EUROPEAN CENTRAL BANK

EUROSYSTEM

T2S CHANGE REQUEST FORM			
General Information (Origin of Request) ☒ User Requirements (URD) or GUI Business Functionality Document (BFD) ☒ Other User Functional or Technical Documentation (SYS)			
Request raised by: Clearstream	**Institute:** CSD	**Date raised:** 11/07/2023	
Request title: T2S should verify whether the certificate used to sign NRO is linked to the user initiating the signature		**Request No.:** T2S 0810 BFD	
Request type: Common	**Classification:** Scope Enhancement	**Urgency:** Fast-track[1]	
1. Legal/business importance parameter[2]: High		**2. Market implementation efforts parameter**[3]: Low	
3. Operational/Technical risk parameter[4]: Low		**4. Financial impact parameter**[5]: Low	
Requestor Category: CSD		**Status:** Implemented	

Reason for change and expected benefits/business motivation:

Non-repudiation of origin (NRO) was introduced into T2S with T2S Change Request *T2S 0466 BFD "Implementation of non-repudiation for U2A",* and subsequently updated via T2S Change Request T2S-0722-BFD "Upgrade of non-repudiation for U2A".

However, it was identified in recent testing activities that there might be a gap in the implementation of NRO. Namely, INC00000032822 / PBI000000225637 highlighted the fact that T2S does not verify whether the logged in user that initiates the action to be signed is linked to the certificate that is used for signing.

This seems to be in conflict with the *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*, which says in Article 2, No.2 that an "[…] *'advanced electronic signature' means an electronic signature which meets the following requirements:*

- *(a) it is uniquely linked to the signatory […]*
- *(b) it is capable of identifying the signatory;*
- *(c) it is created using means that the signatory can maintain under his sole control; and*
- *(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;"*

whereby Article 2, No. 3 clarifies that "'*signatory' means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents*".

In the T2S NRO case, the logged in user initiates the action to be signed, and in order to do so, this user must *"hold a signature-creation device",* i.e. this user must be able to access the token that is used for signing. However, T2S does not verify whether the token used for signing is linked to the signatory, i.e. to the logged in user that initiates the action to be signed.

This gap shall be closed by applying such checks whenever a token is used to sign an NRO activity.

[1] Fast-track justification: A fast-track approach is requested due to the importance of removing the operational security risk that could imply that a user (signing user) might sign a transaction in 4-eyes principle that was previously submitted by a different user (logged-in user).
[2] Legal/business importance parameter was set to High because this change improves the safety of the application.
[3] Market implementation effort parameter was set to Low because this change does not require any changes by T2S Actors. It is implemented purely on T2S side.
[4] Operational/technical risk parameter was set to Low because this change does not imply any operational impact on T2S Actors. It is implemented purely on T2S side.
[5] Low < 100kEUR < Low-Medium < 200 kEUR < Medium < 400kEUR < High < 700kEUR < Very high

Description of requested change:

The following validation rules shall be implemented into T2S and into any related Common Component:

- The certificate DN used for login must be linked to the U2A user (i.e. to the user that is logging in into T2S or any Common Component)
- The certificate DN used for business signature must be linked to the business sending U2A user (i.e. to the user that pushed the submit button to send an instruction, to adjust reference data, to approve any action in 4-eyes mode, or to initiate any other action that requires NRO within T2S or any Common Component).
- The certificate DN used for business signature must be linked to the business sending A2A user (i.e. to the business sending user that sends a message or a file via A2A channel into T2S or into any Common Component).

Submitted annexes / related documents:

Outcome/Decisions:

*ECB on 11 July 2023: the ECB team checked the completeness of the CR template, assigned change request number CR-0810 and informed the CR initiator.
*CRG on 17 October 2023: the CRG agreed to recommend CR-0810 for T2S Steering Level Authorisation, following a fast-track approach.
*AMI-SeCo on 3 November 2023: the AMI-SeCo agreed with the CRG recommendation of CR-0810 for T2S Steering Level Authorisation, following a fast-track approach.
*CSG on 6 November 2023: the CSG agreed to authorise CR-0810, following a fast-track approach.
*NECSG on 6 November 2023: the NECSG agreed to authorise CR-0810, following a fast-track approach.
*MIB on 8 November 2023: the MIB agreed to authorise CR-0810, following a fast-track approach.
*PMG on 12 December 2023: the PMG agreed to launch the detailed assessment of CR-0810 with a view of scoping in R2024.NOV.
*OMG on 22 May 2024: the OMG identified no operation impact from the inclusion of CR-0810 in the scope of R2025.JUN.
*CRG on 29 May 2024: the CRG agreed to recommend to the PMG the inclusion of CR-0810 in the scope of R2025.JUN.
*PMG on 6 June 2024: the PMG agreed to recommend the inclusion of CR-0810 in the scope of R2025.JUN.
*CSG on 12 June 2024: the CSG approved the inclusion of CR-0810 in the scope of R2025.JUN.
*NECSG on 12 June 2024: the NECSG approved the inclusion of CR-0810 in the scope of R2025.JUN.
*MIB on 19 June 2024: the MIB approved the inclusion of CR-0810 in the scope of R2025.JUN.

Documentation to be updated:

T2S UHB
1.2.3 Validation
[…]

Digital Signature NRO	In order to ensure non-repudiation of origin (NRO) for critical transactions, the system foresees the use of a digital signature for specified screens. This means that the user must will be asked to enter a PIN code for signature purposes whenever an instruction is initiated. The certificate used for digital signature must be linked to the logical "user" logged in T2S. With the entry of the PIN, T2S attaches a digital signature to the instruction entered by the T2S actor.

CRDM UHB Book 1

1.2.3 Validation

In CRDM, all submission processes undergo various validations, which take place in the front-end and/or in the back-end. Only correct entries, fulfilling all predefined criteria, can be further processed. To indicate the status of the recently performed action, CRDM uses two different types of messages to indicate a successful or failed validation as described below.

In addition to the automatic validation carried out by CRDM, human validation can be imposed by using the 4-eyes mode.

Furthermore, non-repudiation of origin (NRO) is implemented for a specified number of screens.

[…]

Second User

After the first user has entered, changed or deleted the data, a second user (with the required privilege) has to approve or revoke this action via the *data changes* screen [] either using the 4-eyes mode ID or the search functionality.

As soon as the data changes are positively approved, CRDM marks these data as approved and they are forwarded to further processing.

Digital Signature NRO

In order to ensure non-repudiation of origin (NRO) for critical transactions, the system foresees the use of a digital signature for specified screens: the user must enter a PIN code for signature purposes whenever a specific action is initiated. The certificate used for digital signature must be linked to the logical “user” logged in CRDM. With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the actor.

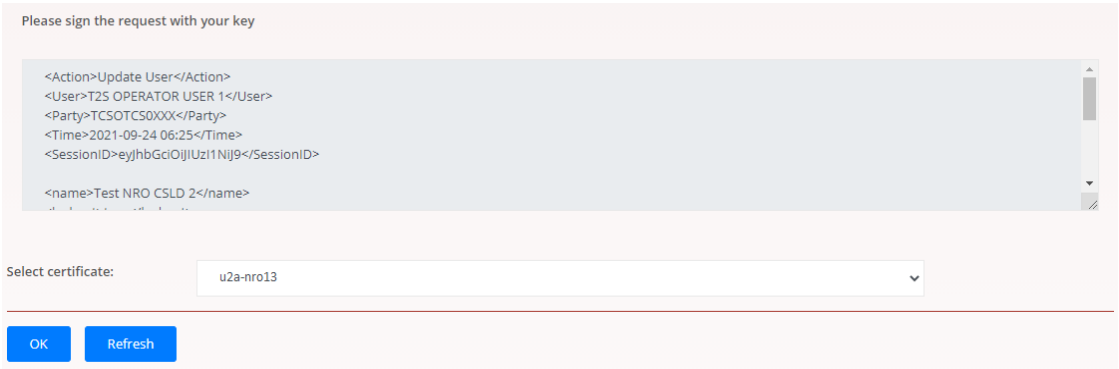

Illustration 1: Digital Signature

[…]

1.2 Digital Signature

1.2.1 Digital Signature (NRO)

Overview

This business section describes in a general way the interaction of the actors with the Digital Signature.

Application of a Digital Signature is applicable for the following GUI screens when performing the listed actions:

Digital Signature	
Cash Account - New/Edit screen	Submit
Standing Order For Reservation – Details screen	Delete Restore
Standing Order For Reservation - New/Edit screen	Submit
Standing Order For Reservation - Search/List screen	Delete Restore
Standing/Predefined Liquidity Transfer Order – Details screen	Delete Restore
Standing/Predefined Liquidity Transfer Order - New/Edit screen	Submit
Standing/Predefined Liquidity Transfer Order - Search/List screen	Delete Restore
Data Changes – Details screen	Submit
Grant/Revoked Privileges - Selection criteria screen	Grant Revoke
Grant/Revoke Role - New/Edit screen	Grant Revoke
Grant/Revoke System Privilege - New/Edit screen	Grant Revoke
Restriction Type - Search/List screen	Delete Restore
Restriction Type - New/Edit screen	Submit

Role - Search/List screen	▪ Delete ▪ Restore
Role - New/Edit screen	▪ Submit
User - Details screen	▪ Delete ▪ Restore
User - New/Edit screen	▪ Submit
User - Select/List screen	▪ Delete ▪ Restore
User-Certificate DN Link - Select/List screen	▪ Delete ▪ Restore
User-Certificate DN Link - New/Edit screen	▪ Submit

Business Scenario

The actor that is performing a business scenario linked to the screens and the buttons listed above must consider these steps as part of the specific business scenario.

1. Select the needed item or input the desired values, then click on the action button (Submit, Delete, Restore, Grant, Revoke).
2. User selects the signing certificate to sign from the drop down list. If the digital identity is not linked to the logged user then the "OK" button is not enabled, and the following error is displayed: "The selected certificate is not linked to the logged user". If the digital identity is linked to the logged user then the "OK" button is enabled.
3. Once ~~prompted~~ clicked the "OK" button, ~~with the request~~ user is requested to ~~of~~ insert~~ing~~ the PIN associated with the digital identity, insert the PIN and click the OK button.

⇨ The action initiated by the actor is concluded and the request is digitally signed.

BFD:

6) Digital Signature: Non-repudiation of origin
For a specific set of sensitive U2A functions the T2S GUI will require the digital signing of an instruction performed either in two-eyes or in four-eyes mode. The user needs a public certificate associated with a private key stored on a portable device (SmartCard or USB-token) or a Remote Hardware Security Module which will be accessible after entering a PIN code. The logged in user that initiates the action to be digitally signed, has to be linked to the public certificate that is used for signing.

Preliminary assessment:

Not available, fast-track approach.

Detailed assessment:

EUROSYSTEM ANALYSIS – GENERAL INFORMATION

T2S Specific Components		Common Components	
LCMM			
	Instructions validation		
	Status management		
	Instruction matching		
	Instructions maintenance		
	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		**Eurosystem Single Market Infrastructure Gateway** (from R6.0 June 2022)	
	Communication		Communication
	Outbound Processing		Outbound Processing
X	Inbound 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
		X	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		No impact
Impacted UDFS chapter		No impact
Additional deliveries for Message Specification (UDFS, MyStandards, MOP contingency templates)		No impact
UHB	1.2.3 Validation 3.2.1 Digital Signature (NRO)	Specification that the certificate used for digital signature must be linked to the logged U2A user
Other impacted documentation (FA Sch. 05, FA Sch. 07)		No impact
Impacted GDPR message/ screen fields		No impact
Other documentations	BFD	6) Digital Signature: Non-repudiation of origin: adding condition

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
The Change requests foresee the following requirements: 1. The certificate DN used for login must be linked to the U2A user (i.e. to the user that is logging in into T2S or any Common Component) 2. The certificate DN used for business signature must be linked to the U2A user. 3. The certificate DN used for business signature must be linked to the business sending A2A user. Point 1 is currently foreseen via ESMIG portal, since the displayed user ID are always linked to provided certificate. Point 3 is realised via Business rule ICSA013 that checks for A2A whether the certificate used to sign is linked to the System User Reference mentioned in the business application header. Point 2 must be realised at level of digital signature, checking that the certificate used for digital signature is linked to the logged U2A user. **Main cost drivers:** - Implementation of new check between certificated DN, business signature and U2A User [51%] - Testing of the new functionality [31%]
Impact on other TARGET Services and projects
Impact on other Eurosystem Services T2, TIPS or Projects, ECMS
Summary of project risk
No risk has been identified during detailed assessment.
Security analysis
No adverse effect has been identified during detailed assessment.

06 May 2024

Cost assessment on Change Requests

T2S-810-SYS – T2S should verify whether the certificate used to sign NRO is linked to the user initiating the signature			
One-off	Assessment costs* - Preliminary - Detailed	 not charged 10,000.00	 Euro Euro
One-off	Development costs	76,153.82	Euro
Annual	Operational costs - Maintenance costs - Running costs	 6,641.04 0.00	 Euro Euro

*The relevant assessment costs will be charged regardless of whether the CR is implemented (Cf. T2S Framework Agreement, Schedule 7, par. 5.2.3).