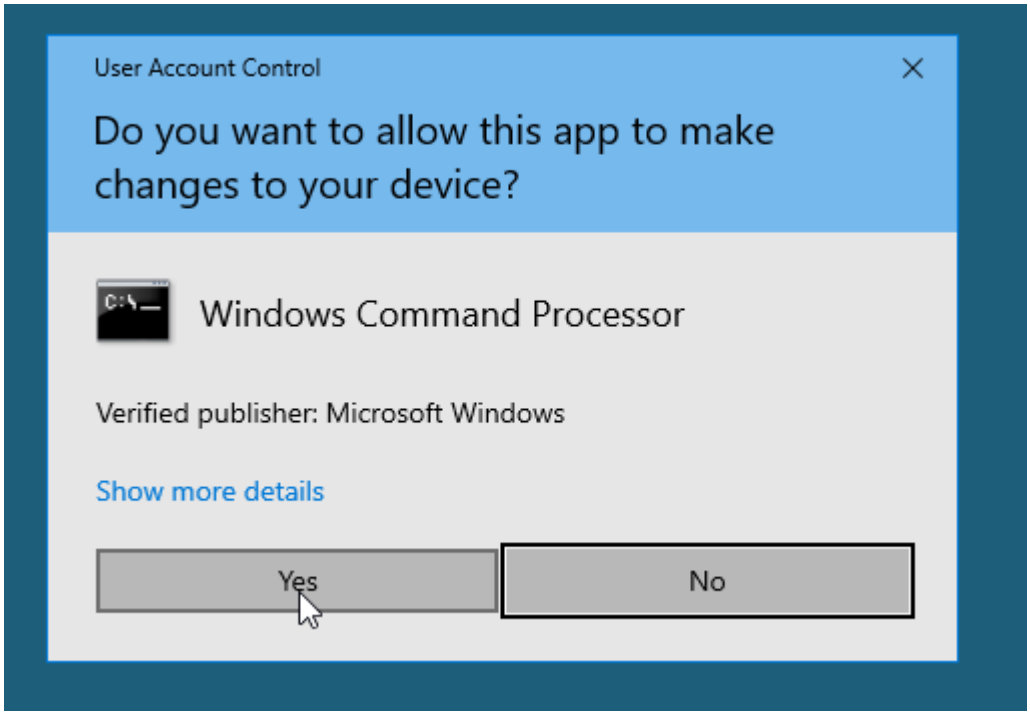


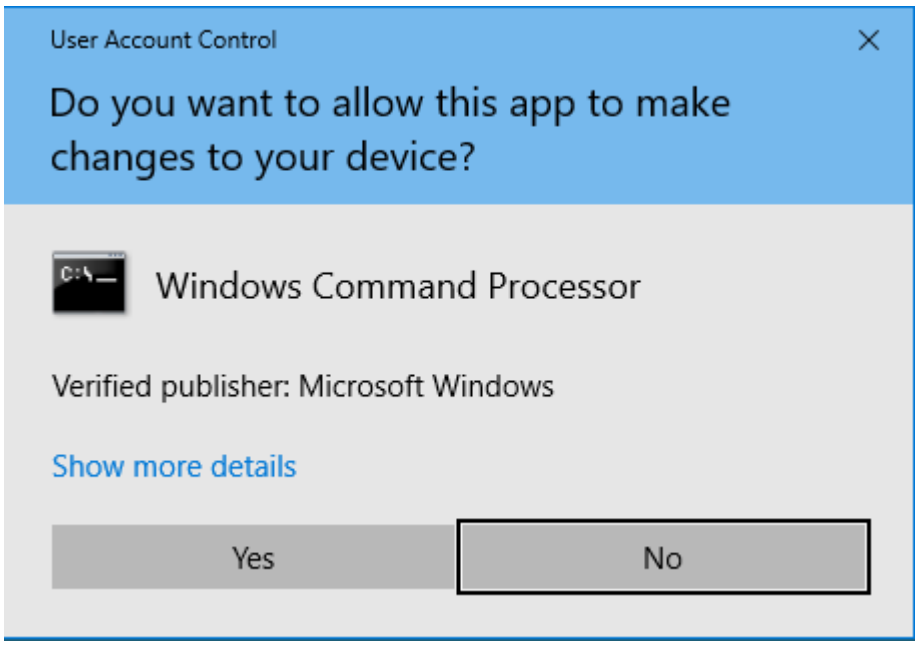
While installing this new functionality is available, please leave the default setting:

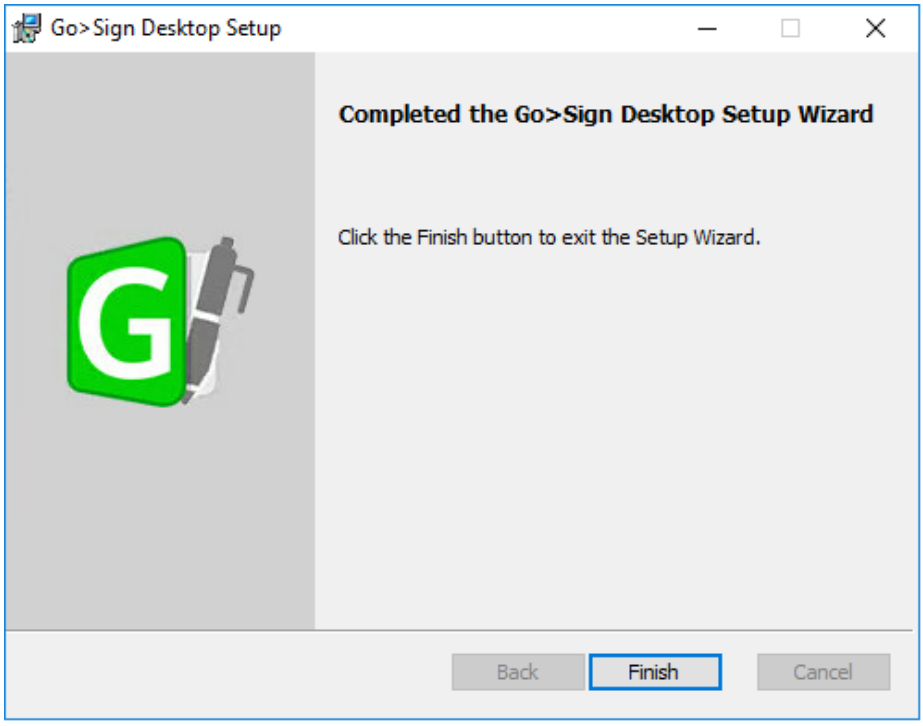

Go>Sign Desktop Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
Install Go>Sign Desktop to:
C:\Program Files\
Change...
Back
Next
Cancel


Go>Sign Desktop Setup
Installing Go>Sign Desktop
Please wait while the Setup Wizard installs Go>Sign Desktop.
Status: Copying new files
Back
Next
Cancel


User Account Control
Do you want to allow this app to make changes to your device?
Go>Sign Desktop
Verified publisher: Ascertia Limited
Show more details
Yes
No


User Account Control
Do you want to allow this app to make changes to your device?
Windows Command Processor
Verified publisher: Microsoft Windows
Show more details
Yes
No



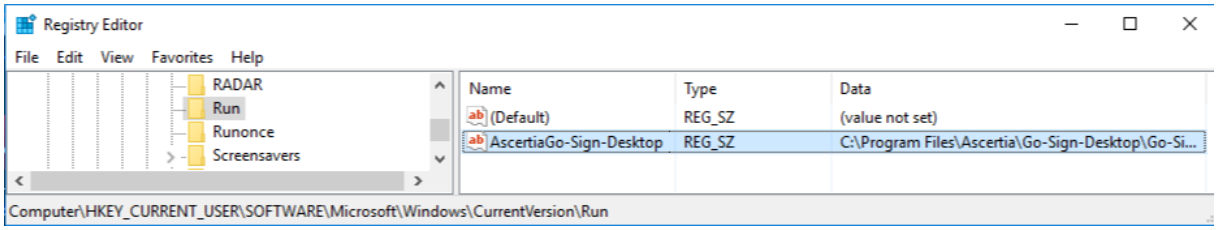


After installing the application, use ”change user/execute” to revert to standard .ini file mapping

4.7.3.2.4 Additional installation steps

Following tasks need to be executed by IT Admin only once before starting the service other service will NOT start at all !

1. The registry key for automatic start of GSD client on administrator login should be removed to avoid unexpected / undesired behaviour of the NRO MU solution (will be fixed in the next release).



2. Execute once from admin the command "C:\Program Files\Ascertia\Go-Sign-Desktop\Go-sign-desktop.exe" (or account that performed installation). This command will add the new GoSign certificate into server admin trust store.

3. Execute once from admin the command "C:\Program Files\Ascertia\Go-Sign-Desktop\GSD.exe" (or account that performed installation). This command will add the new GoSign certificate into LM trust store. Please note, that at this point two self signed certificates will be present in the Admins trust store (certmgr.msc) and one certificate present in the local machine store (certlm.msc).

4. Quit the manually started GoSign Desktop instance (started in the step 2) and then start the service.

GSD.exe applies following changes to local machine registry (HKLM) and adss "GoSign" certificate local computer trust store:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Ascertia]
"URL Protocol"="GSD"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Ascertia\shell]
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Ascertia\shell\open]
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Ascertia\shell\open\command]
@="C:\\Program Files\\Ascertia\\Go-Sign-Desktop\\GSD.exe %1
```

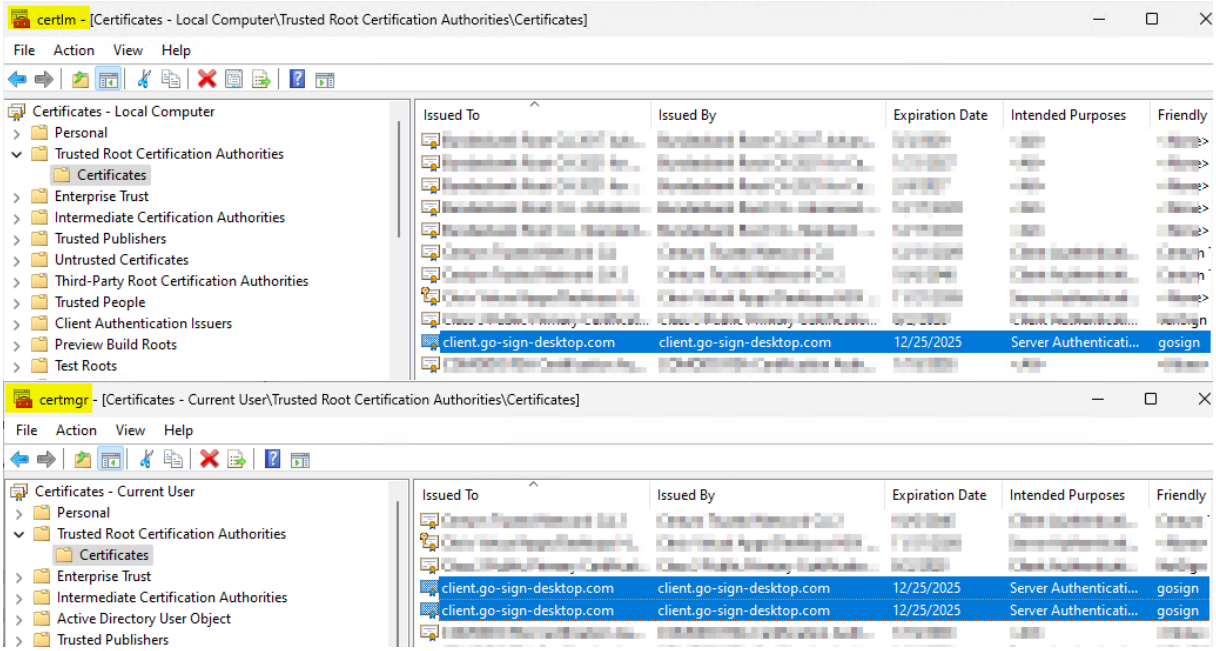
The above registry changes may need to be applied to all users at user logon in case non-persistent profiles. They will allow browsers to correctly trigger the start of GSD user/child instances, when user will be prompted to do so during an NRO task.

All Rights reserved

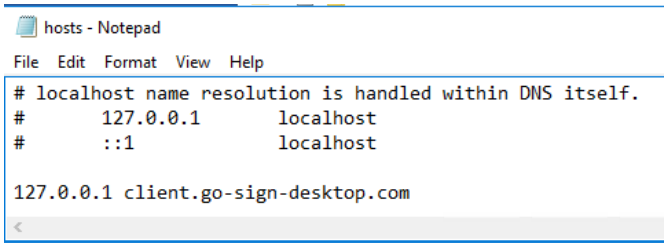
4.7.3.3 Post installation checks

4.7.3.3.1 Post installation checks – IT ADMIN

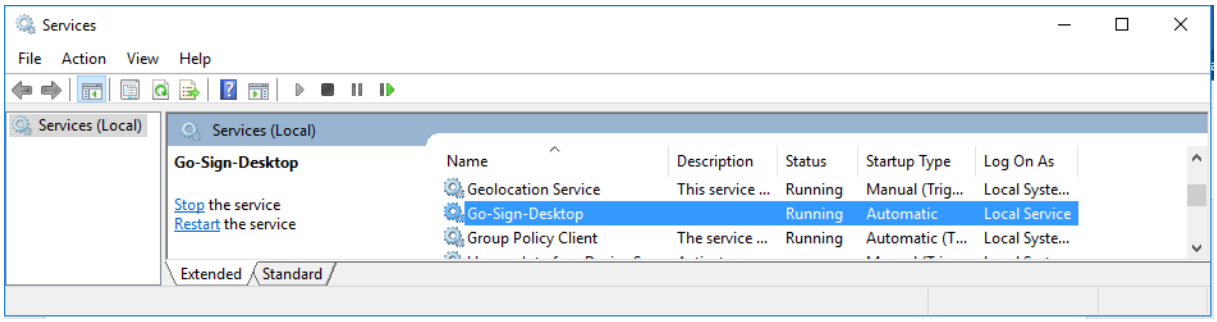
1. ”GoSign” certificate preset in Admin (certmgr.msc, 2x) and LM (certlm.msc) trust store + etc/hosts file correctly updated:

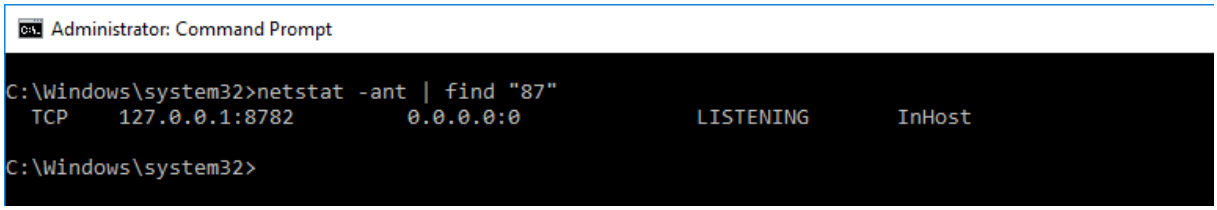


2. Check the etc/hosts file, C:\Windows\System32\drivers\etc



3. Check service running and listening on 8782 (with Local Service account), ”Go-Sign-Desktop” service hast to be started FIRST and will be listening on port 8782



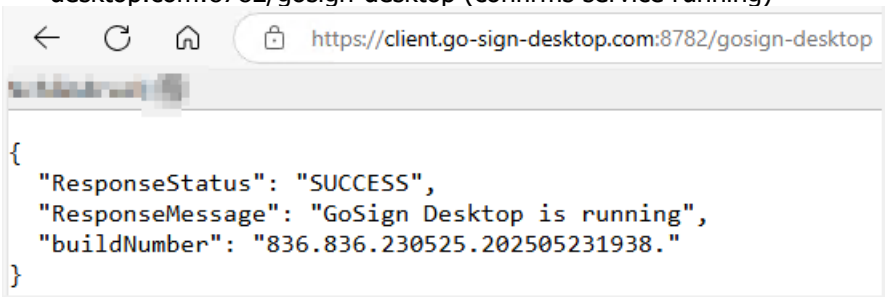


4. child instances will start during NRO task and will listen on higher port e.g. 8784, 8786 etc.
    - Business users have NOT to start manually the GoSign Desktop.exe tray application
5. In case of need, please check and share
    - Service log file "C:\Windows\ServiceProfiles\LocalService\Documents\Ascertia\Go-Sign-Desktop\logs"
    - User log file "%userprofile%\Documents\Ascertia\Go-Sign-Desktop\logs\"

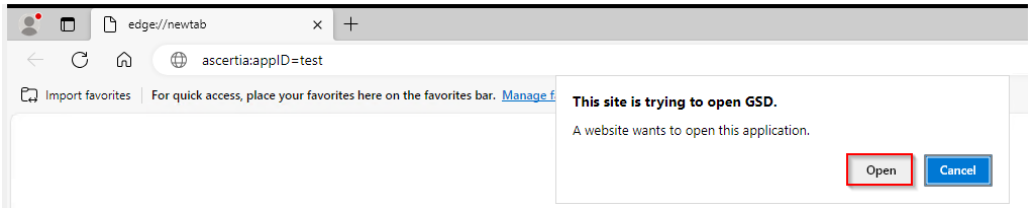
Port 8782 must not be changed into gosign-desktop.properties file otherwise the overall NRO setup will not work.

4.7.3.3.2 Post installation checks – BUSINESS USER / IT ADMIN

- Go-Sign-Desktop service is running, use browser with test URL: https://client.go-sign-desktop.com:8782/gosign-desktop (confirms service running)

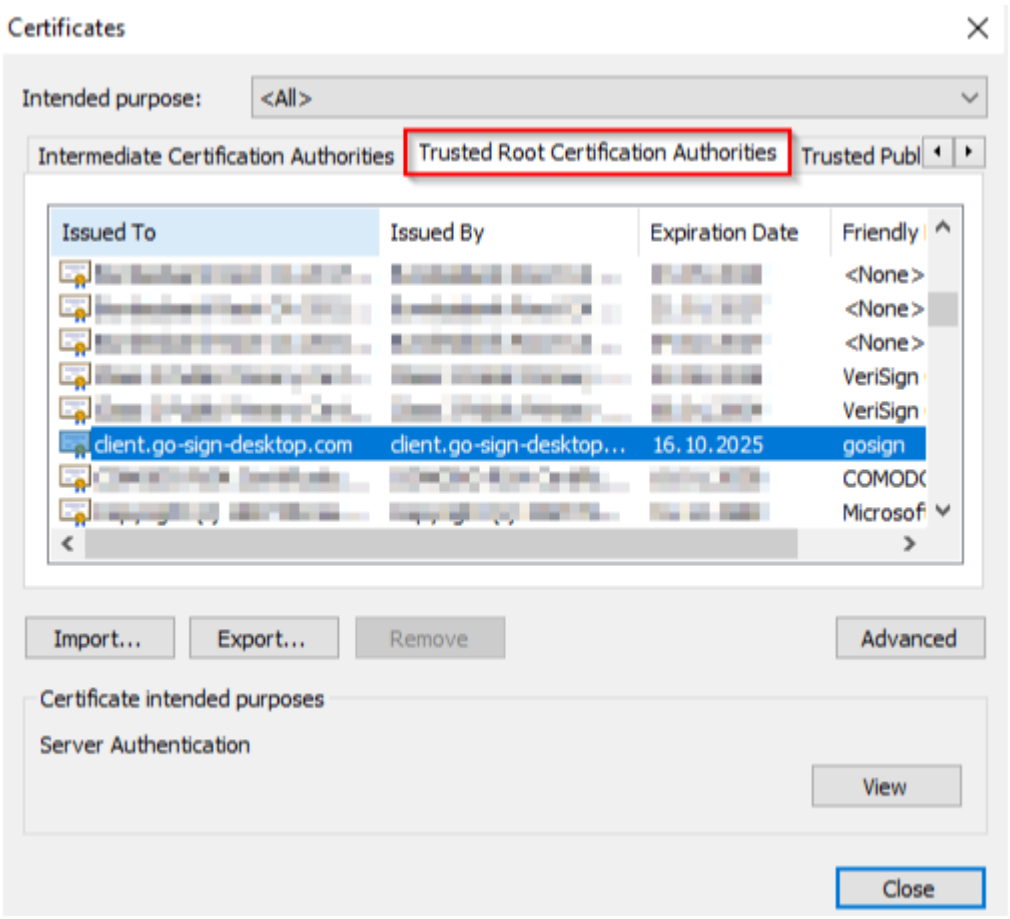


- Check if user is able to start manually a GoSign Desktop child instance
    - Open browser and type the following URL: ascertia:AppId=test



    - confirm to open GSD

User can also check the GoSign certificate is visible at computer level in the browser keystore:



Once logged in, the below URLs can be used by customers to check both:

- the communication path from customer premises to Ascertia backend infrastructure
- the availability of the Ascertia backend infrastructure itself

CERT stage URLs:

SWIFT: https://esmig-cert-dss.emip.swiftnet.sipn.swift.com/adss/gosign/applet/lib/adss_gosign.js

SIA-NEXI: https://esmig-cert-dss.u2a.sianet.sia.eu/adss/gosign/applet/lib/adss_gosign.js

PROD stage URLs:

SWIFT: https://esmig-dss.emip.swiftnet.sipn.swift.com/adss/gosign/applet/lib/adss_gosign.js

SIA-NEXI: https://esmig-dss.u2a.sianet.sia.eu/adss/gosign/applet/lib/adss_gosign.js

Actually, the above URLs are being contacted by the application in order to trigger the NRO sign/verify flow. For this reason, the user or IT Admin is not expected to perform any action with the JS file.

All Rights reserved

In order to properly perform NRO task, users are expected to allow execution of GSD user instance (before actual signature) in order to trigger start of a child GSD application that will then communicate with the GSD service/parent instance.

GSD child instances will listen on greater ports than the GSD service/parent one (8782) and will start dedicated Go-Sign-Desktop.exe application for each different web origin.

All Rights reserved

4.7.3.4 Additional features

4.7.3.4.1 GSD child instance housekeeping

8.3.6 MU release supports dynamic house-keeping of GSD child instances in order to optimize load on the server environment. This feature is disabled by default and could be activated by applying the following changes in the
"C:\Program Files\Ascertia\Go-Sign-Desktop\app\conf\go-sign-desktop.properties"

(and restarting the service):

Parameter	Description	Please take into account the following information when activating HouseKeeping
GOSIGN_DESKTOP_ENABLE_HEART_BEAT **Default = FALSE**	housekeeping is not active (all three of the following parameters are then ignored)	Please set the value to **TRUE** if you want to enable house keeping
GOSIGN_DESKTOP_MAX_IDLE_TIME **Default = 2**	time interval of user session inactivity in minutes until GoSign instance is automatically ended	Please do not exceed WEB session Timeout. Proposal, as starting value = **15** minutes
GOSIGN_DESKTOP_MAX_IDLE_INTERVAL **Default = 1**	the value controls (also in minutes) in which time interval the process runs to check if the house keeping is required for active GoSign instances (Please be aware that the maximum time a GoSign client session lives is the **sum of the two values**: GOSIGN_DESKTOP_MAX_IDLE_TIME + GOSIGN_DESKTOP_MAX_IDLE_INTERVAL)	Proposal, as starting value = **3** minutes
GOSIGN_DESKTOP_MAX_INSTANCES_PER_USER **Default = 2**	Maximum number of parallel GoSign instances per user. Please notice for each different ORIGIN a new GoSign instances must be started (i.e. different browsers or different business applications or different stages)	Maximum **3** or **4** should be enough for standard user

Some additional technical remarks can be considered in order to manage GSD child instances in a Citrix terminal server environment, specifically:

- Two parameters at terminal server level with regards to user session limits policy settings

Session idle timer

The duration after which the Citrix terminates an idle session if there is no user activity (i.e. such as from the mouse, keyboard, or touch for the specified interval.

This setting enables or disables a timer that specifies how long an uninterrupted user device connection to a desktop is maintained if the user supplies no input. When this timer expires, the session is placed in the disconnected state and the Disconnected session timer applies.

Disconnected session timer interval

This setting specifies how many minutes a disconnected, locked desktop can remain locked before the session is logged off.

- Please also activate or check if the following setting is active on your TS infrastructure **https://support.citrix.com/article/CTX891671**

This registry key allows to terminate executables that have been started by / from a published application (only valid for Citrix TS enviroment). Exe to be added in the key would be javaw.exe, in this specific case.

4.7.3.4.2 Log files rolling mechanism

8.3.6 client also implements rolling mechanism for log files which can be controlled via the following parameters (go-sign-desktop.properties):

```
GOSIGN_DESKTOP_LOG_FILE_PATH = default

GOSIGN_DESKTOP_CONF_FILE_PATH = default

GOSIGN_DESKTOP_LOG_FILE_MAX_SIZE = 1 MB

GOSIGN_DESKTOP_LOG_FILE_MAX_COUNTER = 10
```

'GOSIGN_DESKTOP_LOG_FILE_PATH' its default value is 'default':

%userprofile%\Documents\Ascertia\Go-Sign-Desktop\logs\go-sign-desktop.log.

Another path can be entered e.g. '\\\\<file server IP>\\Shared\\gosign' and Go>Sign Desktop will append the username and the file name and start logging at the shared network location.

Child instance should have access to the network location!

go-sign-desktop.properties file moved into new (default) path:

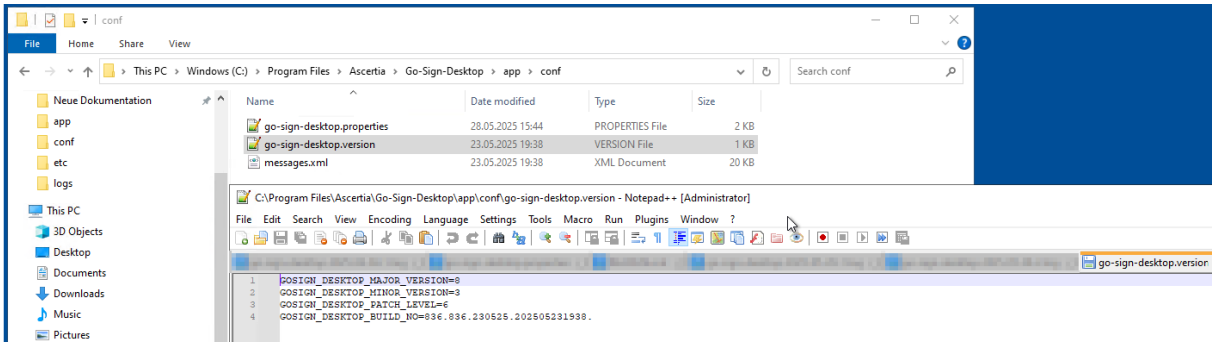
"C:\Program Files\Ascertia\Go-Sign-Desktop\app\conf\go-sign-desktop.properties"

We recommend here GOSIGN_DESKTOP_LOG_FILE_MAX_SIZE = 10 MB.

4.7.3.5 Mandatory troubleshooting information

When opening the incident to 4CB Service Desk, users must provide the following:

- OS and browser in use plus type of installation (MU) and client version



- GSD log file paths:
  - Service log

    “C:\Windows\ServiceProfiles\LocalService\Documents\Ascertia\Go-Sign-Desktop\logs”
  - Child instance log

    “%userprofile%\Documents\Ascertia\Go-Sign-Desktop\logs”
- Copy of

  “C:\Program Files\Ascertia\Go-Sign-Desktop\app\conf\go-sign-desktop.properties”

  (if any changes applied from default values)
- Copy of

  “C:\Windows\ServiceProfiles\LocalService\Documents\Ascertia\Go-Sign-Desktop\GSD.db” file – *if explicitily asked by Service Desk*
- Browser console log file (F12 button)
- Browers network trace file (F12 button) – *only in case of network-related issue and if explicility asked by Service Desk*
- Relevant screenshots reporting any useful exception

It is higly suggested to check any expcetion first with the internal IT/Network support for a preliminary analysis and then with 4CB. NSP may be involved as well in case of network-related issues.

4.7.3.5.1 Client logging information and changing log level

ADSS Go>Sign Desktop application has two log levels. First informational, which is for normal use, and second, debug, which should only be used when investigating performance issues, functionality problems, etc. IT Admin can change Go>Sign Desktop log level at:

- multi user environment

  “C:\Program Files\Ascertia\Go-Sign-Desktop\app\conf\go-sign-desktop.properties”
- single user environment

“%userprofile%\AppData\Roaming\Ascertia\Go-Sign-Desktop\go-sign-desktop.properties”

File. To enable detailed debug logging, follow these instructions:

1. Go to the above path
2. Edit the go-sign-desktop.properties file using a suitable text editor.
3. Change the value of the property GOSIGN_DESKTOP_LOG_MODE from INFO to DEBUG and save the file.
4. Stop ADSS Go>Sign Desktop service and start it again
5. Retry the web failing web transaction to collect relevant trace files

4.7.4 GoSign Desktop client - Support and release policy

Ascertia is supporting current Ascertia GSD software major version 8.3. For this version, when they provide a fix, it increases the „patch“ version number (last number of the version, eg. 8.3.x) and issues a new binary release (eg. 8.3.6). In the same manner, when 4CB opens a ticket related to problems.

Usually, Ascertia releases a new patched version of GSD for issues or requests from 4CB side.

Before distributing any new release to the customer, 4CB tests it by doing an internal regression test, which goes in addition to the tests already done by Ascertia team.

Once a year, 4CB releases a certified version of GSD client which consists in a cumulative patches version or a new major version.

4CB will ask to customer to move to a certified version as:

- Certified version includes security fixes and cumulative patches (and it may already address the customer problem).
- Certified version is subject to full 4CB regression test.
- When a new certified version comes the older one is “decommissioned” and no more regression tests are performed for that old version.
- A patch requires anyway a new patched version built on top of the last available one (i.e. 8.3.7).

- When a ticket is opened on a certified version, 4CB can provide more assistance in reproducing issue, provide evidences when it needs to be routed to Ascertia.

4CB will internally have a regression instance for certified versions, but not for the one the decommissioned one. When tickets are opened on that versions 4CB can just act as a proxy with Ascertia support.

Current release / support policy may be subjected to changes which will be timely discussed and agreed with appropriate stakeholders

The following support/release policy for the GSD (SU and MU client) is foreseen in the medium term:

Q4.2024 Release of new 8.3.6 (836.836.060924.202409061918) client + parallel certification for 6.9.0.20 clients, status = completed
Q1.2025 GoSign version 8.3.6. (836.836.131124.202411131845), security hotfix, status = completed

Q2.2025 GoSign version 8.3.6. (836.836.230525.202505231938), security hotfix, status = in progress

Q4.2025 GSD client 6.9.0.20 is not more certified (3 months upgrade period available). Customer will be asked to upgrade to 8.3.6 , in case of tickets with 6.9.0.20.

Q4.2025 A new client version will be certified and released + parallel certification for 8.3.6 and new client version.

Please keep in mind: Customer should open support request to 4CB only and NOT to Ascertia directly. 4CB will involve Ascertia as appropriate.

All Rights reserved

4.7.5 Annex

4.7.5.1 SU client - Gosign certificate renewal procedure

Once the GoSign certificate will need to be renewed, please execute the following steps in order to proceed with renewal process:

1) Stop Go>Sign Desktop

2) Go to Go>Sign Desktop user directory i.e “C:\Users\%username%\AppData\RoamingAscertia\Go-Sign-Desktop“ and remove the files 'gosign.keystore' and ‘gosign.cer’.

3) Remove the existing GoSign certificate from the personal trust store (certmgr.msc)

4) Restart Go>Sign Desktop, it will prompt to install the new self-signed certificate.

In case of specific tools for installation or software distribution usage, this procedure may be verified in advance, and possibly adapted to needs.

4.7.5.2 MU client - Gosign certificate renewal procedure

Once the GoSign certificate will need to be renewed, please execute the following steps in order to proceed with renewal process:

1) Stop Go>Sign Desktop service;

2) Go to the folder “C:\Users\Public\Ascertia\Go-Sign-Desktop“, and remove all files, including 'gosign.keystore', gosign.cer’ and ‘cacerts’;

3) Remove the existing GoSign certificate from local machine trust store (certlm.msc);

4) Remove the existing GoSign certificate from admin user trust store (certmgr.msc);

5) Open a command line prompt as administrator or as an account that did the installation, then execute “C:\Program Files\Ascertia\Go-Sign-Desktop\Go-sign-desktop.exe”.

In that way, this command will add the GoSign certificate into the administrator trust store.

At the end, mandatorily close the user GSD instance before performing next step.

6) Open a command line prompt as administrator or as an account that did the installation, then execute “C:\Program Files\Ascertia\Go-Sign-Desktop\GSD.exe”.

This command will add the GoSign certificate into the local machine trust store

7) Restart the service

Procedure may need to be verified in advance and possibly adapted, in case specific tools for installation / software distribution have been adopted on customer side.

In case of terminal server cluster, the renewal procedure to follow for server >1 is described in the next section and has to start from step #2.

4.7.5.3 Distributing MU client on Terminal server cluster – suggested procedure

The following procedure has been correctly tested and implemented in order to distribute the MU client in a terminal server cluster:

1) install GSD MU 8.3.6 as described in this guide (on server > 1)
2) stop of any Go-Sign-Desktop instance possibly opened
3) remove GoSign certificate (generated by installation) from local machine trust store
4) remove GoSign certificate (generated by installation) from admin user trust store
5) copy/replace C:\Users\Public\Ascertia\Go-Sign-Desktop\gosign.cer file in server >1 (from server 1)
6) copy/replace C:\Users\Public\Ascertia\Go-Sign-Desktop\cacerts java keystore file in server >1 (from server 1)
7) copy/replace C:\Users\Public\Ascertia\Go-Sign-Desktop\gosign.keystore file in server >1 (from server 1)
8) Execute once from admin the command “C:\Program Files\Ascertia\Go-Sign-Desktop\Go-sign-desktop.exe” (or account that performed installation). This command will add the GoSign certificate into admin trust store. Then mandatorily close the user GSD instance before performing the next step.
9) Execute once from admin the command “C:\Program Files\Ascertia\Go-Sign-Desktop\GSD.exe” (or account that performed installation). This command will add the GoSign certificate into LM trust store
10) Restart the service

4.7.5.4 Most common issues

4.7.5.5 Windows service creation fails

In some specific cases, the installation may generate an incorrect Windows service definition. In the latter case, the service fails to start after the the installation.

To solve the issue it is possible to delete and manually recreate the service by following the steps:

- start command prompt as ADMIN;
- run `sc delete Go-Sign-Desktop`;
- `cd "C:\Program Files\Ascertia\Go-Sign-Desktop";`
- `Go-Sign-DesktopNT.exe //IS//Go-Sign-Desktop --Install="C:\Program Files\Ascertia\Go-Sign-Desktop\Go-Sign-DesktopNT.exe" --Jvm="C:\Program Files\Ascertia\Go-Sign-Desktop\runtime\jre\bin\server\jvm.dll" --`

```
StartMode=jvm --StopMode=jvm --Classpath="C:\Program Files\Ascertia\Go-
Sign-Desktop\app\lib\*";"C:\Program Files\Ascertia\Go-Sign-
Desktop\app\Go-Sign-Desktop.jar" --
StartClass=com.ascertia.adss.gosign.desktop.ASC_DesktopMain --
StartParams=start --
StopClass=com.ascertia.adss.gosign.desktop.ASC_DesktopMain --
StopParams=stop --Startup=auto
```

This procedure, can also be used for recreating the GSD service definition in any other case.

4.7.5.6 Useful log files

The three files attached contain logs of successful signing test cases, done with 6.9.0.20 client (SU: client application; MU: service and child instance;). They are meant to be checked by customer IT support in order to confirm the Ascertia local setup is working correctly, in a terminal server environment or in a desktop one.



SINGLE USER PKCS#11 LOG FILE.txt



MULTI USER PKCS#11 – SERVICE LOG FILE.txt



MULTI USER PKCS#11 – CHILD INSTANCE LOG FILE.txt