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: ESMIG impact on T2S		**Request ref. no:** T2S 0701 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:

The original connectivity models for TARGET2 and T2S are based on the existing License Agreements (LAs) in place with the relevant Network Service Providers (NSPs).

Fig.1 – Existing Target2/T2S connectivity model

On 30th November 2018 a new NSP LA was introduced for TIPS, which entailed the deployment of some common components as part of the T2-T2S Consolidation project. In particular, the Eurosystem Market Infrastructure Gateway (ESMIG) channels all NSP access to TIPS and the Common Reference Data Management component ($CRDM^{TIPS}$).

The A2A/U2A interface layer provided by T2S Interface (INTF) remained in place for handling instructions received through the existing NSP channels and directed to T2S.

- As of June 2022, the usage of common components will be extended to T2S; in particular, ESMIG will handle all connectivity to TIPS and T2S as well as Common Components.
- As of November 2022 the usage of common components will be extended also to the new T2.

Until 11 June 2022 it shall be possible for T2S users to keep on sending messages as they do today.

In June 2022 (R6.0), when the T2S LAs will expire, there will be the final stage of the transition into the “to-be” model outlined below: ESMIG will handle all connectivity to Eurosystem Market Infrastructure Services and common components, including TIPS, CRDM and T2S. All external connections and traffic directed to European Market Infrastructure Services and the related components will be routed through ESMIG to the relevant business interfaces (e.g. T2S INTF).

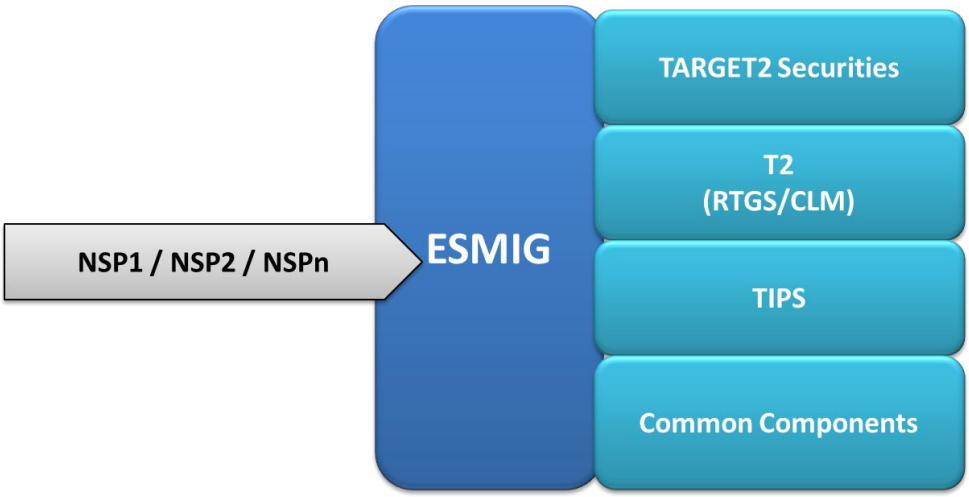


Fig.2 - "To-be" connectivity model

This Change Request describes the impact expected on T2S with the implementation of the “to-be” connectivity model.

Description of requested change:

The T2S connectivity model will shift from the current one to cover new License Agreements potentially including different NSPs from the current ones. The Eurosystem Market Infrastructure Gateway (ESMIG) will handle all connectivity to the system.

Additional changes are listed below.

Interim connection between T2S and TARGET2

TARGET2 will be connected with T2S via new TARGET2 IDM – ESMIG connection between 11 June 2022 and November 2022. Therefore a change is necessary due to different DEP protocol.

External communication with DEP

T2S currently uses a Data Exchange Protocol (DEP) to identify the service used to send messages and files for routing purposes. The current version of the DEP v1 protocol includes the counterpart name, message pattern (Message/File, Real-time/Store&Forward) and logical environment of reference.

With the introduction of ESMIG an enriched DEP v2 protocol will be used including, in addition to the aforementioned values, the addressed service and component name (e.g. T2S, CRDM, CLM etc.). In this way ESMIG will be able to route messages to different Services or components correctly.

Session handling

The ESMIG represents the single access point for the external communication to all market infrastructure services. ESMIG is the access portal for U2A users to all underlying business applications, with a U2A single sign-on architecture which requires the session handling processing, performed only at ESMIG level. T2S currently processes the session handling on the INTF U2A level, which would need to be changed to the new behaviour according to the ESMIG design.

When a DN is authenticated by the Identity Access Manager the ESMIG Portal shows the list of services and common components the user is authorised to access, and the list of logical users linked to the user’s DN, segregated by service, including T2S.

In the specific business case of T2S, after the selection of T2S service and logical user, the user is redirected to the home page of the web application.

Common NRO-functionality

The Non-repudiation of origin functionality (NRO) is intended to protect against the originator's false denial of having sent the message. With the go-live of T2-T2S Consolidation, ESMIG will offer a common functionality for non-repudiation for all services and common components: for this reason, T2S NRO functionality should be changed according to the ESMIG design.

Message Specifications

Changes to the message specifications of acmt.025, acmt.026 and acmt.007, caused by TIPS CR 0033, will be implemented for T2S users with the migration to ESMIG.

DMT access

The Data Migration Tool will be accessible from the ESMIG Portal, and no longer from the SOPS page.

Submitted annexes / related documents:

AR.1.1 Technical Requirements and Compliance Check included in the NSP tender procedure containing DEP samples

https://gareappalti.bancaditalia.it/esop/guest/go/opportunity/detail?opportunityId=244

Annex: GFS Wording Proposal

Proposed wording for the Change request:

UDFS v.5.2 section 1.3.2.3 Authorisation process
Replacement of references to the welcome screen with ESMIG Portal.

GFS

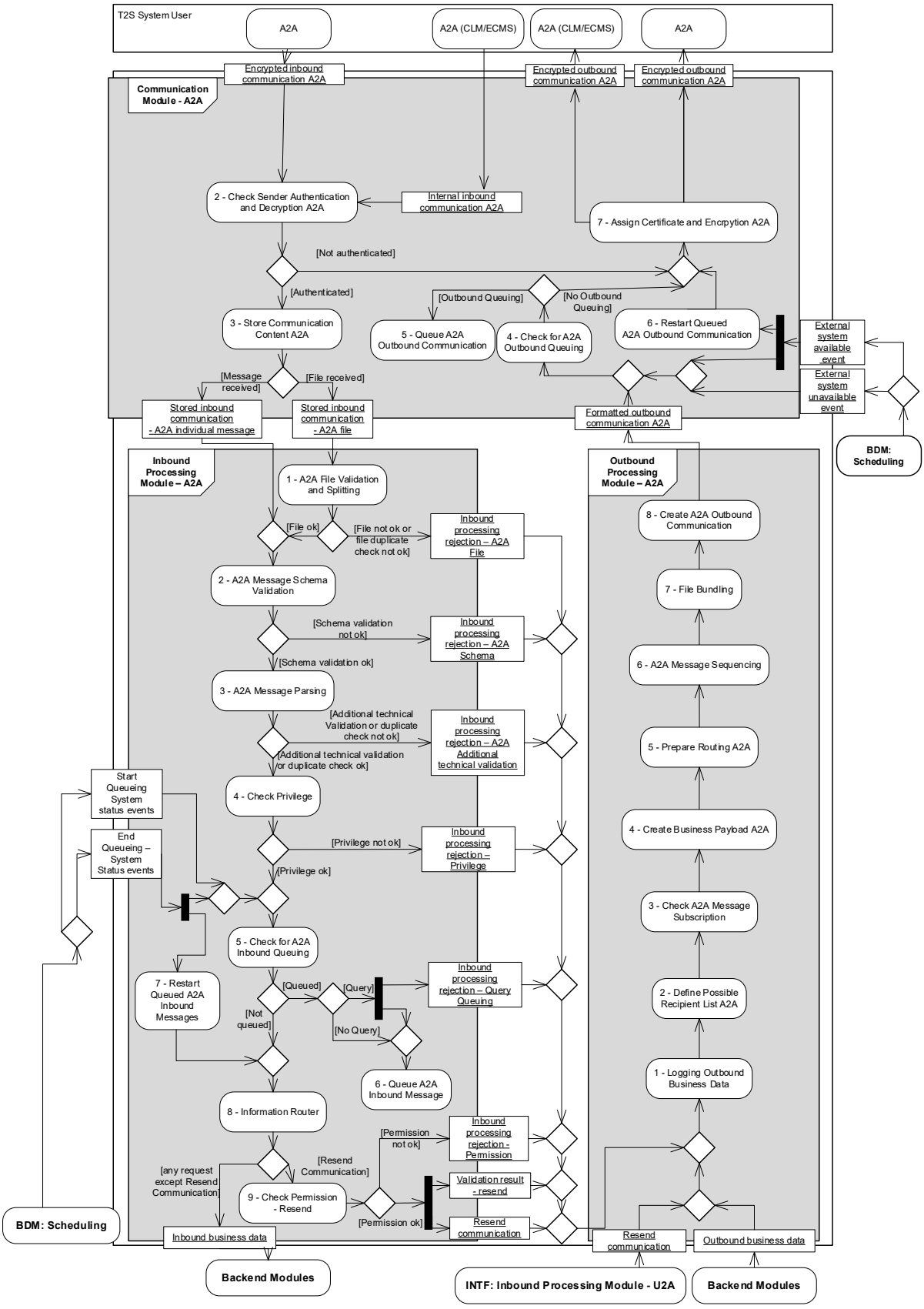
1.1 ESMIG – Introductory chapters, cf. annex

2.3.1 Interface
T2S supports the connectivity of T2S Actors as follows:
l T2S communication is available by using messages or files containing messages in Application-to-Application mode (A2A) that allows direct communication between software applications via XML messages as well as through online-screen based activities in User-to-Application mode (U2A) for activities per-formed by T2S System Users. ~~Flat files are used, as mandatory type of communication, for Securities Valuations only. Additionally CSDs may decide to receive some specific reports via flat file instead of XML;~~

2.3.1.1 Communication Module
The main purpose of the Communication Module is to ensure secure and reliable communication between the T2S platform and T2S Actors. T2S System Users can use Application-to-Application (A2A) and User-to-Application (U2A) communication channels to access the T2S platform. The Outbound Processing Module for Application-to-Application mode provides a single set of standard messages to facilitate communication with multiple external RTGS systems and with multiple external collateral management systems. ~~For Securities Valuation communication only, communication is mandatorily handled via flat files. Additionally CSDs may decide to receive some specific reports via flat file instead of XML.~~

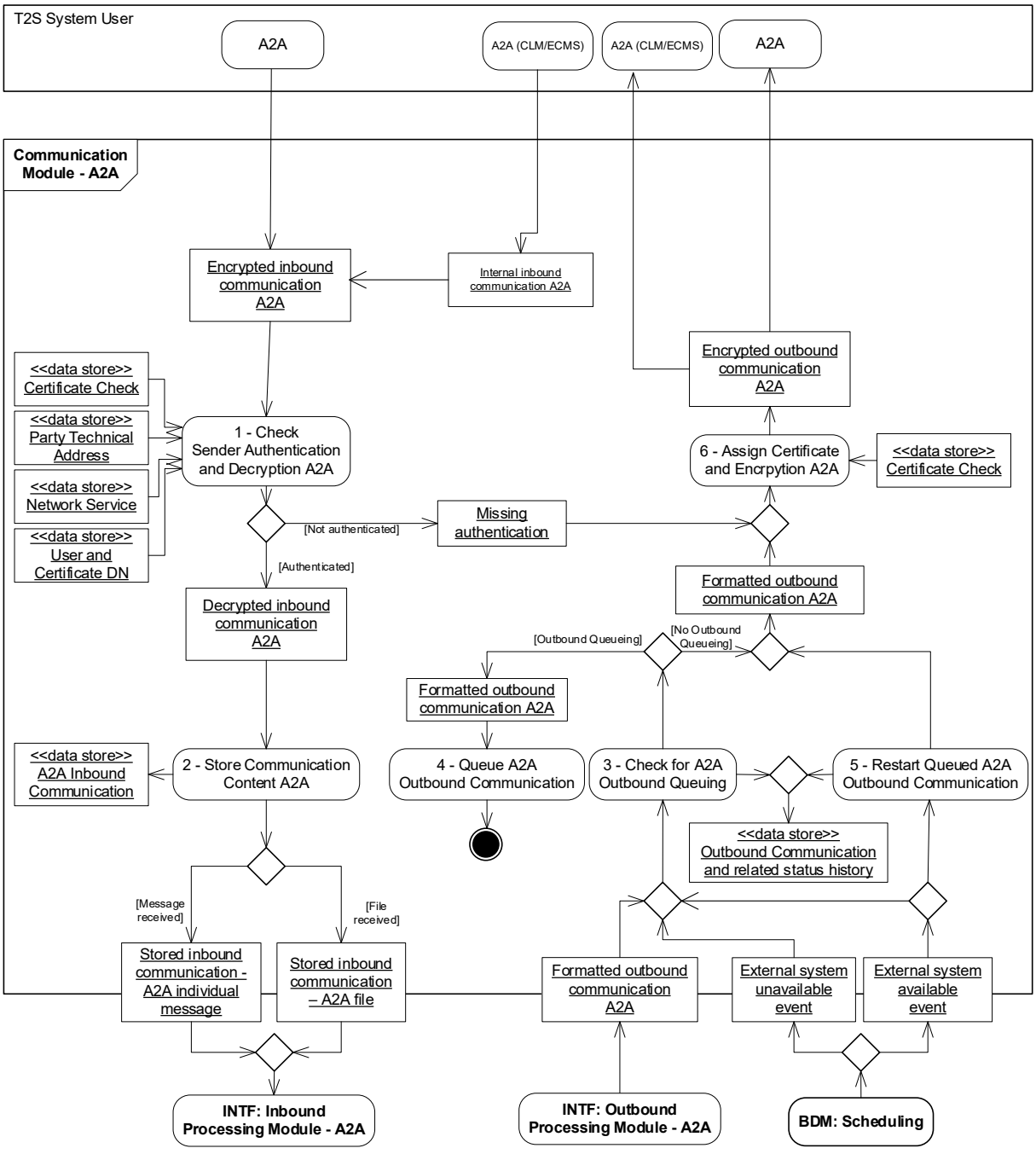
3.2.1 General Introduction
T2S supports access via two communication modes:
l The application-to-application mode (A2A), allowing direct communication between software applications via XML messages ~~and for the specific non-standard case of securities valuation and for specific reports via flat files~~;
l The user-to-application mode (U2A), supporting activities performed manually by the T2S System Users via the Graphical User Interface (GUI).

The following activity diagrams depict the high-level interactions between the modules and functions of the Interface domain.

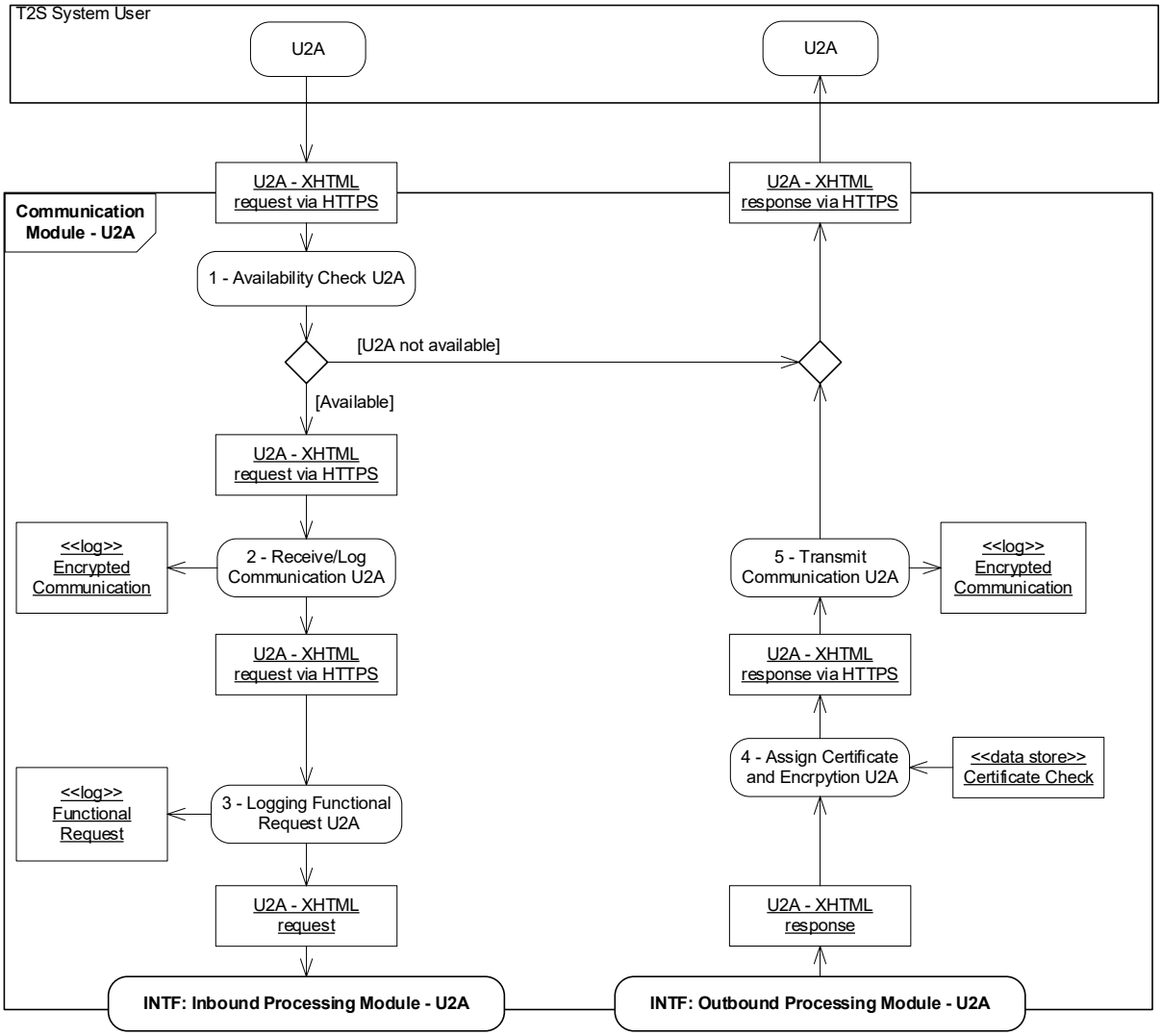

T2S System User
A2A
A2A (CLM/ECMS)
A2A (CLM/ECMS)
A2A
Encrypted inbound communication A2A
Encrypted outbound communication A2A
Encrypted outbound communication A2A
Communication Module - A2A
2 - Check Sender Authentication and Decryption A2A
Internal inbound communication A2A
7 - Assign Certificate and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

3.2.3.1 Description of the module
Additionally, the Communication Module provides functionality to protect the T2S platform against intrusion and unauthorised access. ~~It checks that a trusted party transmitted the inbound communication through a secure channel.~~ It provides an authentication functionality to verify identity of the T2S System User to other functions or modules. ~~Finally, the Communication Module is responsible for the management of Public Key Infrastructure (PKI) certifi-cates, required for the T2S System User authentication, decryption of T2S inbound communication and encryp-tion of T2S outbound communication including compression handling.~~
The Communication Module is composed out of three sub-modules:
- Communication Module for Application-to-Application mode;
- Communication Module for User-to-Application mode;
- ~~Communication Module for Certificate Management~~.

3.2.3.2 Diagram of the module
Communication Module for Application-to-Application mode (A2A)



Communication Module for User-to-Application mode (U2A)



3.2.3.3 Description of the functions of the module
Communication Module – Application-to-Application
~~1 - Receive/Log Communication A2A~~

~~Reference Id INTF.COM-A2A.RLC.1.1~~
~~This function is an entry point for the A2A access of T2S System Users to the T2S Interface domain {T2S.12.060}.~~
~~This function stores the Encrypted Inbound Communication A2A, which T2S receives from a T2S System User, in the log Encrypted Communication for short term traceability.~~
~~The Receive/Log Communication A2A function accepts the inbound communication, which it receives from all technical connectivity channels supported by T2S.~~
~~The function forwards the Encrypted Inbound Communication A2A flow to the Check Sender Authentication and Decryption A2A function. The function also sends a technical acknowledgement in order to confirm the ac-ceptance of a message {T2S.13.087}.~~

1~~2~~ – Check Sender Authentication and Decryption A2A

Reference Id INTF.COM-A2A.CSA.1.1
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}.~~

2~~3~~ – Store Communication Content A2A

3~~4~~ – Check for A2A Outbound Queuing

4~~5~~ – Queue A2A Outbound Communication

5~~6~~ – Restart Queued A2A Outbound Communication

6~~7~~ - Assign Certificate and Encryption A2A
Reference Id INTF.COM-A2A.ACE.1.1
This function receives:
l Formatted outbound communication A2A flows;
l 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 Sys-tem 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 this function enciphers the communication with the public en-cryption 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 re-sponse 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 ESMIG. ~~the function Transmit Communication 2A~~

~~8 – Transmit Communication A2A~~
~~This function receives the Encrypted outbound communication A2A flow. The function stores it in the log En-crypted Communication for short term traceability and sends it to the T2S actor in the A2A mode.~~
~~The function also receives the "Technical Acknowledgement" in order to allow the recipient of the communica-tion to confirm the receipt {T2S.13.088}.~~

Communication Module – User-to-Application
2 - Receive/Log Communication U2A
Reference Id INTF.COM-U2A.RLC.1.1
This function is responsible for the logging of the received U2A-XHTML request via HTTPS. It stores the com-munication in the log Encrypted Communication for short term traceability and then forwards it to the function Logging Functional Request U2A ~~Check Sender Authentication and Decryption U2A~~.

~~3 - Check Sender Authentication and Decryption U2A~~
~~Reference Id INTF.COM-U2A.CSA.1.1~~
~~This function ensures a strong authentication mechanism via two-factor authentication {T2S.18.810} to avoid intrusion and unauthorised access to T2S {T2S.18.770}.~~
~~When starting a new session with the first U2A-XHTML request, the function identifies the sender {T2S.12.120}. The function therefore verifies the login data depending on the defined type of authentication and the remaining data (e.g. Lockout Status) based on the T2S System User information and the used Certifi-cate DN described in Static Data Management {T2S.11.440} and ensures that the communication was sent from a recognised technical address {T2S.12.110}.~~
~~The function requires the authentication credentials on the initial login for the connection to T2S during the start of a T2S session. This authentication remains active for the entire session. Unlike A2A communication, U2A mode does not require user identification data for each action/message.~~
~~The function rejects the request if it cannot authenticate the sender. It also communicates the failed authentica-tion to the user by sending the Missing Authentication flow (including reason information) directly to the function Assign Certificate and Encryption U2A.~~
~~If the user is authenticated, the U2A-XHTML request is routed to the Logging Functional Request U2A function.~~

3~~4~~ – Logging Functional Request U2A

4~~5~~ – Assign Certificate and Encryption U2A
Reference Id INTF.COM-U2A.ACE.1.1
This function receives the U2A-XHTML response flow ~~or a Missing authentication flow~~, creates the enciphered XHTML response and delivers it as the U2A-XHTML response via HTTPS flow to the Transmit Communication U2A function.
5~~6~~ – Transmit Communication U2A

Reference Id INTF.COM-U2A.TRC.1.1
This function receives an U2A-XHTML response via HTTPS, stores it in the log Encrypted Communication for short term traceability and sends it to the original sender.

~~Communication Module – Certificate Management~~
~~The certificate management is closely linked to the connectivity services offered by network providers licensed for T2S. Detailed information will therefore be provided in a specific documentation related to connectivity ser-vices.~~
~~The input and output flows and the data stores regarding certificate maintenance request/response will be de-tailed in the specific documentation related to connectivity services.~~

3.2.3.4 Description of the Input/Output of the module

FLOW	IN/OUT	DESCRIPTION	FROM	TO
...				
~~Technical Acknowledgement~~	~~IN~~		~~T2S System User~~	
...				
~~Technical Acknowledgement~~	~~OUT~~			~~T2S System User~~
~~...~~				

MyStandards Message specifications
With TIPS CR 0033, acmt.025, acmt.026 and acmt.007 schemas will be amended in order to accommodate the new account type “TIPS Ancillary System Technical Account”.
The updated schemas will be available to T2S users with the migration of T2S to ESMIG.
Older versions of the messages will be decommissioned with the go-live of T2-T2S Consolidation.

Outcome/Decisions:

* CRG on the 20 March 2019: The CRG agreed to launch the preliminary assessment of CR-701.
* CRG on the 3 September 2019: The CRG agreed to recommend the CR for authorisation by the T2S Steering Level.
* AMI-SeCo on 16 October 2019: The AMI-SeCo agreed with the recommendation of the CRG.
* CSG on 25 October 2019: The CSG authorised the CR for allocation to a T2S release.
* NECSG on 28 October 2019: The NECSG authorised the CR for allocation to a T2S release.
* MIB on 8 November 2019: The MIB authorised CR-701.
* PMG on 27 March 2020: The PMG proposed to allocate this CR to T2S release 6.0
* CRG on 18 December 2020: The CRG agreed to recommend to the PMG the inclusion of CR-701 in R6.0.
* OMG on 21 December 2020: the OMG identified an operational impact for CR-701.
* PMG on 22 December 2020: the PMG recommended the inclusion of CR-701 in STP for R6.0 for approval by the Steering Level.
* CSG on 7 January 2021: the CSG approved the inclusion of CR-701 in the STP for R6.0.
* NECSG on 7 January 2021: the NECSG approved the inclusion of CR-701 in the STP for R6.0.
* MIB on 11 February 2021: the MIB approved the inclusion of CR-701 in the STP for R6.0
* OMG on 7 April 2021: the OMG confirmed the operational assessment of CR-701.

Preliminary assessment:

- **Impacted modules:** INTF
- **Release: 6.0 (June 2022)**
- **Findings:**

  Due to the current assumption of selecting both the service and the logical user for the U2A access from the ESMIG Portal, this proposal implies the decommissioning of the current T2S Welcome page.

- **Open issues/ questions to be clarified by the originator:**

  None.

Detailed assessment

EUROSYSTEM ANALYSIS – GENERAL INFORMATION

T2S Specific Components		Common Components
LCMM		
	Instructions validation	
x	Status management	
	Instruction matching	
	Instructions maintenance	
x	Penalty Mechanism	
Settlement		
	Standardisation and preparation to settlement	
	Night-time Settlement	
	Daytime Recycling and optimisation	
	Daytime Validation, provisioning & booking	
	Auto-collateralisation	
Liquidity Management		
	Outbound Information Management	
	NCB Business Procedures	
	Liquidity Operations	
T2S Interface *(as of June 2022 without Static Data Management, Communication for SDMG, Scheduler, Billing)*		
X	Communication	
	Outbound Processing	
	Inbound Processing	
Static Data Management *(until June 2022)*		**Common Reference Data Management** *(from R6.0 June 2022)*
	Party data management	Party data management
	Securities data management	Securities data management
	Cash account data management	Cash account data management
	Securities account data management	Securities account data management
	Rules and parameters data management	Rules and parameters data management
Statistics and archive		**Statistics and archive**
	Statistical information (until June 2022)	Short term statistical information
	Legal archiving (until June 2022)	Legal archiving (from R6.0)
		Data Warehouse (from R6.0)
Information *(until June 2022 containing reference data)*		**CRDM business interface** *(from R6.0 June 2022)*
	Report management	Report management
	Query management	Query management
		Communication
		Outbound Processing
		Inbound Processing
Operational Services		
	Data Migration (T2S DMT)	Data Migration (CRDM DMT, from R6.0)
	Scheduling (until June 2022)	Business Day Management (from R6.0)
		Business Day Management business interface (from R6.0)
	Billing (until June 2022)	Billing (from R6.0)

			Billing business interface (from R6.0)
	Operational Monitoring		Operational and Business Monitoring
	MOP contingency templates		

Impact on major documentation		
Document	**Chapter**	**Change**
Impacted GFS chapter	1.1 ESMIG	Introductory chapters
	2.3.1 Interface	Removal of flat file reference
	2.3.1.1 Communication Module	Removal of flat file reference
	3.2.1 General Introduction	Removal of flat file reference and update of diagram
	3.2.3.1 Description of the module	Update of functions
	3.2.3.2 Diagram of the module	Update of diagrams
	3.2.3.3 Description of the functions of the module	Update of functions
	3.2.3.4 Description of the Input/Output of the module	Removal of ACK flow
Impacted UDFS chapter	1.3.2.3 Authorisation process	Replacement of references to the welcome screen with ESMIG Portal.
Additional deliveries for Message Specification (UDFS, MyStandards, MOP contingency templates)	acmt.025 acmt.026 acmt.007	New common schemas will apply for T2S users, These will include changes implemented with TIPS CR 0033, for the usage of a new Cash Account Type for TIPS.
UHB		
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

- Changes to connection TARGET2 – T2S for interim period between ESMIG migration of T2S with 6.0 and go-live of CSLD with R6.2 (not considered in the CR PA, CSLD re-planning impact):
  A change has to be applied to T2S ESMIG instance to support an additional communication channel (over 4CBNET) between T2S and TARGET2 between R6.0 and R6.2 due to the re-planning of the CSLD project to the new go-live to November 2022. T2S must be able to route messages for TARGET2 via ESMIG limiting the impact on TARGET2. The upgrade of the DEP protocol entails the installation of the new version and configuration of the new queues. All the messages from TARGET2 are sent to T2S – INTF only (i.e. no more than 1 component on T2S side can be addressed by this solution).
  Also TARGET2 will be connected with T2S via new TARGET2 IDM – ESMIG connection between June 2022 and November 2022.

  The decommissioning of the A2A flow(s) acmt.025/026 between T2S-INTF and SDMG will be postponed until T2 go-live and managed by a PBI+ an editorial CR.

- Changes to T2S INTF for the connectivity to Target2 (considered in the CR PA)

  All middleware related tasks (e.g. decompression, timeout handling), that will be provided by ESMIG in future, will be removed from INTF.

  A2A-/ U2S-impact:

  - Adapt A2A flows.
  - Delete signature-related business rules.
  - Adapt A2A flows in order to be compatible with new ESMIG interface (new "root element" in messages exchanged with ESMIG).
  - Disable the current Login IAM page and perform the redirection to the T2S Home page
  - Disable the DN and user authentication functionality, which will be performed at ESMIG level.
  - Read and store the new connection parameters coming from ESMIG
  - Adapt the session handling to redirect to the indicated page on logout and parametrize the SSO logout URL.

- Changes to T2S LCMM flat file function for the connectivity to ESMIG (not considered in the PA) The inbound and the outbound flows between LCMM and INTF need to be modified to align them to the new ESMIG software. This means that the message properties block of the inbound and outbound flows that constitute the flat-file report bounded for the Middleware (EoD reporting and Penalties reporting) and the Bulk File received from the Middleware need to be changed.

- Changes to T2S Waterfall process for the connectivity to ESMIG (not considered in the PA).

  The transition from IDM to ESMIG will cause an impact on existing WATERFALL PROCESS also at ESMIG side.Due to the design of T2S and the synchronous processing of transaction, the Waterfall (technical) process ensures that all transactions are taken into account and have at least one settlement attempt when they are received before a certain cut-off time.
  Due to the split off of SDMG to the common components, transactions previously related to SDMG have to be removed from the waterfall process of T2S.

Other functional impacts:

- The Data Migration Tool will become accessible from the ESMIG Portal and no longer from the SOPS page.T2S will migrate to the new message specifications for acmt.025, acmt.026 and acmt.007 impacted by TIPS CR 0033.

Impact on other TARGET Services and projects
This CR has no impact on other services or projects (CSLD, ECMS, TIPS)
Summary of project risk
n.a.
Security analysis
No adverse effect has been identified during security assessment.