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 SYS
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]: (provided by 4CB)
Requestor Category: CSD		**Status:** Authorised at T2S Steering Level

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 business sending 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:

*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.

Documentation to be updated:

Preliminary assessment:

Detailed assessment: