EUROPEAN CENTRAL BANK

EUROSYSTEM

TARGET2-SECURITIES

General Information (Origin of Request)		
☒ User Requirements (URD) or Business Functionality Document ☐ Other User Functional or Technical Documentation (SYS)		
Request raised by: Deutsche Bundesbank on behalf of the German NUG	**Institute:** Deutsche Bundesbank	**Date raised:** 11/12/2013
Request title: User authentication without USB-token/SmartCard for GUI-access		**Request ref. no:** T2S 0444 BFD
Request type: Common	**Urgency:** Normal	
1. Legal/business importance parameter: High	**2. Market implementation efforts parameter:** Medium	
3. Operational/Technical risk parameter: Medium	**4. Financial impact parameter:**	
Requestor Category: Central Bank	**Status:** Authorised at Steering Level	

Reason for change and expected benefits/business motivation:

During various meetings of T2S bodies and T2S WS CSDs and users had reservations concerning the way foreseen by the Eurosystem to implement a strong authentication for U2A access via USB-token or smart card. In the meeting of the German NUG, which took place on 15 November 2013, the issue was raised again and qualified as showstopper by some NUG members. In the meantime various actors have gained an exceptional permission to use a USB-port to migrate to T2S. But it is not sure, how long this permission can be maintained.

A mandatory use of a USB-token/SmartCard for T2S GUI access poses requirements on the user's side on the availability of certain hardware (e.g. USB ports) which is on the one hand not compatible with virtualization technologies (such as Citrix) which are widely used on the user's side, and on the other hand not compliant with internal IT security requirements of a vast majority of users (where USB ports are typically blocked in production environments).

In more detail there are several reasons which hinder to use a USB token or a SmartCard, such as:

- Respectively the usage of USB-ports is restricted/blocked to be compliant with internal IT Security Regulations and Information Security Management Systems.
- The solution must also meet incident/emergency procedures where the user might be required to remotely connect to the user's workstation (e.g. remote-on-call-duty, incident-room/location). Banks are forced by regulators to have back-up office space to be used in emergency cases. If primary site is evacuated and additional hardware is lost, contingency office space cannot be used to access T2S.
- Participants do request a hardware-independent solution as with the current solution they will not be able to receive authentication meaning they will not be able to access the T2S GUI (neither for testing nor for production).

Description of requested change:

NUG members did not question the need for a strong (2-factor) authentication as such. However, they urgently requested an alternative solution that does not depend on the availability of a particular hardware on the user's side (comparable to the one applied for the T2 ICM), and that in particular does not require a USB port as a pre-condition to connect to T2S (e.g. a solution based on disconnected token (SecureID remote token) could be envisaged). A change might also be needed in the NSP's access processes since the Login window is provided by the NSP.

After searching for adequate alternatives meeting the requirements for a strong authentication the DE AMI SeCo NSG deemed the **Soft Token / RSA Token** as viable alternative solution. This RSA / Soft Token is an additional piece of hardware that does not need to be plugged in a USB-port. It regularly generates a new PIN to be entered while log in to the system.

Moreover, this new RSA / Soft Token should not only be used for the Login to the T2S GUI, but also for the NRO function. Currently also the NRO applet uses the USB Token for authentication (via a second certificate stored on the token). Since the alternative RSA / Soft Token is replacing the USB Token, it should be valid for all current use cases of the USB Token.

In addition the Eurosystem is currently working on further market infrastructures:

- The TIPS project (TARGET Instant Payment Settlement) will go live in November 2018. The connection to TIPS will work via the new ESMIG Service (Eurosystem Single Market Infrastructure Gateway). To log in via U2A to TIPS it is planned to use a USB-Token (analogue T2S) as well. The duration of the contracts for TIPS with the NSPs (which determine the usage of the USB Token) will last until 2021.
- The TARGET2/T2S consolidation project will go live in November 2021. The login (for A2A as well as for U2A) will be done via the ESMIG as well. So far no requirements for the login process have been defined.

The DE AMI SeCo NSG pushed for a uniform authentication process to all future Eurosystem services. Therefore the alternative (RSA / Soft Token) should be valid

- For CLM / RTGS services, that are parts of the T2/T2S consolidation, as of November 2021
- For TIPS as of November 2021
- For T2S as of 2022 (as soon as the NSP contracts expire)
- For NRO as soon as the support for the JAVA applet expires.
- For ECMS as of GoLive (planned for November 2022)

Submitted annexes / related documents:

High level description of Impact:

Outcome/Decisions:

***** CRG decision on 16 December 2013: The CRG decided to put the Change Request on hold and invited the directly-connected participants to seek support from the VAN network providers.

***** CRG decision on 10 February 2014: The CRG decided to keep the CR on hold and wait for a more detailed analysis of the current elements and constraints from the T2S PO and the 4CB.

***** CSG meeting on 7-8 April 2014: The T2S Programme Office informed the CSG about the status of Change Request 0444-BFD (User authentication without USB-token for GUI-access), and confirmation has been received from both 4CB and the VANs that a change to the implementation would require changes to the T2S Application and to the Security Services provided by the VAN-NSPs and cannot be made available for the go live. We acknowledge that other implementations may be possible to meet the requirement of "strong authentication" and could be considered in a future release of T2S. Any new implementation in the future would require an end to end solution involving the VAN-NSP providers in any case.

***** E-mail sent by the T2S Programme Office to the CRG on 9 April 2014: The CRG were informed that confirmation has been received from both 4CB and the VANs that a change to the implementation would require changes to the T2S Application and to the Security Services provided by the VAN-NSPs and cannot be made available for the go live. We acknowledge that other implementations may be possible to meet the requirement of "strong authentication" and could be considered in a future release of T2S. Any new implementation in the future would require an end to end solution involving the VAN-NSP providers in any case. We prepared a presentation summarising these main points:

https://www.ecb.europa.eu/paym/t2s/progress/pdf/tg/crg/crg22/2014-04-09_presentation_on_use_of_usb_token_in_t2s.pdf

***** CRG meeting on 28 May 2014: The CRG recommended to park the Change Request potentially for a future release of T2S.

* CRG meeting on 06 September 2016: The CRG agreed to keep the Change Request on hold and do not submit it for preliminary assessment for the time being.

* CRG on the 28 November 2018: The CRG took note that the requirements of the Change Request will be covered by the T2-T2S Consolidation Project.

* CRG on 09 November 2021: the CRG agreed to recommend CR-0444 for authorisation by the T2S Steering Level

*CSG on 17 November 2021: the CSG agreed to authorise CR-444

*NECSG on 17 November 2021: the NECSG agreed to authorise CR-444

*AMI-SeCo on 19 November 2021: the AMI-SeCo agreed with the CRG recommendation of CR-444 for T2S Steering Level Authorisation

*MIB on 24 November 2021: the MIB agreed to authorise CR-444

Documentation to be updated:

The technical changes related to CR-444 is covered by the implementation of CR-701. Therefore, CR-444 has been changed to an editorial CR to reflect changes needed to the BFD.

BFD-chapter 9 Annex B – Technical annex – HW Requirement for PC, page 174

6) HW Requirements for PC
The T2S Web based GUI has no special requirements regarding the PC used to connect to T2S. Thus any standard commercial state-of-the-art PC can be used for the connection via the T2S GUI. Furthermore a computer mouse and a keyboard are required to use the Web based GUI and unless authentication certificates are stored on a Remote Hardware Security Module, at least one USB port is required for authentication facilities (SmartCard reader or USB-token). The T2S GUI does not support specialised hardware devices (for example Braille keyboards etc.).
The recommended resolution will be at least 1024x768.

BFD-chapter 9 Annex B – Technical annex – HW Requirement for PC, page 175

9) Digital Signature: Non-repudiation of origin 13
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 certificate, the technical specification of the key storage, the policies regarding the PIN and its maintenance will be issued by the Network Service Provider (NSP) selected by the T2S Actor.