WS-SecureConversation 1.3 Errata

Committee Draft

30 April 2008

Specification URIs:
This Version:
http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-errata-cd-01.doc
http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-errata-cd-01.pdf
http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-errata-cd-01.html

Previous Version:
N/A

Latest Approved Version:
N/A

Technical Committee:
OASIS WS-TX TC

Chair(s):
Kelvin Lawrence, IBM
Chris Kaler, Microsoft

Editor(s):
Anthony Nadalin, IBM
Marc Goodner, Microsoft
Abbie Barbir, Nortel

Related work:
This specification errata is related to WS-SecureConversation v1.3.

Abstract:
This document lists errata for **WS-SecureConversation 1.3 OASIS Standard** [WS-SecureConversation] produced by the WS-SX Technical Committee. The standard was approved by the OASIS membership on 1 March 2007.

Status:
This document was last revised or approved by the WS-SX TC on the above date. The level of approval is also listed above. Check the "Latest Approved Version" location noted above for possible later revisions of this document.

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/ws-sx .

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.oasis-open.org/committees/ws-sx/ipr.php).

The non-normative errata page for this specification is located at www.oasis-open.org/committees/ws-sx.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

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

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

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

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' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on 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 OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

Table of contents

1 Issues Addressed

The following issues related to WS-SecurityConversation 1.3 as recorded in the [WS-SX Issues] have been addressed in this document.

Issue	Description
ER003	Clarification of policy usage for derived keys in SC
ER015	Change key to crucial in SC
ER013	Review normative RFC 2119 language in WS-SecureConversation
ER017	Conflict Nonce reuse description in the current WS-SC 1.3
i150	Add conformance statements to new versions of Trust/SC/SP
i152	Update policy references to 1.5 for SC, Trust and SP

2 Typographical/Editorial Errors

2.1 Normative language capitalization changes

The following changes do not affect the normative meaning of the text, they are only to properly capitalize 2119 terms. The changes listed below document the changes as they appear in the text. There were many instances of the terms OPTIONAL and REQUIRED in the schema exemplar descriptions that appeared un-capitalized that are not captured below but that have also been addressed. All other 2119 terms that remain un-capitalized are used in their English sense.

Line 236

If a token provides multiple keys then specific bindings and profiles MUST describe how to reference the separate keys

Line 356

In order for the security token service to process this request it MUST have prior knowledge for which Web Service the requestor needs a token

Line 612

the requestor is REQUIRED to re-authenticate the original claims in every renewal request

Line 757

Using a common secret, parties MAY define different key derivations to use.

Line 758

In order to keep the keys fresh (prevent providing too much data for analysis), subsequent derivations MAY be used

Line 784

The nonce seed is REQUIRED

Line 802

When a new key is required, a new <wsc:DerivedKeyToken> MAY be passed referencing the previously generated key

Line 843

then a fault such as wsc:UnknownDerivationSource SHOULD be raised.

2.2 Section 1

Removed lines 17 – 19 (to new section 1.8)

Compliant services are NOT REQUIRED to implement everything defined in this specification. However, if a service implements an aspect of the specification, it MUST comply with the requirements specified (e.g. related "MUST" statements).

2.3 Section 1.6

Line150 changed

[WS-Trust] OASIS Committee Draft, “WS-Trust 1.3”, September 2006
http://docs.oasis-open.org/ws-sx/ws-trust/200512

to

[WS-Trust] OASIS Standard, “WS-Trust 1.3”, 2007
http://docs.oasis-open.org/ws-sx/ws-trust/200512

2.4 Section 1.7

Line 168 changed

[WS-Policy] W3C Member Submission, "Web Services Policy 1.2 - Framework", 25 April 2006.
http://www.w3.org/Submission/2006/SUBM-WS-Policy-20060425/

[WS-PolicyAttachment] W3C Member Submission, "Web Services Policy 1.2 - Attachment" , 25 April 2006.
http://www.w3.org/Submission/2006/SUBM-WS-PolicyAttachment-20060425/

To

[WS-SecurityPolicy] OASIS Standard, “WS-SecurityPolicy 1.2”, 2007
http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702

2.5 Section 2 Secure Context Token (SCT)

Line 230 changed

The behavior is specified by the services policy [WS-Policy] [WS-PolicyAttachment]

to

The behavior is specified by the services policy [WS-SecurityPolicy]

2.6 Section 4 Amending Contexts

Line 537 changed

the message body and key headers using the key associated with the security context

to

the message body and crucial headers using the key associated with the security context

2.7 Section 5 Renewing Contexts

Line 617 changed

over the signature that signs message body and key headers

to

over the signature that signs message body and crucial headers

2.8 Section 6 Canceling Contexts

Line 696 changed

body and key headers using the key associated with the security context

to

body and crucial headers using the key associated with the security context

2.9 Section 7 Deriving Keys

Lines 780-781 changed

If either isn't specified in the policy,

to

If additional information is not specified as explicit elements,

2.10 Section 7.1 Syntax

Line 892 changed

If additional information is not specified (such as explicit elements or policy),

to

If additional information is not specified as explicit elements,

2.11 Section 8 Associating a Security Context

Line 1064 changed

...signature over body and key headers using #sct1...

to

...signature over body and crucial headers using #sct1...

Line 1070 changed

...signature over body and key headers using #sct2...

to

...signature over body and crucial headers using #sct2...

3 Normative Errors

3.1 Section 7.1 Syntax

There are not any cryptographic reasons that the nonce should be reused, this was an editorial mistake in the normative language used.

Line 890 changed

the same nonce SHOULD be used for all subsequent derivations

to

the same nonce SHOULD NOT be used for all subsequent derivations

4 References

[WS-SX Issues] WS-SX TC Issues List
http://docs.oasis-open.org/ws-sx/issues/Issues.xml

[WS-SecureConversation] OASIS Standard, “WS-SecureConversation 1.3", July 2007
http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512

Appendix A. Acknowledgements

The following individuals have participated in the creation of this specification and are gratefully acknowledged.

TC Members during the development of this specification:

Don Adams, Tibco Software Inc.
Jan Alexander, Microsoft Corporation
Steve Anderson, BMC Software
Donal Arundel, IONA Technologies
Howard Bae, Oracle Corporation
Abbie Barbir, Nortel Networks Limited
Charlton Barreto, Adobe Systems
Mighael Botha, Software AG, Inc.
Toufic Boubez, Layer 7 Technologies Inc.
Norman Brickman, Mitre Corporation
Melissa Brumfield, Booz Allen Hamilton
Lloyd Burch, Novell
Scott Cantor, Internet2
Greg Carpenter, Microsoft Corporation
Steve Carter, Novell
Symon Chang, BEA Systems, Inc.
Ching-Yun (C.Y.) Chao, IBM
Martin Chapman, Oracle Corporation
Kate Cherry, Lockheed Martin
Henry (Hyenvui) Chung, IBM
Luc Clement, Systinet Corp.
Paul Cotton, Microsoft Corporation
Glen Daniels, Sonic Software Corp.
Peter Davis, Neustar, Inc.
Martijn de Boer, SAP AG
Werner Dittmann, Siemens AG
Abdeslem DJAOUI, CCLRC-Rutherford Appleton Laboratory
Fred Dushin, IONA Technologies
Petr Dvorak, Systinet Corp.
Colleen Evans, Microsoft Corporation
Ruchith Fernando, WSO2
Mark Fussell, Microsoft Corporation
Vijay Gajjala, Microsoft Corporation
Marc Goodner, Microsoft Corporation
Hans Granqvist, VeriSign

Martin Gudgin, Microsoft Corporation
Tony Gullotta, SOA Software Inc.
Jiandong Guo, Sun Microsystems
Phillip Hallam-Baker, VeriSign
Patrick Harding, Ping Identity Corporation
Heather Hinton, IBM
Frederick Hirsch, Nokia Corporation
Jeff Hodges, Neustar, Inc.
Will Hopkins, BEA Systems, Inc.
Alex Hristov, Otecia Incorporated
John Hughes, PA Consulting
Diane Jordan, IBM
Venugopal K, Sun Microsystems
Chris Kaler, Microsoft Corporation
Dana Kaufman, Forum Systems, Inc.
Paul Knight, Nortel Networks Limited
Ramanathan Krishnamurthy, IONA Technologies
Christopher Kurt, Microsoft Corporation
Kelvin Lawrence, IBM
Hubert Le Van Gong, Sun Microsystems
Jong Lee, BEA Systems, Inc.
Rich Levinson, Oracle Corporation
Tommy Lindberg, Dajeil Ltd.
Mark Little, JBoss Inc.
Hal Lockhart, BEA Systems, Inc.
Mike Lyons, Layer 7 Technologies Inc.
Eve Maler, Sun Microsystems
Ashok Malhotra, Oracle Corporation
Anand Mani, CrimsonLogic Pte Ltd
Jonathan Marsh, Microsoft Corporation
Robin Martherus, Oracle Corporation
Miko Matsumura, Infravio, Inc.
Gary McAfee, IBM
Michael McIntosh, IBM
John Merrells, Sxip Networks SRL
Jeff Mischkinsky, Oracle Corporation
Prateek Mishra, Oracle Corporation
Bob Morgan, Internet2
Vamsi Motukuru, Oracle Corporation
Raajmohan Na, EDS
Anthony Nadalin, IBM
Andrew Nash, Reactivity, Inc.

Eric Newcomer, IONA Technologies
Duane Nickull, Adobe Systems
Toshihiro Nishimura, Fujitsu Limited
Rob Philpott, RSA Security
Denis Pilipchuk, BEA Systems, Inc.
Darren Platt, Ping Identity Corporation
Martin Raepple, SAP AG
Nick Ragouzis, Enosis Group LLC
Prakash Reddy, CA
Alain Regnier, Ricoh Company, Ltd.
Irving Reid, Hewlett-Packard
Bruce Rich, IBM
Tom Rutt, Fujitsu Limited
Maneesh Sahu, Actional Corporation
Frank Siebenlist, Argonne National Laboratory
Joe Smith, Apani Networks
Davanum Srinivas, WSO2
Yakov Sverdlov, CA
Gene Thurston, AmberPoint
Victor Valle, IBM
Asir Vedamuthu, Microsoft Corporation
Greg Whitehead, Hewlett-Packard
Ron Williams, IBM
Corinna Witt, BEA Systems, Inc.
Kyle Young, Microsoft Corporation