Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services

Download the template for comments:
https://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments ONLY to E-SIGNATURES_COMMENTS@list.etsi.org

CAUTION: This DRAFT document is provided for information and is for future development work within the ETSI Technical Committee ESI only. ETSI and its Members accept no liability for any further use/implementation of this Specification. Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at
http://www.etsi.org/standards-search
ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex — FRANCE

Tel.: +33 4 92 94 42 00  Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 — NAF 742 C
Association à but non lucratif enregistrée à la
Sous-préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx.

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommitteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2017. All rights reserved.

DECT™, PLUGTESTSTM, UMTSTM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. 3GPP™ and LTE™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.
## Contents

<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intellectual Property Rights</td>
<td>3</td>
</tr>
<tr>
<td>Foreword</td>
<td>7</td>
</tr>
<tr>
<td>Modal verbs terminology</td>
<td>7</td>
</tr>
<tr>
<td>Executive summary</td>
<td>7</td>
</tr>
<tr>
<td>Introduction</td>
<td></td>
</tr>
<tr>
<td>1 Scope</td>
<td>7</td>
</tr>
<tr>
<td>2 References</td>
<td>7</td>
</tr>
<tr>
<td>2.1 Normative references</td>
<td>7</td>
</tr>
<tr>
<td>2.2 Informative references</td>
<td>8</td>
</tr>
<tr>
<td>3 Definitions, symbols and abbreviations</td>
<td>8</td>
</tr>
<tr>
<td>3.1 Definitions</td>
<td>8</td>
</tr>
<tr>
<td>3.2 Symbols</td>
<td>9</td>
</tr>
<tr>
<td>3.3 Abbreviations</td>
<td>9</td>
</tr>
<tr>
<td>4 Technical approach to the specification of the profiles</td>
<td>9</td>
</tr>
<tr>
<td>4.1 Introduction</td>
<td>9</td>
</tr>
<tr>
<td>4.2 OASIS DSSX TC XML related protocol</td>
<td>9</td>
</tr>
<tr>
<td>4.3 OASIS DSSX TC JSON related protocol</td>
<td>10</td>
</tr>
<tr>
<td>5 Profile(s) for requesting validation of AdES signatures</td>
<td>11</td>
</tr>
<tr>
<td>5.1 Components for requesting validation of AdES signatures</td>
<td>11</td>
</tr>
<tr>
<td>5.1.1 Component for requesting validation</td>
<td>11</td>
</tr>
<tr>
<td>5.1.1.1 Component semantics</td>
<td>11</td>
</tr>
<tr>
<td>5.1.1.2 OASIS XML related component</td>
<td>11</td>
</tr>
<tr>
<td>5.1.1.3 OASIS JSON related component</td>
<td>12</td>
</tr>
<tr>
<td>5.1.2 Component for submitting signature to be validated</td>
<td>13</td>
</tr>
<tr>
<td>5.1.2.1 Component semantics</td>
<td>13</td>
</tr>
<tr>
<td>5.1.2.2 OASIS XML related components</td>
<td>14</td>
</tr>
<tr>
<td>5.1.2.3 OASIS JSON related component</td>
<td>14</td>
</tr>
<tr>
<td>5.1.3 Component for submitting signed documents or representations of the signed documents</td>
<td>14</td>
</tr>
<tr>
<td>5.1.3.1 Component semantics</td>
<td>14</td>
</tr>
<tr>
<td>5.1.3.2 OASIS XML related component</td>
<td>14</td>
</tr>
<tr>
<td>5.1.3.2.1 Additional requirements for contents of dss:InputDocuments</td>
<td>15</td>
</tr>
<tr>
<td>5.1.3.2.1.1 Element dss:Document for sending original documents</td>
<td>15</td>
</tr>
<tr>
<td>5.1.3.2.1.2 Element dss:TransformedData for sending transformed documents</td>
<td>16</td>
</tr>
<tr>
<td>5.1.3.2.1.3 Element dss:DocumentHash for sending digest of documents</td>
<td>16</td>
</tr>
<tr>
<td>5.1.3.3 OASIS JSON related component</td>
<td>16</td>
</tr>
<tr>
<td>5.1.3.3.1 Element doc for sending original documents</td>
<td>16</td>
</tr>
<tr>
<td>5.1.3.3.2 Element transformed for sending transformed documents</td>
<td>16</td>
</tr>
<tr>
<td>5.1.3.3.3 Element docHash for sending digest of documents</td>
<td>17</td>
</tr>
<tr>
<td>5.1.4 Cardinalities for elements used for sending information of documents</td>
<td>17</td>
</tr>
<tr>
<td>5.1.4 Optional components</td>
<td>19</td>
</tr>
<tr>
<td>5.1.4.1 Container for optional components</td>
<td>19</td>
</tr>
<tr>
<td>5.1.4.1.1 Semantics</td>
<td>19</td>
</tr>
<tr>
<td>5.1.4.1.2 OASIS XML related component</td>
<td>19</td>
</tr>
<tr>
<td>5.1.4.1.3 OASIS JSON related component</td>
<td>20</td>
</tr>
<tr>
<td>5.1.4.2 Identifying the profile used for the request</td>
<td>21</td>
</tr>
<tr>
<td>5.1.4.2.1 Semantics</td>
<td>21</td>
</tr>
<tr>
<td>5.1.4.2.2 OASIS XML related components</td>
<td>21</td>
</tr>
<tr>
<td>5.1.4.2.3 OASIS JSON related component</td>
<td>21</td>
</tr>
<tr>
<td>5.1.4.3 Component for identifying under which service policy the validation has to be conducted</td>
<td>22</td>
</tr>
<tr>
<td>5.1.4.3.1 Component semantics</td>
<td>22</td>
</tr>
<tr>
<td>5.1.4.3.2 OASIS XML related component</td>
<td>22</td>
</tr>
</tbody>
</table>
5.1.4.3.3 OASIS JSON related component ................................................................. 22
5.1.4.4 Component for allowing the client to claim for an identity ........................................ 22
5.1.4.4.1 Component semantics ........................................................................ 22
5.1.4.4.2 OASIS XML related component ................................................................ 22
5.1.4.4.3 OASIS JSON related component ......................................................... 22
5.1.4.5 Component for requesting notifications in a certain language ......................... 22
5.1.4.5.1 Component semantics ........................................................................ 22
5.1.4.5.2 OASIS XML related component ......................................................... 22
5.1.4.5.3 OASIS JSON related component ......................................................... 23
5.1.4.6 Component for requesting to set the validation time to a certain instant different from current time .......................................................... 23
5.1.4.6.1 Component semantics ........................................................................ 23
5.1.4.6.2 OASIS XML related component ......................................................... 23
5.1.4.6.3 OASIS JSON related component ......................................................... 23
5.1.4.7 Component for requesting to return the validation time .................................. 23
5.1.4.7.1 Component semantics ........................................................................ 23
5.1.4.7.2 OASIS XML related component ......................................................... 23
5.1.4.7.3 OASIS JSON related component ......................................................... 23
5.1.4.8 Component for passing validation material to the server .................................. 23
5.1.4.8.1 Component semantics ........................................................................ 23
5.1.4.8.2 OASIS XML related component ......................................................... 24
5.1.4.8.3 OASIS JSON related component ......................................................... 24
5.1.4.9 Component for requesting the server to return the identity of the signer .......... 24
5.1.4.9.1 Component semantics ........................................................................ 24
5.1.4.9.2 OASIS XML related component ......................................................... 24
5.1.4.9.3 OASIS JSON related component ......................................................... 24
5.1.4.10 Component for requesting validation against a certain signature policy .......... 24
5.1.4.10.1 Component semantics ........................................................................ 24
5.1.4.10.2 OASIS XML protocol ...................................................................... 24
5.1.4.10.3 OASIS JSON protocol ...................................................................... 25
5.1.4.10.4 Processing model ............................................................................ 25
5.1.4.11 Component for requesting a detailed validation report (as the one to be specified in TS 119 102-2) .............................................................. 26
5.1.4.11.1 Component semantics ........................................................................ 26
5.1.4.11.2 OASIS XML protocol ...................................................................... 26
5.1.4.11.3 OASIS JSON protocol ...................................................................... 26
5.1.4.12 Component for requesting that the validation report is signed by the server a detailed validation report (as the one to be specified in TS 119 102-2) .............................................................. 26
5.1.4.12.1 Component semantics ........................................................................ 26
5.1.4.12.2 OASIS XML protocol ...................................................................... 26
5.1.4.12.3 OASIS JSON protocol ...................................................................... 26
5.1.4.13 Component for requesting the server to return the result of transforming the input document .............................................................. 27
5.1.4.13.1 Component semantics ........................................................................ 27
5.1.4.13.2 OASIS XML protocol ...................................................................... 27
5.1.4.13.3 OASIS JSON related component ......................................................... 27
5.1.4.14 Component for requesting to return the validation of signed ds:Manifest in XAdES signatures .......................................................... 27
5.1.4.14.1 Component semantics ........................................................................ 27
5.1.4.14.2 OASIS XML protocol ...................................................................... 27
5.1.4.14.3 OASIS JSON protocol ...................................................................... 27
5.1.4.15 Component for identifying a request .......................................................... 27
5.1.4.15.1 Component semantics ........................................................................ 27
5.1.4.15.2 OASIS XML protocol ...................................................................... 27
5.1.4.15.3 OASIS JSON protocol ...................................................................... 27
5.1.4.16 Component for asynchronous processing ..................................................... 28
5.1.4.16.1 Asynchronous processing protocol ..................................................... 28
5.1.4.16.2 Component for identifying a request as a subsequent request to an initial request .............................................................. 28
5.1.4.16.2.1 Semantics ..................................................................................... 28
5.1.4.16.2.2 OASIS XML related protocol ......................................................... 28
5.1.4.16.2.3 OASIS JSON related protocol ......................................................... 28
5.2 Components for response to validation request ...................................................... 29
5.2.1 Component for responding to validation request ................................................ 29
5.2.1.1 Component semantics ........................................................................ 29
5.2.1.2 OASIS XML related component ......................................................... 29
5.2.1.3 OASIS JSON related component ......................................................... 30
5.2.2 Component for notifying the validation result ................................................................. 30
5.2.2.1 Component semantics ................................................................................................... 30
5.2.2.2 OASIS XML related component .................................................................................. 30
5.2.2.3 OASIS JSON related component ............................................................................... 30
5.2.3 Optional components ....................................................................................................... 31
5.2.3.1 Container for optional components ....................................................................... 31
5.2.3.1.1 Semantics ............................................................................................................... 31
5.2.3.1.2 OASIS XML related component ........................................................................... 31
5.2.3.1.3 OASIS JSON related component ......................................................................... 32
5.2.3.2 Identifying the profile used ......................................................................................... 33
5.2.3.2.1 Semantics ............................................................................................................... 33
5.2.3.2.2 OASIS XML related components ....................................................................... 33
5.2.3.2.3 OASIS JSON related component ......................................................................... 33
5.2.3.3 Component for indicating the service policy .............................................................. 33
5.2.3.3.1 Component semantics .......................................................................................... 33
5.2.3.3.2 OASIS XML related component ........................................................................ 34
5.2.3.3.3 OASIS JSON related component ......................................................................... 34
5.2.3.4 Component for indicating validation time ................................................................. 34
5.2.3.4.1 Component semantics .......................................................................................... 34
5.2.3.4.2 OASIS XML related component ........................................................................ 34
5.2.3.4.3 OASIS JSON related component ......................................................................... 34
5.2.3.5 Component for returning signer’s identity ................................................................. 34
5.2.3.5.1 Component semantics .......................................................................................... 34
5.2.3.5.2 OASIS XML protocol .......................................................................................... 34
5.2.3.5.3 OASIS JSON protocol ........................................................................................ 34
5.2.3.6 Component for notifying the signature policy applied during the validation ............ 34
5.2.3.6.1 Component semantics .......................................................................................... 34
5.2.3.6.2 OASIS XML protocol .......................................................................................... 34
5.2.3.6.3 OASIS JSON protocol ........................................................................................ 35
5.2.3.7 Component for notifying the signature policies under which the server can conduct validation ........................................................................................................ 35
5.2.3.7.1 Component semantics ........................................................................................ 35
5.2.3.7.2 OASIS XML protocol .......................................................................................... 35
5.2.3.7.3 OASIS JSON protocol ........................................................................................ 35
5.2.3.8 Component for returning the detailed validation report .......................................... 36
5.2.3.8.1 Component semantics .......................................................................................... 36
5.2.3.8.1.1 ETSI XML protocol ......................................................................................... 36
5.2.3.8.1.2 ETSI JSON protocol ......................................................................................... 36
5.2.3.9 Component for returned the detailed validation report signed .................................. 36
5.2.3.9.1 Component semantics .......................................................................................... 36
5.2.3.9.2 OASIS XML protocol .......................................................................................... 36
5.2.3.9.3 OASIS JSON protocol ........................................................................................ 36
5.2.3.10 Component for returning the result of transforming the input document .............. 36
5.2.3.10.1 Component semantics ......................................................................................... 36
5.2.3.10.2 OASIS XML related component ....................................................................... 37
5.2.3.10.3 OASIS JSON related component ....................................................................... 37
5.2.3.11 Component for returning the result of validating ds:Manifest elemens in XAdES signatures ........................................................................................................... 37
5.2.3.11.1 Component semantics ......................................................................................... 37
5.2.3.11.2 OASIS XML protocol ......................................................................................... 37
5.2.3.11.3 OASIS JSON protocol ....................................................................................... 37
5.2.3.12 Components for asynchronous processing ............................................................. 37
5.2.3.12.1 Introduction .......................................................................................................... 37
5.2.3.12.2 Component for indicating not completion of signature(s) validation ................. 37
5.2.3.12.2.1 Semantics ......................................................................................................... 37
5.2.3.12.2.2 OASIS XML protocol ..................................................................................... 37
5.2.3.12.2.3 OASIS JSON protocol .................................................................................... 37
5.2.3.12.3 Component for correlating subsequent requests to the initial response .......... 38
5.2.3.12.3.1 Semantics ........................................................................................................ 38
5.2.3.12.3.2 OASIS XML protocol ..................................................................................... 38
5.2.3.12.3.3 OASIS JSON protocol .................................................................................... 38
6 Profiles for validation and augmentation of signatures ................................................. 38
6.1 Components for requesting validation and augmentation .......................................... 38
6.1.1 Component for requesting validation and augmentation of the signature to a certain level ........................................ 38
6.1.1.1 Component semantics .................................................................................................................. 38
6.1.1.2 OASIS XML related component ............................................................................................. 39
6.1.1.3 OASIS JSON related component ............................................................................................. 39
6.2 Components for response to validation and augmentation request ..................................................... 39
6.2.1 Component for returning the augmented signature ............................................................................. 39
6.2.1.1 Component semantics ............................................................................................................... 39
6.2.1.2 OASIS XML related component ............................................................................................. 39
6.2.1.3 OASIS JSON related component ............................................................................................. 40

7 Auxiliary types ............................................................................................................................................ 40
7.1 Type for extension points .................................................................................................................... 40
7.1.1 AnyType for OASIS XML protocol ............................................................................................... 40
7.1.2 OASIS JSON related component ................................................................................................. 40
7.2 Type for language-qualified strings ..................................................................................................... 40
7.2.1 InternationalStringType type for OASIS XML protocol .............................................................. 40
7.2.2 OASIS JSON related component ................................................................................................. 40
7.3 Type for names ....................................................................................................................................... 40
7.3.1 saml:NameIdentifierType type for OASIS XML protocol .......................................................... 40
7.3.2 OASIS JSON related component ................................................................................................. 40

Annex A (normative): XML and JSON Schema files .................................................................................... 41
A.1 XML Schema file location for namespace http://uri.etsi.org/19442/v1.1.1# ................................. 41
A.2 JSON Schema file location for “$schema” "http://etsi.org/119442/v1.1.1/json#" ............................ 41

Annex (informative): Bibliography .................................................................................................................. 42
Annex (informative): Change History ............................................................................................................ 43
History .......................................................................................................................................................... 44
Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for ETSI members and non-members, and can be found in ETSI SR 000 314: "Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"must" and "must not" are NOT allowed in ETSI deliverables except when used in direct citation.

Executive summary

Propose not to include it.

1 Scope

The present document specifies the semantics of a protocol for requesting to a remote server (and for receiving the corresponding response) the validation and optionally the augmentation of AdES digital signatures compliant with the following ETSI deliverables: ETSI EN 319 122 [3], ETSI EN 319 132 [4], ETSI EN 319 142 [5], ETSI TS 101 733 [6], ETSI TS 102 778 [10], ETSI TS 101 903 [8], ETSI TS 103 171 [9], ETSI TS 103 172 [11], and ETSI TS 103 173 [7].

For the aforementioned semantics the present document specifies two bindings, each one in a different format (XML and JSON).

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 119 172-4 "Electronic Signatures and Infrastructures (ESI); Signature applicability rules for European qualified electronic signatures/seals using trusted lists"

(note: to be completed)

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 and the following apply:

representation of a (signed) document: either the (signed) document itself, its digest, or the result of applying to the (signed) document a certain set of known transformations.

(note: to be completed)
3.2 Symbols
For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

3.3 Abbreviations
For the purposes of the present document, the [following] abbreviations [given in ... and the following] apply:

4 Technical approach to the specification of the profiles.

4.1 Introduction
The present document specifies the semantics of a protocol for requesting the validation and optionally the augmentation of AdES digital signatures to a remote server and for receiving the related response.

For the aforementioned semantics the present document specifies two bindings, each one in a different format (XML and JSON).

The profiles specified in the present document take as starting point a number of OASIS DSS and OASIS DSS-X Technical Committees’ specifications, namely "OASIS Standard: Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0 [1]" and "Asynchronous Processing Abstract Profile of the OASIS Digital Signature Service Version 1.0" [2].

The rest of the document is organized as follows:

1) Sub-clauses 4.2 and 4.3 provide general remarks on the XML and JSON protocols relying on OASIS DSS and DSS-X Technical Committees’ protocols.

2) Clause 5 specifies requirements for all the components for validation protocols (XML and JSON) relying on OASIS DSS and DSS-X Technical Committees’ protocols.

3) Clause 6 specifies requirements for those specific components for augmentation protocols (XML and JSON) relying on OASIS DSS and DSS-X Technical Committees’ protocols.

For each component of the aforementioned protocols, the present document:

1) Defines requirements for the semantics of the component (i.e. its mandatory contents, its optional contents, etc). These requirements are defined in clauses "Component semantics".

2) Defines requirements for the XML component of the XML protocol relying on OASIS DSS and DSS-X Technical Committees’ protocols, which is able to fulfil the semantic requirements already defined. These requirements are defined in clauses named "OASIS XML related component".

3) Defines requirements for the JSON component of the JSON protocol relying on OASIS DSS and DSS-X Technical Committees’ protocols, which is able to fulfil the semantic requirements already defined. These requirements are defined in clauses named "OASIS JSON related component".

4.2 OASIS DSSX TC XML related protocol
The structures described in this specification are contained in the schema files [DSS_Core_XSD], [AdES_XSD], [ASYN_XSD], [SIG_POL_XSD], and [SIGNED_VAL_RESP_XSD] and the xml schema file [ ]. The new elements and types defined in that schema are defined within the XML namespace whose URI value is shown below:

http://uri.etsi.org/19442/v1.1.1#

Table 1 shows the URI values of other XML namespaces and their corresponding prefixes used in the aforementioned schema file and within the present document.
### Table 1

<table>
<thead>
<tr>
<th>URI value of the XML Namespace</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://uri.etsi.org/19442/v1.1.1#">http://uri.etsi.org/19442/v1.1.1#</a></td>
<td>etsival</td>
</tr>
<tr>
<td>urn:oasis:names:tc:dss:1.0:core:schema</td>
<td>dss</td>
</tr>
<tr>
<td>urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#</td>
<td>dssades</td>
</tr>
<tr>
<td>urn:oasis:names:tc:dss:1.0:profiles:asyncronousprocessing:1.0</td>
<td>dssasyn</td>
</tr>
<tr>
<td>urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#</td>
<td>dssvalrep</td>
</tr>
<tr>
<td><a href="http://www.w3.org/2000/09/xmldsig#">http://www.w3.org/2000/09/xmldsig#</a></td>
<td>ds</td>
</tr>
<tr>
<td><a href="http://uri.etsi.org/01903/v1.3.2">http://uri.etsi.org/01903/v1.3.2</a></td>
<td>xades</td>
</tr>
<tr>
<td><a href="http://uri.etsi.org/01903/v1.4.1">http://uri.etsi.org/01903/v1.4.1</a></td>
<td>xadesv141</td>
</tr>
<tr>
<td>urn:oasis:names:tc:SAML:2.0:assertion</td>
<td>saml2</td>
</tr>
<tr>
<td>??URI defined in ETSI TS 119 102-2?7</td>
<td>Etsivr</td>
</tr>
</tbody>
</table>

The present document will reference components in the aforementioned documents and further profiles some of them.

Unless anything said against it, or in the absence of any further requirement defined in the present document, the requirements defined in the aforementioned documents for the of each element present in this profile, shall apply.

Unless anything said against it, or in the absence of a different processing model defined in the present document, the processing model (including results returned by the server) defined in the aforementioned documents for each element present in this profile, shall apply.

**NOTE:** This document does not specify, for instance, that the presence of a certain optional component in the request message imply the presence of a certain optional component in the response message: this is a requirement inherited from the aforementioned OASIS specifications.

In case that a requirement defined in the present document contradicts any requirement defined in "OASIS Standard: Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0" [1] or "Asynchronous Processing Abstract Profile of the OASIS Digital Signature Service Version 1.0" [2], the requirement defined in the present document shall take precedence.

In case that a certain aspect of the processing model defined in the present document contradicts any aspect of the processing model defined in the aforementioned specifications, the processing model defined in the present document shall take precedence.

The present document also specifies elements that are not specified in the aforementioned documents. For these elements, the present document also defines the processing model that the server shall implement. This processing model is specified below the indication Processing model within each clause that specifies one of these elements.

### 4.3 OASIS DSSX TC JSON related protocol

The structures described in this specification are contained in the schema files [DSS_Core_JSHEMA].

Unless anything said against it, or in the absence of any further requirement defined in the present document, the requirements defined in the aforementioned documents for the of each element present in this profile, shall apply.

Unless anything said against it, or in the absence of a different processing model defined in the present document, the processing model (including results returned by the server) defined in the aforementioned documents for each element present in this profile, shall apply.

**NOTE:** This document does not specify, for instance, that the presence of a certain optional component in the request message imply the presence of a certain optional component in the response message: this is a requirement inherited from the aforementioned OASIS specifications.

In case that a requirement defined in the present document contradicts any requirement defined in "OASIS Standard: Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0" [1] the requirement defined in the present document shall take precedence.

In case that a certain aspect of the processing model defined in the present document contradicts any aspect of the processing model defined in the aforementioned specifications, the processing model defined in the present document shall take precedence.
The present document also specifies elements that are not specified in the aforementioned documents. For these elements, the present document also defines the processing model that the server shall implement. This processing model is specified below the indication Processing model within each clause that specifies one of these elements.

5 Profile(s) for requesting validation of AdES signatures

5.1 Components for requesting validation of AdES signatures

5.1.1 Component for requesting validation

5.1.1.1 Component semantics

The message for requesting the validation of an AdES signature to a remote server shall contain the following components:

1) One component for submitting the signature(s) to be validated. Clause 5.1.2 specifies semantic requirements for this component.

2) One component for submitting the signed document(s) or representation(s) of these signed document(s). Clause 5.1.3 specifies semantic requirements for this component.

NOTE 1: The actual request contains the two different components only when the signature(s) and some or all the signed document(s) are detached. This occurs when the signature to validate is a XadES signature or a CadES detached from some or all the document(s) they sign.

NOTE 2: Under certain circumstances one component is able to carry both the signed document and the signature(s) signing it. When the signature(s) to validate are incorporated into the document, the document and the signature(s) that sign it are present within the second component. This is the case of: a PDF document with one or more PadES signatures, or a XML document with one or more XadES enveloped signatures. When the signature to validate envelops the document, the signature and the document that signs it, are present within the first component. This is the case of a XadES enveloping signature or an attached CadES structure.

3) One component identifying the request as a request that has been built according to the profile specified in the present document. Clause 5.1.4.2 specifies semantic requirements for this component.

NOTE 3: OASIS DSS-X XML and JSON protocols specify XML and JSON elements for this purpose as one of the potential optional inputs. The present document, for keeping the highest possible degree of compatibility, re-uses these elements; consequently this component also appears within the sequence of optional inputs. The first consequence of this fact is that any request built according to the present profile has a non-empty container for optional inputs, and that this container always has the component identifying the profile specified in the present document. The second consequence of this fact is that this component is specified in clause 5.1.4.2.

EDITOR’S NOTE: Indeed making the element for identifying one or several profiles an optional direct child of VerifyRequest would make it clearer, as then all the children of OptionalInputs would certainly be optional. Is it worth to raise this request to DSS-X?

The message for requesting the validation of an AdES signature to a remote server may contain other components for requesting to the server additional features. Clause 5.1.4. lists these optional components and contain references to clauses that specify semantic requirements for each component.

5.1.1.2 OASIS XML related component

The element that shall be the component for requesting the validation of AdES signature(s) shall be the root element of the message VerifyRequest as specified in the present clause.

The VerifyRequest element shall be defined as in XML Schema file "[XSDFILESIGVALPROT]", whose location is detailed in clause A.1, and is copied below for information.

```xml
<!targetNamespace="http://uri.etsi.org/19442/v1.1.1" " -->
EDITOR’S NOTE: VERSION 2.0 OF THE CORE DEFINES A SCHEMA FOR COMPONENT dss:OptionalInputs AS A SEQUENCE OF OPTIONS THAT ARE SPECIFIED IN THAT DOCUMENT. FOR OTHER OPTIONS THAT MAY BE DEFINED IN OTHER PROFILES, IT DEFINES A CONTAINER THAT COULD REQUIRE TO ENCODE THEM IN BASE 64 THEM. AS THE PRESENT PROFILE REQUIRES OPTIONS DEFINED IN OTHER DSS PROFILES, AND THEIR ENCAPSULATION IN BASE 64 WOULD NOT BE EASILY JUSTIFIED, THE PRESENT PROFILE IS FORCED TO DEFINE ITS OWN OptionalInputs COMPONENT, WHICH IMPLIES THE DEFINITION OF ITS OWN VerifyRequest.

The contents inherited from dss:RequestBaseType shall be as specified in [1] clause RE QUESTBASETYPE 3.12.

The dss:SignatureObject child shall not contain a dss:TimeStamp element as child.

The client application may assign a value to attribute RequestID, which shall be used for correlating requests and responses.

The dss:SignatureObject child element shall not contain any time-stamp token.

Any optional component specified in clause 5.1.4 shall appear as child of the <dss:OptionalInputs> child element of dss:VerifyRequest element.

Processing model.

The server shall process the components inherited from dss:RequestBaseType as indicated in the corresponding clauses of OASIS Standard: Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0 [1].

The server shall process each child of OptionalInputs component as indicated in the corresponding clause of the present document if the child is not specified in any of the referenced OASIS documents. Otherwise, the server shall follow the processing model defined in the corresponding OASIS document.

The server shall process the dss:SignatureObject component as indicated in the corresponding clauses of OASIS Standard: Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0 [1].

5.1.1.3 OASIS JSON related component

The element that shall be the component for requesting the validation of AdES signature(s) shall be the root element of the message dss-VerifyRequest as specified in the present clause.

The dss-VerifyRequest element shall be defined as in JSON Schema file "[JSONSCHEMAMFILESIGVALPROT], whose location is detailed in clause A.2, and is copied below for information.

```
"dss-VerifyRequest": {
  "$xsd-type": "VerifyRequest",
  "type": "object",
  "properties": {
    "inDocs": {
      "type": "object",
      "$ref": "<DSSXCORESCHEMFILELOCATION>#/definitions/dss-InputDocumentsType"
    },
    "reqID": {
      "type": "string"
    },
    "optInp": {
      "type": "object",
      "$ref": "#/definitions/OptionalInputsVerifyType"
    }
  }
}
```
The inDocs element shall be an instance of dss-InputDocumentsType as specified in [1] clause (JSON_INPUTDOCUMENTS).

The client application may assign a value to element ReqID, which shall be used for correlating requests and responses.

The optInp element shall be an instance of OptionalInputsVerifyType that shall contain one or more optional inputs elements.

The sigObj element shall be an instance instance of dss-SignatureObjectType as specified in [1] clause (JSON_SIGNATUREOBJECT). It shall not encapsulate a time-stamp token child.

Processing model.

The server shall process the contents of an instance of dss-InputDocumentsType dss:RequestBaseType as indicated in the corresponding clauses of OASIS Standard: Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0 [1].

The server shall process each child of the instance of dss-OptionalInputsVerifyType as indicated in the corresponding clause of the present document if the child is not specified in any of the referenced OASIS documents. Otherwise, the server shall follow the processing model defined in the corresponding OASIS document.

The server shall process the instance of dss-SignatureObjectType as indicated in the corresponding clauses of OASIS Standard: Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0 [1].

5.1.2 Component for submitting signature to be validated

5.1.2.1 Component semantics

The protocol shall allow including the signature in two different containers according to the following rules:

1) If the signature IS ENVELOPED within the signed document, it shall be included in a specific container identified as the container for the signed document.

2) If the signature is NOT enveloped then it shall be included in a specific container identified as the container that encloses the signature.

Table 2 shows the cardinalities of the components required in this profile for incorporating signature(s), for requesting the validation of AdES signatures, depending on its types (CAdES, PAdES or XAdES) and their relative position with respect the signed document(s).

Rows in the table show information corresponding to the different types of AdES signatures whose validation is requested, as well as their relative position to the signed document(s).

Columns in the table show different XML elements, which in the validation request message may appear for incorporating signature(s), signed documents, or representations of the signed documents.
Each cell in the table indicates the required cardinality of the component shown in the header of the corresponding column, for the type of signature, located in a relative position to the signed document(s) as indicated in the header of the corresponding row. An integer value indicates an exact number of components, "*" stands for "0 or more", and "0..1" means "0 or 1".

**Table 2. Placement of signatures.**

<table>
<thead>
<tr>
<th>Type of signature</th>
<th>Component containing the signature (enveloping or detached)</th>
<th>Signed document encapsulating the signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>CadES attached</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>CadES detached</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>XadES only enveloping</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>XadES only envelope</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>XadES only detached</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>XadES enveloped and detached</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>XadES enveloping and detached</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>XadES enveloped and enveloping and detached</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>PadES enveloped within the PDF document</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

5.1.2.2 OASIS XML related components

The element that shall be the component for submitting the signature(s) to be validated shall be either:

a) the `dss:DocumentWithSignature` child element of `dss:OptionalInputs` element when the signature(s) is enveloped within the signed document or

b) the `dss:SignatureObject` child element of `VerifyRequest` root element in the case the signature envelopes the signed document(s).

The requirements governing the presence and cardinalities of the aforementioned elements are given in clause 5.1.3.2.

5.1.2.3 OASIS JSON related component

The element that shall be the component for submitting the signature(s) to be validated shall be either:

a) the `docWithSignature` element specified in clause [DSSXDOCUMENTWITHSIGNATURE_JSON][1], child `optInp` element when the signature(s) is enveloped within the signed or

b) the `sigObj` child element of `dss-VerifyRequest` root element in the case the signature envelopes the signed document(s).

The requirements governing the presence and cardinalities of the aforementioned elements are similar to the ones expressed in clause 5.1.3.2.

5.1.3 Component for submitting signed documents or representations of the signed documents

5.1.3.1 Component semantics

The protocol shall allow including the document in several containers depending on its relative position with regards the signature that signs it, and whether it is the actual document what is submitted to the server, or its digest, or a transformed version of the original message:
1) As it has been stated in clause 5.1.2.1 if the document contains the enveloped signature, then they shall be included in a specific container identified as the container for the signed document.

2) As it has been stated in clause 5.1.2.1 if the signature envelops the document, then they shall be included in a specific container identified as the container that encloses the signature.

3) If the document is detached from the signature, then it shall be included in one of the following containers depending whether the actual document is sent to the server or not:
   - If the actual signed document is sent to the server, then it shall be included in a specific container identified as the container that encloses the detached signed document.
   - If the digest of the actual signed document is sent to the server, then it shall be included in a specific container identified as the container that encloses the digest of the actual detached signed document.
   - If the result of transforming a detached document, being this result what has actually been signed, is sent to the server, then this result shall be included in a specific container identified as the container that encloses the result of transforming a detached document, being this result what has actually been signed.

Table 3 shows the cardinalities of the components required in this profile for incorporating signed documents, or signed documents representations (transformed documents and documents digests) for requesting the validation of AdES signatures, depending on the types of the signatures and their relative position with the signed document(s).

Conventions for indicating cardinalities are as in Table 2.

Table 3. Components for documents in validation requests messages.

<table>
<thead>
<tr>
<th>Type of signature</th>
<th>Component</th>
<th>Signed document encapsulating the signature</th>
<th>Detached signed documents</th>
<th>Detached transformed documents</th>
<th>Digest values</th>
</tr>
</thead>
<tbody>
<tr>
<td>CadES attached</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CadES detached</td>
<td></td>
<td>0</td>
<td>0.1</td>
<td>0</td>
<td>0.1</td>
</tr>
<tr>
<td>XadES only enveloping</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>XadES only enveloped</td>
<td></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>XadES only detached</td>
<td></td>
<td>0</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>XadES enveloped and detached</td>
<td></td>
<td>1</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>XadES enveloping and detached</td>
<td></td>
<td>0</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>XadES enveloped and enveloping and detached</td>
<td></td>
<td>1</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>PadES enveloped within the PDF document</td>
<td></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

5.1.3.2 OASIS XML related component

The element that shall be the component for submitting the signed document(s) or the representation(s) of the signed documents shall be either:

a) the dss:InputDocuments child element (as specified in clause [DSSXINPUTDOCUMENTS_XML]) of [1] of dss:VerifyRequest root element for detached documents from the signature or

b) the dss:SignatureObject (as specified in clause [DSSXSIGNATUREOBJECT_XML]) of [1] child element of dss:VerifyRequest root element for documents contained within an enveloping signature.

c) the dss:DocumentWithSignature (as specified in clause [DSSXDOCUMENTWITHISIGNATURE_XML]) of [1] child element of dss:OptionalInputs element for documents that contain enveloped signature(s).

5.1.3.2.1 Additional requirements for contents of dss:InputDocuments

5.1.3.2.1.1 Element dss:Document for sending original documents

If the signature(s) to be validated is(are) XadES signature(s) then the RefURI attribute shall be present either in all the children of dss:Document element or in all the children of dss:InputDocuments element except one.
5.1.3.2.1.2 Element dss:TransformedData for sending transformed documents

If the signature(s) to be validated is(are) XadES signature(s), and if the client wants to submit to the server not the original document, but the result of the set of transformations applied to it before computing the digest that appears within the ds:DigestManifest child element of the corresponding ds:Reference in the XadES signature, then the client shall incorporate the base-64 encoding of the binary representation of the result of applying the same sequence of transformations to the original document into the dss:Base64Data child element of dss:TransformedData child element of dss:InputDocuments.

The client shall submit one dss:TransformedData element for each result of applying a sequence of transformations to one of the original documents.

The dss:TransformedData element shall incorporate the WhichReference attribute.

5.1.3.2.1.3 Element dss:DocumentHash for sending digest of documents

If the signature(s) to be validated is(are) XadES or CadES signature(s), and if the client wants to submit to the server not the signed document, but the digest of the document, then the client shall incorporate the information corresponding to the digest in one dss:DocumentHash child element of dss:InputDocuments. The client shall incorporate one dss:DocumentHash element for each digest of one of the signed documents.

The client shall incorporate the base-64 encoding of this digest value into the ds:DigestValue child element of the dss:DigestInfo child element of dss:DocumentHash.

The client shall incorporate the algorithm identifier of the digest method into the ds:DigestMethod child element of dss:DigestInfo child element of dss:DocumentHash.

If the signature(s) to be validated is(are) XadES then the dss:DocumentHash element shall incorporate the WhichReference attribute.

If the signature(s) to be validated is(are) CadES then the dss:DocumentHash element shall not incorporate the WhichReference attribute.

5.1.3.3 OASIS JSON related component

The element that shall be the component for submitting the signed document(s) or the representation(s) of the signed documents shall be either:

d) the inDocs child element of dss-VerifyRequest root element for detached documents from the signature, or

e) the sigObj child element, as boolean of dss-VerifyRequest root element for documents contained within an enveloping signature, or

f) the docWithSignature element. This is an instance of DocumentWithSignatureType type, specified in clause [DOCUMENTWITHSIGNATURETYPE_JSON] of [1]. It is a child element of OptInp element. It shall be used only for documents that contain enveloped signature(s).

5.1.3.3.1 Element doc for sending original documents

If the signature(s) to be validated is(are) XadES signature(s) then the refURI child element shall be present either in all the children of inDocs element or in all the children of inDocs element except one.

5.1.3.3.2 Element transformed for sending transformed documents

If the signature(s) to be validated is(are) XadES signature(s), and if the client wants to submit to the server not the original document, but the result of the set of transformations applied to it before computing the digest that appears within the ds:DigestManifest child element of the corresponding ds:Reference in the XadES signature, then the client shall incorporate the base-64 encoding of the binary representation of the result of applying the same sequence of transformations to the original document into the base64Data child element of transformed child element of inDocs.

The client shall submit one transformed element for each result of applying a sequence of transformations to one of the original documents.
The transformed element shall incorporate the whichRef element child.

### 5.1.3.3 Element docHash for sending digest of documents

If the signature(s) to be validated is(are) XadES or CadES signature(s), and if the client wants to submit to the server not the signed document, but the digest of the document, then the client shall incorporate the information corresponding to the digest in one component of the di array child element of docHash child element of inDocs.

The client shall incorporate the base-64 encoding of this digest value into the value child element of the aforementioned component of di array element.

The client shall incorporate the algorithm identifier of the digest method into the alg child element of the aforementioned component of di array element.

If the signature(s) to be validated is(are) XadES then the docHash element shall incorporate the whichRef element.

If the signature(s) to be validated is(are) CadES then the docHash element shall not incorporate the whichRef element.

### 5.1.3.4 Cardinalities for elements used for sending information of documents

**Error! Reference source not found.** Shows the cardinalities of the XML and JSON elements required in this profile for incorporating signature(s), signed documents, signed documents representations (transformed documents and documents digests) for requesting the validation of AdES signatures, depending on the types of the signatures and their relative position with the signed document(s).

Columns in the table show information corresponding to the different types of AdES signatures whose validation is requested, as well as their relative position to the signed document(s).

Rows in the table show different XML and JSON elements, which in the validation request message may appear for incorporating signature(s), signed documents, or representations of the signed documents.

Each cell in the table indicates the required cardinality of the XML and JSON element shown in the header of the corresponding row, for the type of signature, located in a relative position to the signed document(s) as indicated in the header of the corresponding column.

Numbers within round brackets identify additional explanatory notes added after the table.

**EDITOR’S REMARK. THE PRESENT PROFILE DOES NOT ALLOW TO SEND A PADES SIGNATURE EXTRACTED FROM THE PDF THAT IT SIGNS AND SEND ONLY THE DIGEST OF WHAT IS ENCRYPTED BY THE PADES SIGNATURE. THE PROBLEM IS THAT A PADES SIGNATURE MAY NOT BE ONLY THE CMS STRUCTURE THAT APPEARS WITHIN THE Signature PDF DICTIONARY, BUT ALSO THE DSS AND THE VRI DICTIONARY….FOR ALLOWING THIS IT WOULD BE NECESSARY TO SPECIFY A STRUCTURE ABLE TO CONTAIN A SEQUENCE OF PDF DICTIONARIES OR A SEQUENCE FORMED BY A CMS STRUCTURE FOLLOWED BY PDF DICTIONARIES… I DO NOT MEAN THAT THIS IS NOT POSSIBLE...JUST THAT I THINK WE SHOULD THINK ABOUT THIS AND TAKE A FORMAL DECISION BEFORE PROPOSING ANYTHING ON THIS LINE.**
Table 4. Components for signatures and documents in validation requests messages for XML profile based on OASIS specifications.

<table>
<thead>
<tr>
<th>Type of signature and relative position</th>
<th>CadES attached</th>
<th>CadES detached</th>
<th>XadES only enveloping</th>
<th>XadES only detached</th>
<th>XadES enveloping &amp; detached</th>
<th>XadES only enveloped &amp; detached</th>
<th>XadES enveloped &amp; detached &amp; enveloping</th>
<th>PadES</th>
</tr>
</thead>
<tbody>
<tr>
<td>dss:SignatureObject</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>sigObject</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dss:DocumentWithSignature with the PDF document incorporating the signature(s)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>docWithSignature with the PDF document incorporating the signature(s)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dss:Document with the detached signed document</td>
<td>0</td>
<td>0..1</td>
<td>0</td>
<td>*</td>
<td>*</td>
<td>0</td>
<td>*</td>
<td>0</td>
</tr>
<tr>
<td>doc with the detached signed document</td>
<td></td>
<td>(1)</td>
<td>(2)</td>
<td>(2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dss:DocumentHash with the digest value of the detached document</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>*</td>
<td>*</td>
<td>0</td>
<td>*</td>
<td>0</td>
</tr>
<tr>
<td>docHash with the digest value of the detached document</td>
<td></td>
<td></td>
<td></td>
<td>(2)</td>
<td>(2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dss:TransformedData with the detached transformed document</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>*</td>
<td>*</td>
<td>0</td>
<td>*</td>
<td>0</td>
</tr>
<tr>
<td>transformed with the detached transformed document</td>
<td></td>
<td></td>
<td></td>
<td>(2)</td>
<td>(2)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTE 1: If the signature to be validated is(are) CadES signature(s) within a CMS structure, then either the signed document within dss:Document/doc child element of dss:InputDocuments/inDocs or the digest of the signed document within dss:DocumentHash/docHashs child element of dss:InputDocuments/inDocs shall be incorporated.

NOTE 2: If the signature to be validated is(are) XadES signature(s) detached from the documents it(they) signs(sign) then the request may incorporate any number of signed documents within dss:Document/doc children elements of dss:InputDocuments/inDocs or any number of digest of the signed documents within dss:DocumentHash/docHash children elements of dss:InputDocuments/inDocs or any number of results of transforming the signed documents within dss:TransformedData/transformed children elements of dss:InputDocuments/inDocs. If the detached XadES signature(s) only signs(sign) one document, then only one of the three aforementioned children elements shall be incorporated.
5.1.4 Optional components

5.1.4.1 Container for optional components

5.1.4.1.1 Semantics

The validation request message may also contain the following components:

1) One component for identifying the profile used for the request. Clause 5.1.4.2.1 specifies semantic requirements for this component.

2) One component for identifying the service policy under which the validation shall be conducted. Clause 5.1.4.3.1 specifies semantic requirements for this component.

3) One component for claiming the client’s identity. Clause 5.1.4.4.1 specifies semantic requirements for this component.

4) One component for requesting the server to generate notifications using a certain language. Clause 5.1.4.5.1 specifies semantic requirements for this component.

5) One component for requesting to set the validation time to a certain instant different from the current time. Clause 5.1.4.6.1 specifies semantic requirements for this component.

6) One component for requesting the server to return information on the signing time. Clause 5.1.4.7.1 specifies semantic requirements for this component.

7) One component for passing to the server validation material in case this is not present within the signature to be validated. Clause 5.1.4.8.1 specifies semantic requirements for this component.

8) Component for requesting the server to return the identity of the signer(s). Clause 5.1.4.9.1 specifies semantic requirements for this component.

9) Component for requesting validation against a certain signature policy. Clause 5.1.4.10.1 specifies semantic requirements for this component.

10) Component for requesting a detailed validation report. Clause 5.1.4.11.1 specifies semantic requirements for this component.

11) Component for requesting that the server signs the validation report. Clause 5.1.4.12.1 specifies semantic requirements for this component.

12) In the case of requesting validation of XadES signatures, one component requesting to the server to return the result of transforming the signed documents, if any transformation is applied. Clause 5.1.4.13.1 specifies semantic requirements for this component.

13) In the case of requesting validation of XadES signatures, request to return the results of the validation of any signed ds:Manifest present in these signatures. Clause 6.1.1.1 specifies semantic requirements for this component.

14) One component for identifying the request. Clause Error! Reference source not found. Specifies semantic requirements for this component.

15) One component for asynchronous processing of the requests and responses. Clause 5.1.4.16.2.1 specifies semantic requirements for this component.

16) One component for requesting the server to augment the signature to a certain level and return the augmented signature. Clause 5.1.4.14.1 specifies semantic requirements for this component.

5.1.4.1.2 OASIS XML related component

The OptionalInputs child element of VerifyRequest shall be an instance of OptionalInputsVerifyType defined as in XML Schema file "[XSDFILESIGVALPROT]", whose location is detailed in clause A.1, and is copied below for information.
The **dss:OptionalInputs** child element of **VerifyRequest** element shall have at least one **dss:Profile** child element.

The following children elements of instances of **dss:OptionalInputsBaseType** type shall not be used: 
**dss:AddTimeStamp** and **dss:SignatureForm**.

Any other children elements of instances of **dss:OptionalInputsBaseType** type not mentioned and profiled in the present document may be present. Their semantics and syntax shall be as specified in [1].

Children elements **xs:any** are placeholders for optional inputs that are not defined in the present document.

**NOTE:** The optional child element **ReturnAugmentedSignature** is the component for requesting augmenting of the signature.

### 5.1.4.1.3 OASIS JSON related component

The **op1Inp** child element of **dss-VerifyRequest** shall be an instance of **OptionalInputsVerifyType** defined as in JSONSchema file "[JSONSCHEMAFILESIGVALPROT]", whose location is detailed in clause A.2, and is copied below for information.

```json
"OptionalInputsVerifyType": {
  "$xsd-type": "OptionalInputsVerifyType",
  "type": "object",
  "properties": {
    "profiles": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "policy": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "claimedIdentity": {
      "type": "object",
      "$ref": "<DSSXCORESCHEMAFILELOCATION>#/definitions/dss-ClaimedIdentityType"
    },
    "lang": {
      "type": "string"
    },
    "useVerificationTime": {
      "type": "object",
      "$ref": "<DSSXCORESCHEMAFILELOCATION>#/definitions/dss-UseVerificationTimeType"
    }
  }
}
```
"returnVerificationTime": {
  "type": "boolean"
},
"addKeyInfo": {
  "type": "object",
  "$ref": ":<DSSXCORESCHEMAFILELOCATION>#/definitions/dss-AdditionalKeyInfoType"
},
"returnSigner": {
  "type": "boolean"
},
"useSigValPol": {
  "type": "object",
  "$ref": ":#/definitions/SigValPolicyType"
},
"returnValReport": {
  "type": "boolean"
},
"signValReport": {
  "type": "boolean"
},
"returnTransformed": {
  "type": "array",
  "items": {
    "type": "object",
    "$ref": ":<DSSXCORESCHEMAFILELOCATION>#/definitions/dss-ReturnTransformedDocumentType"
  }
},
"retResValManifests": {
  "type": "boolean"
},
"requestID": {
  "type": "string"
},
"retAugmentedSig": {
  "type": "object",
  "$ref": ":#/definitions/RetAugmentedSigType"
}
"required": ["profiles"]

EDITOR’S NOTE: MISSING THE EXTENSION MECHANISM ALLOWING AN ARRAY OF ANY TYPE OF OBJECT WHOSE SCHEMA MAY BE SPECIFIED ELSEWHERE

5.1.4.2 Identifying the profile used for the request

5.1.4.2.1 Semantics

The request shall contain one component whose value shall be an identifier notifying that the request has been built using the profile defined by the present document.

The identifier for the profile defined by the present document shall be:

http://uri.etsi.org/19442/v1.1.1/validationprofile#

The request may contain additional components whose values are identifiers of other profiles that have also been used for building the request.

5.1.4.2.2 OASIS XML related components

The element that shall identify each profile implemented by the request shall be the dss:Profile element specified in clause [OPTIONALINPUTSBASETYPE_XML] of [1] and set to the value defined in clause 5.1.4.2.1 of the present document.

A request shall contain one or more dss:Profile elements. The value of the first one shall be the one specified in clause 5.1.4.2.1 of the present document.

5.1.4.2.3 OASIS JSON related component

The element that shall identify the profiles implemented by the request shall be the profiles element.

The array of strings shall have one or more items. The value of the first item shall be the one specified in clause 5.1.4.2.1 of the present document.
5.1.4.3 Component for identifying under which service policy the validation has to be conducted

5.1.4.3.1 Component semantics
This component shall contain a non-ambiguous identifier of the service policy under which the client requests the server to validate the signature.

5.1.4.3.2 OASIS XML related component
The element that shall identify under which service policy the validation has to be conducted shall be the dss:ServicePolicy element specified in clause [OPTIONALINPUTSBASETYPE_XML] of [1].

NOTE: The service policy is not the same as signature policy. The server defines the service policy, and one server may have different service policies offering different features to its clients.

5.1.4.4 Component for allowing the client to claim for an identity

5.1.4.4.1 Component semantics
This component shall provide the identity of the client as a string-valued name.

This component may include sub-components for supporting names federation.

This component may include one sub-component for identifying the format of the string-valued name representing the identity of the client.

This component may include one sub-component for integrating to the string-valued name representing the identity of the client, a different name identifier that has been established by the validation service itself for the client.

This component may also include one sub-component for incorporating any type of additional supporting information for the string-valued name representing the identity of the client.

5.1.4.4.2 OASIS XML related component
The element that shall allow the client claiming for an identity shall be the dss:ClaimedIdentity element specified in clause [OPTIONALINPUTSBASETYPE_XML] of [1].

JC REMARK: IT IS FORESEEN THAT IN VERSION 2.0 OF THE CORE, THE claimedIdentity is built around saml2:NameID element.

NOTE: The dss:ClaimedIdentity element builds on saml2:NameID element and it incorporates all the XML descendant elements and attributes for matching the semantic requirements in 5.1.4.4.

5.1.4.4.3 OASIS JSON related component
The element that shall allow the client claiming for an identity shall be claimedIdentity, an instance of dss-ClaimedIdentityType. This type is specified in clause [CLAIMEDIDENTITYTYPE_JSON] of [1].

5.1.4.5 Component for requesting notifications in a certain language

5.1.4.5.1 Component semantics
This component shall identify a language by a string-valued identifier, whose value shall be one of the identifiers built and registered as specified in RFC 5646 [13].

5.1.4.5.2 OASIS XML related component
The element that shall request the server to return notifications in a certain language shall be the dss:Language element specified in clause [OPTIONALINPUTSBASETYPE_XML] of [1].
The value of this element shall be string compliant with the values defined in RFC 5646 [13].

5.1.4.5.3 OASIS JSON related component

The element that shall request the server to return notifications in a certain language shall be the `lang` element. The contents of this element shall be as specified in clause [NOTIFICATIONSLANGUAGE_JSON] of [1].

The value of this element shall be string compliant with the values defined in RFC 5646 [13].

5.1.4.6 Component for requesting to set the validation time to a certain instant different from current time

5.1.4.6.1 Component semantics

This component shall provide means for indicating to the server that the validation time is either the current time (the time when the server performs the signature validation) or a certain time in the past.

5.1.4.6.2 OASIS XML related component

The element that shall allow to set the validation time to a certain instant different from current time shall be the `UseVerificationTime` element instance of `dss:UseVerificationTimeType` specified in clause [USEVALIDATIONTIME] of [1].

The value of `dss:SpecificTime` child element shall be expressed as Coordinated Universal Time (UTC): its value shall contain year with four digits, month, day, hour, minute, second (without decimal fraction) and the UTC designator “Z”. The time scale shall be based on the second.

**EDITOR’S REMARK: THIS IS THE TEXT IN TRUSTED LIST CLAUSE 5.1.3 OF 119 612.**

5.1.4.6.3 OASIS JSON related component

The element that shall allow to set the validation time to a certain instant different from current time shall be the `useVerificationTime` element instance of `dss-UseVerificationTimeType`. This type is specified in clause [USEVALIDATIONTIMETYPE_JSON] of [1].

5.1.4.7 Component for requesting to return the validation time

5.1.4.7.1 Component semantics

This component shall provide means for requesting to the server to return within the response an indication of the validation time.

5.1.4.7.2 OASIS XML related component

The element that shall allow to request to the server to return the validation time shall be the `ReturnVerificationTime` element instance of `dss:ReturnVerificationTimeType` specified in clause [RETURNVALIDATIONTIME] of [1]

5.1.4.7.3 OASIS JSON related component

The element that shall allow to set the validation time to a certain instant different from current time shall be the `returnVerificationTime` element. The contents of this element shall be as specified in clause [RETURNVALIDATIONTIMETYPE_JSON] of [1].

5.1.4.8 Component for passing validation material to the server

5.1.4.8.1 Component semantics

This element shall convey any type of validation material that the client decides to pass to the server. Specifically this component shall provide mechanisms for passing to the server X509 certificates, Attribute certificates, CRLs, OCSP responses, or other type of validation data.
5.1.4.8.2 OASIS XML related component

The element that shall allow the client to pass validation material to the server shall be the AdditionalKeyInfo element instance of dss:AdditionalKeyInfoType specified in clause [ADDITIONALKEYINFO 5.5.4] of [1].

TO BE DISCUSSED: not sure about this... high levels of AdES signatures already incorporate validation material. Only low levels may not have such material (AdES-B-B/AdES-BES/AdES-T/AdES-C, for instance). Discuss suitability.

5.1.4.8.3 OASIS JSON related component

The element that shall allow the client to pass validation material to the server shall be the addKeyInfo element, instance of dss:AdditionalKeyInfoType. This type specified in clause [ADDITIONALKEYINFOTYPE_JSON] of [1].

5.1.4.9 Component for requesting the server to return the identity of the signer

5.1.4.9.1 Component semantics

This element shall convey an indication to the server for returning the identity of the signer(s).

5.1.4.9.2 OASIS XML related component

The element that shall request the server to return the identity of the signer shall be the ReturnSignerIdentity element. This element shall have the same contents and requirements as the dss:ReturnSignerIdentity element specified in clause [RETURNSIGNEDIDENTITY 5.5.7] of [1].

5.1.4.9.3 OASIS JSON related component

The element that shall request the server to return the identity of the signer shall be the returnSigner element. The contents of this element shall be as specified in clause [RETURNSIGNEDIDENTITY_JSON] of [1].

5.1.4.10 Component for requesting validation against a certain signature policy

5.1.4.10.1 Component semantics

This component shall provide means for unambiguously identifying the signature validation policy against the client requests to validate the digital signature(s).

This component shall also allow the client indicate locations where the signature validation policy may be downloaded from, in case the client wants to indicate them to the server.

5.1.4.10.2 OASIS XML protocol

The element that shall request the server to validate the signature(s) against a certain signature validation policy shall be the UseSignatureValidationPolicy element.

The UseSignatureValidationPolicy element shall be defined as in XML Schema file "[XSDFILESIGVALPROT]", whose location is detailed in clause A.1, and is copied below for information.

```xml
<xs:complexType name="UseSignatureValidationPolicyType">
  <xs:sequence>
    <xs:element name="SignatureValidationPolicyID" type="xs:anyURI"/>
    <xs:element name="SignaturePolicyLocation" type="xs:anyURI" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
```

The SignatureValidationPolicyID child element shall have as value the unique identifier of the signature validation policy as an URI. If the identifier of the signature validation policy is an OID, then the value of this element shall be an URN indicating the value of the aforementioned OID as specified in RFC 3061 [19].

Every SignatureValidationPolicyLocation child element shall have as value one location where the signature validation policy document can be accessed, as an URI value.
5.1.4.10.3 OASIS JSON protocol

The element that shall request the server to validate the signature(s) against a certain signature validation policy shall be the useSigValPol element.

The useSigValPol element shall be an instance of SigValPolicyType defined as in JSON Schema file "[JSONSCHEMAFILESIGVALPROT], whose location is detailed in clause A.2, and is copied below for information.

```
"SigValPolicyType": {
  "type": "object",
  "properties": {
    "sigValPolID": {
      "type": "string"
    },
    "sigValPolLocs": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  }
}
```

The SigValPolID child element shall have as value the unique identifier of the signature validation policy as an URI. If the identifier of the signature validation policy is an OID, then the value of this element shall be an URN indicating the value of the aforementioned OID as specified in RFC 3061 [19].

Every SigValPolLocs child element shall have as value one location where the signature validation policy document can be accessed, as an URI value.

5.1.4.10.4 Processing model

When UseSignatureValidationPolicy/useSigValPol is present in the request the server shall process this element as follows:

1) If the server is able to validate signatures against this signature validation policy it shall proceed to the validation. Once finalized the validation it shall incorporate into the response to the client the AppliedSignatureValidationPolicy/appliedSigValPolicy specified in clause 5.2.3.6.2/5.2.3.6.3.

   NOTE: The way used by the server to conclude whether it is able to validate signatures against a certain signature validation policy is out of the scope of the present document. Access to the signature validation policy document using SignatureValidationPolicyLocation/sigValPolLocs child elements can help in this process.

2) If the server is not able to validate signatures against this signature validation policy it may decide either:

   - not to proceed to validate the signature. Under these circumstances it:
     - shall incorporate in the response to the client a dss:Result/result element with the dss:ResultMajor/maj set to "urn:oasis:names:tc:dss:1.0:resultmajor:Success", and a dss:ResultMinor/min set to http://uri.etsi.org/19442/v1.1.1/notFeasibleSignatureValidationPolicy, and
     - shall incorporate in the response the AvailableSignatureValidationPolicies/availableSigValPols child element as specified in clause 5.2.3.7.2/5.2.3.7.3. The server may include in this element a list of the identifiers of the signature validation policies against which it is able to validate digital signatures.

   - Proceed to validate the signature against a different signature policy. In this case the server shall incorporate in the response the AppliedSignatureValidationPolicy/appliedSigValPol element identifying the signature policy used by the server for validating the signature.
5.1.4.11 Component for requesting a detailed validation report (as the one to be specified in TS 119 102-2)

5.1.4.11.1 Component semantics

This component shall provide means for requesting to the server the generation and return of a detailed validation report. If these mechanisms are used within this component, then the component specified in clause 5.1.4.9 should not be present. If the component specified in clause 5.1.4.9 is present within the request, then these mechanisms should not be used in the component being specified in the present clause.

This component shall provide means for requesting to the server to convey in the detailed validation report the binary values, base 64-encoded, of the X509 certificates, and Attribute certificates, verified during the signature validation.

This component shall provide means for requesting to the server to convey in the detailed validation report the binary values, base 64-encoded, of the revocation values (CRLs, OCSP responses or other), used during the signature validation.

This component shall provide mechanisms for requesting to the server to convey in the detailed validation report textual relevant information on the validation material used during the signature validation.

This component shall provide mechanisms for identifying one level of details among a set of possible different levels of details for the validation report.

5.1.4.11.2 OASIS XML protocol

The element that shall request the server to return a detailed validation report on each signature validated shall be the \texttt{dssvalrep:ReturnVerificationReport} element specified in clause \cite{COMPREHENSIVEVALIDATIONREPORT} of Error! Reference source not found..

5.1.4.11.3 OASIS JSON protocol

The element that shall request the server to return a detailed validation report shall be the \texttt{returnValReport} element set to value \texttt{"true"}.

The server shall interpret the absence of this element or its presence set to value \texttt{"false"} as absence of this request.

5.1.4.12 Component for requesting that the validation report is signed by the server a detailed validation report (as the one to be specified in TS 119 102-2)

5.1.4.12.1 Component semantics

The presence of this element shall indicate that the client is requesting that the server signs the validation report generated after validating the signature(s) in the validation request.

Absence of this element shall indicate that the client requests no signature of the validation report.

5.1.4.12.2 OASIS XML protocol

The element that shall request the server to sign the detailed validation report shall be the \texttt{SignVerificationReport}.

The \texttt{SignVerificationReport} element shall be defined as in XML Schema file \texttt{"[XSDFILESIGVALPROT]"}, whose location is detailed in clause A.1, and is copied below for information.

\begin{verbatim}
<!targetNamespace="http://uri.etsi.org/19442/v1.1.1#" ->
  <xs:element minOccurs="0" name="SignVerificationReport"/>
\end{verbatim}

5.1.4.12.3 OASIS JSON protocol

The element that shall request the server to return a detailed validation report shall be the \texttt{signValReport} element set to value \texttt{"true"}.

The server shall interpret the absence of this element or its presence set to value \texttt{"false"} as absence of this request.
5.1.4.13 Component for requesting the server to return the result of transforming the
input document
The server shall interpret the absence of this element or its presence set to value "false" as absence of this request.

5.1.4.13.1 Component semantics
This component shall not be present when requesting validation of CadES or PadES signatures.
This component shall provide means for identifying one or more signed documents whose transformed versions the
client requests that the server incorporates into the validation response.
The server shall interpret the absence of this element or its presence set to value "false" as absence of this request.

5.1.4.13.2 OASIS XML protocol
The element that shall request the server to return the result of transforming one input document shall be the
ReturnTransformedDocument element instance of dss-ReturnTransformedDocumentType specified in clause
[RETURNTRANSFORMEDDOCUMENT 5.5.9] of [1].
The server shall interpret the absence of this element or its presence set to value "false" as absence of this request.

5.1.4.13.3 OASIS JSON related component
The element that shall request the server to return the result of transforming one input document shall be the
returnTransformed element, instance of dss-ReturnTransformedDocumentType. This type is specified in
clause [RETURNTRANSFORMEDDOCUMENTTYPE_JSON 3.1.45.2] of [1].

5.1.4.14 Component for requesting to return the validation of signed ds:Manifest in
Xades signatures

5.1.4.14.1 Component semantics
This component shall not be present when requesting validation of CadES or PadES signatures.
This component shall notify that the client requests that the server verifies all the ds:Manifest elements present
within the Xades signature.

5.1.4.14.2 OASIS XML protocol
The element that shall request the server to return the result of transforming one input document shall be the
dss:VerifyManifests element specified in clause [VERIFYMANIFESTS 5.5.1.1] of [1].

5.1.4.14.3 OASIS JSON protocol
The element that shall request the server to return the result of transforming one input document shall be
retResValManifests, set to value "true".
The server shall interpret the absence of this element or its presence set to value "false" as absence of this request.

5.1.4.15 Component for identifying a request

5.1.4.15.1 Component semantics
This component shall assign an identifier to the request. It allows correlating a certain response with the request with
this identifier.

5.1.4.15.2 OASIS XML protocol
The element that shall request the server to return the result of transforming one input document shall be the
RequestID attribute specified in clause [REQUESTBASETYPE 3.1.21.1] of [1].

5.1.4.15.3 OASIS JSON protocol
The element that shall identify the request shall be requestID, whose value shall be a string.
5.1.4.16  Component for asynchronous processing

5.1.4.16.1  Asynchronous processing protocol

In asynchronous processing one client usually sends an initial request to the server.

The initial request shall contain, among other things, a request identifier generated by the client, as specified in clause 5.1.4.15.

The server can return a response indicating that the validation has not yet been finished. Within this initial response, the server shall convey a response identifier, as specified in clause 5.2.3.12. Both client and server can correlate the response identifier to the request identifier.

Under this processing mode the client, after a certain time, can send a pending-request to the server. This pending-request shall include the response identifier previously returned by the server. This response identifier allows the server to correlate this pending-request to the initial request, and can return the validation result or return again an indication of “not yet finished”.

If this is the case, the client can send subsequent requests until the server returns a response with the validation result. Each subsequent request shall include the response identifier returned by the server in the response to the initial request.

For managing asynchronous processing, the following components are required:

a) One component for the identifying a request as a pending-request associated to an initial request. This component is specified in clause 5.1.4.16.2.

b) One component that allows correlating the subsequent requests with the response to the initial requests, which included a notification of “not yet finished”. This component is specified in clause 3.1.1 of "Asynchronous Processing Abstract Profile of the OASIS Digital Signature Service Version 1.0" [2]/5.1.4.16.2.3.

5.1.4.16.2  Component for identifying a request as a subsequent request to an initial request

5.1.4.16.2.1  Semantics

This component shall be a request that shall notify to the server to return the response corresponding to a previously sent initial request to the server. Requests of this type are named pending-request hereinafter.

This component shall include an identifier, generated by the server and returned by the server in the response to the initial request, which shall allow correlating the subsequent requests to the initial request and to the subsequent responses.

5.1.4.16.2.2  OASIS XML related protocol

The element that shall indicate to the server that the client is requesting the response corresponding to a previously sent initial request (as part of an asynchronous protocol) shall be the dssasyn:PendingRequest element specified in [PENDINGREQUEST 3.1].

The OASIS XML related asynchronous protocol shall satisfy the requirements specified in [PROFILEOFVERIFYINGPROTOCOL 5] of [2].

5.1.4.16.2.3  OASIS JSON related protocol

The element that shall indicate to the server that the client is requesting the response corresponding to a previously sent initial request (as part of an asynchronous protocol) shall be the PendingRequest element.

The PendingRequest element shall be defined as in JSON Schema file "[JSONSCHEMAMFILESIGVALPROT], whose location is detailed in clause A.2, and is copied below for information.

```
"PendingRequest":{
  "type": "object",
  "properties": {
    "inDocs": {
      "type": "object",
      "$ref": "<<DSSXCORESCHEMAFILELOCATION>#/definitions/dss-InputDocumentsType"
    },
    "reqID": {
      "type": "string"
    },
  }
}
```
Components in Docs, optInp, and sigObj, shall have the same semantics and syntaxes as the components of dss-VerifyRequest with the same names.

5.2 Components for response to validation request

EDITOR’S NOTE: TO BE DISCUSSED: IF A TRANSFORMEDDATA OR DOCUMENTHASH IS PASSED, THERE IS A COMMENT REQUESTING THAT THE VALIDATION REPORT INDICATES THIS FACT.

TWO QUESTIONS:

1. FOR XAdES SIGNATURES THERE COULD BE SEVERAL ELEMENTS OF THEM, AND REPRESENTING DOCUMENTS SIGNED BY DIFFERENT SIGNATURES, THERE SHOULD BE ONE NOTIFICATION PER EACH OF THE AFOREMENTIONED ELEMENTS? Ideally one notification per each would be great. If too tricky at least a “global” notification to mention that “at least one signature” is checked on the hash only.


5.2.1 Component for responding to validation request

5.2.1.1 Component semantics

The validation response message resulting from one request of validation of AdES signature(s), shall contain one component for notifying the validation result.

The validation response message resulting from one request of validation of AdES signature(s), shall contain one component indicating that the response has been built using the profile specified in the present document.

NOTE 3: OASIS DSS-X XML and JSON protocols specify XML and JSON elements for this purpose as one of the potential optional inputs. The present document, for keeping the highest possible degree of compatibility, re-uses these elements; consequently this component also appears within the sequence of optional inputs. The first consequence of this fact is that any response built according to the present profile has a non-empty container for optional inputs, and that this container always has the component identifying the profile specified in the present document. The second consequence of this fact is that this component is specified in clause 5.2.3.2.

EDITOR’S NOTE: Indeed making the element for identifying one or several profiles an optional direct child of VerifyResponse would make it clearer, as then all the children of OptionalOutputs would certainly be optional. Is it worth to raise this request to DSS-X?

The validation response message may contain other components. Clause 5.2.3.1 lists these optional components and contain references to clauses that specify requirements for each component.

5.2.1.2 OASIS XML related component

The element that shall be the component for responding to the validation request of AdES signature(s) shall be the root element of the message VerifyResponse as specified in the present clause.

The VerifyResponse element shall be defined as in XML Schema file "[XSDFILESIGVALPROT]", whose location is detailed in clause A.1, and is copied below for information.

```xml
<!targetNamespace="http://uri.etsi.org/19442/v1.1.1#" ->

<xs:element name="VerifyResponse" type="VerifyResponseType"/>
```
5.2.1.3 OASIS JSON related component

The element that shall be the component for responding to the validation request of AdES signature(s) shall be the root element of the message dss-VerifyResponse as specified in the present clause.

The dss-VerifyResponse element shall be defined as in JSON Schema file "[JSONSCHEMAFILESIGVALPROT], whose location is detailed in clause A.2, and is copied below for information.

```
"dss-VerifyResponse": { 
  "$xsd-type": "VerifyResponse",
  "type": "object",
  "properties": { 
    "result": { 
      "type": "object",
      "$ref": "+DSSCORESCHEMAFILELOCATION>#/definitions/dss-ResultType"
    },
    "reqID": { 
      "type": "string"
    },
    "optOutp": { 
      "type": "object",
      "$ref": "+/definitions/OptionalOutputsVerifyType"
    }
  } 
  "required": ["result","optOutp"]
}
```

5.2.2 Component for notifying the validation result

5.2.2.1 Component semantics

This component shall contain a result major child component indicating whether the server could proceed to perform the validation of the signature(s) (regardless of the result that this validation has thrown) or not.

This component may contain an additional minor result child component indicating the result of the validation of the signature(s) present in the request.

If the request corresponding to the response that encloses this component included a component requesting a detailed validation report, the minor result child component shall not be present.

5.2.2.2 OASIS XML related component

The element that within the response shall notify the validation result shall be the dss:Result element specified in clause [RESULT 3.1.12.1] of [1].

If the request corresponding to the response that encloses this element included the component dssvalrep:ReturnVerificationReport and the value of its dss:ResultMajor child is urn:oasis:names:tc:dss:1.0:resultmajor:Success then the dss:Result shall not contain the dss:ResultMinor.

NOTE: The dss:ResultMinor is not necessary under these circumstances because the details of the validation result will appear in the detailed verification report optional component requested by the client.

5.2.2.3 OASIS JSON related component

The element that within the response shall notify the validation result shall be an instance of the ResultType type specified in clause [RESULT_JSON 3.1.12.2] of [1].
If the request corresponding to the response that encloses this element included the component returnValReport and the value of its maj child is urn:oasis:names:tc:dss:1.0:resultmajor:Success then the result shall not contain the min.

NOTE: The min is not necessary under these circumstances because the details of the validation result will appear in the detailed verification report optional component requested by the client.

5.2.3 Optional components

5.2.3.1 Container for optional components

5.2.3.1.1 Semantics

The validation response message may also contain the following components:

1) One component for identifying the service policy under which the validation was conducted. Clause 5.2.3.3 specifies requirements for this component.

2) One component for indicating the time when the validation was conducted (validation time). Clause 5.2.3.4 specifies requirements for this component.

3) One component for indicating the identity of the signer(s). Clause 5.2.3.5 specifies requirements for this component.

4) One component for notifying the signature policy applied during the validation. Clause 5.2.3.6 specifies requirements for this component.

5) One component for notifying the set of signature policies supported by the server. Clause 5.2.3.7 specifies requirements for this component.

6) One component for returning the detailed validation report. Clause 5.2.3.8 specifies requirements for this component.

7) One component for returned the detailed validation report signed by the validation server. Clause 5.2.3.9 specifies requirements for this component.

8) One component for returning the result of transforming the input document. Clause 5.2.3.10 specifies requirements for this component.

9) One component for returning the results of validating any signed ds:Manifest present in the signature(s). Clause 5.2.3.11 specifies requirements for this component.

10) One component for supporting asynchronous processing of the response messages. Clause 5.2.3.12 specifies requirements for this component. Clause 6.2.1 specifies requirements for this component.

11) One component for returning the augmented signature. This component shall be used in the protocol for validation and augmentation of digital signatures. Clause 6.2.3.3 specifies requirements for this component.

5.2.3.1.2 OASIS XML related component

The OptionalOutputs child element of VerifyResponse shall be an instance of OptionalOutputsVerifyType defined as in XML Schema file "[XSDFILESIGVALPROT]", whose location is detailed in clause A.1, and is copied below for information.

```xml
<xs:complexType name="OptionalOutputsVerifyType">
  <xs:complexContent>
    <xs:extension base="dss:OptionalOutputsBaseType">
      <xs:sequence>
        <xs:element ref="dss:VerifyManifestResults" minOccurs="0" maxOccurs="1"/>
        <xs:element ref="dss:SigningTimeInfo" minOccurs="0" maxOccurs="1"/>
        <xs:element ref="dss:VerificationTimeInfo" minOccurs="0" maxOccurs="1"/>
        <xs:element ref="dss:SignerIdentity" minOccurs="0" maxOccurs="1"/>
        <xs:element ref="AvailableSignatureValidationPolicies" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element ref="dss:UpdatedSignature" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```
The `dss:OptionalOutputs` child element of `VerifyResponse` element shall have at least one `dss:Profile` child element.

Any children element of instances of `dss:OptionalOutputsBaseType` type not mentioned and profiled in the present document may be present. Their semantics and syntax shall be as specified in [1].

Children elements `xs:any` are placeholders for optional outputs that are not defined in the present document.

### 5.2.3.1.3 OASIS JSON related component

The `op1Outp` child element of `dss-VerifyRequest` shall be an instance of `OptionalOutputsVerifyType` defined as in JSONSchema file `"[JSONSCHEMASEFILESIGVALPROT]"`, whose location is detailed in clause A.2, and is copied below for information.

```json
"OptionalOutputsVerifyType": {
  "type": "object",
  "properties": {
    "profiles": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "policy": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "verificationTimeInfo": {
      "type": "object",
      "$ref": "<DSSXCORESCHEMAFILELOCATION>#/definitions/dss-VerificationTimeInfoType"
    },
    "signerIdentity": {
      "type": "object",
      "$ref": "<DSSXCORESCHEMAFILELOCATION>#/definitions/saml2-NameIDType"
    },
    "appliedSigValPolicy": {
      "type": "string"
    },
    "availableSigValPols": {
      "type": "array",
      "items": {
        "type": "object",
        "$ref": "#/definitions/SigValPolicyType"
      }
    },
    "detailedValReports": {
      "type": "array",
      "items": {
        "type": "object",
        "$ref": "<ETSIJSONVALREPORTSCHEMAFILELOCATION>#/definitions/detailedValReport"
      }
    },
    "sigDetailedValReports": {
      "type": "array",
      "items": {
        "type": "object",
        "$ref": "<RFC7515JSONSCHEMAFILE>#/definitions/JWS"
      }
    },
    "transformed": {
      "type": "array",
      "items": {
        "type": "object",
        "$ref": "<DSSXCORESCHEMAFILELOCATION>#/definitions/dss-TransformedDocumentType"
      }
    }
  }
}
```
5.2.3.2 Identifying the profile used

5.2.3.2.1 Semantics

The response shall contain one component whose value shall be an identifier notifying that the response has been built using the profile defined by the present document.

The identifier for the profile defined by the present document shall be the value defined in clause 5.1.4.2.1 of the present document.

The response may contain additional components whose values are identifiers of other profiles that have also been used for building the response.

5.2.3.2.2 OASIS XML related components

The response shall have one or more `dss:AppliedProfile` elements. `dss:AppliedProfile` element is specified in clause [DSSXOPTIONALOUTPUTBASETYPE] of [1]. The value of each `dss:AppliedProfile` element shall be the identifier of one profile.

The value of the first `dss:AppliedProfile` child element in the response shall be the one specified in clause 5.1.4.2.1 of the present document.

5.2.3.2.3 OASIS JSON related component

The element that shall indicate the profiles used for building the response shall be the `profiles` element.

The array of strings shall have at least one item. The value of the first item shall be the one specified in clause 5.1.4.2.1 of the present document.

5.2.3.3 Component for indicating the service policy

5.2.3.3.1 Component semantics

This component shall contain a non-ambiguous identifier of the service policy under which the client requests the server to validate the signature.

5.2.3.3.2 OASIS XML related component

The element that shall identify under which service policy the validation has to be conducted shall be the `dss:AppliedPolicy` element specified in clause [OPTIONALOUTPUTBASETYPE_XML] of [1].
5.2.3.3 OASIS JSON related component

The element that shall identify under which service policy the validation has to be conducted shall be the policy element. The contents of this element shall be as specified in clause [OPTIONALOUTPUTSBASETYPE_JSON] of [1].

5.2.3.4 Component for indicating validation time

5.2.3.4.1 Component semantics

This component shall provide means for indicating to the client the validation time set by the server, which may be the current time or a certain time in the past.

This component shall appear only in the response to requests of validation of XadES signatures that incorporate the component requesting the server to set the validation time at a certain time instant, specified in clause 5.1.4.6.1 of the present document.

5.2.3.4.2 OASIS XML related component

The element that shall report the validation time used by the server shall be the dss:VerificationTimeInfo element specified in clause [VALIDATIONTIME_INRESP] of [1].

5.2.3.4.3 OASIS JSON related component

The element that shall report the validation time used by the server shall be the verificationTimeInfo an instance of dss-VerificationTimeInfoType type specified in clause [VALIDATIONTIME_INRESP_JSON] of [1].

5.2.3.5 Component for returning signer's identity

5.2.3.5.1 Component semantics

This component of a response to a validation request shall return information on the signer’s identity.

This component shall appear only in the response to requests that incorporate the component requesting the server to return these details, specified in clause 5.1.4.9.1 of the present document.

5.2.3.5.2 OASIS XML protocol

The element that shall contain the identity of the signer shall be the dss:SignerIdentity element, specified in clause [DSSSIGNERIDENTITY_INRESP] of [1].

5.2.3.5.3 OASIS JSON protocol

The element that shall contain the identity of the signer shall be the signerIdentity element, whose contents shall be as specified in clause [DSSXSIGNERIDENTITY_INRESP] of [1].

5.2.3.6 Component for notifying the signature policy applied during the validation

5.2.3.6.1 Component semantics

This component shall provide means for returning to the client the identifier of the signature validation policy applied by the server for validating the signature(s).

This component shall appear in the response to requests of validation of digital signatures that incorporate the component requesting the server to validate the signature(s) using a certain signature validation policy, specified in clause 5.1.4.10.1 of the present document. It may also appear in responses to requests that do not incorporate the aforementioned component.

5.2.3.6.2 OASIS XML protocol

The element that shall notify to the client the signature validation policy against which the signature has been validated shall be the AppliedSignatureValidationPolicy element.

The AppliedSignatureValidationPolicy element shall be defined as in XML Schema file 
"[XSDFILESIGVALPROT]", whose location is detailed in clause A.1, and is copied below for information.
The `SignatureValidationPolicyID` child element shall have as value the unique identifier of the signature validation policy used by the server for validating the signature as an URI. If the identifier of the signature validation policy is an OID, then the value of this element shall be an URN indicating the value of the aforementioned OID as specified in RFC 3061 [19].

### 5.2.3.6.3 OASIS JSON protocol

The element that shall notify to the client the signature validation policy against which the signature has been validated shall be the `appliedSigValPol`.

The value of this element shall be the unique identifier of the signature validation policy used by the server for validating the signature as an URI. If the identifier of the signature validation policy is an OID, then the value of this element shall be an URN indicating the value of the aforementioned OID as specified in RFC 3061 [19].

### 5.2.3.7 Component for notifying the signature policies under which the server can conduct validation

#### 5.2.3.7.1 Component semantics

This component shall provide means for returning to the client the identifiers of the signature validation policies under which the server can validate signatures.

This component shall appear only in the response to requests of validation of digital signatures that incorporate the component requesting the server to validate the signature(s) using a certain signature validation policy, specified in clause 5.1.4.10.1 of the present document.

This component shall only appear if the server is not able to validate the signature under the signature validation policy requested by the client in the aforementioned component of the validation request.

#### 5.2.3.7.2 OASIS XML protocol

The element that shall notify to the client the signature validation policies under which the server can conduct validation of digital signatures shall be the `AvailableSignatureValidationPolicies` element.

The `AvailableSignatureValidationPolicies` element shall be defined as in XML Schema file "[XSDFILESIGVALPROT]", whose location is detailed in clause A.1, and is copied below for information.

```xml
<!-targetNamespace="http://uri.etsi.org/19442/v1.1.1#" ->
<xs:element name="AvailableSignatureValidationPolicies" type="AvailableSignatureValidationPoliciesType"/>
<xs:complexType name="AvailableSignatureValidationPoliciesType">
  <xs:sequence>
    <xs:element name="AvailableSignatureValidationPolicyID" type="xs:anyURI" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
```

Each `AvailableSignatureValidationPolicyID` child element shall have as value the unique identifier of one signature validation policy against which the server is able to validate digital signatures, as an URI. If the identifier of the signature validation policy is an OID, then the value of this element shall be an URN indicating the value of the aforementioned OID as specified in RFC 3061 [19].

#### 5.2.3.7.3 OASIS JSON protocol

In the JSON profile derived from OASIS specifications the element that shall notify to the client the signature validation policies under which the server can conduct validation of digital signatures shall be the `availableSigValPol` element.
Each item of the array shall have as value the unique identifier of one signature validation policy against which the server is able to validate digital signatures, as an URI. If the identifier of the signature validation policy is an OID, then the value of this element shall be an URN indicating the value of the aforementioned OID as specified in RFC 3061 [19].

5.2.3.8 Component for returning the detailed validation report

5.2.3.8.1 Component semantics

This component shall contain the detailed validation report for each digital signature that the server has validated in response to one request.

5.2.3.8.1.1 ETSI XML protocol

The element that shall contain the detailed validation report for one digital signature shall be the IndividualReport, which is an instance of etsivr:IndividualReportType, as specified in [12].

5.2.3.8.1.2 ETSI JSON protocol

The element that shall contain the detailed validation report for all the digital signatures shall be the detailedValReports. This element is an array of items. Each item shall contain an instance of <ETSITA110102-2_JSON>, as specified in [12].

5.2.3.9 Component for returned the detailed validation report signed

5.2.3.9.1 Component semantics

This component shall provide means for returning a signature within the validation report.

This component shall appear only in the response to requests of validation of XadES signatures that incorporate the component requesting the server to sign the detailed validation report, specified in clause 5.1.4.12.1 of the present document.

5.2.3.9.2 OASIS XML protocol

The element that shall return the signature over the validation report shall be a ds:Signature element generated by the server.

This ds:Signature element shall be enveloped within the IndividualReport element, which shall be an instance of etsivr:IndividualReportType, as specified in [12].

5.2.3.9.3 OASIS JSON protocol

The element that shall return the signature over the validation report shall be sigDetailedValReports. This element is an array of items.

Each item shall contain an instance of a JSON Web Signature (JWS signature hereinafter) as specified in [14].

Each JWS shall envelop one individual validation report, generated by the server, which shall be an instance of <ETSITA110102-2_JSON>, as specified in [12].

5.2.3.10 Component for returning the result of transforming the input document

5.2.3.10.1 Component semantics

This component shall provide means for returning to the client the result obtained by the server after applying a sequence of transformations to one input document.

This component shall appear only in the response to requests of validation of XadES signatures that incorporate the component requesting the server to return one or more transformed input documents, specified in clause 5.1.4.13 of the present document.
5.2.3.10.2 OASIS XML related component

In the JSON profile derived from OASIS specifications the element transformed element shall be an array. Each item of the array shall contain the results obtained by the server after applying a sequence of transformations to one input document. Each item of the array shall be an instance of the the dss-TransformedDocumentType element specified in clause [DSSXTRANSFORMEDDOCUMENT_INRESP 3.1.46.1] of [1].

5.2.3.10.3 OASIS JSON related component

The element that shall return the result obtained by the server after applying a sequence of transformations to one input document shall be an instance of dss-TransformedDocumentType type specified in clause [DSSTRANSFORMEDDOCUMENT_INRESP_JSON 3.1.46.2] of [1].

5.2.3.11 Component for returning the result of validating ds:Manifest elements in XadES signatures

5.2.3.11.1 Component semantics

This component shall not be present within a response to a request of validation of CadES or PadES signatures. This component shall contain the result of the validation(s) performed by the server on signed the ds:Manifest elements present within the XadES signature(s).

5.2.3.11.2 OASIS XML protocol

The element that shall contain the result of the validation(s) performed by the server on signed the ds:Manifest elements present within the XadES signature(s) shall be the dss:VerifyManifestResults element, specified in clause [VERIFYMANIFESTRESULTS_INRESP 5.5.1.1] of [1].

5.2.3.11.3 OASIS JSON protocol

The element that shall contain the result of the validation(s) performed by the server on signed the ds:Manifest elements present within the XadES signature(s) shall be the manifestValResult element. This element shall be an instance of dss-VerifyManifestResultsType type specified in clause [VERIFYMANIFESTRESULTS_INRESP_JSON 5.5.1.2] of [1].

5.2.3.12 Components for asynchronous processing

5.2.3.12.1 Introduction

For managing asynchronous processing protocol detailed in clause 5.1.4.16.1, the components specified in clauses 5.2.3.12.2 and 5.2.3.12.3 are required:

5.2.3.12.2 Component for indicating not completion of signature(s) validation

5.2.3.12.2.1 Semantics

This component of a response to a validation request shall indicate that the server has not completed the validation of the signature(s) and that consequently the completion of the validation is pending.

5.2.3.12.2.2 OASIS XML protocol

The element that shall indicate that the completion of the validation of the signature(s) is pending shall be shall be the dss:ResultMajor child element of VerifyResponse set to the value "urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending", as specified in clause [VALIDATIONPENDING_INRESP 5.2.1] of [2].

5.2.3.12.2.3 OASIS JSON protocol

The element that shall indicate that the completion of the validation of the signature(s) is pending shall be shall be the maj child element of result child of dss-VerifyResponse set to the value "urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending", as specified in clause [VALIDATIONPENDING_INRESP_JSON 5.2.1] of [2].
5.2.3.12.3 Component for correlating subsequent requests to the initial response

5.2.3.12.3.1 Semantics

This component of a response to a validation request shall contain an identifier for correlating subsequent pending requests associated to a certain initial request.

5.2.3.12.3.2 OASIS XML protocol

The element that shall contain an identifier for correlating subsequent pending requests associated to a certain initial request shall be the `dssasync:ResponseID` as specified in clause [ASYNCORRELATINGID_INRESP 5.2.2] of [2].

5.2.3.12.3.3 OASIS JSON protocol

The element that shall contain an identifier for correlating subsequent pending requests associated to a certain initial request shall be the `respID` whose value shall be as specified in clause [ASYNCORRELATINGID_INRESP 5.2.2] of [2].

6 Profiles for validation and augmentation of signatures.

6.1 Components for requesting validation and augmentation

6.1.1 Component for requesting validation and augmentation of the signature to a certain level

6.1.1.1 Component semantics

This component shall include a URI reference identifying the pre-defined level to which the server is requested to augment the signature after its validation.

Table 5 lists the URIs for the levels specified for AdES signatures in ETSI EN 319 122, ETSI EN 319 132, and ETSI EN 319 142. Numbers in column Notes correspond to the numbers of the notes that follow the table.

<table>
<thead>
<tr>
<th>Signature level</th>
<th>URI</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdES-B-B</td>
<td><a href="http://www.etsi.org/ades/191x2/level/baseline/B-B#">http://www.etsi.org/ades/191x2/level/baseline/B-B#</a></td>
<td>1</td>
</tr>
<tr>
<td>AdES-B-T</td>
<td><a href="http://www.etsi.org/ades/191x2/level/baseline/B-T#">http://www.etsi.org/ades/191x2/level/baseline/B-T#</a></td>
<td>1</td>
</tr>
<tr>
<td>AdES-B-LT</td>
<td><a href="http://www.etsi.org/ades/191x2/level/baseline/B-LT#">http://www.etsi.org/ades/191x2/level/baseline/B-LT#</a></td>
<td>1</td>
</tr>
<tr>
<td>AdES-B-LTA</td>
<td><a href="http://www.etsi.org/ades/191x2/level/baseline/B-LTAA#">http://www.etsi.org/ades/191x2/level/baseline/B-LTAA#</a></td>
<td>1</td>
</tr>
<tr>
<td>AdES-E-BES</td>
<td><a href="http://www.etsi.org/ades/191x2/level/extended/B-BES#">http://www.etsi.org/ades/191x2/level/extended/B-BES#</a></td>
<td>1</td>
</tr>
<tr>
<td>AdES-E-EPES</td>
<td><a href="http://www.etsi.org/ades/191x2/level/extended/E-EPES#">http://www.etsi.org/ades/191x2/level/extended/E-EPES#</a></td>
<td>1</td>
</tr>
<tr>
<td>AdES-E-T</td>
<td><a href="http://www.etsi.org/ades/191x2/level/extended/E-T#">http://www.etsi.org/ades/191x2/level/extended/E-T#</a></td>
<td>1</td>
</tr>
<tr>
<td>AdES-E-C</td>
<td><a href="http://www.etsi.org/ades/191x2/level/extended/E-C#">http://www.etsi.org/ades/191x2/level/extended/E-C#</a></td>
<td>2</td>
</tr>
<tr>
<td>AdES-E-X</td>
<td><a href="http://www.etsi.org/ades/191x2/level/extended/E-X#">http://www.etsi.org/ades/191x2/level/extended/E-X#</a></td>
<td>2</td>
</tr>
<tr>
<td>AdES-E-XL</td>
<td><a href="http://www.etsi.org/ades/191x2/level/extended/E-X-L#">http://www.etsi.org/ades/191x2/level/extended/E-X-L#</a></td>
<td>2</td>
</tr>
<tr>
<td>AdES-E-A</td>
<td><a href="http://www.etsi.org/ades/191x2/level/extended/E-A#">http://www.etsi.org/ades/191x2/level/extended/E-A#</a></td>
<td>2</td>
</tr>
<tr>
<td>AdES-E-LTV</td>
<td><a href="http://www.etsi.org/ades/191x2/level/extended/E-LTV#">http://www.etsi.org/ades/191x2/level/extended/E-LTV#</a></td>
<td>3</td>
</tr>
</tbody>
</table>

NOTE 1: The levels identified in these rows are levels that CadES, PadES, and XadES signatures can reach.

NOTE 2: The levels identified in these rows are levels that CadES and XadES signatures can reach, but not PadES signatures.

NOTE 2: The levels identified in these rows are levels that only PadES signatures can reach.

Table 6 lists the URIs for the levels specified for AdES signatures in the different ETSI TSs, namely ETSI TS 101 733, ETSI TS 102 778, ETSI TS 101 903, ETSI TS 103 171, ETSI TS 103 172, and ETSI TS 103 173. Numbers in column Notes correspond to the numbers of the notes that follow the table.
Table 6: AdES signature levels in ETSI EN 319 1X2 and URIs

<table>
<thead>
<tr>
<th>Signature level</th>
<th>URI</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdES-B</td>
<td><a href="http://www.etsi.org/ades/etsits/level/baseline/B-B#">http://www.etsi.org/ades/etsits/level/baseline/B-B#</a></td>
<td>3</td>
</tr>
<tr>
<td>AdES-T</td>
<td><a href="http://www.etsi.org/ades/etsits/level/baseline/B-T#">http://www.etsi.org/ades/etsits/level/baseline/B-T#</a></td>
<td>3</td>
</tr>
<tr>
<td>AdES-LT</td>
<td><a href="http://www.etsi.org/ades/etsits/level/baseline/B-LT#">http://www.etsi.org/ades/etsits/level/baseline/B-LT#</a></td>
<td>3</td>
</tr>
<tr>
<td>AdES-LTA</td>
<td><a href="http://www.etsi.org/ades/etsits/level/baseline/B-LTA#">http://www.etsi.org/ades/etsits/level/baseline/B-LTA#</a></td>
<td>3</td>
</tr>
<tr>
<td>AdES-BES</td>
<td><a href="http://www.etsi.org/ades/etsits/level/BES#">http://www.etsi.org/ades/etsits/level/BES#</a></td>
<td>3</td>
</tr>
<tr>
<td>AdES-EPES</td>
<td><a href="http://www.etsi.org/ades/etsits/level/EPES#">http://www.etsi.org/ades/etsits/level/EPES#</a></td>
<td>3</td>
</tr>
<tr>
<td>AdES-C</td>
<td><a href="http://www.etsi.org/ades/etsits/level/C#">http://www.etsi.org/ades/etsits/level/C#</a></td>
<td>4</td>
</tr>
<tr>
<td>AdES-X</td>
<td><a href="http://www.etsi.org/ades/etsits/level/X#">http://www.etsi.org/ades/etsits/level/X#</a></td>
<td>4</td>
</tr>
<tr>
<td>AdES-A</td>
<td><a href="http://www.etsi.org/ades/etsits/level/A#">http://www.etsi.org/ades/etsits/level/A#</a></td>
<td>4</td>
</tr>
<tr>
<td>AdES-LTV</td>
<td><a href="http://www.etsi.org/ades/etsits/level/LTV#">http://www.etsi.org/ades/etsits/level/LTV#</a></td>
<td>5</td>
</tr>
</tbody>
</table>

NOTE 3: The levels identified in these rows are levels that CadES, PadES, and XadES signatures can reach.

NOTE 4: The levels identified in these rows are levels that CadES and XadES signatures can reach, but not PadES signatures.

NOTE 5: The levels identified in these rows are levels that only PadES signatures can reach.

6.1.1.2 OASIS XML related component

The element that shall request the augmenting of the signature after its validation shall be the ReturnAugmentedSignature element.

The ReturnAugmentedSignature element shall be defined as in XML Schema file "[XSDFILESIGVALPROT]", whose location is detailed in clause A.1, and is copied below for information.

```xml
<!targetNamespace="http://uri.etsi.org/19442/v1.1.1#" ->
<xs:element name="ReturnAugmentedSignature" type="ReturnAugmentedSignatureType"/>
<xs:attribute name="Level" type="xs:anyURI" use="required" />
</xs:complexType>
```

The Level attribute of the aforementioned element shall take one of the values in Table 5 and Table 6 except the URIs identifying levels AdES-B, AdES-E-BES, AdES-E-EPES, AdES-B, AdES-BES, and AdES-EPES.

Processing model.

If the server manages to augment the signature, it shall return the augmented signature within the dss:UpdatedSignature element or within the dss:DocumentWithSignature as specified in clause 6.2.1.2.

6.1.1.3 OASIS JSON related component

TO BE COMPLETED

6.2 Components for response to validation and augmentation request

6.2.1 Component for returning the augmented signature

6.2.1.1 Component semantics

This component shall incorporate the augmented signature. The signature shall be either detached from the document(s) that it signs, enveloped in one of the documents that it signs, or enveloping one of the documents that it signs.

6.2.1.2 OASIS XML related component

In the XML profile derived from OASIS specifications the elements that allow to return one augmented signature after its validation shall be dss:UpdatedSignature and dss:DocumentWithSignature.
The server shall incorporate the `dss:UpdatedSignature` element, as specified in clause [RETURNUPDATEDSIG 5.5.8.1] of [1], into the response for returning an augmented non enveloped signature.

The server shall incorporate the `dss:DocumentWithSignature` element, as specified in clause [DSSXDOCUMENTWITHSIGNATURE] of [1], into the response for returning an augmented non enveloped signature.

6.2.1.3 OASIS JSON related component

The element that allows to return one augmented signature after its validation shall be the `augmentedSig` element.

The server shall incorporate the `augSig` element into the response for returning an augmented non enveloped signature. The `augSig` element shall contain the augmented digital signature base-64 encoded.

The server shall incorporate the `docWithSig` element into the response for returning augmented signature(s) enveloped within one document. The `docWithSig` element shall contain the augmented digital signature base-64 encoded.

7 Auxiliary types

These are types that are used in the definition of other types in XML schema. In case of specifying a JSON format, this will be the place for types that are re-used in the definition of other types.

7.1 Type for extension points

Common types and elements for requesting validation of any AdES signature type.

7.1.1 AnyType for OASIS XML protocol

7.1.2 OASIS JSON related component

7.2 Type for language-qualified strings

7.2.1 InternationalStringType type for OASIS XML protocol

7.2.2 OASIS JSON related component

7.3 Type for names

7.3.1 saml:NameIdentifierType type for OASIS XML protocol

The DSS protocol includes an element of type `saml:NameIdentifierType`. This is from SAML 1.1. Current version of SAML is 2.0. Element Type `NameIDType` is defined there. Likely it would be worth to use the more recent one. Both types allow for including contents as specified for `ds:X509SubjectName`, as well as other types of names.

**TO BE DISCUSSED: SAML 1.1 OR SAML 2?**

7.3.2 OASIS JSON related component
Annex A (normative):
XML and JSON Schema files

A.1 XML Schema file location for namespace
   http://uri.etsi.org/19442/v1.1.1#

   The file at [XSDFILESIGVALPROT_URL] ([XSDFILESIGVALPROT]) contains the definitions of elements and
   types defined within the namespace whose URI value is http://uri.etsi.org/19442/v1.1.1#.

A.2 JSON Schema file location for "$schema"
   "http://etsi.org/119442/v1.1.1/json#"

   The file at [JSONFILESIGVALPROT_URL] ([JSONSCHEMAFILESIGVALPROT]) contains the definitions of elements
   and types defined within the JSON schema whose "$schema" value is "http://etsi.org/119442/v1.1.1/json#"
Annex (informative):
Bibliography

•
Annex (informative):
Change History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Information about changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Month year&gt;</td>
<td>&lt;#&gt;</td>
<td>&lt;Changes made are listed in this cell&gt;</td>
</tr>
</tbody>
</table>
## History

<table>
<thead>
<tr>
<th>Document history</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>V0.0.3</strong></td>
</tr>
<tr>
<td><strong>V0.0.4</strong></td>
</tr>
<tr>
<td><strong>V0.0.5</strong></td>
</tr>
</tbody>
</table>

*Latest changes made on 2016-05-20*