



1

2

Entity Seal Profile of the OASIS Digital Signature Service

3

4

Committee Draft, 24 December 2004
(Working Draft 06)

5

6

Document identifier:

7

oasis-dss-1.0-profiles-eseal-spec-cd-01

8

Location:

9

<http://docs.oasis-open.org/dss/>

10

Editor:

11

Nick Pope, *individual* <pope@secstan.com>

12

Contributors:

13

John Messing, *American Bar Association*

14

Dallas Powell, *Individual*

15

Juan Carlos Cruellas, *Individual*

16

Trevor Perrin, *individual*

17

Abstract:

18

This draft defines a profile of the OASIS DSS protocol and XML signature for the purpose of creating and verifying entity seals.

19

20

Status:

21

This is a **Committee Draft** produced by the OASIS Digital Signature Service Technical Committee. Committee members should send comments on this draft to

22

dss@lists.oasis-open.org.

23

24

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 Digital Signature Service TC web page at <http://www.oasis-open.org/committees/dss/ipr.php>.

25

26

27

28

Table of Contents

29	1	Introduction	4
30	1.1	Notation	4
31	1.2	Namespaces	4
32	2	Profile Features.....	5
33	2.1	Identifier.....	5
34	2.2	Scope	5
35	2.3	Relationship To Other Profiles	5
36	2.4	Signature Object.....	5
37	2.5	Transport Binding.....	5
38	2.6	Security Binding	5
39	2.6.1	Security Requirements.....	5
40	2.6.2	TLS X.509 Mutual Authentication	5
41	3	Profile of Signing Protocol.....	6
42	3.1	Element <SignRequest>	6
43	3.1.1	Element <OptionalInputs>	6
44	3.1.2	Element <InputDocuments>	6
45	3.2	Element <SignResponse>	6
46	3.2.1	Element <Result>	6
47	3.2.2	Element <OptionalOutputs>	6
48	3.2.3	Element <SignatureObject>.....	7
49	4	Profile of Verifying Protocol.....	8
50	4.1	Element <VerifyRequest>	8
51	4.1.1	Element <OptionalInputs>	8
52	4.1.2	Element <SignatureObject>.....	8
53	4.1.3	Element <InputDocuments>	8
54	4.2	Element <VerifyResponse>	8
55	4.2.1	Element <Result>	8
56	4.2.2	Element <OptionalOutputs>	8
57	5	Profile of ESeal Signatures.....	9
58	6	Server Processing Rules	10
59	6.1	Sign	10
60	6.2	Verify	10
61	7	Editorial Issues.....	11
62	8	References.....	12
63	8.1	Normative	12

64 Appendix A. Revision History 13
65 Appendix B. Notices 14
66

67 1 Introduction

68 The DSS signing and verifying protocols are defined in **[DSSCore]**. As defined in that document,
69 these protocols have a fair degree of flexibility and extensibility. This document profiles the core
70 to support creation and validation of a "seal" created by a given Entity or Organization on
71 electronic data.

72 The seal is a form of electronic signature which:

- 73 a) protects the integrity of the document,
- 74 b) includes the time at which the seal was applied proving that the data existed at the given
75 time,
- 76 c) includes the identity of the entity requesting the seal,
- 77 d) may include a statement of intent for applying the seal.

78 This profile includes a few options that require further profiling for implementing interoperable
79 systems.

80 1.1 Notation

81 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD",
82 "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be
83 interpreted as described in IETF RFC 2119 **[RFC 2119]**. These keywords are capitalized when
84 used to unambiguously specify requirements over protocol features and behavior that affect the
85 interoperability and security of implementations. When these words are not capitalized, they are
86 meant in their natural-language sense.

87 This specification uses the following typographical conventions in text: `<ns:Element>`,
88 `Attribute`, **Datatype**, `OtherCode`.

89 1.2 Namespaces

90 Conventional XML namespace prefixes are used in this document:

- 91 • The prefix `dss:` (or no prefix) stands for the DSS core namespace **[Core-XSD]**.
- 92 • The prefix `ds:` stands for the W3C XML Signature namespace **[XMLSig]**.
- 93 • The prefix `xades:` stands for the ETSI XML Advanced Electronic Signature namespace
94 **[XAdES]**

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

98 2 Profile Features

99 2.1 Identifier

100 urn:oasis:names:tc:dss:1.0:profiles:eseal

101 2.2 Scope

102 This document profiles the DSS signing and verifying protocols defined in **[DSSCore]** and profiles
103 the XML signature format for entity seals created by a given Entity or Organization on electronic
104 data.

105 2.3 Relationship To Other Profiles

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

107 2.4 Signature Object

108 This profile supports the creation and verification of [XMLSig] signatures as defined in section 5.

109 2.5 Transport Binding

110 This profile is transported using the HTTP POST Transport Binding defined in **[DSSCore]**.

111 2.6 Security Binding

112 2.6.1 Security Requirements

113 This profile MUST use security bindings that:

- 114 • Authenticates the requester to the DSS server
- 115 • Authenticates the DSS server to the DSS client
- 116 • Protects the integrity of a request, response and the association of response to the
117 request.
- 118 • Optionally, protects the confidentiality of a request and response

119 The following is recommended to meet these requirements..

120 2.6.2 TLS X.509 Mutual Authentication

121 This profile is secured using the TLS X.509 Mutual Authentication Binding defined in **[DSSCore]**.

122 3 Profile of Signing Protocol

123 3.1 Element <SignRequest>

124 3.1.1 Element <OptionalInputs>

125 The optional inputs from [DSSCore]:

- 126 • <dss:ClaimedIdentity>
- 127 • MUST be supported by the DSS server. This MAY be sent by the client to provide the
128 claimed identity of the requester. If present the <Name> element of
129 <dss:ClaimedIdentity> MUST be authenticated by the Security Binding.
- 130 • <dss:SignedProperties>

131 MAY be supported by the DSS server. If present this MAY be used by the client to request the
132 CommitmentTypeIndication property. The CommitmentTypeIndication property is requested
133 using the identifier and value as defined in [DSS-XAdES].

134

135 3.1.2 Element <InputDocuments>

136 At least one of the following types of InputDocuments from [DSSCore]:

- 137 • <dss:DocumentHash>
- 138 • <dss:Document>

139 MUST be supported by the DSS server. The DSS client may use either form.

140 If the client uses an element that is not supported by the server, the server SHOULD return
141 ResultMinor set to indicate NotSupported and ResultMessage set to text providing further
142 details.

143 3.2 Element <SignResponse>

144 3.2.1 Element <Result>

145 This profile defines no additional <ResultMinor> codes.

146 3.2.2 Element <OptionalOutputs>

147 This profile requires no optional options.

148 **3.2.3 Element <SignatureObject>**

149 If successful, the server MUST return a <ds:Signature> with the signature properties as defined in
150 section 5.

151 **4 Profile of Verifying Protocol**

152 **4.1 Element <VerifyRequest>**

153 **4.1.1 Element <OptionalInputs>**

154 This profile places no specific requirements on the optional inputs.

155 **4.1.2 Element <SignatureObject>**

156 The server MUST support <ds:Signature>.

157 **4.1.3 Element <InputDocuments>**

158 The at least one of the input document element from [DSSCore]:

- 159 • <dss:DocumentHash>
160 • <dss:Document>

161 MUST be supported by the DSS server. The DSS client may use either form. Other elements
162 MAY be supported.

163 **4.2 Element <VerifyResponse>**

164 **4.2.1 Element <Result>**

165 This profile defines no additional <ResultMinor> codes.

166 **4.2.2 Element <OptionalOutputs>**

167 This profile places no specific requirements on the optional outputs.

168 5 Profile of ESeal Signatures

169 The signature form used by the profile is an XML Signature as defined in **[XMLSig]**.

170 The XML signature **MUST** contain the element `<xades:SignedProperties>` within the
171 element `<xades:QualifyingProperties>` as defined in **[XAdES]** within the `<ds:object>`
172 element of the XML signature.

173 The following property must be present within the `<xades:SignedProperties>` element:

- 174 • `<xades:SigningTime>`

175 In addition, the following may be present:

- 176 • `<xades:CommitmentTypeIndication>`

177 The following property must be present within a `<ds:SignatureProperty>` element:

- 178 • `<dss:RequesterIdentity>`

179 The digest value of the `<ds:SignatureProperty>` and the `<xades:SignedProperties>`
180 elements shall be included in the signature references.

181 **6 Server Processing Rules**

182 **6.1 Sign**

183 In addition to the processing rules define in **[Core-XSD]** the server MUST:

- 184 a) ensure that the requester is authorized to request an ESeal,
185 b) authenticate that requester is as identified in <dss:RequesterIdentity> and, if
186 present, <dss:ClaimedIdentity>

187 **6.2 Verify**

188 In addition to the processing rules define in **[Core-XSD]** the server MUST:

- 189 a) ensure that the properties required in section 5 are present.

190

191 **7 Editorial Issues**

192 1) *Requirements for additional text identified by in line editorial comments.*

193 2) *Statement of Intent requires further work. Is this a general DSS requirement? This is*
194 *similar to XAdES commitment type but does not require an OID.*

195 **Resolution:** *Used XadES Commitment type. WD-02*

196

8 References

197

8.1 Normative

- 198 **[Core-XSD]** T. Perrin et al. *DSS Schema*. OASIS, **(MONTH/YEAR TBD)**
- 199 **[DSSCore]** T. Perrin et al. *Digital Signature Service Core Protocols and Elements*.
200 OASIS, **(MONTH/YEAR TBD)**
- 201 **[DSS-XAdES]** Juan Carlos Cruellas et al. *XAdES Profile of the OASIS Digital Signature*
202 *Service*
- 203 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*.
204 IETF RFC 2396, August 1998.
205 <http://www.ietf.org/rfc/rfc2396.txt>.
- 206 **[XAdES]** XML Advanced Electronic Signatures ETSI TS 101 903, February 2002
207 *(shortly to be re-issued)*
208 http://pda.etsi.org/pda/home.asp?wki_id=1UFEyx7ORuBCDGED3liJH
- 209 **[XML-ns]** T. Bray, D. Hollander, A. Layman. *Namespaces in XML*. W3C
210 Recommendation, January 1999.
211 <http://www.w3.org/TR/1999/REC-xml-names-19990114>
- 212 **[XMLSig]** D. Eastlake et al. *XML-Signature Syntax and Processing*. W3C
213 Recommendation, February 2002.
214 <http://www.w3.org/TR/1999/REC-xml-names-19990114>
- 215
- 216
- 217
- 218
- 219
- 220 •

Appendix A. Revision History

Rev	Date	By Whom	What
wd-01	2004-03-07	Nick Pope	Initial version
wd-02	2004-03-14	Nick Pope	Filling in further details
wd-03	2004-04-12	Nick Pope	Completing details
wd-04	2004-06-13	Nick Pope	Updating technical details of carrying "RequesterIdentity"
wd-05	2004-11-13	Nick Pope	Updating in line with comments from Trevor

Appendix B. Notices

223 OASIS takes no position regarding the validity or scope of any intellectual property or other rights
224 that might be claimed to pertain to the implementation or use of the technology described in this
225 document or the extent to which any license under such rights might or might not be available;
226 neither does it represent that it has made any effort to identify any such rights. Information on
227 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS
228 website. Copies of claims of rights made available for publication and any assurances of licenses
229 to be made available, or the result of an attempt made to obtain a general license or permission
230 for the use of such proprietary rights by implementors or users of this specification, can be
231 obtained from the OASIS Executive Director.

232 OASIS invites any interested party to bring to its attention any copyrights, patents or patent
233 applications, or other proprietary rights which may cover technology that may be required to
234 implement this specification. Please address the information to the OASIS Executive Director.

235 Copyright © OASIS Open 2003. *All Rights Reserved.*

236 This document and translations of it may be copied and furnished to others, and derivative works
237 that comment on or otherwise explain it or assist in its implementation may be prepared, copied,
238 published and distributed, in whole or in part, without restriction of any kind, provided that the
239 above copyright notice and this paragraph are included on all such copies and derivative works.
240 However, this document itself does not be modified in any way, such as by removing the
241 copyright notice or references to OASIS, except as needed for the purpose of developing OASIS
242 specifications, in which case the procedures for copyrights defined in the OASIS Intellectual
243 Property Rights document must be followed, or as required to translate it into languages other
244 than English.

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

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