Web Services Security
X.509 Certificate Token Profile 1.1

OASIS Approved Errata, 01 November 2006

OASIS Identifier:

wss-v1.1-errata-os-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).

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 vailable; 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 implementors 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.

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

This section is non-normative.

Table of Contents

1 Issues Addressed

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

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

2 Typographical/Editorial Errors

2.1 Section 3.3.2 Reference to a Binary Security Token

Changed lines 348 and 349 from

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

to

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

2.2 Section 3.3.3 Reference to an Issuer and Serial Number

Changed lines 384 and 385 from

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

to

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

2.3 Section 3.4 Encryption

Changed line 430 from

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

to

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

Changed line 480 from

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

to

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

Changed line 494 from

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

to

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

3 Normative Errors

3.1 Section 2.2 Namespaces

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

3.2 Section 3.1 Token Types

Deleted following row from table at line 177

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

3.3 Section 3.2 Token References

Changed line 204 from

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

to

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

4 References

The following are normative references

[Glossary] Informational RFC 2828, *Internet Security Glossary*, May 2000. http://www.ietf.org/rfc/rfc2828.txt

[KEYWORDS] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, RFC 2119, Harvard University, March 1997, http://www.ietf.org/rfc/rfc2119.txt

[RFC2246] T. Dierks, C. Allen., *The TLS Protocol Version, 1.0.* IETF RFC 2246 January 1999. http://www.ietf.org/rfc/rfc2246.txt

[SOAP11] W3C Note, "SOAP: Simple Object Access Protocol 1.1," 08 May 2000.

[SOAP12] W3C Recommendation, "SOAP Version 1.2 Part 1: Messaging Framework", 23 June 2003.

[URI] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax," RFC 3986, MIT/LCS, Day Software, Adobe Systems, January 2005.

[WS-Security] A. Nadalin et al., Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), OASIS Standard, http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.1.pdf.

[PKCS7] *PKCS #7: Cryptographic Message Syntax Standard* RSA Laboratories, November 1, 1993. http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html

[PKIPATH] http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-X.509-200110-S!Cor1

[X509] ITU-T Recommendation X.509 (1997 E): Information Technology - *Open Systems Interconnection - The Directory: Authentication Framework*, June 1997.

The following are non-normative references

[XML-ns] T. Bray, D. Hollander, A. Layman. *Namespaces in XML. W3C Recommendation.* January 1999. http://www.w3.org/TR/1999/REC-xml-names-19990114

[XML Encrypt] W3C Recommendation, "XML Encryption Syntax andProcessing," 10 December 2002

[XML Signature] D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. *XML-Signature Syntax and Processing*, W3C Recommendation, 12 February 2002.

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
Sundeep	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

Appendix B: Revision History

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