1

2 Web Services Security:

3 X.509 Token Profile 1.0

4 Errata 1.0

5 Committee Draft 200401, October 2004

6 **Document identifier:**
7 {*WSS: SOAP Message Security }-{X509 Profile*}-{*1.0*} (Word) (PDF)

8 **Document Location:**
9 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0-errata-
10 004

11 **Errata Location:**
12 http://www.oasis-open.org/committees/wss

13 **Editors:**

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

14 **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

Abstract:

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

Status:

This version of the errata is a working draft of the committee. As such, it may change prior to incorporation into a future OASIS Standard. Please send comments to the editors. If you are on the wss@lists.oasis-open.org list for committee members, send comments there. If you are not on that list, subscribe to the wss-comment@lists.oasis-open.org list and send comments there. To subscribe, send an email message to wss-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message. For patent disclosure information that may be essential to the implementation of this specification, and any offers of licensing terms, refer to the Intellectual Property Rights section of the OASIS Web Services Security Technical Committee (WSS TC) web page at http://www.oasis-open.org/committees/wss/ipr.php. General OASIS IPR information can be found at http://www.oasis-open.org/who/intellectualproperty.shtml.

Table of Contents

1 Issues Addressed

The following issues have been addressed in this document:

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)

2 Typographical Errors

None

3 Normative Errors

3.1 Table Of Contents

On lines 113-115, replace
#x509v3, #x509PKIPathv1 and #PKCS7
with
#x509, #x509PKIPathv1 and #PKCS7.

3.2 Section 2.2 Namespaces

Delete lines 155-158:
`http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd`
`http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd`
and replace it with:
`http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd`
`http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd`

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

3.3 Section 3.1 Token Types

Delete first cell at line 172:

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

and replace it with

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

3.4 Section 3.1.1 X509v3 Token Type

Delete section heading at line 174:
3.1.1 X509v3 Token Type
and replace it with:
3.1.1 X509 Token Type

Delete line 176:
the scope of this specification.
and replace it with
the scope of this specification.

3.5 Section 3.2 Token References

Add after line 195:

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

3.6 Section 3.2.1 Reference to a Subject Key Identifier

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"

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.

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…

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="…#X509"
EncodingType="…#Base64Binary">
```

4 Non-Normative Errors

None

5 Clarifications

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
#X509	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509
#X509PKIPathv1	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509PKIPathv1
#X509v3SubjectKeyIdentifier	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3SubjectKeyIdentifier

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

This section is non-normative.

Appendix B: Notices

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

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

This section is non-normative.