EUROPEAN CENTRAL BANK

EUROSYSTEM

General Information (Origin of Request) ☐ User Requirements (URD) / BFD ☒ Other User Functional or Technical Documentation (SYS)		
Request raised by: Eurosystem	**Institute:** 4CB	**Date raised:** 25/10/2019
Request title: Upgrade of non-repudiation for U2A		**Request ref. no:** T2S-0722-BFD
Request type: Common	**Classification:** Maintenance	**Urgency:** Fast-track
1. Legal/business importance parameter: Medium		**2. Market implementation efforts parameter:** Medium
3. Operational/Technical risk parameter: Medium		**4. Financial impact parameter:** No financial impact
Requestor Category: 4CB		**Status:** Allocated to a release

Reason for change and expected benefits/business motivation:

After the deployment of CR-466 in T2S, the general URD requirement that *"… a very high level of security is requested in terms of confidentiality, authentication, integrity, access control and non-repudiation of the T2S information"* was eventually fulfilled so that changes performed via the T2S Graphical User Interface (GUI) could not be denied by its originator.

Main Repudiation Scenarios	Non-repudiation services
Originator denies having sent a U2A instructions **or** **One entity argues on the U2A instruction content**	Non-repudiation of origin (**NRO**) provides the recipient with the evidence NRO which ensures that the originator will not be able to deny having sent the U2A instruction The evidence of origin is generated by the originator and held by the recipient.

After consultation of the various bodies (CRG, ISSG and Legal experts), the CSDs opted for the use of a digital signature for critical / user-selected transactions only via X.509 standard certificates stored in a secure USB device (e.g. USB token) or accessible via a secret PIN code.

Current solution is based on Java applet that are recalled by the web application screens via Java Script (embedded in the html pages). Applet allows calling the APIs of the USB token, which allows on turn the generation of the digital signature (PKCS#11 standard protocol).

After several years from its development, such technology (based on NPAPI - Netscape Plugin API plugin) has been considered not safe enough and also shows performance problems in comparison with the possibilities offered by plug-in free technologies (e.g. HTML5).

This led to:

- browser vendors to phase out NPAPI support starting from 2013; IE11 is the only browser still supporting Java applet, but for IE 11 the support is limited. For Windows 7 it will end 14/01/2020 and for Windows 10 in 14/10/2025 .

- Oracle to announce that applet support may be removed any time in Java SE8 (as of March 2019) even if there are currently no plans to remove the components required to run applets

After a thorough investigation of the market solutions, it was decided to extend the adoption of the Ascertia solution (ADSS server + ADSS Go>Sign Client Apps) that is currently used in T2 Internet Access and CoreNet context and that has already proved to be reliable, stable and responsive from a performance point a view.

Once IE11 will not be supported anymore, the usage of the GoSign Desktop client, in particular, will be mandatory.

The solution that will be implemented will also allow using customer certificates stored on remotely connected HSM (and not only on locally-connected HSM as the existing USB tokens) as of June 2022 (R6.0 – date of migration from T2S to ESMIG).

Description of requested change:

The change activity includes the installation and customization of the Ascertia Desktop Signing Services (ADSS) components (server and client modules), the adaption of T2S GUI application and for those users whose IT configuration does not contain the Applet technology anymore the possibility to have a dedicated desktop software (Go>Sign Desktop).

The organisational aspects concerning the provision of this software will be dealt with updating the NRO technical document which will also provide steps for the Go>Sign Desktop installation.

Go>Sign Client applications installation and customization support will be offered by T2S Service Desk and 4CBs technical and administration teams.

As this will be the U2A NRO solution adopted by ESMIG for T2 –T2S – TIPS services and ECMS only one Go>Sign Desktop application version will be used and distributed.

Go>Sign Client applications are already in use in TARGET2 for Internet Access and Contingency Network, 4CBs will guarantee that no different client versions are needed by TARGET2 and T2S even before the go-live of CSLD project. Until T2 will go in Production (November 2021), TARGET2 and T2S GUI users will have to use different certificates. After T2 Production, NSPs certificates will be supported as in the current scenario.

Impact for the customers will be clearly described in the updated NRO technical documentation (including the revised qualified configuration) while ADSS Go>Sign software licensing costs will be covered as part of the Change Request.

During an ad interim phase, the following technical distinction is made:

a.) Microsoft Internet Explorer IE11 supports Java Applet technology, thus the access to T2S U2A NRO via Ascertia Applet is given

b.) Other browsers will use Ascertia Desktop only client

Due to significantly different signature / verification processes, IBM applet cannot co-exist with Ascertia Desktop client that is why the Ascertia applet will have to be deployed (thus replacing the IBM one) while the T2S GUI will select the applet or the desktop client according to the browser used.

Ascertia applet is provided directly by Ascertia while IBM applet will not be used anymore as soon as the “Ascertia-enabled T2S GUI” application will be deployed. The applet download mechanism will be the same as it is currently (i.e. provided by T2S GUI); more information and screens will be provided in the updated technical document.

Additional information on the future scenario:

- Ascertia code is signed with a publicly trusted code-signing certificate. When the Go>Sign Desktop package is installed, it trusts the package as the code signing certificate issuer is trusted in the underlying trust store of the browsers of that machine.
- As long the Applet will be used a JRE is needed (higher than current one required by Ascertia applet); when only the Go Sign Desktop feature will be used the JRE will not be needed any more;
- Current U2A NRO solution also functions with the higher JRE version needed for the new U2A NRO.

Applet solution will coexist with the desktop client solution once implemented for at least 6 months. The de-scoping of the Java applet will be handled via minor change.

The de-scoping of the Java applet will be handled via minor change.

- No dependencies between T2S GUI authentication process and future signature mechanism as they involve different components of the T2S infrastructure (as it is now for the existing IBM Applet solution).
- The list of affected screens as defined in CR-0466 will remain unchanged.

Submitted annexes / related documents:

CR-466 “Implementation of non-repudiation for U2A”:
https://www.ecb.europa.eu/paym/target/t2s/governance/pdf/crg/ecb.targetseccrg140602_T2S-0466-BFD.en.pdf

T2S Non Repudiation of Origin (NRO): Upgrade of non-repudiation service for U2A (CR-0722): Technical Document, v1.7

Documentation to be updated:

BFD Annex B - Technical annex:

9) Digital Signature: Non-repudiation of origin

[..]

The signing procedure ~~is based on a Java applet which~~ has to be supported by the software configuration (browser versions ~~(Mozilla Firefox and Microsoft Internet Explorer)~~, third party software) installed on the user PC connected to the T2S system, as specified in the NRO technical documentation.

Proposed wording for the Change request:

a) UHB – Chapter 1.2.3. Validation – Digital Signature – NRO

Digital Signature – NRO

In order to ensure non-repudiation of origin (NRO) for critical transactions, the use of a digital signature has been implemented for specified screens. This means that the user will be asked to enter a PIN code for signature purposes whenever an instruction is initiated. With the entry of the PIN, T2S attaches a digital signature to the instruction entered by the T2S actor.

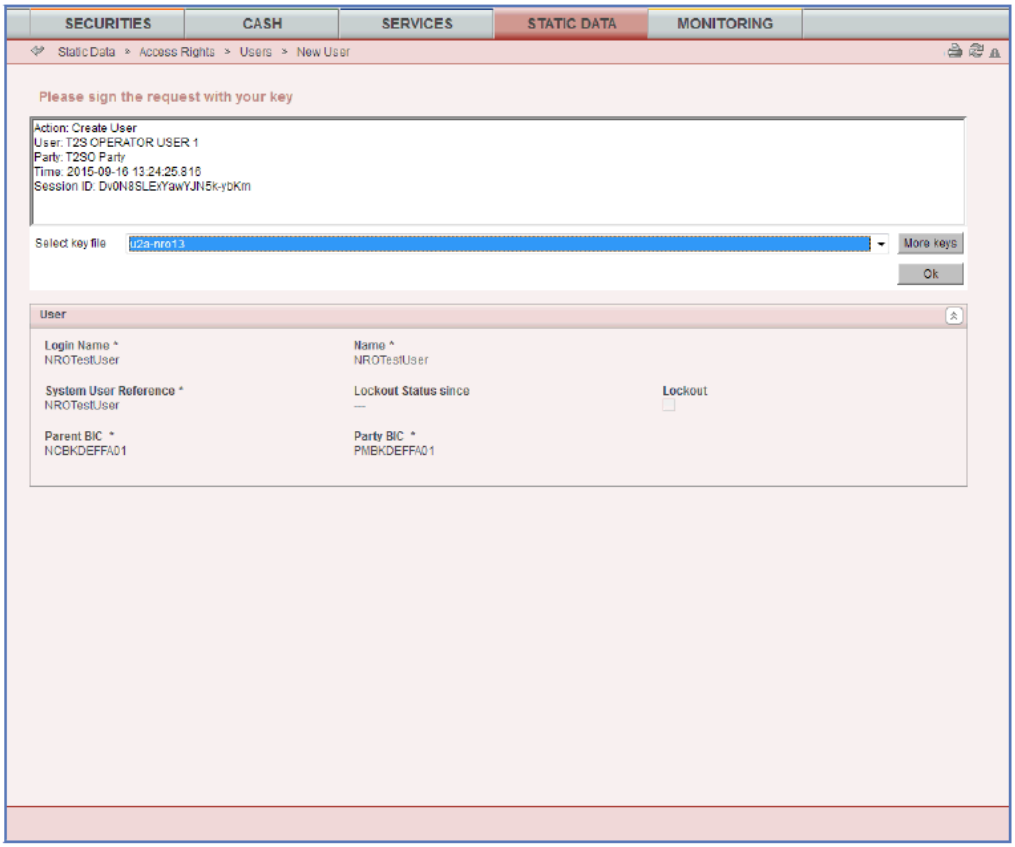

Illustration 19: Digital signature

b) NRO technical Documentation V1.6.1 to be updated

c) NRO Go>Sign Desktop client: Installation Guide to be added to the NRO technical document

d) T2S BFD Annex 9: references to Java applet must be updated.

Outcome/Decisions:

* CRG on 8 November 2019: The CRG agreed to recommend the CR for authorisation by the T2S Steering Level.

* AMI-SeCo on 15 November 2019: The AMI-SeCo agreed to the recommendation of the CRG.

* CSG on 15 November 2019: The CSG is in favour of authorising CR-722.

* NECSG on 15 November 2019: The NECSG is in favour of authorising CR-722.

* MIB on 4 December 2019: The MIB authorised CR-722.

* CRG on 20 March 2020, during a joint teleconference with PMG, CRG, OMG & SMG members, the T2S actors agreed to recommend the allocation of CR-722 to R5.0.

* CRG on 24 March 2020: The CRG supports the recommendation to implement CR-722 in T2S release 5.0.

* OMG on 24 March 2020: The OMG agrees with the outcome of the joint workshop to implement CR-722 in T2S release 5.0.

* CSG on 21 and 22 April 2020: The CSG approved the allocation CR-722 to R5.0.

* NECSG on 24 April 2020: The NECSG approved the allocation of CR-722 to R5.0.

* MIB on 25 May 2020: The MIB approved the inclusion of CR-722 in R5.0.

* PMG on 12 February 2021: the PMG agreed to de-scope CR-722 from R5.0 and proposed the inclusion of CR-722 in the scope of R5.2.

* CSG on 23 February 2021: the CSG approved the de-scoping of CR-722 from R5.0 and the inclusion of CR-722 in the scope of R5.2.

* NECSG on 23 February 2021: the NECSG approved the de-scoping of CR-722 from R5.0 and the inclusion of CR-722 in the scope of R5.2.

* MIB on 15 March 2021: the MIB approved the de-scoping of CR-722 from R5.0 and the inclusion of CR-722 in the scope of R5.2.

Detailed assessment

EUROSYSTEM ANALYSIS – GENERAL INFORMATION

Impact On T2S	**Static data management**		**Interface**	
		Party data management		Communication
		Securities data management		Outbound processing
		T2S Dedicated Cash account data management		Inbound processing
		Securities account data management	X	NRO process
		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
			X	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		
Impacted UDFS chapter		
Additional deliveries for Message Specification		
UHB		
Other documentations	Business Functionality for T2S Graphical User Interface, Version 2.1	references to Java applet must be updated
Links with other requests		
T2S-0466-BFD Implementation of non-repudiation for U2A		

OVERVIEW OF THE IMPACT OF THE REQUEST ON THE T2S SYSTEM AND ON THE PROJECT
Summary of functional, development, infrastructure and migration impacts
The CR requires adaptation of the U2A NRO signature flow to implement the new Ascertia Signing process, being able to invoke the Ascertia solution or the current NRO Solution depending on the browser used (IE11 for the current NRO, otherwise the Ascertia solution). The communication to the new Ascertia Server in 4CB Network has to be established. The layout of NRO signing process has to be modified to be compliant to the Ascertia Interface: signing, confirmation, response and denial. The update requires also an adjustment in LeA for the storage of the signature. Further to the magnitude of the above mentioned changes in INTF U2A the following delivery path in the scope of T2S Release 5.0 is suggested:

• Technical Groups approval by 07 March 2020 • Steering Level approval by22 April 2020 • 4CB start of implementation on 23 April2020 • Start of EAT on 11 January 2021 • Activation in EAC on 5 February 2021 (R5.0 first CR package) • Activation in UTEST on 9 April 2021 • Activation in PROD on 12 June 2021 The CR-0722 does not have any impact on the other scope items already included in T2S 5.0
Summary of project risk
Security analysis
No potentially adverse effect was identified during the security assessment.