



1 2

---

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

---

## Errata 1.0

### OASIS Standard 200401, June 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-001>

#### 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	Vaideeswaran	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

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-  
 25 open.org list and send comments there. To subscribe, send an email message to wss-  
 26 comment-request@lists.oasis-open.org with the word "subscribe" as the body of the  
 27 message. For patent disclosure information that may be essential to the implementation  
 28 of this specification, and any offers of licensing terms, refer to the Intellectual Property  
 29 Rights section of the OASIS Web Services Security Technical Committee (WSS TC) web  
 30 page at <http://www.oasis-open.org/committees/wss/ipr.php>. General OASIS IPR  
 31 information can be found at <http://www.oasis-open.org/who/intellectualproperty.shtml>.

---

32

## 33 Table of Contents

34	1	Typographical Errors.....	4
35	2	Normative Errors.....	5
36	3	Non-Normative Errors .....	6
37	4	Clarifications .....	7
38		Appendix A: Revision History .....	8
39		Appendix B: Notices .....	9

---

40

---

## 41 1 Typographical Errors

42

43 In Section 7.1 SecurityTokenReference Element, delete the following line (652):

44 This optional attribute is used to type the usage of the `<wsse:SecurityToken>`.

45 and replace it with:

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

47

48

49

---

## 2 Normative Errors

50

51

52 In Section 2.2 Namespaces, delete lines 185-188:

53 <http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd>

54 <http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd>

55 and replace it with:

56 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd>

57 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd>

58

59 In Section 2.2 Namespaces, add the following after line 198:

60 URI fragments defined in WSS: SOAP Message Security 1.0 are relative to a base URI of

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

62

63 In Section 4.2 Id Schema, delete the following line (421):

64 namespace} is "<http://www.w3.org/2001/XMLSchema>" and which {name} is "Id."

65 and replace with:

66 namespace} is "<http://www.w3.org/2001/XMLSchema>" and which {type} is "ID."

67

68 In Section 5 Security Header, delete the following line (495):

69 The receiver must generate a fault if unable to interpret or process security tokens

70 and replace with:

71 The receiver MUST generate a fault if unable to interpret or process security tokens

72

73 In Section 7.1 SecurityTokenReference Element, delete line 734:

74 If a `<wsse:SecurityTokenReference>` is used outside of the `<wsse:Security>` header

75 and replace it with:

76 If a `<wsse:SecurityTokenReference>` is used outside of the security header processing

77

78 In Section 7.3 KeyIdentifiers, add after line 735:

79 The `<wsse:KeyIdentifier>` element is only allowed inside a

80 `<wsse:SecurityTokenReference>` element.

81

82 In Section 7.4 Embedded References, schema shows ValueType attribute but no wsu:Id attribute

83 in the schema. The ValueType should be replaced with a wsu:Id.

84

85 In Section 7.4 Embedded References, add after line 769:

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

87 element.

88

89 In Section 8.1 Algorithms, delete URI in table (line 683):

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

91 and replace with:

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

93

94

95

---

## 3 Non-Normative Errors

100

101

102 In Section 3.4 Example, delete the following lines (301-304):

```
103 (005) <xxx:CustomToken wsu:Id="MyID"  
104         xmlns:xxx="http://fabrikam123/token">
```

```
105 (006)     FHUIORv...
```

```
106 (007) </xxx:CustomToken>
```

107 and replace it with:

```
108 (005) <wsse:BinarySecurityToken ValueType=" http://fabrikam123#CustomToken "  
109     EncodingType="...#Base64Binary" wsu:Id=" MyID ">
```

```
110 (006)     FHUIORv...
```

```
111 (007) </wsse:BinarySecurityToken>
```

112

113 In Section 6.2.1 Username, delete line 532:

114 A string label for this security token.

115 and replace it with:

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

117

118 In Section 6.3.2 Encoding Binary Security Tokens, delete the following lines (606-612):

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

126

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

128

129 In Section 11 Extended Example, delete lines 1382-1396

```
130 (015)         <ds:KeyInfo>  
131 (016)                 <wsse:KeyIdentifier  
132                     EncodingType="...#Base64Binary"  
133                     ValueType="...#X509v3">MIGfMa0GCSq...  
134 (017)         </wsse:KeyIdentifier>  
135 (018) </ds:KeyInfo>
```

136 and replace it with

```
137 (015)         <ds:KeyInfo>  
138                 <wsse:SecurityTokenReference>  
139 (016)                 <wsse:KeyIdentifier  
140                     EncodingType="...#Base64Binary"  
141                     ValueType="...#X509v3">MIGfMa0GCSq...  
142 (017)         </wsse:KeyIdentifier>  
143 (018)         </ds:KeyInfo>  
144                 </wsse:SecurityTokenReference>  
145 (019) <xenc:CipherData>
```

146

147

148

---

## 4 Clarifications

149

150 Section 8.3 Signing Tokens

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

157

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

URI Fragment	Full URI
#Base64Binary	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary</a>
#STR-Transform	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#STR-Transform">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#STR-Transform</a>
#X509v3	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3</a>

---

159 **Appendix A: Revision History**

Rev	Date	What
1	06/25/04	First Draft of Errata

160

161 This section is non-normative.

---

## Appendix B: Notices

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

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

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

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

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

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

192

193 This section is non-normative.