



# Entity Seal Profile of the OASIS Digital Signature Service

## Committee Specification

13 February 2007

### This Version:

<http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-eseal-spec-cs-v0.1-r1.html>

<http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-eseal-spec-cs-v0.1-r1.pdf>

### Latest Version:

<http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-eseal-spec-cs-v0.1-r1.html>

<http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-eseal-spec-cs-v0.1-r1.pdf>

### Technical Committee:

OASIS Digital Signature Services TC

### Chair(s):

Nick Pope, Thales eSecurity

Juan Carlos Cruellas, Centre d'aplicacions avançades d'Internet (UPC)

### Editor:

Nick Pope, Thales eSecurity

### Abstract:

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

### Status:

This document was last revised or approved by the OASIS Digital Signature Services TC on the above date. The level of approval is also listed above. Check the current location noted above for possible later revisions of this document. This document is updated periodically on no particular schedule.

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>.

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/ipr.php>).

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

---

## Notices

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

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

50 Copyright © OASIS® 1993–2007. All Rights Reserved. OASIS trademark, IPR and other policies  
51 apply.

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

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

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

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

## Table of Contents

|     |       |                                       |    |
|-----|-------|---------------------------------------|----|
| 74  | 1     | Introduction .....                    | 4  |
| 75  | 1.1   | Terminology.....                      | 4  |
| 76  | 1.2   | Namespaces .....                      | 4  |
| 77  | 1.3   | Normative References .....            | 4  |
| 78  | 2     | Profile Features.....                 | 6  |
| 79  | 2.1   | Identifier.....                       | 6  |
| 80  | 2.2   | Scope .....                           | 6  |
| 81  | 2.3   | Relationship To Other Profiles .....  | 6  |
| 82  | 2.4   | Signature Object.....                 | 6  |
| 83  | 2.5   | Transport Binding.....                | 6  |
| 84  | 2.6   | Security Binding .....                | 6  |
| 85  | 2.6.1 | Security Requirements.....            | 6  |
| 86  | 2.6.2 | TLS X.509 Mutual Authentication ..... | 6  |
| 87  | 3     | Profile of Signing Protocol.....      | 7  |
| 88  | 3.1   | Element <SignRequest> .....           | 7  |
| 89  | 3.1.1 | Element <OptionalInputs> .....        | 7  |
| 90  | 3.1.2 | Element <InputDocuments> .....        | 7  |
| 91  | 3.2   | Element <SignResponse> .....          | 7  |
| 92  | 3.2.1 | Element <Result> .....                | 7  |
| 93  | 3.2.2 | Element <OptionalOutputs> .....       | 7  |
| 94  | 3.2.3 | Element <SignatureObject>.....        | 7  |
| 95  | 4     | Profile of Verifying Protocol.....    | 8  |
| 96  | 4.1   | Element <VerifyRequest> .....         | 8  |
| 97  | 4.1.1 | Element <OptionalInputs> .....        | 8  |
| 98  | 4.1.2 | Element <SignatureObject>.....        | 8  |
| 99  | 4.1.3 | Element <InputDocuments> .....        | 8  |
| 100 | 4.2   | Element <VerifyResponse> .....        | 8  |
| 101 | 4.2.1 | Element <Result> .....                | 8  |
| 102 | 4.2.2 | Element <OptionalOutputs> .....       | 8  |
| 103 | 5     | Profile of ESeal Signatures.....      | 9  |
| 104 | 6     | Server Processing Rules .....         | 10 |
| 105 | 6.1   | Sign .....                            | 10 |
| 106 | 6.2   | Verify .....                          | 10 |
| 107 | A.    | Acknowledgements.....                 | 11 |
| 108 |       |                                       |    |

---

## 109 1 Introduction

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

114 The seal is a form of electronic signature which:

- 115 a) protects the integrity of the document,
- 116 b) includes the time at which the seal was applied proving that the data existed at the given  
117 time,
- 118 c) includes the identity of the entity requesting the seal,
- 119 d) may include a statement of intent for applying the seal.

120 This profile includes a few options that require further profiling for implementing interoperable  
121 systems.

### 122 1.1 Terminology

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

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

### 131 1.2 Namespaces

132 Conventional XML namespace prefixes are used in this document:

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

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

### 140 1.3 Normative References

- |     |                    |   |
|-----|--------------------|---|
| 141 | <b>[Core-XSD]</b>  | S. Drees et al. <i>DSS Schema</i> . OASIS, February, 2007   |
| 142 | <b>[DSSCore]</b>   | S. Drees et al. <i>Digital Signature Service Core Protocols and Elements</i> .<br>143 OASIS, February, 2007   |
| 144 | <b>[DSS-XAdES]</b> | Juan Carlos Cruellas et al. <i>XAdES Profile of the OASIS Digital Signature<br/>145 Service</i>   |
| 146 | <b>[RFC 2119]</b>  | S. Bradner. <i>Key words for use in RFCs to Indicate Requirement Levels</i> .<br>147 IETF RFC 2396, August 1998.<br>148 <a href="http://www.ietf.org/rfc/rfc2396.txt">http://www.ietf.org/rfc/rfc2396.txt</a> . |
| 149 | <b>[XAdES]</b>     | XML Advanced Electronic Signatures ETSI TS 101 903, February 2002<br>150 ( <i>shortly to be re-issued</i> )   |

151 [http://pda.etsi.org/pda/home.asp?wki\\_id=1UFEyx7ORuBCDGED3liJH](http://pda.etsi.org/pda/home.asp?wki_id=1UFEyx7ORuBCDGED3liJH)  
152 **[XML-ns]** T. Bray, D. Hollander, A. Layman. *Namespaces in XML*. W3C  
153 Recommendation, January 1999.  
154 <http://www.w3.org/TR/1999/REC-xml-names-19990114>  
155 **[XMLSig]** D. Eastlake et al. *XML-Signature Syntax and Processing*. W3C  
156 Recommendation, February 2002.  
157 <http://www.w3.org/TR/1999/REC-xml-names-19990114>  
158  
159

---

## 160 2 Profile Features

### 161 2.1 Identifier

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

### 163 2.2 Scope

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

### 167 2.3 Relationship To Other Profiles

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

### 169 2.4 Signature Object

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

### 171 2.5 Transport Binding

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

### 173 2.6 Security Binding

#### 174 2.6.1 Security Requirements

175 This profile MUST use security bindings that:

- 176 • Authenticates the requester to the DSS server
- 177 • Authenticates the DSS server to the DSS client
- 178 • Protects the integrity of a request, response and the association of response to the  
179 request.
- 180 • Optionally, protects the confidentiality of a request and response

181 The following is recommended to meet these requirements..

#### 182 2.6.2 TLS X.509 Mutual Authentication

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

---

## 184 3 Profile of Signing Protocol

### 185 3.1 Element <SignRequest>

#### 186 3.1.1 Element <OptionalInputs>

187 The optional inputs from [DSSCore]:

- 188 • <dss:ClaimedIdentity> MUST be supported by the DSS server. This MAY be sent  
189 by the client to provide the claimed identity of the requester. If present the <Name>  
190 element of <dss:ClaimedIdentity> MUST be authenticated by the Security Binding.
- 191 • <dss:SignedProperties> MAY be supported by the DSS server. If present this  
192 MAY be used by the client to request the CommitmentTypeIndication property. The  
193 CommitmentTypeIndication property is requested using the identifier and value as  
194 defined in [DSS-XAdES].

195

#### 196 3.1.2 Element <InputDocuments>

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

- 198 • <dss:DocumentHash>
- 199 • <dss:TransformedData>

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

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

### 204 3.2 Element <SignResponse>

#### 205 3.2.1 Element <Result>

206 This profile defines no additional <ResultMinor> codes.

#### 207 3.2.2 Element <OptionalOutputs>

208 This profile requires no optional options.

#### 209 3.2.3 Element <SignatureObject>

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

---

212 **4 Profile of Verifying Protocol**

213 **4.1 Element <VerifyRequest>**

214 **4.1.1 Element <OptionalInputs>**

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

216 **4.1.2 Element <SignatureObject>**

217 The server MUST support <ds:Signature>.

218 **4.1.3 Element <InputDocuments>**

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

- 220
- <dss:DocumentHash>
  - <dss:TransformedData>
- 221

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

224 **4.2 Element <VerifyResponse>**

225 **4.2.1 Element <Result>**

226 This profile defines no additional <ResultMinor> codes.

227 **4.2.2 Element <OptionalOutputs>**

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



---

229 **5 Profile of ESeal Signatures**

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

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

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

- 235
- `<xades:SigningTime>`

236 In addition, the following may be present:

- 237
- `<xades:CommitmentTypeIndication>`

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

- 239
- `<dss:RequesterIdentity>`

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

---

242 **6 Server Processing Rules**

243 **6.1 Sign**

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

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

248 **6.2 Verify**

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

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

251

---

252 **A. Acknowledgements**

253 The following individuals have participated in the creation of this specification and are gratefully  
254 acknowledged:

255 **Participants:**

256 John Messing, *American Bar Association*

257 Dallas Powell, *Individual*

258 Juan Carlos Cruellas, *Individual*

259 Trevor Perrin, *individual*

260