EUROPEAN CENTRAL BANK
EUROSYSTEM

TARGET2-SECURITIES

General Information (Origin of Request) □ User Requirements (URD) or GUI Business Functionality Document (BFD) ☒ Other User Functional or Technical Documentation (SYS)		
Request raised by: 4CB	**Institute:** 4CB	**Date raised:** 14/06/2013
Request title: Digital signature on business layer		**Request ref. no:** T2S 0418 SYS
Request type: Common	**Urgency:** Normal	
1. Legal/business importance parameter: Low	**2. Market implementation efforts parameter:** Low	
3. Operational/Technical risk parameter: Low	**4. Financial impact parameter:** No cost impact	
Requestor Category: ECB	**Status:** Authorised at Steering Level	

Reason for change / expected benefits / business case:

The current UDFS 1.2.1 already states that signatures have to be constructed for each of the T2S message types. The following message types on Business Layer, support NRO (Non Repudiation of Emission):

1) File with multiple ISO 20022 messages. The structure is described in UDFS 1.2.1 section 3.2.2.1.3
2) Single ISO20022 Business Application Header and message. The structure is described in UDFS 1.2.1 section 3.2.2.1.3

Signing services have to use ISO20022 Business variant and includes following requirements:

1. Validation of digital signatures (XAdES-BES signatures);
2. Verification of certificates used for digital signing;

However, the current version UDFS 1.2.1 does not include the details of the Digital Signature. In order to provide all T2S Actors with the necessary details, it is foreseen to include a dedicated annex in the UDFS.

This information should allow the T2S Actor to understand T2S behaviour and is necessary to implement the respective handling in the T2S Actors application.

With the inclusion of the description into the UDFS, the handling of Digital Signature would be legally binding. Furthermore by enhancing the information on the Digital Signature, the T2S Actors get the necessary information to implement the respective handling in the T2S Actor's application.

Description of Request:

The design goal for the proposed construction of signatures is that as much as possible is handled by standard XML Digital Signature processing specifications and as little as possible by application specific processing. This makes it less likely that errors and/or discrepancies occur in the different implementations, and therefore improve the overall security of the solution.

The purpose of the requested change is to support a standard Signing on Business layer. This means verification of certificates used for digital signing, validation and creation of digital signatures for Multi and single business messages.

<u>Signature field within the schema head.001 and head.002:</u>

Referring the Sgntr/xs:any element the Process Contents have to be changed from "lax" into "strict", so that validation should be strictly applied to the elements found in the position of the corresponding any or anyAttribute element, respectively, in the XSD representation by setting its processContents attribute to "strict". This allows elements from a specific namespace with strict validation.

The current "lax" definition causes invalid messages and is not in line with other defined T2S customised schemas (e. g. messages which use the SupplementaryDataEnvelope).

Proposed wording for the SYS Change request:
Proposed Implementation Release: UDFS version 2.0

The following figures/definitions/sections have to be updated as follows:

3.2.2.1.1 Application Header (Update of the provided sample)

<Sgntr>
~~<Sgn xmlns="http://www.w3.org/2000/09/xmldsig#"> user signature </Sgn>~~
<ds:Signature>…</ds:Signature>[1]
</Sgntr>

3.2.2.1.2 File Header (Update of the provided sample)

<Sgntr>
~~<Sgn xmlns="http://www.w3.org/2000/09/xmldsig#"> user signature </Sgn>~~
<<ds:Signature>…</ds:Signature>[1]
</Sgntr>

3.2.2.1.3 Digital Signature managed within the ~~Application~~ Business Layer

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 standard.

The (NRO) 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.

File (meaning multi-message):

The signature is part of the file header. It is over the list of BAH‟s and ISO 20022 messages and covers the whole <XChg> element of the Business File (head.002), except for the signature itself.

Single message:

The signature is over the ISO 20022 message and takes into account ~~all~~ the business processing relevant information specified within the BAH (e. g. pair of BICs for definition of the instructing party), except for the signature itself .The digital signature grouped in the BAH itself is not part of this signature calculation.

Further details referring the Digitale Signature construction on Business Layer can be retrieved from Annex 4.7 “Digitale Signature on Business Layer”.

3.3.5.1 BusinessApplicationHeaderV01 (head.001.001.01)

Sgntr/xs:any element the Process Contents have to be changed from “lax” into “strict”
(Schema and documentation; References/Links)

3.3.5.1.3 The message in business context

Update of all XML samples according to the detailed construction of the <Sgntr> field (see above).

3.3.5.2 BusinessFileHeaderV01 (head.002.001.01)

[1] The detailed structure and of the signature field and the concept behind can be found within the Annex 4.7 “Digitale Signature on Business Layer”.

Sgntr/xs:any element the Process Contents have to be changed from “lax” into “strict”
(Schema and documentation; References/Links)

3.3.5.2.3 The message in business context

Update of all XML samples according to the detailed construction of the <Sgntr> field (see above).

4.7 (New Appendix) “Digital Signature on Business Layer”

See separate document.

Submitted annexes / related documents:

Annex 4.7

The updated schemas of the impacted messages will be available after the approval under the following link:
http://www.bundesbank.de/Redaktion/EN/Documentation/4zb/HtmlDoc/v1.2.1/CR/CR-Overview.pdf

High level description of Impact:

Outcome/Decisions:

- CRG meeting of 12 July 2013: The CRG decided to make some minor wording updates on the Change Request for clarification purposes and recommended the approval of the updated Change Request.

- CSG resolution on 12 August 2013: Following a written procedure, the CSG adopted the resolution to approve the Change Requests.

- Advisory Group’s advice on 12 August 2013: Following a written procedure, the AG was in favour of the Change Request.

4.7 Digitale Signature on Business Layer

The scope of this Annex is to provide detailed information for experts, which have to specify and handle the generation and verification of Digitale Signatures on Business Layer.

4.7.1 Mechanism and Introduction for signature constructions

This Annex outlines how signatures are constructed for the T2S Business messages. The following business message types have been identified:

- Message Type 1: File with multiple ISO 20022 messages. The structure is described in UDFS section 3.2.2.1.3;
- Message Type 2: Single ISO20022 Business Application Header and message. The structure is described in UDFS section 3.2.2.1.3;

The design goal for the proposed construction of signatures in the following sections is that as much as possible is handled by standard XML Digital Signature processing specifications and as little as possible by T2S specific processing. This makes it less likely that errors and/or discrepancies occur in the different implementations, and therefore improve the overall security of the solution.

4.7.2 Use of XML and canonicalization algorithm

Exclusive XML canonicalization[1] has to be performed for above mentioned business messages on extracted data. It is important to ensure a context free extraction otherwise the signatures will be broken if either the message or the signature itself is modified due to inherited namespaces.

This implies that the canonicalization algorithm specified in the SignedInfo element and in all the references should be in line with following information:

http://www.w3.org/2001/10/xml-exc-c14n#

[1] Exclusive XML Canonicalization http://www.w3.org/TR/xml-exc-c14n/

4.7.3 Message Type 1: File with multiple ISO 20022 messages

For message type 1) the requirement in the UDFS section 3.2.2.1.3 states:

”The ~~Non-repudiation of origin~~ (NRO)[2] 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.

File (meaning multi-message):

The signature is part of the file header. It is over the list of

BAH's and ISO 20022 messages and covers the whole <XChg> element of the Business File (head.002), except for the signature itself*.”*

The signature, in particular, covers the whole BusinessFileHeader <XChg> element, except for the signature itself. So consequently the following field will be not taken into account for Signature calculation:

Xchg/PyldDesc/ApplSpcfcInf/Sgntr/ds:Signature[3]

Hence a signature will then be constructed as follows:

- One reference (in blue below) points out the XChg itself. This is done using the same document reference URI = ””, which means the entire document. To leave the signature element itself out of the digest calculation, the transform ”#enveloped-signature” is used.
- One reference (in yellow below) points to the KeyInfo element of the signature itself. This is a XAdES[4] requirement.

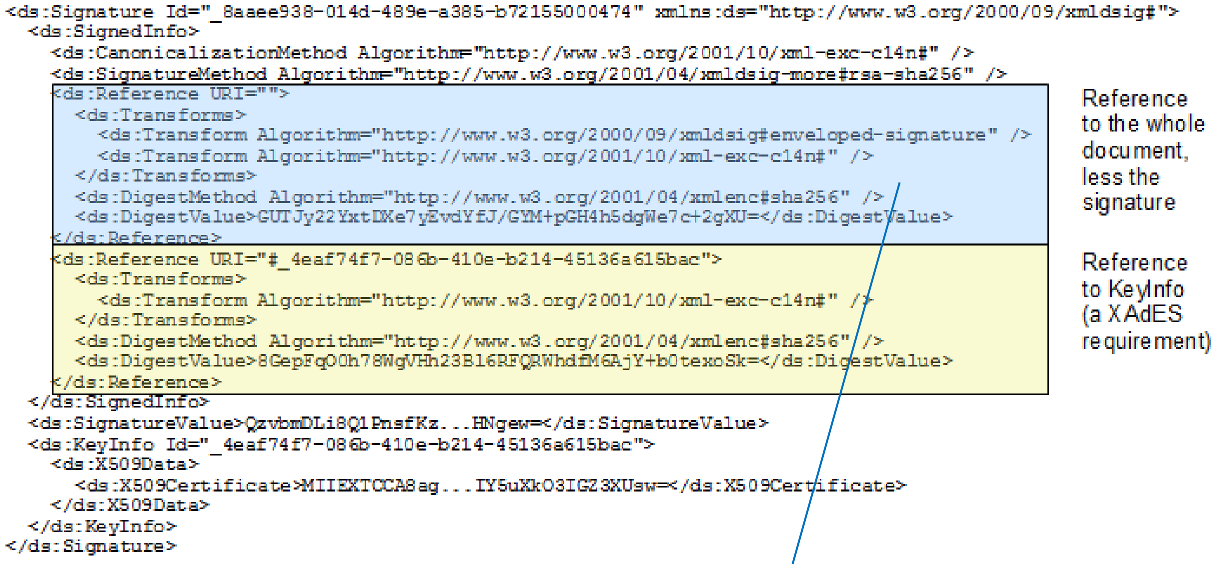
1) A Message Type 1[5] signature example is reported in the below picture:

[2] Non-repudiation of origin is intended to protect against the originator's false denial of having sent the message.

[3] Due to the XAdES requirement the ds:KeyInfo element inside the ds:Signature is covered/protected by the signature.

[4] ETSI TS 101 903 V1.4.2 (2010-12) XML Advanced Electronic Signatures

[5] T2S is configured to produce and generate rsa-sha256 signatures, and use sha256 digest. T2S can also validate a rsa-sha1 signature if it receives such a signature.

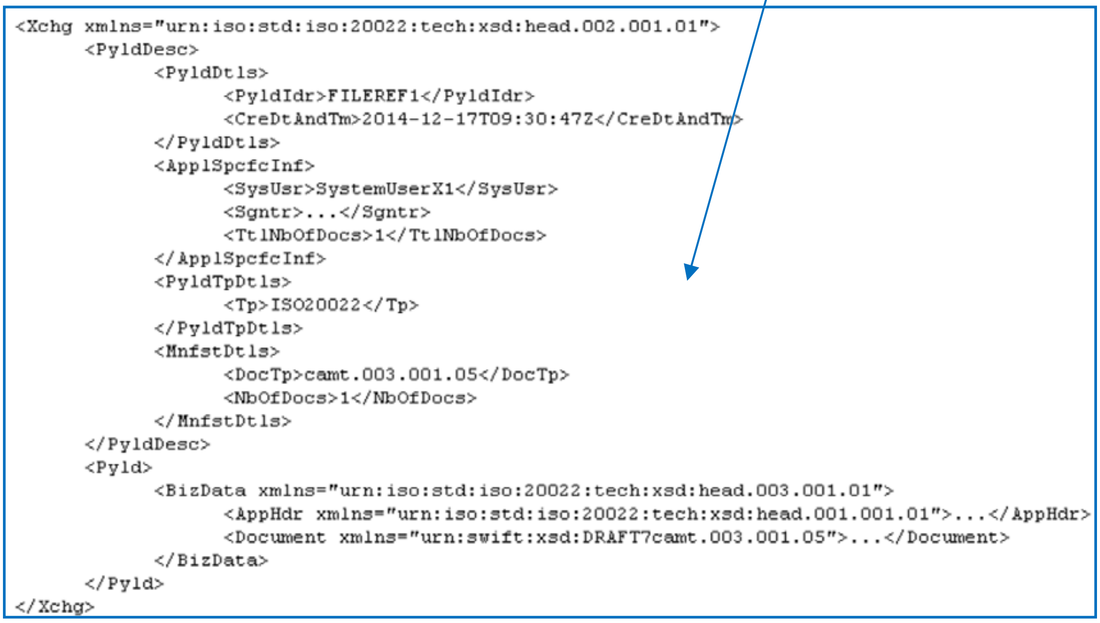


```
<ds:Signature Id="_8aaee938-014d-489e-a385-b72155000474" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <ds:Reference URI="">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>GUTJy22YxtDXe7yEvdYfJ/GYM+pGH4h5dgWe7c+2gXU=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#_4eaf74f7-086b-410e-b214-45136a615bac">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>8GepFqO0h78WgVHh23B16RFQRWhdfM6AjY+b0texoSk=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>QzvbmDLi8Q1PnsfKz...HNgew=</ds:SignatureValue>
  <ds:KeyInfo Id="_4eaf74f7-086b-410e-b214-45136a615bac">
    <ds:X509Data>
      <ds:X509Certificate>MIIEXTCCA8ag...IY5uXkO3IGZ3XUsw=</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
```

Reference to the whole document, less the signature

Reference to KeyInfo (a XAdES requirement)

Reference to the message (head.002):



```
<Xchg xmlns="urn:iso:std:iso:20022:tech:xsd:head.002.001.01">
      <PyldDesc>
            <PyldDtls>
                  <PyldIdr>FILEREF1</PyldIdr>
                  <CreDtAndTm>2014-12-17T09:30:47Z</CreDtAndTm>
            </PyldDtls>
            <ApplSpcfcInf>
                  <SysUsr>SystemUserX1</SysUsr>
                  <Sgntr>...</Sgntr>
                  <TtlNbOfDocs>1</TtlNbOfDocs>
            </ApplSpcfcInf>
            <PyldTpDtls>
                  <Tp>ISO20022</Tp>
            </PyldTpDtls>
            <MnfstDtls>
                  <DocTp>camt.003.001.05</DocTp>
                  <NbOfDocs>1</NbOfDocs>
            </MnfstDtls>
      </PyldDesc>
      <Pyld>
            <BizData xmlns="urn:iso:std:iso:20022:tech:xsd:head.003.001.01">
                  <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">...</AppHdr>
                  <Document xmlns="urn:swift:xsd:DRAFT7camt.003.001.05">...</Document>
            </BizData>
      </Pyld>
</Xchg>
```

2) A Message Type 1 structure example (including signature) is provided in XML format outside of this document:

   http://www.bundesbank.de/4zb/download/v2.0/businessfileheader/s_head.002.001.01.xml[6]

4.7.4 Message Type 2: single ISO 20022 message[7]

For message type 2) the requirement in UDFS section 3.2.2.1.3 states:

"Single message: The signature is over the ISO 20022 message and takes into account the business processing relevant information specified within the BAH (e. g. pair of BICs for definition of the instructing party), except for the signature itself. The digital signature grouped in the BAH itself is not part of this signature calculation."

So consequently the following field will be not taken into account for Signature calculation:

AppHdr/Sgntr/ds:Signature[8]

In this case the BAH and the ISO 20022 message are considered not to be in the same document.

"Technically speaking, the Application Header is a separate XML document standing apart from the XML documents which represent the business message instance itself."

Since the documents that are referenced do not carry an ID attribute[9] that could be used for identifying the specific document[10], it has been decided to use a T2S specific reference for the business message,T2S ensures that the BAH and the corresponding ISO message are always stored together.

[6] Final Link depends on the usage of MyStandards for UDFS 2.0.
[7] See also MUG (Message user guide) for BAH; http://www.iso20022.org/bah.page
[8] Due to the XAdES requirement the ds:KeyInfo element inside the ds:Signature is covered/protected by the signature.
[9] ISO20022 do not support and specify an ID attribute, that can be used by T2S to uniquely identify BAH and ISO message.

T2S Specific Reference for document signature

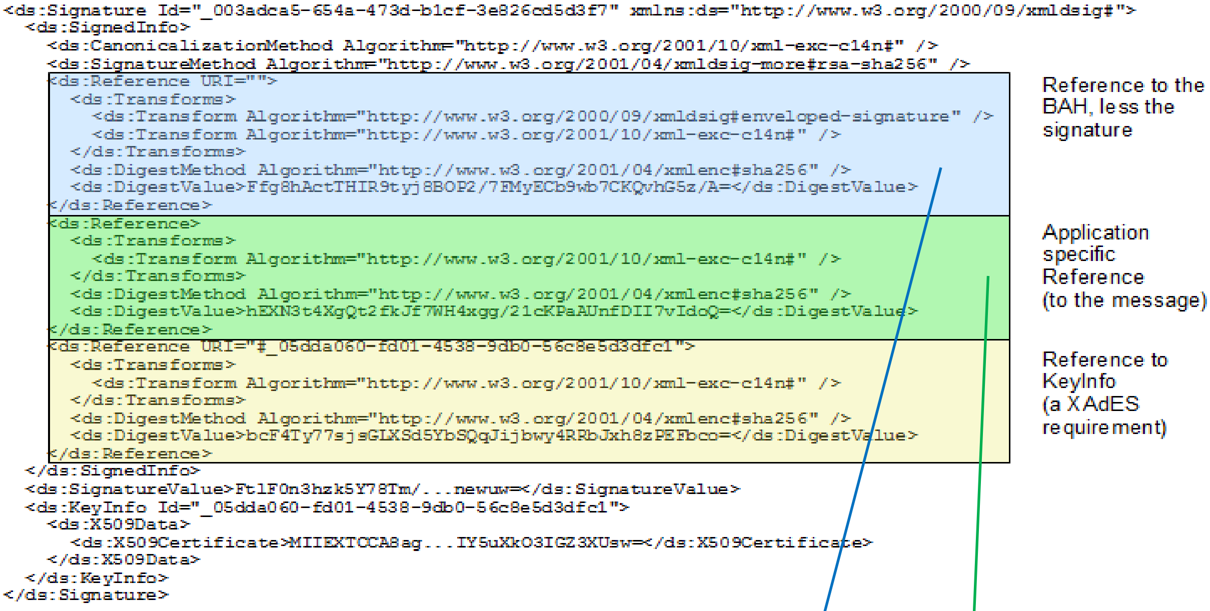
In the XML Digital Signature standard there is the possibility to use a reference with no URI i.e. omitting the URI attribute entirely. However there can be at most one such reference in a signature, and handling of it is T2S specific, and not covered by the XML Digital Signature standard[11]. Hence the reference to the message must be given by the context and known by the application.

The signature will then be constructed as follows:

- One reference (in blue below) points out the BAH (AppHdr) itself. This is done using the same document reference URI = "", which means the entire document. To leave the signature element itself out of the digest calculation, the transform"#enveloped-signature" is used;
- One reference (in green below) is application specific and refers to the business message (no URI). The application will provide the signature API with the relevant message. The signature API is customized to resolve the no URI reference to this message;
- One reference (in yellow below) points to the KeyInfo element of the signature itself (XAdes requirements).

[11] XML Signature Syntax and Processing (Second Edition), W3C Recommendation 10 June 2008, "http://www.w3.org/TR/xmldsig-core/"

1) A message type 2[12] signature example (with application specific reference) is reported in the below picture:



```
<ds:Signature Id="_003adca5-654a-473d-b1cf-3e826cd5d3f7" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <ds:Reference URI="">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>Ffg8hActTHIR9tyj8BOP2/7FMyECb9wb7CKQvhG5z/A=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference>
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>hEXN3t4XgQt2fkJf7WH4xgg/21cKPaAUnfDII7vIdoQ=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#_05dda060-fd01-4538-9db0-56c8e5d3dfc1">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>bcF4Ty77sjsGLXSd5YbSQqJijbwy4RRbJxh8zPEFbco=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>Ft1F0n3hzk5Y78Tm/...newuw=</ds:SignatureValue>
  <ds:KeyInfo Id="_05dda060-fd01-4538-9db0-56c8e5d3dfc1">
    <ds:X509Data>
      <ds:X509Certificate>MIIEXTCCA8ag...IY5uXkO3IGZ3XUsw=</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
```

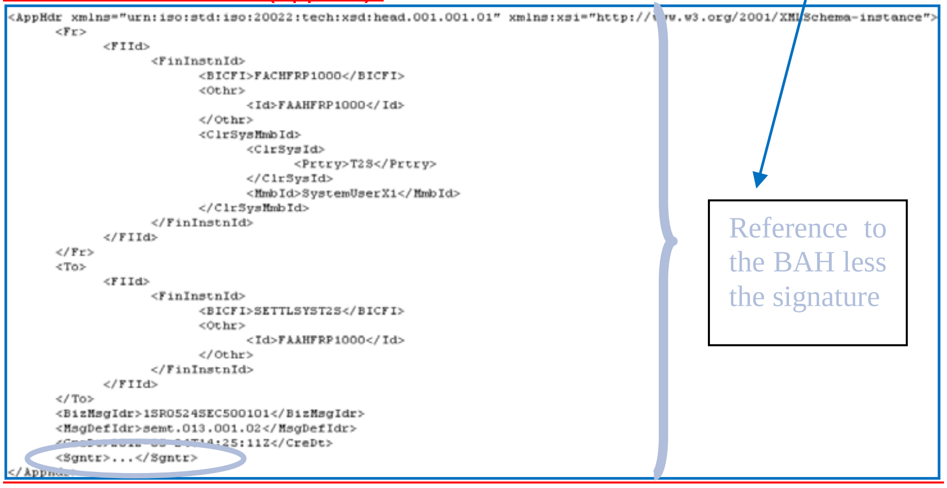
Reference to the BAH, less the signature

Application specific Reference (to the message)

Reference to KeyInfo (a XAdES requirement)

General remark: The signature is over the ISO 20022 message and takes into account the business processing relevant information specified within the Message Header (BAH), except the signature itself. The Digital Signature in the BAH itself is NOT part of this signature calculation.

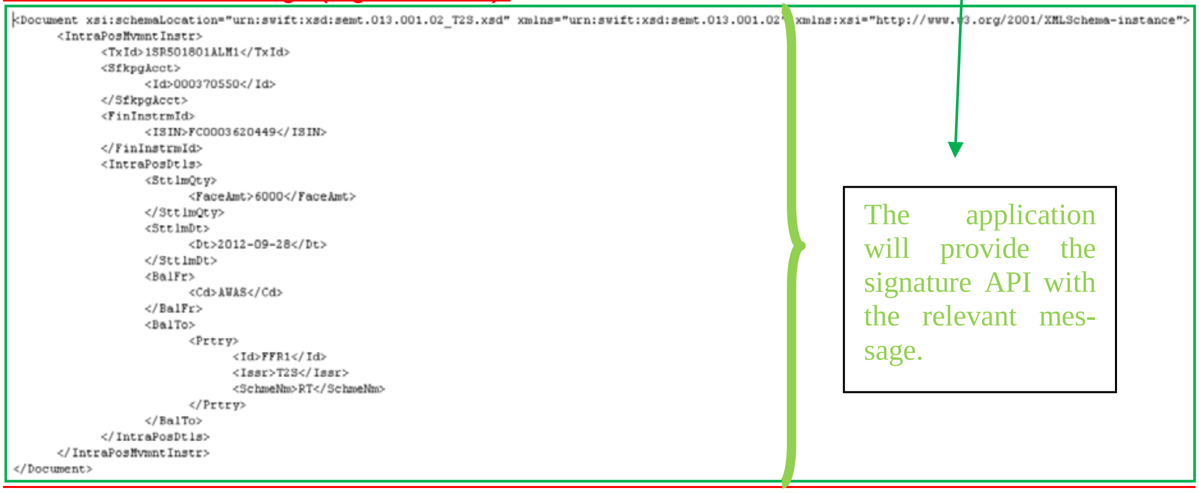
Reference to the BAH (AppHdr):



```
<AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
	<Fr>
		<FIId>
			<FinInstnId>
				<BICFI>FACHFRP1000</BICFI>
				<Othr>
					<Id>FAAHFRP1000</Id>
				</Othr>
				<ClrSysMmbId>
					<ClrSysId>
						<Prtry>T2S</Prtry>
					</ClrSysId>
					<MmbId>SystemUserX1</MmbId>
				</ClrSysMmbId>
			</FinInstnId>
		</FIId>
	</Fr>
	<To>
		<FIId>
			<FinInstnId>
				<BICFI>SETTLSYST2S</BICFI>
				<Othr>
					<Id>FAAHFRP1000</Id>
				</Othr>
			</FinInstnId>
		</FIId>
	</To>
	<BizMsgIdr>1SR0524SEC500101</BizMsgIdr>
	<MsgDefIdr>semt.013.001.02</MsgDefIdr>
	<CreDt>2012-03-24T14:25:11Z</CreDt>
	<Sgntr>...</Sgntr>
</AppHdr>
```

Reference to the BAH less the signature

Reference to the message (e.g. semt.013):

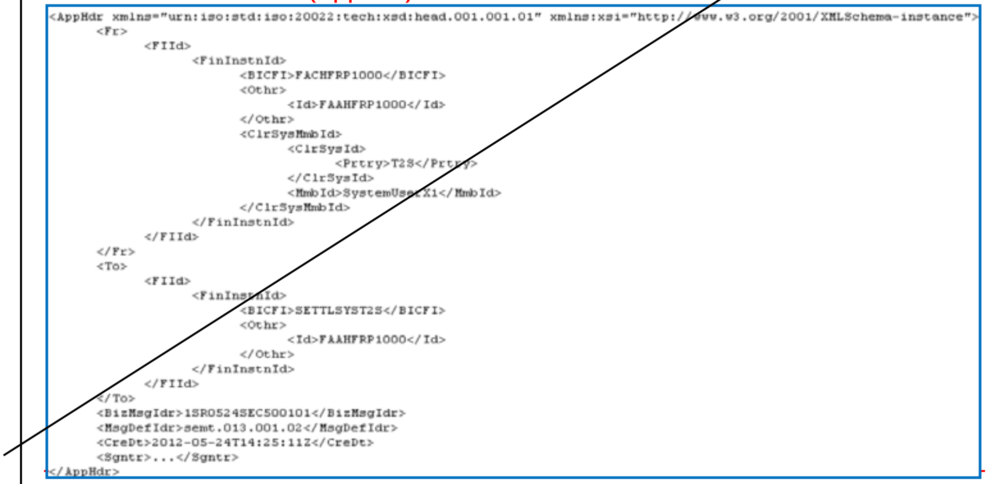


```
<Document xsi:schemaLocation="urn:swift:xsd:semt.013.001.02_T2S.xsd" xmlns="urn:swift:xsd:semt.013.001.02" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
	<IntraPosMvmntInstr>
		<TxId>1SR501801ALM1</TxId>
		<SfkpgAcct>
			<Id>000370550</Id>
		</SfkpgAcct>
		<FinInstrmId>
			<ISIN>FC0003620449</ISIN>
		</FinInstrmId>
		<IntraPosDtls>
			<SttlmQty>
				<FaceAmt>6000</FaceAmt>
			</SttlmQty>
			<SttlmDt>
				<Dt>2012-09-28</Dt>
			</SttlmDt>
			<BalFr>
				<Cd>AWAS</Cd>
			</BalFr>
			<BalTo>
				<Prtry>
					<Id>FFR1</Id>
					<Issr>T2S</Issr>
					<SchmeNm>RT</SchmeNm>
				</Prtry>
			</BalTo>
		</IntraPosDtls>
	</IntraPosMvmntInstr>
</Document>
```

The application will provide the signature API with the relevant message.

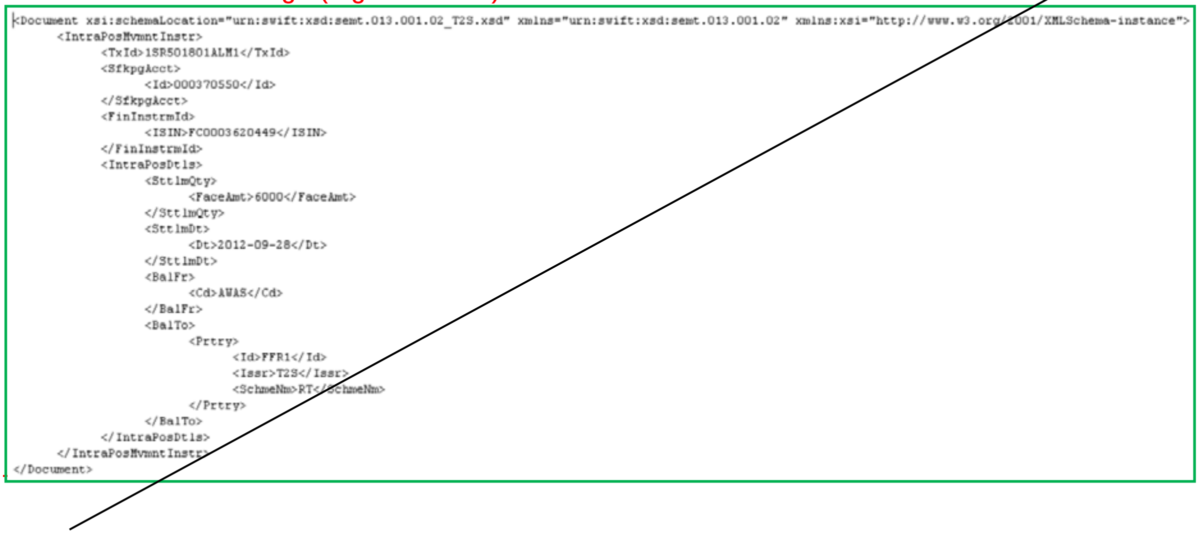
[12] T2S is configured to produce and generate rsa-sha256 signatures, and use sha256 digest. T2S can also validate a rsa-sha1 signature if it receives such a signature.

~~Reference to the BAH (AppHdr):~~



```
<AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <Fr>
        <FIId>
            <FinInstnId>
                <BICFI>FACHFRP1000</BICFI>
                <Othr>
                    <Id>FAAHFRP1000</Id>
                </Othr>
                <ClrSysMmbId>
                    <ClrSysId>
                        <Prtry>T2S</Prtry>
                    </ClrSysId>
                    <MmbId>SystemUserX1</MmbId>
                </ClrSysMmbId>
            </FinInstnId>
        </FIId>
    </Fr>
    <To>
        <FIId>
            <FinInstnId>
                <BICFI>SETTLSYST2S</BICFI>
                <Othr>
                    <Id>FAAHFRP1000</Id>
                </Othr>
            </FinInstnId>
        </FIId>
    </To>
    <BizMsgIdr>1SR0524SEC500101</BizMsgIdr>
    <MsgDefIdr>semt.013.001.02</MsgDefIdr>
    <CreDt>2012-05-24T14:25:11Z</CreDt>
    <Sgntr>...</Sgntr>
</AppHdr>
```

~~Reference to the message (e.g. semt.013):~~



```
<Document xsi:schemaLocation="urn:swift:xsd:semt.013.001.02_T2S.xsd" xmlns="urn:swift:xsd:semt.013.001.02" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <IntraPosMvmntInstr>
        <TxId>1SR501801ALM1</TxId>
        <SfkpgAcct>
            <Id>000370550</Id>
        </SfkpgAcct>
        <FinInstrmId>
            <ISIN>FC0003620449</ISIN>
        </FinInstrmId>
        <IntraPosDtls>
            <SttlmQty>
                <FaceAmt>6000</FaceAmt>
            </SttlmQty>
            <SttlmDt>
                <Dt>2012-09-28</Dt>
            </SttlmDt>
            <BalFr>
                <Cd>AWAS</Cd>
            </BalFr>
            <BalTo>
                <Prtry>
                    <Id>FFR1</Id>
                    <Issr>T2S</Issr>
                    <SchmeNm>RT</SchmeNm>
                </Prtry>
            </BalTo>
        </IntraPosDtls>
    </IntraPosMvmntInstr>
</Document>
```

2) A Message Type 2 structure example (including signature) is provided in XML format outside of this document:

http://www.bundesbank.de/4zb/download/v2.0/businessapplicationheader/s_Semt.01_.SR.501801a.1_HDR.xml[13]

4.7.5 T2S usage of ds:Object, Attribute ID of the Signature and KeyInfo, Anchor of trust:

- **Usage of block "Object":**

In message type 1 and 2 the ds:Object element is not used when constructing the signature. The T2S signature API (Application Programming Interface) follows standard XML Signature Processing which defines what happens when a ds:Object element is encountered:

- If the ds:Object (or its content) is referenced in ds:SignedInfo, then the API will verify this reference as part of the signature verification;
- If the ds:Object is not referenced in ds:SignedInfo, then the API will ignore it, when performing the cryptographic check of the signature.

[13] Final Link depends on the usage of MyStandards for UDFS 2.0.

However if the ds:Object contains e.g. XAdES Qualifying properties, these will be examined in order to determine the signature format, I.e. is the signature a XAdES-BES or XAdES-T or XAdES-C.

T2S recommendation is to not use in message type 1 and 2 the ds:Object element.

- **Usage of Attribute ID of the block "Signature":**

T2S will generate the ID attribute of the Signature element when building a signature to be sent to counterparts. The ID attribute is optional for signatures sent to T2S. If present the value of the ID attribute must be an underscore ("_") followed by a universally unique identifier (UUID), that is either timebased (UUID version 1) or random (UUID version 4). The UUID generating system is responsible for ensuring that all the UUID's in a single document are unique.

- **Usage of block "KeyInfo":**

The XAdES standard allows two different methods to comply with the XAdES-BES requirement. In T2S it has been decided to use the one that includes the signer certificate in the KeyInfo element:

  - Element KeyInfo must be present and must include the ds:X509Data/ds:X509Certificate containing the signing certificate.
  - The ID attribute on the KeyInfo element is mandatory and the value of the ID attribute must be a underscore ("_") followed by a universally unique identifier (UUID), that is either timebased (UUID version 1) or random (UUID version 4).
  - The SignedInfo element must reference the KeyInfo element using the ID attribute.

Usage of the alternative ds:Object/QualifyingProperties/SignedProperties/SignedSignatureProperties/SigningCertificate element is not allowed.

- **Anchor of trust**

It is necessary that the parties have enough information to validate the signatures. This is ensured by having the same anchor of trust in both ends and providing certificates in KeyInfo. Depending on the Certificate Authority (CA) structure and the chosen anchor of trust, the number of certificates included in the KeyInfo element may vary:

- In case of a root CA that issues intermediate CA certificates that in turn issue the signer certificates, the chain in the KeyInfo element depends on the chosen anchor of trust:
  - If the anchor of trust is the intermediate CA, then the chain in the KeyInfo element need only to contain the signer certificate;
  - If the anchor of trust is the root CA, the chain in the KeyInfo element must include both the signer certificate and the intermediate CA certificate.
- In case of a root CA that issues signer certificates directly, the root CA is the anchor of trust: The chain in the KeyInfo element needs only to contain the signer certificate.

The parties communicating must use the same certificates as anchor of trust. It is up to T2S for each CA to choose the certificate (root or intermediate) that constitutes the anchor of trust.

```
- <Xchg xmlns="urn:iso:std:iso:20022:tech:xsd:head.002.001.01">
  - <PyldDesc>
    - <PyldDtls>
        <PyldIdr>FILEREF1</PyldIdr>
        <CreDtAndTm>2014-12-17T09:30:47Z</CreDtAndTm>
      </PyldDtls>
    - <ApplSpcfcInf>
        <SysUsr>SystemUserX1</SysUsr>
      - <Sgntr>
        - <ds:Signature Id="_8af629dd-bb2c-4207-b0b4-c3edb7d17444" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          - <ds:SignedInfo>
              <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
              <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            - <ds:Reference URI="#_f6fa91c7-ee9f-4702-8f08-820bd7a86ac2">
              - <ds:Transforms>
                  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                <ds:DigestValue>wFOmYpRxS6RAOxOdrlZKfmV3Tza4jVWW8Afg0efdogU=</ds:DigestValue>
              </ds:Reference>
            - <ds:Reference URI="">
              - <ds:Transforms>
                  <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                <ds:DigestValue>LQSkT1Mksb6iSiyqwCmAAs/ZKd9Nkwl068Kukx9JP/U=</ds:DigestValue>
              </ds:Reference>
            </ds:SignedInfo>

              <ds:SignatureValue>rLCX6pUzTEYGAHMNu/NczFwbXVgncgVsjmhCNNNsXjbU8CqJeytFM3XJFvPocqqTX2ZsPg+GAE89xFBb2xe7j8Z1m
          - <ds:KeyInfo Id="_f6fa91c7-ee9f-4702-8f08-820bd7a86ac2">
            - <ds:X509Data>

                  <ds:X509Certificate>MIID0DCCArigAwIBAgIBBTANBgkqhkiG9w0BAQsFADBMMQswCQYDVQQGEwJGUjEcMBoGA1UECgwTS2V5bm
              </ds:X509Data>
            </ds:KeyInfo>
          </ds:Signature>
        </Sgntr>
        <TtlNbOfDocs>1</TtlNbOfDocs>
      </ApplSpcfcInf>
    - <PyldTpDtls>
        <Tp>ISO20022</Tp>
      </PyldTpDtls>
    - <MnfstDtls>
        <DocTp>camt.003.001.05</DocTp>
        <NbOfDocs>1</NbOfDocs>
      </MnfstDtls>
    </PyldDesc>
  - <Pyld>
    - <BizData xmlns="urn:iso:std:iso:20022:tech:xsd:head.003.001.01">
      - <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
        - <Fr>
          - <FIId>
            - <FinInstnId>
                <BICFI>CSDPARTCPNT</BICFI>
              - <Othr>
                  <Id>CSDBICIDXXX</Id>
                </Othr>
              </FinInstnId>
            </FIId>
          </Fr>
        - <To>
          - <FIId>
            - <FinInstnId>
                <BICFI>CSDBICIDXXX</BICFI>
              - <Othr>
                  <Id>SYSTEMIDT2S</Id>
                </Othr>
              </FinInstnId>
            </FIId>
          </To>
          <BizMsgIdr>REF3</BizMsgIdr>
          <MsgDefIdr>camt.003.001.05</MsgDefIdr>
          <CreDt>2014-12-17T09:30:47Z</CreDt>
        </AppHdr>
      - <Document xmlns="urn:swift:xsd:DRAFT7camt.003.001.05">
        - <GetAcct>
          - <MsgHdr>
              <MsgId>REF3</MsgId>
            - <ReqTp>
              - <Prtry>
                  <Id>CASB</Id>
                </Prtry>
              </ReqTp>
            </MsgHdr>
          - <AcctQryDef>
            - <AcctCrit>
              - <NewCrit>
                - <SchCrit>
                  - <AcctId>
                    - <EQ>
                      - <Othr>
```

```
                        <Id>T2SDEDICATEDCASHACCOUNT1</Id>
                      </Othr>
                    </EQ>
                  </AcctId>
                  <Ccy>EUR</Ccy>
                - <AcctOwnr>
                  - <FinInstnId>
                      <BIC>ACCTOWNRXXX</BIC>
                    </FinInstnId>
                  </AcctOwnr>
                - <AcctSvcr>
                  - <FinInstnId>
                      <BIC>ACCTSVCRXXX</BIC>
                    </FinInstnId>
                  </AcctSvcr>
                </SchCrit>
              </NewCrit>
            </AcctCrit>
          </AcctQryDef>
        </GetAcct>
      </Document>
    </BizData>
  </PyId>
</Xchg>
```

```
- <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  - <Fr>
    - <FIId>
      - <FinInstnId>
          <BICFI>FACHFRP1000</BICFI>
        - <Othr>
            <Id>FAAHFRP1000</Id>
          </Othr>
        - <ClrSysMmbId>
          - <ClrSysId>
              <Prtry>T2S</Prtry>
            </ClrSysId>
            <MmbId>SystemUserX1</MmbId>
          </ClrSysMmbId>
        </FinInstnId>
      </FIId>
    </Fr>
  - <To>
    - <FIId>
      - <FinInstnId>
          <BICFI>SETTLSYST2S</BICFI>
        - <Othr>
            <Id>FAAHFRP1000</Id>
          </Othr>
        </FinInstnId>
      </FIId>
    </To>
    <BizMsgIdr>1SR0524SEC500101</BizMsgIdr>
    <MsgDefIdr>semt.013.001.02</MsgDefIdr>
    <CreDt>2012-05-24T14:25:11Z</CreDt>
  - <Sgntr>
    - <ds:Signature Id="_be4dd7de-c63a-43a6-9b62-f69290939eb6" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      - <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
        - <ds:Reference URI="#_98742d60-2afc-4fa7-a731-828756ce47b1">
          - <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <ds:DigestValue>vB/xxu+qkEVUH5i9uVdBHOXOp6+XDsAn/iHxH+UiMGo=</ds:DigestValue>
          </ds:Reference>
        - <ds:Reference URI="">
          - <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <ds:DigestValue>hWGkHPu5IMYxe4KFYyaMOFWYq0w2pi+BYnYvHEwm/Z8=</ds:DigestValue>
          </ds:Reference>
        - <ds:Reference>
          - <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <ds:DigestValue>10eHeNdJM1v177M0HzFsmP0IBMYvdPXVuRcR77hAgUg=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>

          <ds:SignatureValue>HllitYLicuu5drRrzu5CFxk5GZ3LD00nEPCrXkfWiu54y0zA3P2r6AIe1cYIdueY8nioLEvcZcvKVS4zt6bbHv8RRaWmU+Jfl3
      - <ds:KeyInfo Id="_98742d60-2afc-4fa7-a731-828756ce47b1">
        - <ds:X509Data>

              <ds:X509Certificate>MIID0DCCArigAwIBAgIBBTANBgkqhkiG9w0BAQsFADBMMQswCQYDVQQGEwJGUjEcMBoGA1UECgwTS2V5bmVjd
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
    </Sgntr>
  </AppHdr>
```