



Web Services Security

X.509 Certificate Token Profile 1.1

OASIS Errata Committee Draft 01, 25 August 2006

OASIS Identifier:

wss-v1.1-spec-errata-X509TokenProfile

Document Location:

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

Technical Committee:

Web Service Security (WSS)

Chairs:

Kelvin Lawrence, IBM

Chris Kaler, Microsoft

Editors:

Anthony Nadalin, IBM

Abstract:

This document describes how to use X.509 Certificates with the Web Services Security: SOAP Message Security specification [WS-Security] specification.

Status:

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

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

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 WS-Security TC web page (<http://www.oasis-open.org/committees/wss/ipr.php>).

33 **Notices**

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

46

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

48

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

58

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

61

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

67

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

70

71 This section is non-normative.

72 **Table of Contents**

73 1 Issues Addressed 4
74 2 Typographical/Editorial Errors 5
75 2.1 Section 3.3.2 Reference to a Binary Security Token 5
76 2.2 Section 3.3.3 Reference to an Issuer and Serial Number..... 5
77 2.3 Section 3.4 Encryption 5
78 3 Normative Errors..... 6
79 3.1 Section 2.2 Namespaces 6
80 3.2 Section 3.1 Token Types 6
81 3.3 Section 3.2 Token References..... 6
82 4 References..... 7
83 Appendix A: Acknowledgments 8
84 Appendix B: Revision History 11
85

86 **1 Issues Addressed**

87 The following issues related to the Web Services Security X.509 Certificate Token Profile 1.1
88 listed in the Web Services Committee Issues List [WSS-Issues] have been addressed in this
89 document:

Issue	Description
457	Remove #x509v1 from table
458	Fix typographical Errors
460	Change #ThumbPrintSHA1 to #ThumbprintSHA1

90 2 Typographical/Editorial Errors

91 2.1 Section 3.3.2 Reference to a Binary Security Token

92 Changed lines 348 and 349 from

```
93 <ds:Reference URI="#body"></ds:Reference>  
94 <ds:Reference URI="#binarytoken"></ds:Reference>
```

95 to

```
96 <ds:Reference URI="#body">...</ds:Reference>  
97 <ds:Reference URI="#binarytoken">...</ds:Reference>
```

98 2.2 Section 3.3.3 Reference to an Issuer and Serial Number

99 Changed lines 384 and 385 from

```
100 <ds:Reference URI="#body"></ds:Reference>  
101 <ds:Reference URI="#keyinfo"></ds:Reference>
```

102 to

```
103 <ds:Reference URI="#body">...</ds:Reference>  
104 <ds:Reference URI="#keyinfo">...</ds:Reference>
```

105 2.3 Section 3.4 Encryption

106 Changed line 430 from

```
107 xenc:EncryptionMethod Algorithm="..."/>
```

108 to

```
109 xenc:EncryptionMethod Algorithm="..."/>
```

110

111 Changed line 480 from

```
112 soap-message-security-1.1#ThumbPrintSHA1" >LKiQ/CmFrJDJqCLFcyjhlsmZ/+0=
```

113 to

```
114 soap-message-security-1.1#ThumbprintSHA1" >LKiQ/CmFrJDJqCLFcyjhlsmZ/+0=
```

115

116 Changed line 494 from

```
117 <xenc:EncryptedData Id="encrypted" Type="...">
```

118 to

```
119 <xenc:EncryptedData Id="encrypted" Type="...">
```

120

121 **3 Normative Errors**

122 **3.1 Section 2.2 Namespaces**

123 Deleted following row from table at line 158

#X509PKIPathv1	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509PKIPathv1
----------------	---

124 **3.2 Section 3.1 Token Types**

125 Deleted following row from table at line 177

Single certificate	#x509v1	An X.509 v1 certificate capable of signature-verification at a minimum.
--------------------	---------	---

126

127 **3.3 Section 3.2 Token References**

128 Changed line 204 from

129 X.509 SubjectKeyIdentifier reference. A subject key identifier may only be used to
130 to

131 X.509 SubjectKeyIdentifier reference. A subject key identifier MAY only be used to

4 References

132

133 The following are normative references

- 134 **[Glossary]** Informational RFC 2828, *Internet Security Glossary*, May 2000.
135 <http://www.ietf.org/rfc/rfc2828.txt>
- 136 **[KEYWORDS]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
137 RFC 2119, Harvard University, March 1997,
138 <http://www.ietf.org/rfc/rfc2119.txt>
- 139 **[RFC2246]** T. Dierks, C. Allen., *The TLS Protocol Version, 1.0*. IETF RFC 2246
140 January 1999. <http://www.ietf.org/rfc/rfc2246.txt>
- 141 **[SOAP11]** W3C Note, "SOAP: Simple Object Access Protocol 1.1," 08 May 2000.
- 142 **[SOAP12]** W3C Recommendation, "SOAP Version 1.2 Part 1: Messaging
143 Framework", 23 June 2003.
- 144 **[URI]** T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers
145 (URI): Generic Syntax," RFC 3986, MIT/LCS, Day Software, Adobe
146 Systems, January 2005.
- 147 **[WS-Security]** A. Nadalin et al., *Web Services Security: SOAP Message Security 1.1*
148 (WS-Security 2004), OASIS Standard, [http://docs.oasis-](http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.1.pdf)
149 [open.org/wss/2004/01/oasis-200401-wss-soap-message-security-](http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.1.pdf)
150 1.1.pdf.
- 151 **[PKCS7]** *PKCS #7: Cryptographic Message Syntax Standard* RSA Laboratories,
152 November 1, 1993. [http://www.rsasecurity.com/rsalabs/pkcs/pkcs-](http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html)
153 7/index.html
- 154 **[PKIPATH]** [http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-](http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-X.509-200110-S!Cor1)
155 REC-X.509-200110-S!Cor1
- 156 **[X509]** ITU-T Recommendation X.509 (1997 E): *Information Technology - Open*
157 *Systems Interconnection - The Directory: Authentication Framework*,
158 June 1997.

159

160 The following are non-normative references

- 161 **[XML-ns]** T. Bray, D. Hollander, A. Layman. *Namespaces in XML. W3C*
162 *Recommendation*. January 1999. [http://www.w3.org/TR/1999/REC-xml-](http://www.w3.org/TR/1999/REC-xml-names-19990114)
163 names-19990114
- 164 **[XML Encrypt]** W3C Recommendation, "XML Encryption Syntax and Processing," 10
165 December 2002
- 166 **[XML Signature]** D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. *XML-*
167 *Signature Syntax and Processing*, W3C Recommendation, 12 February
168 2002.

169

Appendix A: Acknowledgments

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

172

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	Oblix
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

173

174

Appendix B: Revision History

Rev	Date	By Whom	What
01	08-25-2006	Anthony Nadalin	Issue 457, 458, 460

175