Comment Resolution Account for <document name and version number>
Prepared: <date>

Comment #	Public review	Date provided	Link to email	Commenter
1.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis	ETSI ESI STF 524
2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis	ETSI ESI STF 524
2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis	ETSI ESI STF 524

Comment provided / Issue raised

Clause 4.1.5 Component AttachmentReference. Second paragraph is misleading:

COMMENT:
Original text: “Below follows a list of the sub-components that MAY be present within this component”, and then follows a list of two subcomponents, one of which is AttRefURI

Clause 4.2.1. “An input document can also be a <ds:Manifest>, allowing the client to handle manifest creation while using the server to create the rest of the signature.”
An initial search of the keywords ds:Manifest and Manifest does not hit any sentence explaining or developing how this situation can be managed and what does “allowing the client to handle manifest creation” actually means.

REQUEST: CLARIFY THE TEXT, MAYBE ADDING SOME ADDITIONAL TEXT IN THE PROCESSING CLAUSES FOR THE CASE THE INPUTDOCUMENT CONTAINS A DS:MANIFEST, IF NOT, DELETE IT.

AK: Just took text as it was in DSS v1.0: it was as it is. There is no problem in adding more text. Most of the text was taken from old v1.0 to prevent additional problems to compliant implementations.

Clause 4.2.1.2. The new XML Schema does not allow that in a certain request appear sub-components of different type. With the current XML Schema one instance of InputDocumentsType can only have EITHER one or more Document, OR one or more TransformedData, OR one or more DocumentHash. An InputDocumentsType instance MAY NOT have, with the current definition one Document, one TransformedData and one DocumentHash, for instance. Core v1.0 actually ALLOWED THE PRESENCE OF INPUTS OF DIFFERENT NATURE.

REQUEST: MODIFY THE XML SCHEMA FOR ALLOWING PRESENCE OF INPUTS OF DIFFERENT NATURE (A CHOICE WITH MAXOCCURS=2UNBOUNDED” WOULD MAKE IT.

TC decision on resolution

The irritation 'MAY' is excluded from the mentioned sentence. It is now:

'Below follows a list of the sub-components that constitute this component'

Extend the SiognbedReference component with another element:

<xs:attribute name="InManifest" type="xs:boolean" use="optional" default="false"/>

Fix XML schema, align test cases, check generated documentation and JSON scheme

Documented in Issue

https://issues.oasis-open.org/browse/DSSX-25

https://issues.oasis-open.org/browse/DSSX-26

https://issues.oasis-open.org/browse/DSSX-27

2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis·ETSI ESI STF 524

2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis·ETSI ESI STF 524

Clause 4.2.6. SignRequest. When one reads the text “Below follows a list of the sub-components that MAY be present within this component:” one thinks that it is misleading, as this component inherits from RequestBaseType and other sub-components may appear. At the end of all the requirements for the new subcomponents, the text fixes the situation “A set of sub-components is inherited from component 5.1.10 and is not repeated here”

REQUEST: makes it clear since the very beginning that the sub-components of RequestBaseType and the new ones listed below may appear. Also include the name of the base type RequestBaseType and not only the clause number for facilitating reading.

This situation appears in a good number (if not in all) those clauses where a type is derived from a base type.

REQUEST: make changes in all these clauses as indicated above.

Clause 4.2.7 SignResponse. As previous comment.

The proposed solution is implemented.

Befoire the definition of the sub-componentes tghere is the following text inserted:

'This components externds the component RequestBase. The inheritied sub-components are not repeated here.'

Aligned schema and documentation

https://issues.oasis-open.org/browse/DSSX-28
https://issues.oasis-open.org/browse/DSSX-29

2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis-	ETSI ESI STF 524

Clause 4.3.5.

COMMENT: The definition of the component ReturnAugmentedSignature allows for multiple occurrences of this component. One could think that this essentially means that in theory one request could order to the server to augment one signature to one level, another signature to another level, and so on. However, the contents of the type AugmentSignatureInstructionType DOES NOT allow to refer to any signature in the request, so in the end it seems as if one would like to request to the server to augment all the signatures in the request to different levels and retrieve them (i.e., would be like requesting to augment one signature to XAdES-B-T level, then to XAdES-B-LT, and then to XAdES-B-LTA, and return the three augmented signatures). In principle, this does not seem to make lot of sense.

ETSI ESI has decided that in one request the ReturnAugmentedSignature will appear ONLY ONE TIME, with ONE URI value and this will mean that the server is requested to augment all the signatures to the identified level, if possible. The rationale behind is to make things easier for the server.

REQUEST: Modify the specification of the ReturnAugmentedSignature and its type to make it compatible with ETSI ESI, i.e., make maxOccurs of ReturnAugmentedSignature =”1”, and specify that the server shall try to augment all the signatures to the level identified in that component.

Dropped the type at all as it's nothing more than an URI.

https://issues.oasis-open.org/browse/DSSX-30

2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis-	ETSI ESI STF 524

Clause 4.3.4.2. XML Schema for OptionalInputsSignType.

The definition of SignRequest includes the following sub-component:

```
<xs:element minOccurs="0" name="OptionalInputs"
                type="dss2:OptionalInputsSignType"/>
```

And then the definition of OptionalInputsSignType is as follows:

```
<xs:complexType name="OptionalInputsSignType">
  <xs:complexContent>
    <xs:extension base="dss2:OptionalInputsBaseType">
      <xs:sequence>
        <xs:choice>
          <xs:element maxOccurs="1" minOccurs="0" name="SignatureType"
                type="xs:anyURI"/>
          <xs:element maxOccurs="1" minOccurs="0" name="IntendedAudience"
                type="dss2:IntendedAudienceType"/>
          <xs:element maxOccurs="unbounded" minOccurs="0"
name="KeySelector"
                type="dss2:KeySelectorType"/>
          <xs:element maxOccurs="1" minOccurs="0" name="Properties"
                type="dss2:PropertiesHolderType"/>
          <xs:element maxOccurs="unbounded" minOccurs="0"
name="IncludeObject"
                type="dss2:IncludeObjectType"/>
          <xs:element default="false" maxOccurs="1" minOccurs="0"
                name="IncludeEContent" type="xs:boolean"/>
          <xs:element maxOccurs="1" minOccurs="0" name="SignaturePlacement"
                type="dss2:SignaturePlacementType"/>
          <xs:element maxOccurs="1" minOccurs="0" name="SignedReferences"
                type="dss2:SignedReferencesType"/>
          <xs:element maxOccurs="1" minOccurs="0" name="Nonce"
                type="xs:integer"/>
          <xs:element maxOccurs="1" minOccurs="0" name="SignatureAlgorithm"
                type="xs:string"/>
          <xs:element maxOccurs="1" minOccurs="0"
name="SignatureQualityLevel"
                type="xs:anyURI"/>
        </xs:choice>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

With these definitions one SignRequest CAN HAVE ONLYONE OPTIONAL INPUT (PLEASE NOTE THAT IN THE DEFINITION OF OptionalInputsBaseType THE SEQUENCE ONLY HAS ONE ELEMENT: A CHOICE BETWEEN A NUMBER OF OPTIONS, BUT ONLY ONE. Note also

Fix XML schema, align test cases, check generated documentation and JSON scheme

2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis-	ETSI ESI STF 524

Clause 4.3.5.2. XML schema for OptionalInputsVerifyType

The definition of VerifyRequest includes the following sub-component
<xs:element minOccurs="0" name="OptionalInputs"
type="dss2:OptionalInputsVerifyType"/>

And clause 4.3.5.2 defines:

```
<xs:complexType name="OptionalInputsVerifyType">
  <xs:complexContent>
    <xs:extension base="dss2:OptionalInputsBaseType">
      <xs:sequence>
        <xs:choice>
          <xs:element maxOccurs="1" minOccurs="0" name="UseVerificationTime"
                type="dss2:UseVerificationTimeType"/>
          <xs:element default="false" maxOccurs="1" minOccurs="0"
                name="ReturnVerificationTimeInfo" type="xs:boolean"/>
          <xs:element maxOccurs="unbounded" minOccurs="0"
                name="AdditionalKeyInfo"
                type="dss2:AdditionalKeyInfoType"/>
          <xs:element default="false" maxOccurs="1" minOccurs="0"
                name="ReturnProcessingDetails" type="xs:boolean"/>
          <xs:element default="false" maxOccurs="1" minOccurs="0"
                name="ReturnSigningTimeInfo" type="xs:boolean"/>
          <xs:element default="false" maxOccurs="1" minOccurs="0"
                name="ReturnSignerIdentity" type="xs:boolean"/>
          <xs:element maxOccurs="unbounded" minOccurs="0"
                name="ReturnAugmentedSignature"
                type="dss2:AugmentSignatureInstructionType"/>
          <xs:element maxOccurs="unbounded" minOccurs="0"
                name="ReturnTransformedDocument"
                type="dss2:ReturnTransformedDocumentType"/>
          <xs:element maxOccurs="1" minOccurs="0"
                name="ReturnTimestampedSignature"
                type="dss2:AugmentSignatureInstructionType"/>
          <xs:element default="false" maxOccurs="1" minOccurs="0"
                name="VerifyManifests" type="xs:boolean"/>
        </xs:choice>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

Again, the sequence only has ONE child, which is a choice of the children of the <choice> component, but ONLY ONE, and consequently this schema does not allow to have more than one optional input.

REQUEST: EITHER SUPPRESS THE CHOICE WITHIN THE SEQUENCE OR

Valid remark, the OptionalInputsVerifyType must offer a way to contain more than one distinct type of optional element.

Proposed solution changing the definition of OptionalInputsVerifyType in the way as proposed in https://issues.oasis-open.org/browse/DSSX-31 for OptionalInputsSignType: drop xs:choice.

2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis-ETSI ESI STF 524

2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis-ETSI ESI STF 524
2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis-ETSI ESI STF 524

Clause 4.3.6.2 OptionalOutputsBaseType.
Same comment as above and same request.
REQUEST: EITHER SUPPRESS THE CHOICE WITHIN THE SEQUENCE OR ADD A MAXOCCURS TO THE SEQUENCE.

Clause 4.3.8.2 OptionalOutputsVerifyType.
Same comment as above and same request.
REQUEST: EITHER SUPPRESS THE CHOICE WITHIN THE SEQUENCE OR ADD A MAXOCCURS TO THE SEQUENCE.

Clause 6.3.1 Sub process ‘update Signature’.

COMMENT: in the title and within the text of the clause the term “update of signature” is used, which seems a problem inherited from version 1.0. Now the new term for this process is augment and augmented signature, according to AdES terminology in ETSI ENs.

REQUEST:
1. Replace the title by “augmentation of signature”.
2. Replace “update” by “augment” or “augmentation” depending on the context.
3. Replace ReturnUpdatedSignature by ReturnAugmentedSignature.

Valid remark, the OptionalOutputsBaseType must offer a way to contain more than one distinct type of optional element.

Proposed solution changing the definition of OptionalOutputsBaseType in the way as proposed in https://issues.oasis-open.org/browse/DSSX-31 for OptionalInputsSignType: drop xs:choice.

Valid remark, the OptionalOutputsVerifyType must offer a way to contain more than one distinct type of optional element.

Proposed solution changing the definition of OptionalOutputsVerifyType in the way as proposed in https://issues.oasis-open.org/browse/DSSX-31 for OptionalInputsSignType: drop xs:choice.

Updated the core document and the BPMN processes accordingly.

https://issues.oasis-open.org/browse/DSSX-33

https://issues.oasis-open.org/browse/DSSX-34

https://issues.oasis-open.org/browse/DSSX-35

2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis	ETSI ESI STF 524

2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis	ETSI ESI STF 524

Clause 4.3.8. OptionalOutputsVerify and Clause 4.3.32 AugmentedSignature
COMMENT:
Clause 4.3.8 only allows one instance of AugmentedSignature, and AugmentedSignature may only contain one SignatureObject. It is not possible to return more than one AugmentedSignature if no changes are done to the XML schema. In addition to that if the augmented signature is within it is returned within the component DocumentWithSignature, which makes it difficult to notice that it is an augmented signature.

REQUESTS:
1. Make it possible that a response may contain more than one AugmentedSignature occurrences.
2. Make it possible that an item of AugmentedSignature may also contain a DocumentWithSignature sub-component…in other words, make its content a choice of either a SignatureObject OR a DocumentWithSignature, so that it is clear that regardless where the signature appears in the response it is clear that it is an augmented signature.

AK: The requirement for returning detailed information of validation of several signatures is more an item for profiles than for the core.
JC: very good point. I fully agree. TS 119 442 is a profile of the DSS-X core 2.0 that defines new types/elements and restricts the usage of certain elements in the core: expands it and restricts it.

LR: I have not been able to read the specification, but I plan to do it.
Frederick: We have some few comments. Maybe we could bring them later on or present them now
Clause 4.3.4.

COMMENTS:
They are SignatureType refer to 7.1, which does not exist. It should be 9.1.
When I look to the URIs we are missing URIs for PDF signatures
AK: we took the URIs coming from DSS 1.0.
JC: after DSS 1.0 became a OASIS standard, a number of profiles were created for managing PDF signatures (generation) as well.
LR: there is a component drafted that you can pass to the server with a pdf document asking to the server to generate a PAdES signature.
AK: the list is informal in the core, not limiting anything. I will take a look to the ETSI Profile for signing.

Adapted the proposed changes and aligned the documentation

Public Comment 201809c00001s14: missing URI definitions. Nothing to do.

https://issues.oasis-open.org/browse/DSSX-37

https://issues.oasis-open.org/browse/DSSX-38

2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis·ETSI ESI STF 524

2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis·ETSI ESI STF 524
2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis·ETSI ESI STF 524
2.	DSS-X core2.0 csprd01	9.28.2018	https://www.oasis·ETSI ESI STF 524

Clause 7

QUESTION: in this model is the server the one that decides whether the management is done synchronous or asynchronous. Could it be possible to consider the possibility of allowing the client to have the possibility of deciding this?
AK: are there use cases for this?
FP, LR: there are few use cases for this…for instance when the client does not want to wait until the server finishes, but it prefers to leave this, do something else and come back later on. This is more for server to server communication.
AK: this is a good point and we should think about it.
JC: I guess that this would also impact the validation protocol, not only the sign protocol.
AK: indeed, clause 7 affects both.

Some references in some places of the text are wrong. In clause 4.X.X there is the text saying: “requirements specified in this document in section 5:XX” when it should read “4.X.X”

Clause 4.1.11 Component ResponseBase. Incomplete sentence at the end of the clause:

COMMENT:
At the end of the clause there is an incomplete sentence.
« The optional ResponseID element MUST contain one instance of a string. » [DSS-4.1.11-4].
The ResponseID element …

Clause 4.3.6 Component OptionalOutputsBase. Statement non very clear.
COMMENT:
It is stated “« If a server does not recognize or can not handle any optional input, it MUST reject the request with a ResultMajor code of RequesterError and a ResultMinor code of NotSupported. »”. The statement refers to OptionalInputBase component, it is not clear if it is a repetition (in such case it doesn’t seem appropriate in the clause concerning OptionalOutputBase component) or it should be referred to the client instead of the server (in this case it seems strange having a statement imposing a condition to the client) or something else.

Added a specific optional input element to enforce async processing
Double checked the document for wrong references.

Using OpenOffice for review of the specification's docx file. Broken reference are quite obvious in OpenOffice in contrast to Mirosoft Word.

Added a complete sentence explaining the use of ResponseID.

Extended the section describing the 'Asynchronous Processing Model' with more details regarding the dependency between RequestID and ResponseID.

Component OptionalOutputsBase. Statement not very clear. Drop the misleading sentence.

https://issues.oasis-open.org/browse/DSSX-40

https://issues.oasis-open.org/browse/DSSX-41

https://issues.oasis-open.org/browse/DSSX-42

https://issues.oasis-open.org/browse/DSSX-43

2.	DSS-X core2.0 csprd01	8.29.2018	https://lists.oasis-(	Dazza Greenwood

[...] Are there any libraries or other open source projects implementing this updated protocol?

I'd like to try it out as a way to better understand the how the functionality and flow are intended to work. [...]

Ongoing tasks to compile a list of known implementations

https://issues.oasis-open.org/browse/DSSX-24