



Web Services Security: X.509 Token Profile 1.0

Errata 1.0

OASIS Standard 200401, ~~September~~ 2004

Document identifier:

{WSS: SOAP Message Security }-{X509 Profile}-{1.0} (Word) (PDF)

Document Location:

<http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0-errata-003>

Errata Location:

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

Editors:

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

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

Deleted: June

Deleted: 1

Formatted: Portuguese (Brazil)

Field Code Changed

Formatted: Portuguese (Brazil)

Formatted: Portuguese (Brazil)

Formatted Table

Deleted: June

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

Deleted: June

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

15

16 **Abstract:**

17 | This document contains a list of errata against WSS ~~X.509~~ Token Profile 1.0 that have
18 | been approved by the WSS Technical Committee.

Deleted: Username

19 **Status:**

20 | This version of the errata is a working draft of the committee. As such, it may change
21 | prior to incorporation into a future OASIS Standard. Please send comments to the
22 | editors. If you are on the wss@lists.oasis-open.org list for committee members, send
23 | comments there. If you are not on that list, subscribe to the wss-comment@lists.oasis-
24 | open.org list and send comments there. To subscribe, send an email message to wss-
25 | comment-request@lists.oasis-open.org with the word "subscribe" as the body of the
26 | 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

Deleted: June

32 **Table of Contents**

33 [1 Issues Addressed](#) 4

34 [2 Typographical Errors](#) 4

35 [3 Normative Errors](#) 5

36 [3.1 Table Of Contents](#)..... 5

37 [3.2 Section 2.2 Namespaces](#) 5

38 [3.3 Section 3.1 Token Types](#) 5

39 [3.4 Section 3.1.1 X509v3 Token Type](#) 5

40 [3.5 Section 3.2 Token References](#)..... 5

41 [3.6 Section 3.2.1 Reference to a Subject Key Identifier](#) 6

42 [3.7 Section 3.3.1 Key Identifier](#) 6

43 [3.8 Section 3.1.2 X509PKIPathv1 Token Type](#) 6

44 [3.9 Section 3.1.3 PKCS7 Token Type](#) 7

45 [3.10 Section 3.3.2 Reference to a Binary Security Token](#)..... 7

46 [4 Non-Normative Errors](#)..... 8

47 [5 Clarifications](#)..... 9

48 [Appendix A: Revision History](#) 10

49 [Appendix B: Notices](#)..... 11

51 **1 Issues Addressed**

52 [The following issues have been addressed in this document:](#)

53

ISSUE	DESCRIPTION
260	Editorial comments on X.509 Token profile - post v1 review period.
264	Post review period comments: Errors in WSS core and username/x.509 profile examples
281	X509 Token profile - sample still uses QName. (BinarySecurityToken attributes)

54 **2 Typographical Errors**

55 None

56

57

Deleted: 1 [Issues Addressed](#) . 4¶

2 [Typographical Errors](#) . 4¶

3 [Normative Errors](#) 5¶

3.1 [Table Of Contents](#) 5¶

3.2 [Section 2.2 Namespaces](#) 5¶

3.3 [Section 3.1.2 X509PKIPathv1 Token Type](#) 6¶

3.4 [Section 3.1.3 PKCS7 Token Type](#) 7¶

3.5 [Section 3.3.2 Reference to a Binary Security Token](#) . 7¶

4 [Non-Normative Errors](#) 8¶

5 [Clarifications](#) . 9¶

[Appendix A: Revision History](#) 10¶

[Appendix B: Notices](#) 11¶

1 [Typographical Errors](#) . 4¶

2 [Normative Errors](#) . 5¶

2.1 [Table Of Contents](#) 5¶

2.2 [Section 2.2 Namespaces](#) 5¶

2.3 [Section 3.1.2 X509PKIPathv1 Token Type](#) 5¶

2.4 [Section 3.1.3 PKCS7 Token Type](#) 5¶

2.5 [Section 3.3.2 Reference to a Binary Security Token](#) 5¶

3 [Non-Normative Errors](#) . 6¶

4 [Clarifications](#) . 7¶

[Appendix A: Revision History](#) 8¶

[Appendix B: Notices](#) 9¶

1 [Typographical Errors](#) . 4¶

2 [Normative Errors](#) 5¶

3 [Non-Normative Errors](#) . 6¶

4 [Clarifications](#) . 7¶

[Appendix A: Revision History](#) 8¶

[Appendix B: Notices](#) 9¶

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Deleted: June

Formatted: Bullets and Numbering

58

3 Normative Errors

59

3.1 Table Of Contents

Formatted: Heading 2,H2,h2,Level 2 Topic Heading

60

On lines 113-115, replace #x509v3, #x509PKIPathv1 and #PKCS7 with x509v3, x509PKIPathv1 and PKCS7.

Deleted: In the Table of Contents o

Formatted: ElementDesc Char1

61

62

3.2 Section 2.2 Namespaces

Formatted: Indent: Left: 0.5"

Formatted: Bullets and Numbering

63

Delete lines 155-158:

Deleted: ¶ In Section 2.2 Namespaces,

Formatted: ElementDesc

64

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

Deleted: d

65

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

66

and replace it with:

67

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

68

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

69

70

71

72

73

Add the following after line 161:

Formatted: ElementDesc

74

URI fragments defined in WSS: X.509 Certificate Token Profile 1.0 are relative to a base URI of

Deleted: n Section 2.2 Namespaces, a

75

76

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

Formatted: Bullets and Numbering

77

78

79

3.3 Section 3.1 Token Types

80

Delete first cell at line 172:

Formatted: Normal, Indent: Left: 0.5"

Single certificate	#X509v3	An X.509 v3 signature-verification certificate
--------------------	---------	--

Formatted Table

81

and replace it with

Formatted: Normal, Indent: Left: 0.5"

Single certificate	#X509	An X.509 signature-verification certificate
--------------------	-------	---

Formatted Table

Formatted: Bullets and Numbering

82

3.4 Section 3.1.1 X509v3 Token Type

83

Delete section heading at line 174:

Formatted: ElementDesc

84

3.1.1 X509v3 Token Type

85

and replace it with:

86

3.1.1 X509 Token Type

87

88

Delete line 176:

89

the scope of this specification.

90

and replace it with

91

the scope of this specification.

Formatted: Bullets and Numbering

92

3.5 Section 3.2 Token References

93

Add after line 195:

94

"A subject key identifier may only be used to reference an X.509v3 certificate."

Deleted: June

3.6 Section 3.2.1 Reference to a Subject Key Identifier

Formatted: Bullets and Numbering

Delete line 204:
"Reference to a Subject Key Identifier"
and replace it with
"Reference to an X.509v3 Subject Key Identifier"

Delete line 205:
"The <wsse:KeyIdentifier> element is used to specify a reference to an X.509 certificate by means of a"
and replace it with
"The <wsse:KeyIdentifier> element is used to specify a reference to an X.509v3 certificate by means of a"

Delete table at line 209:

Subject Key Identifier	ValueType URI	Description
Certificate Key Identifier	#X509SubjectKeyIdentifier	Value of the certificate's X.509 SubjectKeyIdentifier

and replace it with:

Subject Key Identifier	ValueType URI	Description
Certificate Key Identifier	#X509v3SubjectKeyIdentifier	Value of the certificate's X.509v3 SubjectKeyIdentifier

Delete line 213-215:
"ValueType attribute with the value #X509SubjectKeyIdentifier and its contents MUST be the value of the certificate's X.509 SubjectKeyIdentifier extension, encoded as per the <wsse:KeyIdentifier> element's"
and replace it with:
"ValueType attribute with the value #X509v3SubjectKeyIdentifier and its contents MUST be the value of the certificate's X.509v3 SubjectKeyIdentifier extension, encoded as per the <wsse:KeyIdentifier> element's"

Formatted: Bullets and Numbering

3.7 Section 3.3.1 Key Identifier

Delete line 252:.
"<wsse:KeyIdentifier> element which specifies the X.509 subject key identifier of the signing certificate."
and replace it with:
"<wsse:KeyIdentifier> element which specifies the X.509v3 subject key identifier of the signing certificate."

Delete line 276:

ValueType="...#X509SubjectKeyIdentifier">

and replace it with:

ValueType="...#X509v3SubjectKeyIdentifier">

3.8 Section 3.1.2 X509PKIPathv1 Token Type

Delete the following line (178):
The #X509PKIPathv1 token type MAY be used to represent a certificate path.
and replace it with:
The X509PKIPathv1 token type MAY be used to represent a certificate path.

Deleted: ¶

Formatted: Bullets and Numbering

Deleted: ¶
In Section 3.1.2 X509PKIPathv1 Token Type, d

Formatted: ElementDesc

Deleted: June

136
137
138
139
140

141

142
143
144
145
146
147
148
149
150
151
152
153

154

3.9 Section 3.1.3 PKCS7 Token Type

Delete the following line (180):
The #PKCS7 token type MAY be used to represent a certificate path...
and replace it with:
The PKCS7 token type MAY be used to represent a certificate path...

Formatted: Bullets and Numbering

Deleted: ¶
In Section 3.1.3 PKCS7 Token Type, d

Formatted: ElementDesc

Formatted: Bullets and Numbering

3.10 Section 3.3.2 Reference to a Binary Security Token

Delete the following lines (306-309):
<wsse:BinarySecurityToken
wsu:Id="binarytoken"
ValueType="wsse:X509v3"
EncodingType="wsse:Base64Binary">
and replace it with
<wsse:BinarySecurityToken
wsu:Id="binarytoken"
ValueType="...#X509v3"
EncodingType="...#Base64Binary">

Deleted: ¶
In Section 3.3.2 Reference to a Binary Security Token, d

Formatted: ElementDesc

Deleted: ¶
¶
¶

Deleted: June

155

4 Non-Normative Errors

156

157 None

Deleted: June

Formatted: Bullets and Numbering

158

5 Clarifications

159

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
#PKCS7	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#PKCS7
#X509v3	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3
#X509PKIPathv1	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509PKIPathv1
#X509SubjectKeyIdentifier	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentifier

160

Deleted: ¶

Deleted: June

161 **Appendix A: Revision History**

Rev	Date	What
1	06/25/04	First Draft of Errata
<u>2</u>	07/06/04	Updated per comments on list

162
163 This section is non-normative.

Deleted: June

Appendix B: Notices

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

174 OASIS invites any interested party to bring to its attention any copyrights, patents or patent
175 applications, or other proprietary rights which may cover technology that may be required to
176 implement this specification. Please address the information to the OASIS Executive Director.
177 Copyright © OASIS Open 2002-2004. *All Rights Reserved.*

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

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

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

194
195 This section is non-normative.