EUROPEAN CENTRAL BANK
EUROSYSTEM

TARGET2-SECURITIES

General Information (Origin of Request) ☐ User Requirements (URD) ☒ Other User Functional or Technical Documentation (SYS)		
Request raised by: 4CB	**Institute:** 4CB	**Date raised:** 14/11/2014
Request title: A2A signature for information messages		**Request ref. no:** T2S 0479 SYS
Request type: Common	**Urgency:** Normal	
1. Legal/business importance parameter: Medium	**2. Market implementation efforts parameter:** Medium	
3. Operational/Technical risk parameter: Medium	**4. Financial impact parameter:** No cost impact	
Requestor Category: 4CB	**Status:** Rejected at Steering Level	

Reason for change and expected benefits/business motivation:

Further to User Testing results CSDs insisted on the need that all A2A outbound messages of T2S have to be signed digitally to ensure the integrity of the messages. Precisely, this market request highlighted a deviation between the current UDFS description stating that all A2A outbound messages are signed digitally also on application level (BAH/BFH) and the implementation according to which query results, reactions on erroneous inbound messages for queries and reports are not signed at BAH/BFH level.

Based on the experience and volumetric assumptions during NFT/EOD reporting, it was observed that providing two signatures i.e. one at DEP level and one at Application Layer, results into negative impact on performance. Therefore this exception of not providing the signature on application layer for query results, reactions on erroneous inbound messages for queries and reports has been implemented, as information in the reports and query responses were considered to a "lower" confidentiality /security level compare to instructing requests with "high" confidentiality/security.

The Data Exchange Protocol (DEP) is the network communication protocol used between T2S and the VAN provider and on DEP level the digital signature for A2A outbound messages concerning the above mentioned exceptions is provided as follows:

- Query results (including pull reports) and reactions on erroneous inbound messages for queries are signed if the Non-repudiation flag (NR) is set to true for which there is a dependency on the used VAN. SWIFT always requests NR “true” whereas SIA/COLT leave it up to the User to set the NR flag to “true”. The later means that the NR flag has set to “true”, if the response should be signed. The signature in the query response depends on the incoming signature in the query request.

- Pushed Reports are not digitally signed

In summary, to fulfil the users’ request an adaptation is needed for A2A outbound messages concerning reports since reports are neither signed at application level (BAH/BFH) nor at DEP level. With regards of the query usage and the corresponding signature handling on DEP level for the response, the users of VAN are – as far as they wish to receive signed responses - recommended to set the NR flag for Real time communication every time on “true”.

Description of requested change:

This Change Request requires the following two changes

a) DEP signature is mandatory for pushed reports. In case of timeout and oversize management scenario the corresponding answer sent via SnF channel has to contain a DEP signature.

b) UDFS has to be amended, clarifying the exceptions concerning the signature of A2A outbound messages on application level (no BAH/BFH signature for query results, reactions on erroneous inbound messages for queries and reports). INTF application has to be changed for reports to ensure a digital signature on DEP level.

The following table describes the Signature Handling on DEP and Application Level:

	Signature on DEP level	**Signature on Application Layer (BAH/BFH)**
Outbound Communication (SnF)	X **(New)** including query responses due to timeout and oversize management	(X) Except pushed reports and query responses due to oversize and timeout handling.
Outbound Communication (RT)	(X) Available if incoming RT is signed.	(X) Except query results and reactions on erroneous inbound messages for queries

Note:

- T2S users have to add signatures to all T2S A2A inbound messages on BAH or BFH (Application Level) as for these messages the technical sender may diverge from the business sender.
- Receipt Acknowledgements (admi.007) are not signed at Application Layer if the BAH is not used (Please refer to UDFS 2.0 chapter 3.3.2.3 ReceiptAcknowledgementV01 (admi.007.001.01) p. 912).
- Quality/Security of the standard used for DEP signature and signature on application level is the same.

Submitted annexes / related documents:

Proposed wording for the SYS Change request:

UDFS Section 3.2.2.1.3 Digital Signature managed within the Business Layer, page 882

The purpose of this signature is to authenticate the business sender and guarantee the integrity of the business payload. This business signature should be compliant with the W3C XAdES 241standard.
The (NRO)242 signature is stored in the BAH in case of individual messages or in the file header in case of messages grouped into a file. In case messages grouped into a file, the BAH of the included individual messages does not include a signature. Exception: BAH-/BFH-signature is not present in report and query response messages sent by T2S.

UDFS Section 3.3.5.1 BusinessApplicationHeaderV01 (head.001.001.01), page 1086 ff

Alignment and clarification of UDFS referring the non usage of BAH signature for reports and query responses.

Add additional information within the T2S-use field "AppHdr/Sgntr": Certificate, which identifies the business sending user in combination with the system user reference for single messages. Either the Digital signature is part of the File (in case of multi messages) or it's part of the BAH in case of single messages. Exception: BAH-/BFH-Signature is not present in receipt acknowledgement, report and query response messages.

UDFS Section 3.3.5.1.3 The message in business context, page 1093

Message example 5: head.001.001.01_T2S_StatementOfAccountSentByT2S_Example.xml should be updated not to have the signature.

The T2S-specific schema and documentation in HTML/PDF format as well as the message examples are provided outside of this document under the following link:

http://www.swift.com/mystandards/T2S/head.001.001.01_T2S

High level description of Impact:

Clarification provided referring the usage of Digital Signature on Business Level:

- UDFS section 3.2.2.1.3 Digital Signature managed within the Business Layer

UDFS Section 3.3.5.1 BusinessApplicationHeaderV01 (head.001.001.01).

Outcome/Decisions:

* CRG meeting of 15 December 2014: The CRG put the Change Request on hold.

* CRG meeting of 6 February 2015: The CRG put the Change Request on hold.

* CRG meeting of 12 March 2015: The CRG agreed to wait for the ISSG feedback on the compensating control and put the Change Request on hold.

* CRG meeting of 28 April 2015: The CRG recommended the rejection of the Change Request. The CRG agreed to introduce a non-editorial change in Change Request T2S-0522-SYS (Non-editorial Change Request on UDFS) to add a footnote in the UDFS to clarify that the digital signature is not yet implemented for reports and query responses.

* Advisory Group’s advice on 7 May 2015: Following a written procedure, the AG was in favour of the rejection of the Change Request.

* CSG meeting on 7-8 May 2015: The CSG adopted the resolution to reject the Change Request.