



Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)

Errata 1.0

Committee Draft 200512, December 2005

Document identifier:

{WSS: SOAP Message Security }-{1.0} (Word) (PDF)

Document Location:

<http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0-errata-004>

Errata Location:

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

Editors:

Anthony	Nadalin	IBM
Chris	Kaler	Microsoft
Phillip	Hallam-Baker	VeriSign
Ronald	Monzillo	Sun

Contributors:

Gene	Thurston	AmberPoint
Frank	Siebenlist	Argonne National Lab
Merlin	Hughes	Baltimore Technologies
Irving	Reid	Baltimore Technologies
Peter	Dapkus	BEA
Hal	Lockhart	BEA
Symon	Chang	CommerceOne
Srinivas	Davanum	Computer Associates
Thomas	DeMartini	ContentGuard
Guillermo	Lao	ContentGuard
TJ	Pannu	ContentGuard
Shawn	Sharp	Cyclone Commerce
Ganesh	Vaideswaran	Documentum

Sam	Wei	Documentum
John	Hughes	Entegrity
Tim	Moses	Entrust
Toshihiro	Nishimura	Fujitsu
Tom	Rutt	Fujitsu
Yutaka	Kudo	Hitachi
Jason	Rouault	HP
Paula	Austel	IBM
Bob	Blakley	IBM
Joel	Farrell	IBM
Satoshi	Hada	IBM
Maryann	Hondo	IBM
Michael	McIntosh	IBM
Hiroshi	Maruyama	IBM
David	Melgar	IBM
Anthony	Nadalin	IBM
Nataraj	Nagaratnam	IBM
Wayne	Vicknair	IBM
Kelvin	Lawrence	IBM (co-Chair)
Don	Flinn	Individual
Bob	Morgan	Individual
Bob	Atkinson	Microsoft
Keith	Ballinger	Microsoft
Allen	Brown	Microsoft
Paul	Cotton	Microsoft
Giovanni	Della-Libera	Microsoft
Vijay	Gajjala	Microsoft
Johannes	Klein	Microsoft
Scott	Konersmann	Microsoft
Chris	Kurt	Microsoft
Brian	LaMacchia	Microsoft
Paul	Leach	Microsoft
John	Manferdelli	Microsoft
John	Shewchuk	Microsoft
Dan	Simon	Microsoft
Hervey	Wilson	Microsoft
Chris	Kaler	Microsoft (co-Chair)
Prateek	Mishra	Netegrity
Frederick	Hirsch	Nokia
Senthil	Sengodan	Nokia
Lloyd	Burch	Novell
Ed	Reed	Novell
Charles	Knouse	Oblix
Steve	Anderson	OpenNetwork (Sec)
Vipin	Samar	Oracle
Jerry	Schwarz	Oracle
Eric	Gravengaard	Reactivity
Stuart	King	Reed Elsevier
Andrew	Nash	RSA Security
Rob	Philpott	RSA Security
Peter	Rostin	RSA Security

Martijn	de Boer	SAP
Blake	Dournaee	Sarvega
Pete	Wenzel	SeeBeyond
Jonathan	Tourzan	Sony
Yassir	Elley	Sun Microsystems
Jeff	Hodges	Sun Microsystems
Ronald	Monzillo	Sun Microsystems
Jan	Alexander	Systinet
Michael	Nguyen	The IDA of Singapore
Don	Adams	TIBCO
John	Weiland	US Navy
Phillip	Hallam-Baker	VeriSign
Mark	Hays	Verisign
Hemma	Prafullchandra	VeriSign

17

Abstract:

18

19

20

This document contains a list of errata against WSS OASIS Standard Version 1.0 that have been approved by the WSS Technical Committee.

Status:

21

22

23

24

25

26

27

28

29

30

31

32

This version of the errata is a working draft of the committee. As such, it may change prior to incorporation into a future OASIS Standard. Please send comments to the editors. If you are on the wss@lists.oasis-open.org list for committee members, send comments there. If you are not on that list, subscribe to the wss-comment@lists.oasis-open.org list and send comments there. To subscribe, send an email message to wss-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message. For patent disclosure information that may be essential to the implementation of this specification, and any offers of licensing terms, refer to the Intellectual Property Rights section of the OASIS Web Services Security Technical Committee (WSS TC) web page at <http://www.oasis-open.org/committees/wss/ipr.php>. General OASIS IPR information can be found at <http://www.oasis-open.org/who/intellectualproperty.shtml>.

33

34 Table of Contents

35	1	Issues Addressed	5
36	2	Typographical Errors.....	6
37	2.1	Section 7.1 SecurityTokenReference Element	6
38	3	Normative Errors.....	7
39	3.1	Section 2.2 Namespaces	7
40	3.2	Section 4.2 Id Schema	7
41	3.3	Section 5 Security Header	7
42	3.4	Section 7.1 SecurityTokenReference Element	7
43	3.5	Section 7.2 KeyIdentifiers	7
44	3.6	Section 7.3 Key Identifiers	8
45	3.7	Section 7.4 Embedded Reference	8
46	3.8	Section 8.1 Algorithms	8
47	3.9	Section 8.3 Signing Tokens	8
48	4	Non-Normative Errors	9
49	4.1	Section 3.4 Examples	9
50	4.2	Section 6.2.1 Username.....	9
51	4.3	Section 6.3.2 Encoding Binary Security Tokens	9
52	4.4	Section 7.3 Key Identifiers	9
53	4.5	Section 8.3 Signing Tokens	10
54	4.6	Section 11 Extended Example	10
55	5	Clarifications	11
56	5.1	Section 8.3 Signing Tokens	11
57		Appendix A: Revision History	12
58		Appendix B: Notices	13

59

60
61
62

1 Issues Addressed

The following issues have been addressed in this document:

ISSUE	DESCRIPTION
327	Timestamp ValueType needs to be clarified
328	Errata on STR transform
256	STR attributes are not protected
264	Post review period comments: Errors in WSS core and username/x.509 profile examples.
290	Inconsistency in the KeyIdentifier encoding type default between core and SAML
444	Request to remove the WS-Security 1.0 errata from WSS page or fix it

63 **2 Typographical Errors**

64 **2.1 Section 7.1 SecurityTokenReference Element**

65 Delete the following line (652):

66 This optional attribute is used to type the usage of the `<wsse:SecurityToken>`.
67 and replace it with:

68 This optional attribute is used to type the usage of the
69 `<wsse:SecurityTokenReference>`.

70 3 Normative Errors

71 3.1 Section 2.2 Namespaces

72 Delete lines 185-188:
73 <http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd>
74
75 <http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd>
76 and replace it with:
77 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd>
78 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd>
79
80 Add the following after line 198:
81 Notice – The schema <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd> MUST be updated, the update is to change the reference
82 <http://www.w3.org/TR/xmlldsig-core/xmlldsig-core-schema.xsd> to
83 <http://www.w3.org/TR/2002/REC-xmlldsig-core-20020212/xmlldsig-core-schema.xsd>
84
85
86 URI fragments defined in WSS: SOAP Message Security 1.0 are relative to a base URI of
87 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0>
88

89 3.2 Section 4.2 Id Schema

90 Delete line 421:
91 namespace} is "<http://www.w3.org/2001/XMLSchema>" and which {name} is "Id."
92 and replace it with:
93 namespace} is "<http://www.w3.org/2001/XMLSchema>" and which {type} is "ID."

94 3.3 Section 5 Security Header

95 Delete the line 495:
96 The receiver must generate a fault if unable to interpret or process security tokens
97 and replace it with:
98 The receiver MUST generate a fault if unable to interpret or process security tokens

99 3.4 Section 7.1 SecurityTokenReference Element

100 Delete line 634:
101 If a <wss:SecurityTokenReference> is used outside of the <wss:Security> header
102 and replace it with:
103 If a <wss:SecurityTokenReference> is used outside of the security header processing

104 3.5 Section 7.2 KeyIdentifiers

105 Add after line 735:
106 The <wss:KeyIdentifier> element is only allowed inside a
107 <wss:SecurityTokenReference> element.

108 **3.6 Section 7.3 Key Identifiers**

109 Delete table at line 761

URI	Description
#Base64Binary	XML Schema base 64 encoding (default)

110

111 And replace with

URI	Description
#Base64Binary	XML Schema base 64 encoding

112

113 Delete the following line

114 “encoded. For example, a hash value may be encoded using base 64 encoding (the
115 default).”

116 and replace it with

117 “encoded. For example, a hash value may be encoded using base 64 encoding”.

118

119

120 **3.7 Section 7.4 Embedded Reference**

121 Schema shows ValueType attribute but no wsu:Id attribute in the schema. The
122 ValueType should be replaced with a wsu:Id.

123

124 Add after line 769:

125 The <wsse:Embedded> element is only allowed inside a
126 <wsse:SecurityTokenReference> element.

127 **3.8 Section 8.1 Algorithms**

128 Delete URI in table (line 863):

129 <http://www.w3.org/TR/2003/NOTE-soap12-n11n-20030328/>

130 and replace it with:

131 <http://www.w3.org/TR/soap12-n11n/>

132 **3.9 Section 8.3 Signing Tokens**

133 Delete lines 1293 and 1294

134 “instants that specify leap seconds. If, however, other time types are used, then the
135 ValueType attribute (described below) MUST be specified to indicate the data type of
136 the time format.”

137 and replace it with

138 “instants that specify leap seconds.”

139 4 Non-Normative Errors

140 4.1 Section 3.4 Examples

141 Delete lines 305-308:

```
142 (005) <xxx:CustomToken wsu:Id="MyID"  
143         xmlns:xxx="http://fabrikam123/token">  
144 (006)     FHUIORv...  
145 (007) </xxx:CustomToken>
```

146 and replace it with:

```
147 (005) <wsse:BinarySecurityToken ValueType="  
148 http://fabrikam123#CustomToken "  
149     EncodingType="...#Base64Binary" wsu:Id=" MyID ">  
150 (006)     FHUIORv...  
151 (007) </wsse:BinarySecurityToken>
```

152 4.2 Section 6.2.1 Username

153 Delete line 532:

154 A string label for this security token.

155 and replace it with:

156 A string label for this security token. The wsu:Id allow for an open attribute model.

157 4.3 Section 6.3.2 Encoding Binary Security Tokens

158 Delete the following lines (606-612):

159 When a <wsse:BinarySecurityToken> is included in a signature—that is, it is referenced
160 from a <ds:Signature> element—care should be taken so that the canonicalization
161 algorithm (e.g., Exclusive XML Canonicalization [EXC-C14N]) does not allow
162 unauthorized replacement of namespace prefixes of the QNames used in the attribute or
163 element values. In particular, it is RECOMMENDED that these namespace prefixes be
164 declared within the <wsse:BinarySecurityToken> element if this token does not carry the
165 validating key (and consequently it is not cryptographically bound to the signature).

166
167 No replacement text is needed. QNames have been replaced by URIs.

168 4.4 Section 7.3 Key Identifiers

169 Delete the following line (757-760):

170 *“/wsse:SecurityTokenReference/wsse:KeyIdentifier/@EncodingType*

171 The optional `EncodingType` attribute is used to indicate, using a URI, the
172 encoding format of the `KeyIdentifier` (`#Base64Binary`). The base values
173 defined in this specification are used (Note that URI fragments are relative to this
174 document's URI):”

175 and replace it with:

176 *“/wsse:SecurityTokenReference/wsse:KeyIdentifier/@EncodingType*

177 The optional `EncodingType` attribute is used to indicate, using a URI, the
178 encoding format of the `KeyIdentifier` (`#Base64Binary`). This specification
179 defines the `EncodingType` URI values appearing in the following table. A token
180 specific profile MAY define additional token specific `EncodingType` URI values. A

181 KeyIdentifier MUST include an EncodingType attribute when its ValueType is not
182 sufficient to identify its encoding type."
183

184 4.5 Section 8.3 Signing Tokens

185 Delete the following lines (1034-1036)"
186 "The transform takes a single mandatory parameter, a <ds:CanonicalizationMethod>
187 element, which is used to serialize the input node set."
188 and replace it with:
189 "The transform takes a single mandatory parameter, a <ds:CanonicalizationMethod>
190 element, which is used to serialize the output node set."

191 4.6 Section 11 Extended Example

192 Delete lines 1392-1396

```
193 (015) <ds:KeyInfo>  
194 (016) <wsse:KeyIdentifier  
195 EncodingType="...#Base64Binary"  
196 ValueType="...#X509v3">MIGfMa0GCSq...  
197 (017) </wsse:KeyIdentifier>  
198 (018) </ds:KeyInfo>
```

199 and replace it with

```
200 (015) <ds:KeyInfo>  
201 <wsse:SecurityTokenReference>  
202 (016) <wsse:KeyIdentifier  
203 EncodingType="...#Base64Binary"  
204 ValueType="...#X509v3">MIGfMa0GCSq...  
205 (017) </wsse:KeyIdentifier>  
206 </wsse:SecurityTokenReferenece>  
207 (018) </ds:KeyInfo>
```

208

5 Clarifications

209

5.1 Section 8.3 Signing Tokens

210

211

212

213

214

215

216

217

Signing a SecurityTokenReference (STR) provides authentication and integrity protection of only the STR and not the referenced security token (ST). If signing the ST is the intended behavior, the STR Dereference Transform (STRDT) may be used which replaces the STR with the ST for digest computation, effectively protecting the ST and not the STR. If protecting both the ST and the STR is desired, you may sign the STR twice, once using the STRDT and once not using the STRDT.

The following table lists the full URI for each URI fragment referred to in the specification.

URI Fragment	Full URI
#Base64Binary	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary
#STR-Transform	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#STR-Transform
#X509	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509

218

Appendix A: Revision History

Rev	Date	What
1	06/25/04	First Draft of Errata
2	07/06/04	Updated per comments on list
3	09/19/04	Updated per comments on list
4	10/01/04	Updated per comments on list
5	12/07/05	Issue 444

219

220

This section is non-normative.

221

Appendix B: Notices

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

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

234 Copyright © OASIS Open 2002-2005. *All Rights Reserved.*

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

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

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

251

252 This section is non-normative.