EUROPEAN CENTRAL BANK

EUROSYSTEM

General Information (Origin of Request) ☐ User Requirements (URD) ☒ Other User Functional or Technical Documentation (SYS)		
Request raised by: 4CB	**Institute:** 4CB	**Date raised:** 28/02/2019
Request title: T2-T2S Consolidation and ECMS will require an internal communication within the consolidated platform		**Request ref. no:** T2S 0702 SYS
Request type: Common	**Classification:** Maintenance	**Urgency:** Normal
1. Legal/business importance parameter: Medium	**2. Market implementation efforts parameter:** Low	
3. Operational/Technical risk parameter: Medium	**4. Financial impact parameter:** No financial impact	
Requestor Category: Eurosystem	**Status:** Implemented	

This Change Request is one of the T2S Change Requests related to the T2-T2S Consolidation Project. The tentative distribution of these Change Requests per functional area and T2S release is summarised in the table below (as of 2 November 2020):

	R4.0 (Jun 2020)	R4.2 (Nov 2020)	R5.0 (Jun 2021)	R5.2 (Nov 2021)	R6.0 (Jun 2022)	R6.2 (Nov 2022)
					T2S>ESMIG	
ESMIG (Connectivity)					CR-701	
CRDM (Reference data)	CR-719	CR-721	CR-704 CR-696		CR-705	
BILL (Billing)				CR-697	CR-706	
BDM (Business day)		CR-698			CR-707	
DWH (Historical data)					CR-699	
LEA (Legal archiving)					CR-700	
T2–T2S communication		CR-702 (ICL) CR-703 (camt.050)	CR-729			CR-734
Liquidity management			CR-708 (Outbound LT) CR-709 (Cash sweep)			
Maintenance window			CR-710			

Reason for change and expected benefits/business motivation:

At present, T2S middleware handles all incoming and outgoing communication with all T2S actors and other external systems (e.g. RTGS systems). For sending data to and receiving data from T2S the Data Exchange Protocol is used by T2S. The T2S actors can use the Application-to-Application (A2A) and User-to-Application (U2A) communication channels to access the T2S platform. For the A2A communication all incoming and outgoing messages and files are based on XML and comply with the ISO 20022 standard and specific requirements defined by T2S. Exceptions are flat files which are used for covering specific demands. Furthermore T2S uses a digital signature for incoming and outgoing communication.

In course of the CSLD project the T2S middleware will be replaced by ESMIG. ESMIG will only take over the external communication of T2 (CLM and RTGS), T2S, TIPS and ECMS. Therefore a new communication layer needs to be implemented for the internal communication of T2S with ECMS and CLM to ensure a proper data exchange.

Description of requested change:

T2S will establish a communication layer for the internal communication of T2S with ECMS and CLM. ESMIG will only be used for the external communication.

The communication (incoming and outgoing) between T2S, ECMS and CLM is A2A-only and based on messages that comply with the ISO20022 standard. Messages can be exchanged individually or in files or via flat files (exceptions for special reports). For the communication between CLM and T2S the following messages will be used:

- camt.025
- camt.050
- admi.007
- head.001
- camt.019
- camt.053 (provided that the CR 709 will be approved)
- camt.003 (Query Type Code CASB/OACC/OVAL)
- camt.004 (Query Type Code CASB/OACC/OVAL)

For the communication between ECMS and T2S the following messages will be used (:

- Admi.007
- Camt.019
- Camt.054
- head.001
- Sese.020
- Sese.023
- sese.024
- Sese.025
- Sese.027
- Sese.032
- Statement of Holdings (flat file);
- Statement of Transactions (flat file), and
- Statement of Pending Instructions (flat file)

This is not applied in the communication between the services and the common components (e.g. CRDM) where different channels (flat files, internal calls) will be implemented.

In this respect all auto-coll reference data messages (Reda.025, Reda.027, Reda.028, Reda.XXX (T2S CR-384), Reda.XXX (T2S CR-572)) and the Valuation Flat Files referring to CRDM are not handled via Internal Communication Layer. For these cases an own communication between CRDM and ECMS will be established.

The exchange of internal data between the services is handled via MQ SSL channels. In this context the data encryption of the communication is done on transport level. Moreover a certificate for authentication is provided on transport level by using the MQ SSL channel.

All internal communication between the services will use the T2S defined Business Application Header (except for flat files).

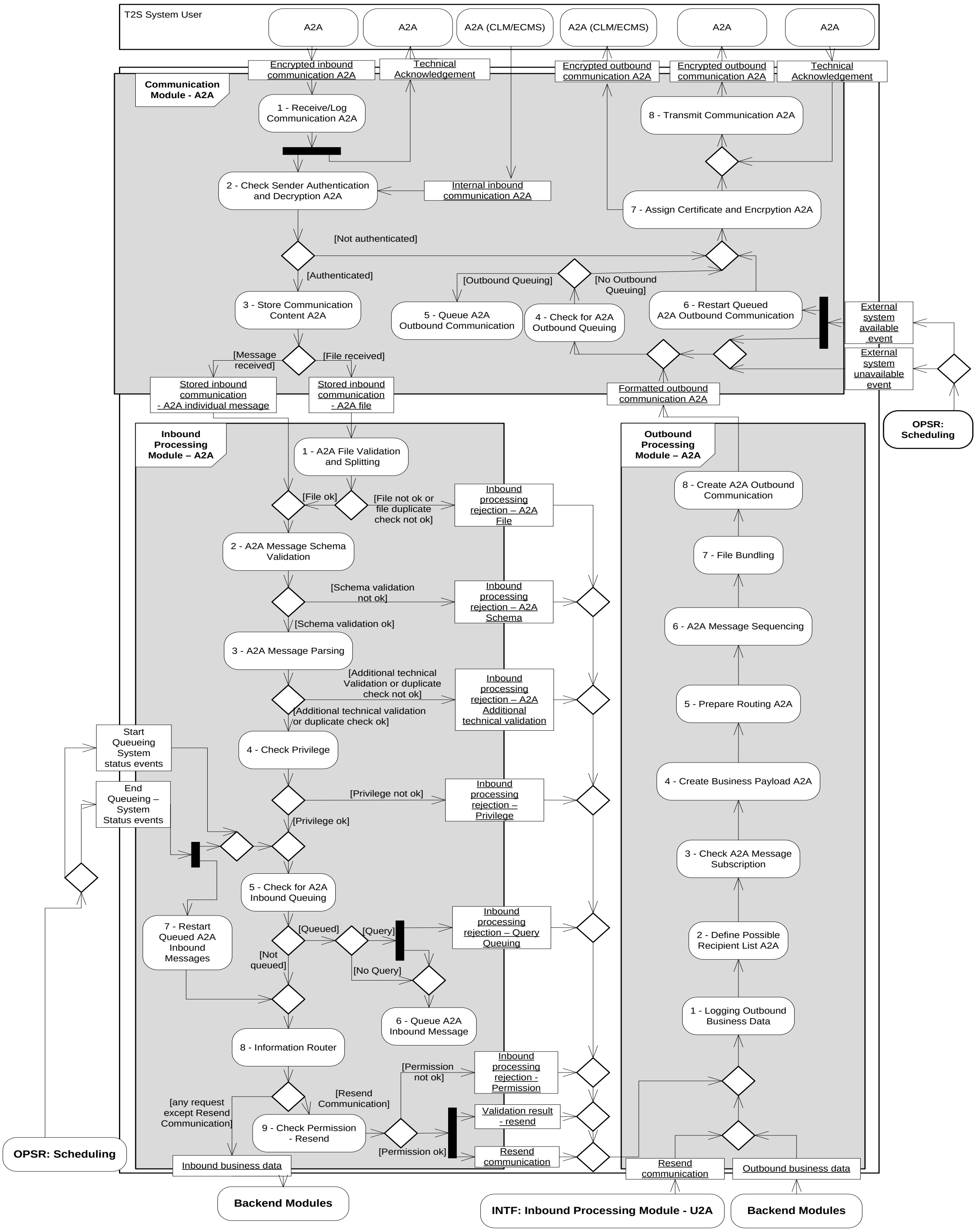
Signature will not be used for internal communication. In consequence any information about the Certificate DN for authentication the Business sending user in T2S is provided by the internal sender service for incoming messages. This will not apply to external communication.

Submitted annexes / related documents:

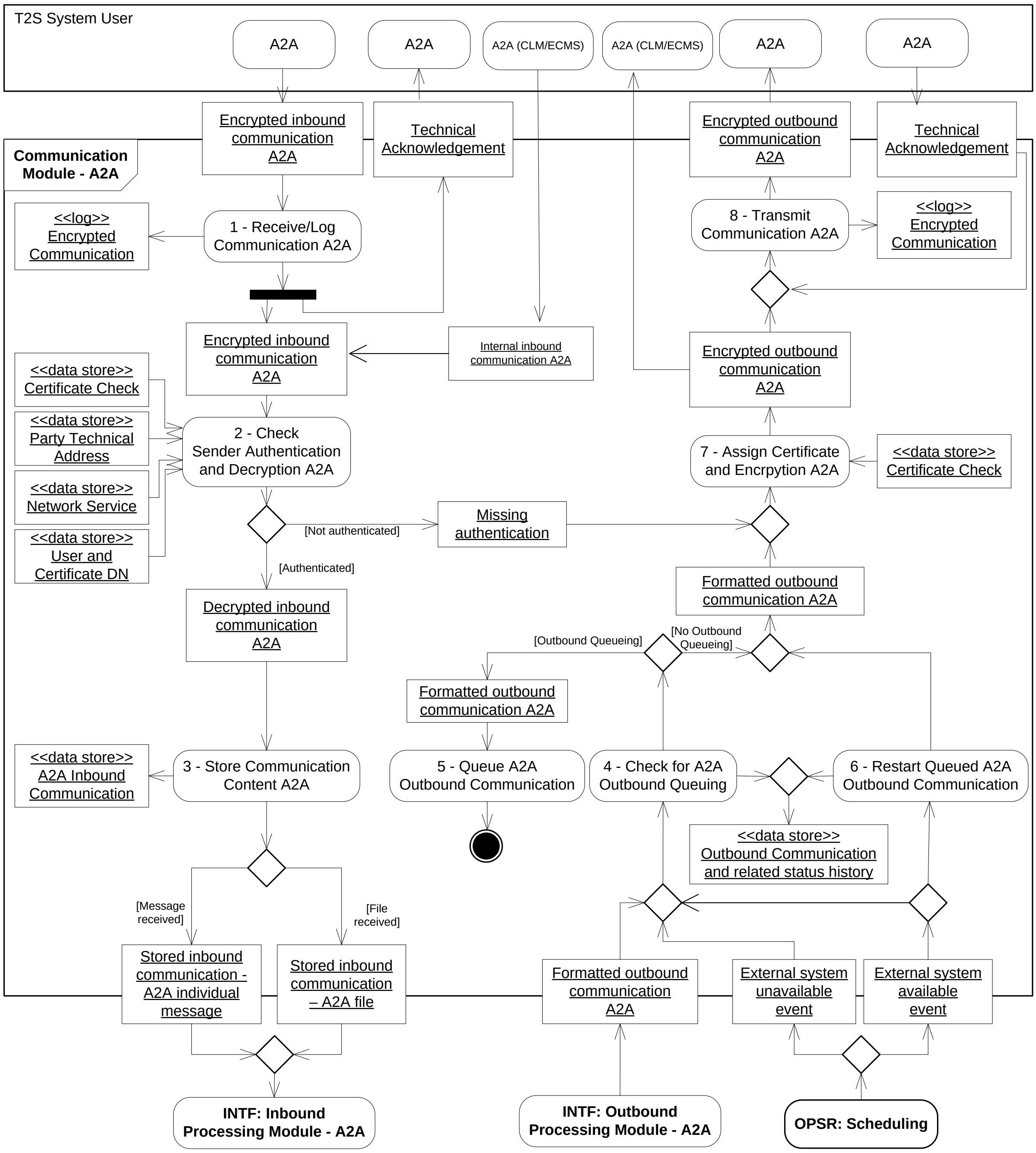
Proposed wording for the Change request:

GFS:

3.2.1 General Introduction


T2S System User
A2A
A2A
A2A (CLM/ECMS)
A2A (CLM/ECMS)
A2A
A2A
Encrypted inbound communication A2A
Technical Acknowledgement
Encrypted outbound communication A2A
Encrypted outbound communication A2A
Technical Acknowledgement
Communication Module - A2A
1 - Receive/Log Communication A2A
2 - Check Sender Authentication and Decryption A2A
Internal inbound communication A2A
8 - Transmit Communication A2A
7 - Assign Certificate and Encrpytion A2A
[Not authenticated]
[Authenticated]
[Outbound Queuing]
[No Outbound Queuing]
3 - Store Communication Content A2A
5 - Queue A2A Outbound Communication
4 - Check for A2A Outbound Queuing
6 - Restart Queued A2A Outbound Communication
External system available event
External system unavailable event
OPSR: Scheduling
[Message received]
[File received]
Stored inbound communication - A2A individual message
Stored inbound communication - A2A file
Formatted outbound communication A2A
Inbound Processing Module – A2A
1 - A2A File Validation and Splitting
[File ok]
[File not ok or file duplicate check not ok]
Inbound processing rejection – A2A File
2 - A2A Message Schema Validation
[Schema validation not ok]
Inbound processing rejection – A2A Schema
[Schema validation ok]
3 - A2A Message Parsing
[Additional technical Validation or duplicate check not ok]
Inbound processing rejection – A2A Additional technical validation
[Additional technical validation or duplicate check ok]
4 - Check Privilege
[Privilege not ok]
Inbound processing rejection – Privilege
[Privilege ok]
Start Queueing System status events
End Queueing – System Status events
5 - Check for A2A Inbound Queuing
7 - Restart Queued A2A Inbound Messages
[Queued]
[Query]
[Not queued]
[No Query]
Inbound processing rejection – Query Queuing
6 - Queue A2A Inbound Message
8 - Information Router
[Permission not ok]
Inbound processing rejection - Permission
[any request except Resend Communication]
[Resend Communication]
9 - Check Permission - Resend
Validation result - resend
[Permission ok]
Resend communication
Inbound business data
OPSR: Scheduling
Backend Modules
Outbound Processing Module – A2A
8 - Create A2A Outbound Communication
7 - File Bundling
6 - A2A Message Sequencing
5 - Prepare Routing A2A
4 - Create Business Payload A2A
3 - Check A2A Message Subscription
2 - Define Possible Recipient List A2A
1 - Logging Outbound Business Data
Resend communication
Outbound business data
INTF: Inbound Processing Module - U2A
Backend Modules

3.2.3.2 Diagram of the module


T2S System User
A2A
A2A
A2A (CLM/ECMS)
A2A (CLM/ECMS)
A2A
A2A
Communication Module - A2A
Encrypted inbound communication A2A
Technical Acknowledgement
Encrypted outbound communication A2A
Technical Acknowledgement
<<log>> Encrypted Communication
1 - Receive/Log Communication A2A
8 - Transmit Communication A2A
<<log>> Encrypted Communication
Encrypted inbound communication A2A
Internal inbound communication A2A
Encrypted outbound communication A2A
<<data store>> Certificate Check
<<data store>> Party Technical Address
<<data store>> Network Service
<<data store>> User and Certificate DN
2 - Check Sender Authentication and Decryption A2A
7 - Assign Certificate and Encrpytion A2A
<<data store>> Certificate Check
[Not authenticated]
Missing authentication
[Authenticated]
Formatted outbound communication A2A
Decrypted inbound communication A2A
[Outbound Queueing]
[No Outbound Queueing]
Formatted outbound communication A2A
<<data store>> A2A Inbound Communication
3 - Store Communication Content A2A
5 - Queue A2A Outbound Communication
4 - Check for A2A Outbound Queuing
6 - Restart Queued A2A Outbound Communication
<<data store>> Outbound Communication and related status history
[Message received]
[File received]
Stored inbound communication - A2A individual message
Stored inbound communication – A2A file
Formatted outbound communication A2A
External system unavailable event
External system available event
INTF: Inbound Processing Module - A2A
INTF: Outbound Processing Module - A2A
OPSR: Scheduling

3.2.3.3 Description of the functions of the module 2 – Check Sender Authentication and Decryption A2A

This function ensures that users without authentication are not able to compromise the communication processing in T2S. It uses a strong authentication mechanism with PKI (Public Key Infrastructure) **{T2S.11.440}** to avoid intrusion and unauthorised access to T2S **{T2S.18.770}**.
For every Encrypted inbound communication A2A flow the function identifies the sender and checks if the digital signature of the inbound communication corresponds to the certificate of the sender.
Furthermore this function also receives the *Internal inbound communication A2A flow* that handles the inbound communication sent by CLM or ECMS to T2S. This function also identifies the T2S System User, the used Certificate DN and the communicating T2S Party **{T2S.12.120}** and it checks the party technical address **{T2S.12.110}** and the network service used for the communication by associating the sender information of the inbound communication with the relating static data in-formation.

The function rejects the Encrypted inbound communication A2A or the *Internal inbound communication A2A* if one of these checks fails. The function forwards the Missing authentication flow (including error information) to the Assign Certificate and Encryption A2A function and initiate the process to deliver it to the sender if the mandatory routing information(that means the data of the original sender) is available. Otherwise, the message Missing authentication cannot be delivered.

If the function has positively checked the sender authentication of the communication, it converts the Encrypted inbound communication A2A flow and the *Internal inbound communication A2A flow* into the Decrypted inbound communication A2A flow (including decompression if necessary) and routes it to the function Store Communication Content A2A.

3.2.3.3 Description of the functions of the module 7 - Assign Certificate and Encryption A2A

This function receives:

- Formatted outbound communication A2A flows;
- Missing authentication flows.

In case of the Missing Authentication flow this function creates the related XML error message.

For both cases the function checks if the receiver of the communication will be CLM/ECMS or another T2S System User. In case the receiver of the communication is CLM or ECMS the function delivers the Encrypted outbound communication A2A directly.

In case the T2S System user is different to CLM/ECMS ~~For both cases~~ this function enciphers the communication with the public encryption key of the receiver and compresses it if necessary.

If the processing for real-time requests takes longer than the T2S timeout limit the transfer mode of the response changes to store and forward. If the communication exceeds the size limitation for the Message-Channel T2S sends the communication via the File Channel. Communications that exceed also the size limitation of the File Channel are blocked by the network.

After that the function delivers the Encrypted outbound communication A2A to the function Transmit Communication ~~U~~A2A.

3.2.3.4 Description of the Input/ Output of the module

Flow	IN/OUT	Description	FROM	TO
…	…	…	…	…
Encrypted inboundcommunicationA2A	IN	Messages and files received by T2S via A2A	T2S System User	
Internal inbound communication A2A	IN	Messages and files received by T2S from CLM/ECMS	T2S System User	

High level description of Impact:

Outcome/Decisions:

*CRG on the 20 March 2019: The CRG agreed to launch the preliminary assessment of CR-702.

* CRG on the 21 May 2019: The CRG agreed to recommend this Change Request for authorisation by the Steering Level.

* AMI-SeCo on the 28 May 2019: The AMI-SeCo has agreed to the recommendation of the CRG to authorise this Change Request.

* CSG on 29 May 2019: The CSG has agreed to authorise this Change Request via a written consultation.

* NECSG on 29 May 2019: The NECSG has agreed to authorise this Change Request via a written consultation.

* MIB on the 18 June 2019: The MIB agreed to authorise CR-702.

* PMG on 21 June 2019: The PMG proposed to the T2S Steering Level the Change Request for R4.2.

* CRG on the 3 September 2019: The CRG agreed to recommend to the PMG the implementation of the CR in R4.2

* PMG 4 September 2019: The PMG recommended to the Steering Level the approval of CR-702 for R4.2

* OMG on 23 September 2019: the OMG did not identify a potential operational impact for the CR.

* NECSG on 7 October 2019: the NECSG approves the allocation of the CR to the scope of R4.2.

* CSG on 7 October 2019: the CSG approves the allocation of the CR to the scope of R4.2

* MIB on 8 November 2019: The MIB approved of the inclusion of the CR in R4.2.

Preliminary Assessment:

- **Impacted modules:** INTF inbound and outbound processing
- **Findings:** no specific issues
- **Release Allocation:** Targeted T2S R4.2 has been confirmed, might be subject to change with result of CR Detailed Assessment
- **Open questions:** no open questions

EUROSYSTEM ANALYSIS – GENERAL INFORMATION

Impact On T2S	**Static data management**		**Interface**	
		Party data management	X	Communication
		Securities data management		Outbound processing
		T2S Dedicated Cash account data management		Inbound processing
		Securities account data management		
		Rules and parameters data management		
	Settlement		**Liquidity management**	
		Standardisation and preparation to settlement		Outbound Information Management
		Night-time Settlement		NCB Business Procedures
		Daytime Recycling and optimisation		Liquidity Operations
		Daytime Validation, provisioning & booking	**LCMM**	
		Auto-collateralisation		Instructions validation
				Status management
	Operational services			Instruction matching
		Data Migration		Instructions maintenance
		Scheduling	**Statistics, queries reports and archive**	
		Billing		Report management
		Operational monitoring		Query management

				Statistical information
				Legal archiving
		All modules (Infrastructure request)		
		No modules (infrastructure request)		
		Business operational activities		
		Technical operational activities		

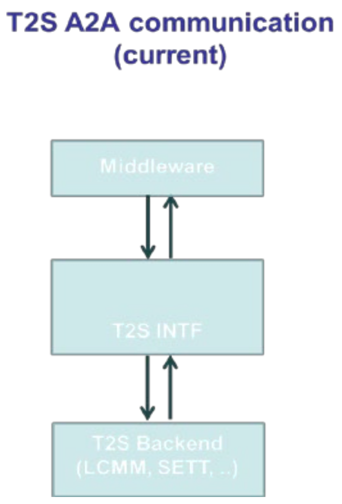
Impact on major documentation		
Document	**Chapter**	**Change**
Impacted GFS chapter	3.2.1 General Introduction	Update Overall Diagram A2A to introduce new flow
	3.2.3.2 Diagram of the module	Update the Diagram of the module to introduce new flow
	3.2.3.3 Description of the functions of the module 2 – Check Sender Authentication and Decryption A2A	Update of the description regarding the new flow that needs to be introduced
	3.2.3.3 Description of the functions of the module 7 - Assign Certificate and Encryption A2A	Update of the description regarding the internal and external communication
	3.2.3.4 Description of the Input/ Output of the module	Introduction of new flow
Impacted UDFS chapter		

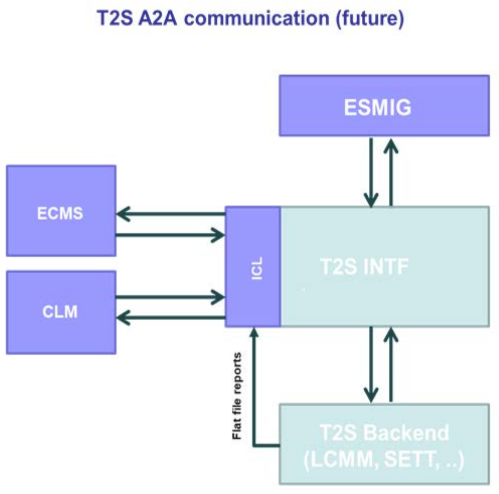
Links with other requests				
Links	Reference		Title	

OVERVIEW OF THE IMPACT OF THE REQUEST ON THE T2S SYSTEM AND ON THE PROJECT

Summary of functional, development, infrastructure and migration impacts

In course of the CSLD project the T2S middleware will be replaced by ESMIG. As ESMIG will only be used for the external communication, T2S will establish a communication layer for the internal communication of T2S with ECMS and CLM. The Internal Communication Layer is not the T2S INTF but will be linked to the T2S INTF and LCMM.
The following graphics are showing the current and the future structure:





The Communication between T2S and CLM and ECMS is based on usage of

- ISO Messages/Files
- ISO reporting or flat file reporting (the later directly from backend module without passing through INTF)

In this respect the following messages are exchanged by the T2S INTF and CLM via Internal Communication Layer:

- camt.025
- camt.050
- admi.007
- head.001
- camt.019
- camt.053 (provided that the CR 709 will be approved)
- camt.003 (Query Type Code CASB/OACC/OVAL)
- camt.004 (Query Type Code CASB/OACC/OVAL)

Between the T2S INTF and ECMS the following messages are exchanged via Internal Communication Layer:

- Admi.007
- Camt.019
- Camt.054
- head.001
- Sese.020
- Sese.023
- Sese.024
- Sese.025
- Sese.027
- Sese.032

Moreover the following flat files are exchanged between LCMM and ECMS via Internal Communication Layer:

- Statement of Holdings (flat file);
- Statement of Transactions (flat file), and
- Statement of Pending Instructions (flat file)

All auto-coll reference data messages (Reda.025, Reda.027, Reda.028, Reda.XXX (T2S CR-384), Reda.XXX (T2S CR-572)) and the Valuation Flat Files referring to CRDM are not handled via Internal Communication Layer. For these cases an own communication between CRDM and ECMS will be established.

All internal communication between the services will use the T2S defined Business Application Header (except for flat files).

Signature will not be used for internal communication. In consequence any information about the Certificate DN for authentication the Business sending user in T2S is provided by the internal sender service for incoming messages.

In this respect a new flow for the incoming internal communication (ISO messages/files) must be created and needs to be introduced in the INTF. Furthermore a check to guarantee the differentiation between external communication and communication (ISO messages/ files) relating to CLM and ECMS must be included in the outbound processing. The INTF will only handle ISO messages and files. Flat File Reports will not be routed through the INTF.

Main Cost Drivers

The main cost drivers of this CR are the implementation of a new input flow to receive the communication (ISO messages/files) from CLM and ECMS and to introduce a check in the outbound processing that ensures the sending of outbound communication(ISO messages/files) relevant for CLM and ECMS to the internal communication layer.

In addition, the CR-0702 will support the connectivity to T2 (CLM) and Target2 CUST (PMG AP from 18 July 2019): Each party in T2S has to configure its routing rules for the communication with T2S, indicating among other parameters the Network Service and the Party Technical Address. The same rules will apply also for the internal communication layer. Using the Network Service and the Party Technical Address specified in the routing rules, T2S will be able to distinguish between communications to be routed via the internal communication layer or communications to be routed via ESMIG.

With this approach, the connection to Target2 CUST will remain unchanged and will be performed through T2S Middleware as it is performed now. On the other hand the connection to CLM will be performed through the internal communication channel. It is important to highlight that T2S –Target2 CUST connection is based on T2S-Middleware and also that on T2S side it is not possible to have a parallel connection with T2S-Middleware and T2S-ESMIG.
Summary of project risk
None.
Security analysis
No adverse effect has been identified during security assessment.