



1
2

3 Web Services Security: 4 SOAP Message Security 1.1 5 (WS-Security 2004)

6 **OASIS Errata Committee Draft, 25 August 2006**

7 **OASIS identifier:**

8 wss-v1.1-errata-SOAPMessageSecurity

9 **Location:**

10 <http://docs.oasis-open.org/wss/v1.1/>

11 **Technical Committee:**

12 Web Service Security (WSS)

13 **Chairs:**

14 Kelvin Lawrence, IBM

15 Chris Kaler, Microsoft

16 **Editors:**

17 Anthony Nadalin, IBM

18 **Abstract:**

19 This specification describes enhancements to SOAP messaging to provide message
20 integrity and confidentiality. The specified mechanisms can be used to accommodate a
21 wide variety of security models and encryption technologies.

22
23 This specification also provides a general-purpose mechanism for associating security
24 tokens with message content. No specific type of security token is required, the
25 specification is designed to be extensible (i.e.. support multiple security token formats).
26 For example, a client might provide one format for proof of identity and provide another
27 format for proof that they have a particular business certification.

28
29 Additionally, this specification describes how to encode binary security tokens, a
30 framework for XML-based tokens, and how to include opaque encrypted keys. It also
31 includes extensibility mechanisms that can be used to further describe the characteristics
32 of the tokens that are included with a message.

33 **Status:**

34 This is an **OASIS Draft** listing errata for the **OASIS Standard** produced by the Web
35 Services Security Technical Committee. The standard was approved by the OASIS
36 membership on 1 February 2006.

37

38 Technical Committee members should send comments on this specification to the
39 technical Committee's email list. Others should send comments to the Technical
40 Committee by using the "Send A Comment" button on the Technical Committee's web
41 page at **www.oasisopen.org/committees/wss**.
42

43 For patent disclosure information that may be essential to the implementation of this
44 specification, and any offers of licensing terms, refer to the Intellectual Property Rights
45 section of the OASIS Web Services Security Technical Committee (WSS TC) web page
46 at <http://www.oasis-open.org/committees/wss/ipr.php>. General OASIS IPR information
47 can be found at <http://www.oasis-open.org/who/intellectualproperty.shtml>.

49 Notices

50 OASIS takes no position regarding the validity or scope of any intellectual property or other rights
51 that might be claimed to pertain to the implementation or use of the technology described in this
52 document or the extent to which any license under such rights might or might not be available;
53 neither does it represent that it has made any effort to identify any such rights. Information on
54 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS
55 website. Copies of claims of rights made available for publication and any assurances of licenses
56 to be made available, or the result of an attempt made to obtain a general license or permission
57 for the use of such proprietary rights by implementors or users of this specification, can be
58 obtained from the OASIS Executive Director. OASIS invites any interested party to bring to its
59 attention any copyrights, patents or patent applications, or other proprietary rights which may
60 cover technology that may be required to implement this specification. Please address the
61 information to the OASIS Executive Director.

62

63 Copyright (C) OASIS Open 2002-2006. All Rights Reserved.

64

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

74

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

77

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

83

84 OASIS has been notified of intellectual property rights claimed in regard to some or all of the
85 contents of this specification. For more information consult the online list of claimed rights.

86

87 This section is non-normative.

88 **Table of Contents**

89 1 Issues Addressed 5
90 2 Typographical/Editorial Errors 6
91 2.1 Section 7.2 Direct References 6
92 2.2 Section 7.3 Key Identifiers 6
93 2.3 Section 8.6 Example 6
94 2.4 Section 9.4.4 6
95 2.5 Section 11 Extended Example 6
96 3 Normative Errors..... 7
97 3.1 Section 8.3 Signing Tokens 7
98 3.2 Section 7.3 Key Identifiers 7
99 4 References..... 8
100 Appendix A: Acknowledgements 10
101 Appendix B: Revision History 13
102

103 **1 Issues Addressed**

104 The following issues related to the Web Web Services Security: SOAP Message Security 1.1
105 (WS-Security 2004) listed in the Web Services Committee Issues List [[WSS-Issues](#)] have been
106 addressed in this document:
107

Issue	Description
455	Remove the #x509v3 table entry
459	Fix Typographical Errors
463	Fix Typographical Errors

108

109 2 Typographical/Editorial Errors

110 2.1 Section 7.2 Direct References

111 Added brackets to element names `wsse:SecurityTokenReference`, `wsse:Embedded`
112 `<wsse:Reference` and `wsse:KeyIdentifier` on lines 938 and 939

113 2.2 Section 7.3 Key Identifiers

114 Line 980 changed:
115 The `<wsse:KeyIdentifier>` element SHALL is placed in the
116 to
117 The `<wsse:KeyIdentifier>` element SHALL be placed in the

118 2.3 Section 8.6 Example

119 Changed line 1514 from:
120 `...#X509v3`
121 to
122 `http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3`

123 2.4 Section 9.4.4

124 Changed line 1776 from:
125 `<wsse11:EncryptedHeader>` then process as per section 9.5.2 Decryption and stop
126 to
127 `<wsse11:EncryptedHeader>` then process as per section 9.4.2 Decryption and stop
128
129 Changed line 1770 from:
130 Decrypt the contents of the `<xenc:EncryptedData>` element as per section 9.5.2
131 to
132 Decrypt the contents of the `<xenc:EncryptedData>` element as per section 9.4.2

133 2.5 Section 11 Extended Example

134 Changed line 1916 from:
135 `...#X509v3`
136 to
137 `http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3`
138
139 Changed line 1929 from:
140 `...#X509v3`
141 to
142 `http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3`

143

3 Normative Errors

144

3.1 Section 8.3 Signing Tokens

145

Removed the #x509v3 table entry at line 1399 and then change the example in same document at lines 1514, 1915 and 1927 to <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3>.

146

147

148

3.2 Section 7.3 Key Identifiers

149

Changed table entry on line 1014 from

http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbPrintSHA1	If the security token type that the Security Token Reference refers to already contains a representation for the thumbprint, the value obtained from the token MAY be used. If the token does not contain a representation of a thumbprint, then the value of the <code>KeyIdentifier</code> MUST be the SHA1 of the raw octets which would be encoded within the security token element were it to be included. A thumbprint reference MUST occur in combination with a required to be supported (by the applicable profile) reference form unless a thumbprint reference is among the reference forms required to be supported by the applicable profile, or the parties to the communication have agreed to accept thumbprint only references.
---	---

150

to

http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbprintSHA1	If the security token type that the Security Token Reference refers to already contains a representation for the thumbprint, the value obtained from the token MAY be used. If the token does not contain a representation of a thumbprint, then the value of the <code>KeyIdentifier</code> MUST be the SHA1 of the raw octets which would be encoded within the security token element were it to be included. A thumbprint reference MUST occur in combination with a required to be supported (by the applicable profile) reference form unless a thumbprint reference is among the reference forms required to be supported by the applicable profile, or the parties to the communication have agreed to accept thumbprint only references.
---	---

151

4 References

- 152
- 153 **[GLOSS]** Informational RFC 2828, "Internet Security Glossary," May 2000.
- 154 **[KERBEROS]** J. Kohl and C. Neuman, "The Kerberos Network Authentication Service
155 (V5)," RFC 1510, September 1993, <http://www.ietf.org/rfc/rfc1510.txt> .
- 156 **[KEYWORDS]** S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels,"
157 RFC 2119, Harvard University, March 1997.
- 158 **[SHA-1]** FIPS PUB 180-1. Secure Hash Standard. U.S. Department of
159 Commerce / National Institute of Standards and Technology.
160 <http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.txt>
- 161 **[SOAP11]** W3C Note, "SOAP: Simple Object Access Protocol 1.1," 08 May 2000.
- 162 **[SOAP12]** W3C Recommendation, "SOAP Version 1.2 Part 1: Messaging
163 Framework", 23 June 2003.
- 164 **[SOAPSEC]** W3C Note, "SOAP Security Extensions: Digital Signature," 06 February
165 2001.
- 166 **[URI]** T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers
167 (URI): Generic Syntax," RFC 3986, MIT/LCS, Day Software, Adobe
168 Systems, January 2005.
- 169 **[XPath]** W3C Recommendation, "XML Path Language", 16 November 1999
- 170
- 171 The following are non-normative references included for background and related material:
- 172 **[WS-SECURITY]** "Web Services Security Language", IBM, Microsoft, VeriSign, April 2002.
173 "WS-Security Addendum", IBM, Microsoft, VeriSign, August 2002.
174 "WS-Security XML Tokens", IBM, Microsoft, VeriSign, August 2002.
- 175 **[XMLC14N]** W3C Recommendation, "Canonical XML Version 1.0," 15 March 2001.
- 176 **[EXCC14N]** W3C Recommendation, "Exclusive XML Canonicalization Version 1.0," 8
177 July 2002.
- 178 **[XMLENC]** W3C Working Draft, "XML Encryption Syntax and Processing," 04 March
179 2002.
- 180 W3C Recommendation, "Decryption Transform for XML Signature", 10 December 2002.
- 181 **[XML-ns]** W3C Recommendation, "Namespaces in XML," 14 January 1999.
- 182 **[XMLSCHEMA]** W3C Recommendation, "XML Schema Part 1: Structures," 2 May 2001.
183 W3C Recommendation, "XML Schema Part 2: Datatypes," 2 May 2001.
- 184 **[XMLSIG]** D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. *XML-
185 Signature Syntax and Processing*, W3C Recommendation, 12 February
186 2002.
- 187 **[X509]** S. Santesson, et al, "Internet X.509 Public Key Infrastructure Qualified
188 Certificates Profile,"
189 [http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=
190 T-REC-X.509-200003-1](http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-X.509-200003-1)
- 191 **[WSS-SAML]** OASIS Working Draft 06, "Web Services Security SAML Token Profile",
192 21 February 2003

193	[WSS-XrML]	OASIS Working Draft 03, "Web Services Security XrML Token Profile",
194		30 January 2003
195	[WSS-X509]	OASIS, "Web Services Security X.509 Certificate Token Profile", 19
196		January 2004, http://www.docs.oasis-open.org/wss/2004/01/oasis-
197		200401-wss-x509-token-profile-1.0
198	[WSSKERBEROS]	OASIS Working Draft 03, "Web Services Security Kerberos Profile", 30
199		January 2003
200	[WSSUSERNAME]	OASIS, "Web Services Security UsernameToken Profile" 19 January
201		2004, http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
202		username-token-profile-1.0
203	[WSS-XCBF]	OASIS Working Draft 1.1, "Web Services Security XCBF Token Profile",
204		30 March 2003
205	[XMLID]	W3C Recommendation, "xml:id Version 1.0", 9 September 2005.
206	[XPOINTER]	"XML Pointer Language (XPointer) Version 1.0, Candidate
207		Recommendation", DeRose, Maler, Daniel, 11 September 2001.

Appendix A: Acknowledgements

Current Contributors:

Michael	Hu	Actional
Maneesh	Sahu	Actional
Duane	Nickull	Adobe Systems
Gene	Thurston	AmberPoint
Frank	Siebenlist	Argonne National Laboratory
Hal	Lockhart	BEA Systems
Denis	Pilipchuk	BEA Systems
Corinna	Witt	BEA Systems
Steve	Anderson	BMC Software
Rich	Levinson	Computer Associates
Thomas	DeMartini	ContentGuard
Merlin	Hughes	Cybertrust
Dale	Moberg	Cyclone Commerce
Rich	Salz	Datapower
Sam	Wei	EMC
Dana S.	Kaufman	Forum Systems
Toshihiro	Nishimura	Fujitsu
Kefeng	Chen	GeoTrust
Irving	Reid	Hewlett-Packard
Kojiro	Nakayama	Hitachi
Paula	Austel	IBM
Derek	Fu	IBM
Maryann	Hondo	IBM
Kelvin	Lawrence	IBM
Michael	McIntosh	IBM
Anthony	Nadalin	IBM
Nataraj	Nagaratnam	IBM
Bruce	Rich	IBM
Ron	Williams	IBM
Don	Flinn	Individual
Kate	Cherry	Lockheed Martin
Paul	Cotton	Microsoft
Vijay	Gajjala	Microsoft
Martin	Gudgin	Microsoft
Chris	Kaler	Microsoft
Frederick	Hirsch	Nokia
Abbie	Barbir	Nortel
Prateek	Mishra	Oracle
Vamsi	Motukuru	Oracle
Ramana	Turlapi	Oracle
Ben	Hammond	RSA Security
Rob	Philpott	RSA Security
Blake	Dournaee	Sarvega
Sundeeep	Peechu	Sarvega
Coumara	Radja	Sarvega
Pete	Wenzel	SeeBeyond
Manveen	Kaur	Sun Microsystems
Ronald	Monzillo	Sun Microsystems

Jan	Alexander	Systinet
Symon	Chang	TIBCO Software
John	Weiland	US Navy
Hans	Granqvist	VeriSign
Phillip	Hallam-Baker	VeriSign
Hemma	Prafullchandra	VeriSign

210 Previous Contributors:

Peter	Dapkus	BEA
Guillermo	Lao	ContentGuard
TJ	Pannu	ContentGuard
Xin	Wang	ContentGuard
Shawn	Sharp	Cyclone Commerce
Ganesh	Vaideeswaran	Documentum
Tim	Moses	Entrust
Carolina	Canales-Valenzuela	Ericsson
Tom	Rutt	Fujitsu
Yutaka	Kudo	Hitachi
Jason	Rouault	HP
Bob	Blakley	IBM
Joel	Farrell	IBM
Satoshi	Hada	IBM
Hiroshi	Maruyama	IBM
David	Melgar	IBM
Kent	Tamura	IBM
Wayne	Vicknair	IBM
Phil	Griffin	Individual
Mark	Hayes	Individual
John	Hughes	Individual
Peter	Rostin	Individual
Davanum	Srinivas	Individual
Bob	Morgan	Individual/Internet2
Bob	Atkinson	Microsoft
Keith	Ballinger	Microsoft
Allen	Brown	Microsoft
Giovanni	Della-Libera	Microsoft
Alan	Geller	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
Jeff	Hodges	Neustar
Senthil	Sengodan	Nokia
Lloyd	Burch	Novell
Ed	Reed	Novell
Charles	Knouse	Obliv
Vipin	Samar	Oracle
Jerry	Schwarz	Oracle

Eric	Gravengaard	Reactivity
Andrew	Nash	Reactivity
Stuart	King	Reed Elsevier
Martijn	de Boer	SAP
Jonathan	Tourzan	Sony
Yassir	Elley	Sun
Michael	Nguyen	The IDA of Singapore
Don	Adams	TIBCO
Morten	Jorgensen	Vordel

211

212 **Appendix B: Revision History**

Rev	Date	By Whom	What
01	08-25-2006	Anthony Nadalin	Issue 455, 459, 463

213

214

This section is non-normative.