



Signature Policy Profile of the OASIS Digital Signature Services Version 1.0

Committee Draft 01

18 May 2009

Specification URIs:

This Version:

<http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy-cd01.doc>
<http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy-cd01.html>
<http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy-cd01.pdf>
(Authoritative)

Previous Version:

N/A

Latest Version:

<http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy.doc>
<http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy.html>
<http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy.pdf>

Technical Committee:

OASIS Digital Signature Services eXtended (DSS-X) TC

Chair(s):

Juan Carlos Cruellas, *UPC-DAC* <cruellas@ac.upc.edu>
Stefan Drees, Individual Member, <stefan@drees.name>.

Editor(s):

Juan Carlos Cruellas, , *UPC-DAC*, <pvde@sonnenglanz.net>

Related work:

This specification is related to:

- OASIS Digital Signature Service Core Protocols, Elements and Bindings. Version 1.0.

Abstract:

TBC

Status:

This document was last revised or approved by the OASIS DSS-X TC on the above date. The level of approval is also listed above. Check the "Latest Version" location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at <http://www.oasis-open.org/committees/dss-x/>.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (<http://www.oasis-open.org/committees/dss-x/ipr.php>).

The non-normative errata page for this specification is located at <http://www.oasis-open.org/committees/dss-x/>.

Notices

Copyright © OASIS ® 2009. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", [insert specific trademarked names and abbreviations here] are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

Table of Contents

NOTICES	3
TABLE OF CONTENTS	4
1 INTRODUCTION	5
1.1 TERMINOLOGY	5
1.2 NAMESPACES	5
1.3 NORMATIVE REFERENCES	6
1.4 NON NORMATIVE REFERENCES	6
2 OVERVIEW	7
2.1 PROFILE FEATURES	8
2.1.1 <i>Scope</i>	8
2.1.2 <i>Relationship To Other Profiles</i>	8
2.1.3 <i>Element <dss:SignatureObject></i>	8
2.2 PROFILE OF SIGNING PROTOCOL	8
2.2.1 <i>Element <dss:SignRequest></i>	8
2.2.1.1 <i>Element <dss:OptionalInputs></i>	8
2.2.1.1.1 <i>New Optional Inputs</i>	8
2.2.1.1.1.1 <i>Optional Input <GenerateUnderSignaturePolicy></i>	8
2.2.1.1.1.2 <i>Optional Input <ReturnSupportedSignaturePolicies></i>	9
2.2.2 <i>Element <dss:SignResponse></i>	9
2.2.2.1 <i>Element <dss:Result></i>	9
2.2.2.2 <i>Element <dss:OptionalOutputs></i>	10
2.2.2.2.1 <i>Optional Output <UsedSignaturePolicy></i>	10
2.2.2.2.2 <i>Optional Output <SupportedSignaturePolicies></i>	10
2.3 PROFILE OF VERIFYING PROTOCOL	10
2.3.1 <i>Element <dss:VerifyRequest></i>	10
2.3.1.1 <i>Element <dss:OptionalInputs></i>	10
2.3.1.1.1 <i>New Optional Inputs</i>	11
2.3.1.1.1.1 <i>Optional Input <VerifyUnderSignaturePolicy></i>	11
2.3.2 <i>Element <dss:VerifyResponse></i>	11
2.3.2.1 <i>Element <dss:OptionalOutputs></i>	11
2.3.2.1.1 <i>New Optional Outputs</i>	12
2.3.2.1.1.1 <i>Optional Input <VerifiedUnderSignaturePolicy></i>	12
3 CONFORMANCE	13
3.1 CONFORMANCE LEVEL 1	13
3.2 CONFORMANCE LEVEL 2	13
A. REVISION HISTORY	14

1 Introduction

ETSI has specified formats for Advanced Electronic Signatures (AdES) built on XML signatures as specified [XMLSig] -TS 101 903: “XML Advanced Electronic Signatures (XAdES)- and CMS signatures – TS 101 733: “CMS Advanced Electronic Signatures (CAAdES)”-.

The DSS signing and verifying protocols are defined in [DSSCore]. The “Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 1.0” [AdES-DSS] profiles [DSSCore] for requesting generation and verification of AdES signatures to a centralized server.

AdES signatures may contain explicit identifiers of Signature Policy, which provides rules for generating and verifying these signatures.

This document extends [DSSCore] protocol specifying a number of operations for managing generation and verification of electronic signatures under the rules established by a Signature Policy, as identified in [SigPol-DSS-Req].

1.1 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in **Error! Reference source not found.**

1.2 Namespaces

All schema listings in the current document are excerpts from the schema file [SigPol-DSS-XSD]. In the case of a disagreement between the schema file and this document, the schema file takes precedence.

This schema is associated with the following XML namespace:

```
urn:oasis:names:tc:dss-x:1.0:profiles:SignaturePolicy:schema#
```

The table below lists the namespaces referenced in this specification.

Prefix	Namespace	Specification(s)
ds	http://www.w3.org/2000/09/xmlsig#	[XMLSig]
dss	urn:oasis:names:tc:dss:1.0:core:schema	[DSSCore]
xades	http://uri.etsi.org/01903/v1.3.2#	[XAdES]
dssades	urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#	[AdES-DSS]
xs	http://www.w3.org/2001/XMLSchema	[XMLSchema]
vr	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	[DSSVerRep]

28 Applications MAY use different namespace prefixes, and MAY use whatever namespace
29 defaulting/scoping conventions they desire, as long as they are compliant with the Namespaces in XML
30 specification [XML-ns].

31 1.3 Normative References

- 32
- 33 **[AdES-DSS]** OASIS Standard, "Advanced Electronic Signature Profiles of the OASIS Digital
34 Signature Service Version 1.0". April 2007 [http://docs.oasis-](http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-AdES-spec-v1.0-os.pdf)
35 [open.org/dss/v1.0/oasis-dss-profiles-AdES-spec-v1.0-os.pdf](http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-AdES-spec-v1.0-os.pdf).
36
- 37 **[CAAdES]** CMS Advanced Electronic Signatures. ETSI TS 101 733, January 2007.
38
- 39 **[Core-XSD]** OASIS Standard, *DSS Schema*. February 2007.
40
- 41 **[DSS Core]** OASIS Standard, "Digital Signature Service Core Protocols, Elements and
42 Bindings. Version 1.0" April 2007. [http://docs.oasis-open.org/dss/v1.0/oasis-dss-](http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf)
43 [core-spec-v1.0-os.pdf](http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf).
44
- 45 **[DSSCore]** OASIS Standard, *Digital Signature Service Core Protocols and Elements*.
46 February 2007.
47
- 48 **[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
49 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
50
- 51 **[RFC 3001]** M. Mealling. *A URN Namespace of Object Identifiers*. IETF RFC 3001,
52 November 2000.
53
- 54 **[RFC 3852]** R. Housley. *Cryptographic Message Syntax (CMS)*, IETF RFC 3852, July 2004.
55
- 56 **[SigPol-DSS-XSD]** OASIS Standard, "Signature Policy Profile Schema",
57
- 58 **[XAdES]** Advanced Electronic Signatures. ETSI TS 101 733. March 2006.
59
- 60 **[XMLSig]** D. Eastlake et al. *XML-Signature Syntax and Processing*.
61 <http://www.w3.org/TR/1999/REC-xml-names-19990114>, W3C Recommendation,
62 February 2002.
63
- 64 **[XML-ns]** T. Bray, D. Hollander, A. Layman. *Namespaces in XML*.
65 <http://www.w3.org/TR/1999/REC-xml-names-19990114>, W3C Recommendation,
66 January 1999.
- 67 **[XMLSchema]** Henry S. Thompson, David Beech, Murray Maloney, Noah Mendelson. *XML*
68 *Schema Part 1: Structures Second Edition*. <http://www.w3.org/TR/xmlschema-1/>,
69 W3C Recommendation 28 October 2004.
- 70 **[DSSVerRep]** Ingo Henkel, Detlef Hühnlein. *Profile for comprehensive multi-signature*
71 *verification reports for OASIS Digital Signature Services Version 1.0*
72

73 1.4 Non Normative References

- 74 **[SigPol-DSS-Req]** Juan Carlos Cruellas. *Requirements for specifying the Signature Policy Profile of*
75 *the OASIS Digital Signature Services*, OASIS, November 2007

2 Overview

76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115

This profile supports a number of operations for managing generation and verification of electronic signatures under the rules established by a Signature Policy, as identified in [SigPol-DSS-Req].

For the generation of electronic signatures, the following operations apply:

SignRequest. This operation supports:

Requesting generation of a signature under a certain signature policy, allowing clients to explicitly identify that signature policy in the request. This identification may be through the usage of both, a URI or an OID.

Passing to the server the location and/or the digest of the electronic document where the signature policy is specified .

Requesting to the server the incorporation within the signature to be generated the identifier of the signature policy under which it has been created, using syntaxes defined in [XAdES] or [CAAdES].

Requesting also a list of the supported signature policies supported by the server.

SignResponse. This operation supports delivery of:

Electronic signatures with the identifier of the signature policy under which they have been generated.

Indication of the signature policy under which the signature has been generated within `<dss:SignResponse>` .

Digest of the electronic document where the signature policy is defined, as a double check facility for the client.

A code error in case the server may not sign with the requested signature policy.

The list of supported signature policy identifiers.

For electronic signature verification (and updating) the following operations apply:

VerifyRequest. This operation supports requests for:

Request the verification of a signature under a certain signature policy, if the signature does not contain an identifier of such policy, by using an identifier of that policy.

Requesting signature verification under the signature policies identified within the signature, if any identifier is present there.

Passing to the server the location and/or the digest of the electronic document where the signature policy is specified.

Requesting return of explicit indication of the signature policies under which the electronic signatures have been verified.

Requesting also a list of the supported signature policies supported by the server.

VerifyResponse. This operation supports delivery of:

116 Indication of the signature policies under which the server has verified the electronic
117 signatures mentioned above.

118 Digest of the electronic document where the signature policy is defined, as a double check
119 facility for the client.

120 A code error in case the server may not verify the electronic signature(s) with the requested
121 signature policy(ies).

122 The list of supported signature policy identifiers.

123 **2.1 Profile Features**

124 **2.1.1 Scope**

125 This document profiles the DSS signing and verifying protocols defined in [DSSCore].

126 **2.1.2 Relationship To Other Profiles**

127 The profile in this document is based on the [DSSCore]. The profile in this document may be
128 implemented.

129
130 This profile provides means for the explicit management of signature policies with [DSSCore] and other
131 existing profiles like [AdES-DSS], and as such, it may be used in conjunction with these specifications.
132

133 **2.1.3 Element <dss:SignatureObject>**

134 This profile supports requests for generation and verification of electronic signatures under a given
135 signature policy.

136

137 Although this specification does not impose any constraint the format of the signatures generated by the
138 servers or sent to the servers for verification, it nicely fits with formats of advanced signatures as defined
139 in [XAdES] and [CAAdES].

140

141 **2.2 Profile of Signing Protocol**

142 **2.2.1 Element <dss:SignRequest>**

143 This clause profiles the <dss:SignRequest> element.

144 **2.2.1.1 Element <dss:OptionalInputs>**

145 This profile does not impose any restrictions on any optional input specified in the [DSSCore] or other
146 profiles.

147

148 This profile defines a new Optional Input as indicated below.

149 **2.2.1.1.1 New Optional Inputs**

150 **2.2.1.1.1.1 Optional Input <GenerateUnderSignaturePolicy>**

151 This optional input will specify the signature policy under which the server is requested to generate the
152 electronic signature.

153 Below follows the schema for this element:

154

```

155 <xs:element name="GenerateUnderSignaturePolicy"
156 type="SignaturePolicyDetailsType"/>
157
158 <xs:complexType name="SignaturePolicyDetailsType">
159   <xs:sequence>
160     <xs:element name="SignaturePolicyIdentifier" type="xs:anyURI"/>
161     <xs:element name="SignaturePolicyLocation" type="xs:anyURI"
162       minOccurs="0"/>
163     <xs:element name="DigestAndAlgorithm"
164       type="xades:DigestAlgAndValueType" minOccurs="0"/>
165   </xs:sequence>
166 </xs:complexType>

```

167

168 Element `<SignaturePolicyIdentifier>` contains the identifier of the signature policy as an URI.
 169 Signature policies MAY be identified by an URI or by OIDs. Should the signature policy identifier
 170 requested by the client be an OID, this element will contain a URN built from the actual value of this OID
 171 as specified in [RFC 3001].

172

173 Element `<SignaturePolicyLocation>` is optional and contains the location where the electronic
 174 document specifying the identified signature policy may be found.

175

176 Element `<DigestAndAlgorithm>` is optional and contains the digest value of the aforementioned
 177 electronic document and the identifier of the digest algorithm used for computing such a value.

178 **2.2.1.1.2 Optional Input `<ReturnSupportedSignaturePolicies>`**

179 This optional input is an empty element, which, when present instructs the server to return within the
 180 corresponding `<dss:SignResponse>` the `<SupportedSignaturePolicies>` Optional Output identifying all the
 181 signature policies supported by this server as described later on in this document.

182 Below follows the schema for this element:

183

```

184 <xs:element name="ReturnSupportedSignaturePolicies" />

```

185

186 **2.2.2 Element `<dss:SignResponse>`**

187 This clause profiles the `<dss:SignResponse>` element.

188 **2.2.2.1 Element `<dss:Result>`**

189 This profile adds the following `<ResultMinor>` values to the ones already specified in the [DSSCore] for
 190 those cases where the `<ResultMajor>` code is Success.

191

192 `urn:oasis:names:tc:dss-x:1.0:resultminor:error:SignaturePolicyNotSupported`

193 The server does not support the signature policy identified in the request.

194 `urn:oasis:names:tc:dss-x:1.0:resultminor:error:SignaturePolicyDigestFailure`

195 The server computed a digest value on the electronic document defining the signature policy that was
 196 not equal to the value included in the request,.

197 `urn:oasis:names:tc:dss-x:1.0:resultminor:error:SignaturePolicyIdentifierError`

198 The server concluded that the identifier of the signature policy was not correctly built.

199

200 **2.2.2.2 Element <dss:OptionalOutputs>**

201 This profile does not impose any restrictions on any optional output specified in the [DSSCore] or other
202 profiles other than those explicitly mentioned in the clauses below.

203

204 This profile defines new Optional Outputs as indicated below.

205 **2.2.2.2.1.1 Optional Output <UsedSignaturePolicy>**

206 This optional output will provide to the client details of the signature policy under which the server has
207 actually generated the electronic signature.

208 Below follows the schema for this element:

209

```
210 <xs:element name="UsedSignaturePolicy" type="SignaturePolicyDetailsType"/>
```

211

212 No additional constraints are specified for the contents of this element.

213 **2.2.2.2.1.2 Optional Output <SupportedSignaturePolicies>**

214 This optional output will provide to the client details of the signature policies under which the server is
215 able to generate electronic signatures.

216 Below follows the schema for this element:

217

```
218 <xs:element name="SupportedSignaturePolicies">  
219   <xs:complexType>  
220     <xs:sequence>  
221       <xs:element name="SupportedSignaturePolicy"  
222         type="SignaturePolicyDetailsType" maxOccurs="unbounded"/>  
223     </xs:sequence>  
224   </xs:complexType>  
225 </xs:element>
```

226

227 No additional constraints are specified for the contents of <SupportedSignaturePolicy> elements.

228

229 **2.3 Profile of Verifying Protocol**

230 **2.3.1 Element <dss:VerifyRequest>**

231 This clause profiles the <dss:VerifyRequest> element.

232 **2.3.1.1 Element <dss:OptionalInputs>**

233 This profile does not impose any restrictions on any optional input specified in the [DSSCore] or other
234 profiles.

235

236 This profile defines a new Optional Input as indicated below.

237 2.3.1.1.1 New Optional Inputs

238 2.3.1.1.1.1 Optional Input <VerifyUnderSignaturePolicy>

239 This optional input allows to instruct the server to use certain signature policy for verifying all (or selected)
240 signatures that do not contain an explicit indication of having been produced under a certain signature
241 policy.

242 Signatures containing such an explicit indication MUST be verified using the explicitly indicated signature
243 policy, regardless the contents of the optional input specified in this section.

244

```
245 <xs:element name="VerifyUnderSignaturePolicy"  
246 type="VerifyUnderSignaturePolicyType"/>  
247  
248 <xs:complexType name="VerifyUnderSignaturePolicyType">  
249   <xs:sequence>  
250     <xs:element name="DefaultPolicy" type="SignaturePolicyDetailsType"  
251 minOccurs="0"/>  
252     <xs:element ref="ExplicitPolicies" minOccurs="0"/>  
253   </xs:sequence>  
254 </xs:complexType>  
255  
256 <xs:element name="ExplicitPolicies" type="PolicySignaturePairsType" />  
257 <xs:complexType name="PolicySignaturePairsType">  
258   <xs:sequence>  
259     <xs:element ref="PolicySignaturePair" maxOccurs="unbounded"/>  
260   </xs:sequence>  
261 </xs:complexType>  
262  
263 <xs:element name="PolicySignaturePair" type="PolicySignaturePairType" />  
264 <xs:complexType name="PolicySignaturePairType">  
265   <xs:sequence>  
266     <xs:element ref="SignatureIdentifier" />  
267     <xs:element ref="SignaturePolicy" />  
268   </xs:sequence>  
269 </xs:complexType>  
270 <xs:element name="SignaturePolicy" type="SignaturePolicyDetailsType" />  
271 <xs:element name="SignatureIdentifier" type="vr:SignatureIdentifierType" />
```

272

273 Optional element <DefaultPolicy> specifies a default policy that the server should use for verifying
274 any found signature that: does not have any explicit indication of signature policy and that it is not
275 referenced within the <ExplicitPolicies> element.

276 Optional element <ExplicitPolicies> is a list of [signature , signature policy] pairs, each one
277 instructing the server to verify the referenced signature of the pair with the signature policy indicated in
278 the pair. Should the referenced signature contain an explicit indication of a different signature policy, the
279 server will use this last one and will issue a warning reporting this situation.

280 2.3.2 Element <dss:VerifyResponse>

281 2.3.2.1 Element <dss:OptionalOutputs>

282 This profile does not impose any restrictions on any optional output specified in the [DSSCore] or other
283 profiles other than those explicitly mentioned in the clauses below.

284 This profile defines new Optional Outputs as indicated below.

285 2.3.2.1.1 New Optional Outputs

286 2.3.2.1.1.1 Optional Input <VerifiedUnderSignaturePolicy>

287 This optional output will be returned by the server to indicate under what signature policy a certain
288 signature has been verified.

```
289 <xs:element name="VerifiedUnderSignaturePolicy"  
290 type="VerifiedUnderSignaturePolicyType"/>  
291  
292 <xs:complexType name="VerifiedUnderSignaturePolicyType">  
293 <xs:sequence>  
294 <xs:element ref="SignaturePolicy" />  
295 <xs:element ref="SignatureIdentifier" minOccurs="0"/>  
296 </xs:sequence>  
297 </xs:complexType>
```

298
299 Mandatory <SignaturePolicy> will identify the signature policy used.

300 Optional <SignatureIdentifier> references the signature that was verified under such a signature
301 policy.

302 Should this optional output be present within the <vr:IndividualSignatureReport> then
303 <VerifiedUnderSignaturePolicy> will not contain the <SignatureIdentifier> optional
304 element (as this element will actually appear as child of <vr:IndividualSignatureReport>).

305 Should this optional output not be present within the <vr:IndividualSignatureReport> and
306 <SignatureIdentifier> not present, this optional output will report that all the signatures found have
307 been verified with the same signature policy indicated in <SignaturePolicy> element.

308 **3 Conformance**

309 The present profile defines two conformance levels. These two levels are defined in the clauses below.

310 **3.1 Conformance Level 1**

311 Any implementation of this profile is conformant with this specification if:

- 312 1. It fully supports the signing protocol, satisfying the the MUST or REQUIRED level requirements
313 defined in this specification for the aforementioned protocol.
- 314 2. It only supports <VerifyUnderSignaturePolicy>'s <DefaultPolicy> child in the
315 <dss:VerificationRequest> element.
- 316 3. It only supports <VerifiedUnderSignaturePolicy>'s <SignaturePolicy> child in the
317 <dss:VerificationResponse> element.
- 318 4. It satisfies the MUST or REQUIRED level requirements defined in this specification except those
319 that affect the not supported elements of the verification protocol (namely
320 <VerifyUnderSignaturePolicy>'s <SignatureIdentifier> child and
321 <VerifiedUnderSignaturePolicy>'s <SignatureIdentifier> child).

322 **3.2 Conformance Level 2**

323 Any implementation of this profile is conformant with this specification if:

- 324 1. It fully supports the signing protocol, satisfying the the MUST or REQUIRED level requirements
325 defined in this specification.
- 326 2. It fully supports the verification protocol, satisfies the MUST or REQUIRED level requirements
327 defined in this specification for the aforementioned protocol.

328

329

A. Revision History

330

[optional; should not be included in OASIS Standards]

331

Revision	Date	Editor	Changes Made
0.1	2008-04-25	Juan Carlos Cruellas	Initial Draft. No profile for verification protocol.
0.2	2008-06-09	Juan Carlos Cruellas	Addition of verification protocol and two conformance levels.

332

333