



XML Timestamping Profile of the OASIS Digital Signature Services

Working Draft 06 (Committee Draft), 28 June 2004

Document identifier:

oasis-dss-1.0-profiles-timestamping-spec-wd-06

Location:

<http://www.oasis-open.org/committees/dss>

Editor:

Trevor Perrin, *individual* <trevp@trevp.net>

Contributors:

Dimitri Andivahis, Surety
Juan Carlos Cruellas, *individual*
Frederick Hirsch, Nokia
Pieter Kasselmann, Betrusted
Andreas Kuehne, *individual*
Paul Madsen, Entrust
John Messing, American Bar Association
Tim Moses, Entrust
Nick Pope, *individual*
Rich Salz, DataPower
Ed Shallow, Universal Postal Union

Abstract:

This document profiles the OASIS DSS core protocols for the purpose of creating and verifying XML-encoded time-stamps.

Status:

This is a **Committee Draft** produced by the OASIS Digital Signature Service Technical Committee. Committee members should send comments on this draft to dss@lists.oasis-open.org.

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>.

34 **Table of Contents**

35 1 Introduction 3
36 1.1 Notation 3
37 1.2 Namespaces 3
38 2 Profile Features..... 4
39 2.1 Identifier..... 4
40 2.2 Scope 4
41 2.3 Relationship To Other Profiles 4
42 2.4 Signature Object..... 4
43 2.5 Transport Binding..... 4
44 2.6 Security Binding 4
45 3 Profile of Signing Protocol..... 5
46 3.1 Element <SignRequest> 5
47 3.1.1 Element <OptionalInputs> 5
48 3.1.2 Element <InputDocuments> 5
49 3.2 Element <SignResponse> 5
50 3.2.1 Element <Result> 5
51 3.2.2 Element <OptionalOutputs> 5
52 3.2.3 Element <SignatureObject>..... 5
53 4 Profile of Verifying Protocol..... 6
54 4.1 Element <VerifyRequest> 6
55 4.1.1 Element <OptionalInputs> 6
56 4.1.2 Element <SignatureObject>..... 6
57 4.1.3 Element <InputDocuments> 6
58 4.2 Element <VerifyResponse> 6
59 4.2.1 Element <Result> 6
60 4.2.2 Element <OptionalOutputs> 6
61 5 Editorial Issues..... 7
62 6 References..... 8
63 6.1 Normative 8
64 Appendix A. Revision History 9
65 Appendix B. Notices 10
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 these
70 protocols to limit their flexibility and extend them in concrete ways. The resulting profile is
71 suitable for implementation and interoperability.

72 The following sections describe how to understand the rest of this document.

73 1.1 Notation

74 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”,
75 “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this specification are to be
76 interpreted as described in IETF RFC 2119 **[RFC 2119]**. These keywords are capitalized when
77 used to unambiguously specify requirements over protocol features and behavior that affect the
78 interoperability and security of implementations. When these words are not capitalized, they are
79 meant in their natural-language sense.

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

82 1.2 Namespaces

83 Conventional XML namespace prefixes are used in this document:

- 84 • The prefix `dss:` stands for the DSS core namespace **[Core-XSD]**.

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

88

89 2 Profile Features

90 2.1 Identifier

91 urn:oasis:names:tc:dss:1.0:profiles:timestamping

92 2.2 Scope

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

94 2.3 Relationship To Other Profiles

95 This profile is based directly on the [DSSCore].

96 2.4 Signature Object

97 This profile supports the creation and verification of `<dss:Timestamp>` elements as defined in
98 [DSSCore]. These elements can wrap different types of time-stamp tokens; this profile does not
99 specify or constrain the internal structure of the `<dss:Timestamp>`, unless the
100 `<dss:SignatureType>` optional input is used (see section 3.1.1).

101 2.5 Transport Binding

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

103 2.6 Security Binding

104 This profile is secured using the TLS X.509 Server Authentication Binding defined in [DSSCore].

105

106

107 3 Profile of Signing Protocol

108 3.1 Element <SignRequest>

109 3.1.1 Element <OptionalInputs>

110 The <dss:SignatureType> optional input from [DSSCore] is supported and may be sent by
111 the client. No other optional inputs are supported.

112 The <dss:SignatureType> optional input may be one of these values, from section 7.2 of
113 [DSSCore]:

114 - oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken

115 - urn:ietf:rfc:3161

116 Servers may support other values. However, servers are under no obligation to support *any*
117 particular values. Thus, clients using the <dss:SignatureType> optional input may not
118 interoperate with certain servers.

119 3.1.2 Element <InputDocuments>

120 The client MUST only send <dss:DocumentHash> input documents. The client MUST NOT
121 send <dss:Document> input documents.

122 If the client is not sending the <dss:SignatureType> optional input, then the client SHOULD
123 only send a single input document, since some types of time-stamps (e.g. RFC 3161) can only
124 cover one document per time-stamp.

125 If the client *is* sending the <dss:SignatureType> optional input, then the client MAY send
126 multiple input documents, if the client knows that the specified time-stamp type can handle them.

127 3.2 Element <SignResponse>

128 3.2.1 Element <Result>

129 This profile defines no additional <ResultMinor> codes.

130 3.2.2 Element <OptionalOutputs>

131 The server MUST NOT return any optional outputs.

132 3.2.3 Element <SignatureObject>

133 The server MUST return a <dss:Timestamp> signature object.

134 **4 Profile of Verifying Protocol**

135 **4.1 Element <VerifyRequest>**

136 **4.1.1 Element <OptionalInputs>**

137 The client MUST NOT send any optional inputs.

138 **4.1.2 Element <SignatureObject>**

139 The client MUST send a `<dss:Timestamp>` signature object.

140 **4.1.3 Element <InputDocuments>**

141 The client MUST only send `<dss:DocumentHash>` input documents. The client MUST NOT
142 send `<dss:Document>` input documents.

143 **4.2 Element <VerifyResponse>**

144 **4.2.1 Element <Result>**

145 This profile defines no additional `<dss:ResultMinor>` codes.

146 **4.2.2 Element <OptionalOutputs>**

147 The server MUST return the `<dss:SigningTime>` optional output, as defined in [DSSCore],
148 with its `ThirdPartyTimestamp` attribute set to `False`. The `<dss:SigningTime>` output will
149 indicate when the time-stamp was performed.

150 The server MUST NOT return any other optional outputs.

151 5 Editorial Issues

152 1) What type of signature object should be supported? An <XMLTimeStampToken> (like
153 now) or a more generic <Timestamp>?

154 **This profile supports a generic Timestamp; a profile of this profile could make it more**
155 **specific.**

156 2) What bindings should be used? A SOAP binding (like now) or a simple HTTP POST
157 binding?

158 **We're referencing an HTTP POST binding, for now.**

159 3) Are the clients required to verify received timestamps? Does this eliminate the need for
160 an authenticated binding in the signing profile?

161 **Right now it says no.**

162 **6 References**

163 **6.1 Normative**

- 164 **[Core-XSD]** T. Perrin et al. *DSS Schema*. OASIS, **(MONTH/YEAR TBD)**
- 165 **[DSSCore]** T. Perrin et al. *Digital Signature Service Core Protocols and Elements*.
166 OASIS, **(MONTH/YEAR TBD)**
- 167 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*.
168 IETF RFC 2396, August 1998.
169 <http://www.ietf.org/rfc/rfc2396.txt>.
- 170 **[XML-ns]** T. Bray, D. Hollander, A. Layman. *Namespaces in XML*. W3C
171 Recommendation, January 1999.
172 <http://www.w3.org/TR/1999/REC-xml-names-19990114>
- 173 **[XMLSig]** D. Eastlake et al. *XML-Signature Syntax and Processing*. W3C
174 Recommendation, February 2002.
175 <http://www.w3.org/TR/1999/REC-xml-names-19990114>
176
177
178
179
180

Appendix A. Revision History

Rev	Date	By Whom	What
wd-01	2004-01-06	Trevor Perrin	Initial version
wd-02	2004-01-20	Trevor Perrin	Added "Type of Signature Object" section, and editorial issues 1-3; organized references
wd-03	2004-02-03	Trevor Perrin	Reorganized; based around <dss:Timestamp> instead of XMLTimeStampToken.
Wd-04	2004-02-29	Trevor Perrin	Changed Verify Response to use <SigningTime> optional output.
Wd-06	2004-06-28	Trevor Perrin	Mentioned as committee draft

Appendix B. Notices

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

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

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

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

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

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