Web Services Security: SAML Token Profile 1.1

OASIS Errata Committee Draft 1.0, 12 September 2006

Document Identifier:

wss-v1.1-errata-cd-SAMLTokenProfile

Location:

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

Technical Committee:

OASIS Web Services Security (WSS) TC

Chairs:

Kelvin Lawrence IBM
Chris Kaler Microsoft

Editors

Ronald Monzillo Sun

Abstract:

This document contains approved errata pertaining to the OASIS Standard, Web Services Security: SAML Token Profile 1.1 **[WSS: SAML Token Profile 1.1]** . The errata has been approved by the OASIS Web Services Technical Committee.

Status:

This document is an **OASIS Committee Draft** listing committee approved errata for the **OASIS Standard.** 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.oasis-open.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 Technical Committee web page (www.oasisopen.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 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 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.

Table of Contents

1 Issues Addressed

Corrections to the following issues, as they pertain to the OASIS Standard, Web Services Security: SAML Token Profile 1.1 **[WSS: SAML Token Profile 1.1],** are defined in this document:

Issue	Description
463	Errors in WSS-Security specification and profile. (sent to Kelvin)
464	Assertion substitution and holder-of-key

The issues are described in detail in the Issues List [WSS-Issues] of the OASIS Web Services Security Technical Committee.

2 Editorial/Typographical Corrections

Issue 463

In “Table-1 Namespace Prefixes” of section 2.2 “Namespaces”, corrected URI for xenc by adding missing “#” to the end of the URI.

3 Corrections to Non-Normative Content

Issue 464

In section 3.5.1.1, Attesting Entity“, inserted the following paragraph (with footnote) following line 695:

> The attesting entity MAY protect against substitution of a different but equivalently confirmed[1] assertion by including, as described in section 3.4.3 "SAML Assertion Referenced from SignedInfo", the SAML assertion (or an unambiguous reference to it) in the content signed to demonstrate knowledge of the confirmation key.

Added the parenthetical phrase “(including any SAML statements)” to the second paragraph of section 3.5.1.2. “Receiver”, such that it reads as follows:

> If the receiver determines that the attesting entity has demonstrated knowledge of a subject confirmation key, then the subjects and claims of the SAML statements confirmed by the key MAY be attributed to the attesting entity and any content of the message (including any SAML statements) whose integrity is protected by the key MAY be considered to have been provided by the attesting entity.

Added the following paragraph to the end of section 4.5 “Message Modification”.

> To ensure that message receivers can have confidence that an assertion with an equivalent confirmation key has not been substituted for the assertion used by the attesting entity, the attesting entity MAY include the assertion (or an unambiguous reference to it) in the attested for (i.e., signed) message content.

[1] Two holder-of-key confirmed assertions are equivalently confirmed if they may be confirmed using the same confirmation key.

4 Corrections to Normative Content

None

5 References

[WSS: SAML Token Profile 1.1] Oasis Standard, R. Monzillo, .C. Kaler, A. Nadalin, P. Hallem-Baker (Editors), Web Services Security: SAML Token Profile 1.1, 01 February 2006.

[WSS-Issues] OASIS Web Services Security Issues List, Version 90, 16 August 2006 http://www.oasis-open.org/apps/org/workgroup/wss/download.php/19774/OASIS%20Web%20Services%20Security%20Issues%20List%2090.htm

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	Hallem-Baker	VeriSign
Hemma	Prafullchandra	VeriSign

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