



# Entity Seal Profile of the OASIS Digital Signature Service

2<sup>nd</sup> Committee Draft, 11 September 2006 (wd-07)

**Document identifier:**

oasis-dss-1.0-profiles-eseal-spec-cd-r2

**Location:**

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

**Editor:**

Nick Pope, *individual*

**Contributors:**

John Messing, *American Bar Association*

Dallas Powell, *Individual*

Juan Carlos Cruellas, *Individual*

Trevor Perrin, *individual*

**Abstract:**

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

**Status:**

This is a **Public review Draft** produced by the OASIS Digital Signature Service Technical Committee. Comments may be submitted to the TC by any person by clicking on "Send A Comment" on the TC home page at:

[http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=dss](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss).

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>.

## 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>.....	6
49	4	Profile of Verifying Protocol.....	7
50	4.1	Element <VerifyRequest> .....	7
51	4.1.1	Element <OptionalInputs> .....	7
52	4.1.2	Element <SignatureObject>.....	7
53	4.1.3	Element <InputDocuments> .....	7
54	4.2	Element <VerifyResponse> .....	7
55	4.2.1	Element <Result> .....	7
56	4.2.2	Element <OptionalOutputs> .....	7
57	5	Profile of ESeal Signatures .....	8
58	6	Server Processing Rules .....	9
59	6.1	Sign .....	9
60	6.2	Verify .....	9
61	7	Editorial Issues.....	<b>Error! Bookmark not defined.</b>
62	8	References.....	10
63	8.1	Normative .....	10

64	Appendix A. Revision History .....	11
65	Appendix B. Notices .....	12
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> MUST be supported by the DSS server. This MAY be sent  
127 by the client to provide the claimed identity of the requester. If present the <Name>  
128 element of <dss:ClaimedIdentity> MUST be authenticated by the Security Binding.
- 129 • <dss:SignedProperties> MAY be supported by the DSS server. If present this  
130 MAY be used by the client to request the CommitmentTypeIndication property. The  
131 CommitmentTypeIndication property is requested using the identifier and value as  
132 defined in [DSS-XAdES].

133

#### 134 3.1.2 Element <InputDocuments>

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

- 136 • <dss:DocumentHash>
- 137 • <dss:TransformedData>

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

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

### 142 3.2 Element <SignResponse>

#### 143 3.2.1 Element <Result>

144 This profile defines no additional <ResultMinor> codes.

#### 145 3.2.2 Element <OptionalOutputs>

146 This profile requires no optional options.

#### 147 3.2.3 Element <SignatureObject>

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

---

150 **4 Profile of Verifying Protocol**

151 **4.1 Element <VerifyRequest>**

152 **4.1.1 Element <OptionalInputs>**

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

154 **4.1.2 Element <SignatureObject>**

155 The server MUST support <ds:Signature>.

156 **4.1.3 Element <InputDocuments>**

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

- 158     • <dss:DocumentHash>  
159     • <dss:TransformedData>

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

162 **4.2 Element <VerifyResponse>**

163 **4.2.1 Element <Result>**

164 This profile defines no additional <ResultMinor> codes.

165 **4.2.2 Element <OptionalOutputs>**

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

---

## 167 5 Profile of ESeal Signatures

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

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

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

- 173 • `<xades:SigningTime>`

174 In addition, the following may be present:

- 175 • `<xades:CommitmentTypeIndication>`

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

- 177 • `<dss:RequesterIdentity>`

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



---

180 **6 Server Processing Rules**

181 **6.1 Sign**

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

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

186 **6.2 Verify**

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

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

190

## 7 References

191

### 7.1 Normative

192

[Core-XSD]

T. Perrin et al. *DSS Schema*. OASIS, (MONTH/YEAR TBD)

193

[DSSCore]

T. Perrin et al. *Digital Signature Service Core Protocols and Elements*. OASIS, (MONTH/YEAR TBD)

194

[DSS-XAdES]

Juan Carlos Cruellas et al. *XAdES Profile of the OASIS Digital Signature Service*

195

[RFC 2119]

S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2396, August 1998.

196

197

198

199

<http://www.ietf.org/rfc/rfc2396.txt>.

200

[XAdES]

XML Advanced Electronic Signatures ETSI TS 101 903, February 2002 (*shortly to be re-issued*)

201

202

[http://pda.etsi.org/pda/home.asp?wki\\_id=1UFEyx7ORuBCDGED3liJH](http://pda.etsi.org/pda/home.asp?wki_id=1UFEyx7ORuBCDGED3liJH)

203

[XML-ns]

T. Bray, D. Hollander, A. Layman. *Namespaces in XML*. W3C Recommendation, January 1999.

204

205

<http://www.w3.org/TR/1999/REC-xml-names-19990114>

206

[XMLSig]

D. Eastlake et al. *XML-Signature Syntax and Processing*. W3C Recommendation, February 2002.

207

208

<http://www.w3.org/TR/1999/REC-xml-names-19990114>

209

210

211

212

213

214

•

---

## 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
wd-06 / cd-01	2004-12-24	Nick Pope	CD text
wd-07	2006-06-12	Nick Pope	Revised to align with Core cd-r03. Uses TransformedData instead of Document

---

## Appendix B. Notices

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

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

229 Copyright © OASIS Open 2006. *All Rights Reserved.*

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

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

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