



Web Services Security: SOAP Message Security 1.0 (WS-Security 2004) Errata 1.0 Committee Draft 200401, October 2004

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 | Obliv |
| 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 |

16

17 **Abstract:**

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

20 **Status:**

21 This version of the errata is a working draft of the committee. As such, it may change
 22 prior to incorporation into a future OASIS Standard. Please send comments to the
 23 editors. If you are on the wss@lists.oasis-open.org list for committee members, send
 24 comments there. If you are not on that list, subscribe to the wss-comment@lists.oasis-open.org
 25 list and send comments there. To subscribe, send an email message to wss-comment-request@lists.oasis-open.org
 26 with the word "subscribe" as the body of the message. For patent disclosure information that may be essential to the implementation
 27 of this specification, and any offers of licensing terms, refer to the Intellectual Property
 28 Rights section of the OASIS Web Services Security Technical Committee (WSS TC) web
 29 page at <http://www.oasis-open.org/committees/wss/ipr.php>. General OASIS IPR
 30 information can be found at <http://www.oasis-open.org/who/intellectualproperty.shtml>.
 31

32

33 Table of Contents

| | | | |
|----|-----|---|----|
| 34 | 1 | Issues Addressed | 5 |
| 35 | 2 | Typographical Errors..... | 6 |
| 36 | 2.1 | Section 7.1 SecurityTokenReference Element | 6 |
| 37 | 3 | Normative Errors..... | 7 |
| 38 | 3.1 | Section 2.2 Namespaces | 7 |
| 39 | 3.2 | Section 4.2 Id Schema | 7 |
| 40 | 3.3 | Section 5 Security Header | 7 |
| 41 | 3.4 | Section 7.1 SecurityTokenReference Element | 7 |
| 42 | 3.5 | Section 7.2 KeyIdentifiers | 7 |
| 43 | 3.6 | Section 7.3 Key Identifiers | 7 |
| 44 | 3.7 | Section 7.4 Embedded Reference | 8 |
| 45 | 3.8 | Section 8.1 Algorithms | 8 |
| 46 | 3.9 | Section 8.3 Signing Tokens | 8 |
| 47 | 4 | Non-Normative Errors | 9 |
| 48 | 4.1 | Section 3.4 Examples | 9 |
| 49 | 4.2 | Section 6.2.1 Username..... | 9 |
| 50 | 4.3 | Section 6.3.2 Encoding Binary Security Tokens | 9 |
| 51 | 4.4 | Section 7.3 Key Identifiers | 9 |
| 52 | 4.5 | Section 8.3 Signing Tokens | 10 |
| 53 | 4.6 | Section 11 Extended Example | 10 |
| 54 | 5 | Clarifications | 11 |
| 55 | 5.1 | Section 8.3 Signing Tokens | 11 |
| 56 | | Appendix A: Revision History | 12 |
| 57 | | Appendix B: Notices | 13 |

58

59
60
61

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 |

62 **2 Typographical Errors**

63 **2.1 Section 7.1 SecurityTokenReference Element**

64 Delete the following line (652):

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

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

69 3 Normative Errors

70 3.1 Section 2.2 Namespaces

71 Delete lines 185-188:
72 <http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd>
73
74 <http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd>
75 and replace it with:
76 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd>
77 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd>
78
79 Add the following after line 198:
80 URI fragments defined in WSS: SOAP Message Security 1.0 are relative to a base URI of
81 [http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-](http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0)
82 [message-security-1.0](http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0)

83 3.2 Section 4.2 Id Schema

84 Delete line 421:
85 namespace} is "<http://www.w3.org/2001/XMLSchema>" and which {name} is "Id."
86 and replace it with:
87 namespace} is "<http://www.w3.org/2001/XMLSchema>" and which {type} is "ID."

88 3.3 Section 5 Security Header

89 Delete the line 495:
90 The receiver must generate a fault if unable to interpret or process security tokens
91 and replace it with:
92 The receiver MUST generate a fault if unable to interpret or process security tokens

93 3.4 Section 7.1 SecurityTokenReference Element

94 Delete line 634:
95 If a <wsse:SecurityTokenReference> is used outside of the <wsse:Security> header
96 and replace it with:
97 If a <wsse:SecurityTokenReference> is used outside of the security header processing

98 3.5 Section 7.2 KeyIdentifiers

99 Add after line 735:
100 The <wsse:KeyIdentifier> element is only allowed inside a
101 <wsse:SecurityTokenReference> element.

102 3.6 Section 7.3 Key Identifiers

103 Delete table at line 761

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

104
105

And replace with

| URI | Description |
|---------------|-----------------------------|
| #Base64Binary | XML Schema base 64 encoding |

106
107
108
109
110
111
112
113

Delete the following line

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

and replace it with

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

114

3.7 Section 7.4 Embedded Reference

115
116
117
118
119
120

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

Add after line 769:

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

121

3.8 Section 8.1 Algorithms

122
123
124
125

Delete URI in table (line 863):

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

and replace it with:

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

126

3.9 Section 8.3 Signing Tokens

127
128
129
130
131
132

Delete lines 1293 and 1294

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

and replace it with

“instants that specify leap seconds.”

133

4 Non-Normative Errors

134

4.1 Section 3.4 Examples

135 Delete lines 305-308:

```
136 (005) <xxx:CustomToken wsu:Id="MyID"  
137         xmlns:xxx="http://fabrikam123/token">  
138 (006)     FHUIORv...  
139 (007) </xxx:CustomToken>
```

140 and replace it with:

```
141 (005) <wsse:BinarySecurityToken ValueType="  
142 http://fabrikam123#CustomToken "  
143     EncodingType="...#Base64Binary" wsu:Id=" MyID ">  
144 (006)     FHUIORv...  
145 (007) </wsse:BinarySecurityToken>
```

146

4.2 Section 6.2.1 Username

147

Delete line 532:

148

A string label for this security token.

149

and replace it with:

150

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

151

4.3 Section 6.3.2 Encoding Binary Security Tokens

152

Delete the following lines (606-612):

153

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

154

155

156

157

158

159

160

161

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

162

4.4 Section 7.3 Key Identifiers

163

Delete the following line (757-760):

164

"/wsse:SecurityTokenReference/wsse:KeyIdentifier/@EncodingType

165

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

166

167

168

169

and replace it with:

170

"/wsse:SecurityTokenReference/wsse:KeyIdentifier/@EncodingType

171

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

172

173

174

175 KeyIdentifier MUST include an EncodingType attribute when its ValueType is not
176 sufficient to identify its encoding type."
177

178 4.5 Section 8.3 Signing Tokens

179 Delete the following lines (1034-1036)"
180 "The transform takes a single mandatory parameter, a <ds:CanonicalizationMethod>
181 element, which is used to serialize the input node set."
182 and replace it with:
183 "The transform takes a single mandatory parameter, a <ds:CanonicalizationMethod>
184 element, which is used to serialize the output node set."

185 4.6 Section 11 Extended Example

186 Delete lines 1392-1396

```
187 (015) <ds:KeyInfo>  
188 (016) <wsse:KeyIdentifier  
189 EncodingType="...#Base64Binary"  
190 ValueType="...#X509v3">MIGfMa0GCSq...  
191 (017) </wsse:KeyIdentifier>  
192 (018) </ds:KeyInfo>
```

193 and replace it with

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

202
203
204
205
206
207
208
209
210
211

5 Clarifications

5.1 Section 8.3 Signing Tokens

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 |

212

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 | 0919/04 | Updated per comments on list |
| 4 | 10/01/04 | Updated per comments on list |

213

214

This section is non-normative.

Appendix B: Notices

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

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

228 Copyright © OASIS Open 2002-2004. *All Rights Reserved.*

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

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

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

245

246 This section is non-normative.