



---

# Web Services Security: X.509 Token Profile 1.0

---

## Errata 1.0

### Committee Draft 200401, October 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-004>

#### 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
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

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.

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

---

31

## 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

---

50

## 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 QNames. (BinarySecurityToken attributes)

---

## 54 2 Typographical Errors

55

56 None

57

---

## 58 3 Normative Errors

### 59 3.1 Table Of Contents

60 On lines 113-115, replace  
61 #x509v3, #x509PKIPathv1 and #PKCS7  
62 with  
63 #x509, #x509PKIPathv1 and #PKCS7.

### 64 3.2 Section 2.2 Namespaces

65 Delete lines 155-158:  
66 <http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd>  
67  
68 <http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd>  
69  
70 and replace it with:  
71 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd>  
72  
73 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd>  
74  
75

76 IAdd the following after line 161:  
77 URI fragments defined in WSS: X.509 Certificate Token Profile 1.0 are relative to a base  
78 URI of  
79 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0>  
80

### 81 3.3 Section 3.1 Token Types

82 Delete first cell at line 172:

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

83 and replace it with

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

### 84 3.4 Section 3.1.1 X509v3 Token Type

85 Delete section heading at line 174:  
86 3.1.1 X509v3 Token Type  
87 and replace it with:  
88 3.1.1 X509 Token Type  
89

90 Delete line 176:  
91 the scope of this specification.  
92 and replace it with  
93 the scope of this specification.

### 94 3.5 Section 3.2 Token References

95 Add after line 195:

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

### 97 **3.6 Section 3.2.1 Reference to a Subject Key Identifier**

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

102  
103 Delete line 205:  
104 "The <wsse:KeyIdentifier> element is used to specify a reference to an X.509  
105 certificate by means of a"  
106 and replace it with  
107 "The <wsse:KeyIdentifier> element is used to specify a reference to an X.509v3  
108 certificate by means of a"

109  
110 Delete table at line 209:

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

111 and replace it with:

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

112  
113 Delete line 213-215:  
114 "ValueType attribute with the value #X509SubjectKeyIdentifier and its contents  
115 MUST be the value of the certificate's X.509 SubjectKeyIdentifier extension, encoded as  
116 per the <wsse:KeyIdentifier> element's"  
117 and replace it with:  
118 "ValueType attribute with the value #X509v3SubjectKeyIdentifier and its contents  
119 MUST be the value of the certificate's X.509v3 SubjectKeyIdentifier extension, encoded  
120 as per the <wsse:KeyIdentifier> element's"

### 121 **3.7 Section 3.3.1 Key Identifier**

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

128  
129 Delete line 276:

```
130 ValueType="...#X509SubjectKeyIdentifier">
```

131 and replace it with:

```
132 ValueType="...#X509v3SubjectKeyIdentifier">
```

### 133 **3.8 Section 3.1.2 X509PKIPathv1 Token Type**

134 Delete the following line (178):  
135 The #X509PKIPathv1 token type MAY be used to represent a certificate path.

136 and replace it with:  
137 The X509PKIPathv1 token type MAY be used to represent a certificate path.

### 138 **3.9 Section 3.1.3 PKCS7 Token Type**

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

### 143 **3.10 Section 3.3.2 Reference to a Binary Security Token**

144 Delete the following lines (306-309):  
145 <wsse:BinarySecurityToken  
146 wsu:Id="binarytoken"  
147 ValueType="wsse:X509v3"  
148 EncodingType="wsse:Base64Binary">  
149 and replace it with  
150 <wsse:BinarySecurityToken  
151 wsu:Id="binarytoken"  
152 ValueType="...#X509"  
153 EncodingType="...#Base64Binary">  
154  
155

---

156 **4 Non-Normative Errors**

157

158 None



159

## 5 Clarifications

160

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>
#PKCS7	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#PKCS7">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#PKCS7</a>
#X509	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509</a>
#X509PKIPathv1	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509PKIPathv1">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509PKIPathv1</a>
#X509v3SubjectKeyIdentifier	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3SubjectKeyIdentifier">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3SubjectKeyIdentifier</a>

161

---

162 **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	09/02/04	Updated per comments on list
4	10/01/04	Updated per comments on list

163

164 This section is non-normative.

---

## Appendix B: Notices

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

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

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

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

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

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

195

196 This section is non-normative.