WS-SecurityPolicy 1.2 Errata

Committee Draft

30 April 2008

Specification URIs:
This Version:
http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-errata-cd-01.doc
http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-errata-cd-01.pdf
http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-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-SecurityPolicy v1.2.

Abstract:

This document lists errata for **WS-SecurityPolicy 1.2 OASIS Standard** [WS-SecurityPolicy] produced by the WS-SX Technical Committee. The standard was approved by the OASIS membership on 1 July 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

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-SecurityPolicy 1.2 as recorded in the [WS-SX Issues] have been addressed in this document.

Issue	Description
ER001	Inconsistent IncludeToken URI between spec and schema xsd file
ER002	Editorial comments on SP
ER004	Wrong Security Context Token assertion in example
ER007	Minor editorial addition to <ContentEncryptedElements> Assertion
ER009	Policy Assertion Parameters and alternatives
ER010	Typo in the Security Header Layout section
ER011	Modification request for issue PR014
ER006	Presence of wsu:Timestamp when [Timestamp] is false
ER014	Review normative RFC 2119 language in WS-SecurityPolicy
i165	SP errata

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 121

Extensibility points in the exemplar MAY NOT be described in the corresponding text

Line 130

WS-SecurityPolicy SHOULD be applicable to any version of SOAP

Line 321

Assertions MAY be used to further qualify a specific aspect of another assertion. For example, an assertion describing the set of algorithms to use MAY qualify the specific behavior of a security binding

Line 338

Any REQUIRED message elements (e.g. timestamps) in the wsse:Security header

Line 347

Note that a service MAY choose to reject messages despite them conforming to its policy, for example because a client certificate has been revoked. Note also that a service MAY choose to accept messages that do not conform to its policy.

Line 365

This section defines properties that are referenced later in this document describing the RECOMMEDED or REQUIRED attachment points for various assertions.

Line 489

Multiple instances of this element MAY appear within this assertion and SHOULD be treated as separate references in a signature when message security is used

Line 571

Multiple instances of this element MAY appear within this assertion and SHOULD be treated as separate references

Line 597

Multiple instances of this element MAY appear within this assertion and SHOULD be treated as separate references

Line 628

Multiple instances of this element MAY appear within this assertion and SHOULD be treated as a combined XPath expression

Line 658

Any token assertion MAY also carry an OPTIONAL sp:IncludeToken attribute

Line 659

This attribute indicates whether the token SHOULD be included

Line 664 (in table)

an external reference to the token SHOULD be used.

Subsequent related messages sent between the recipient and the initiator MAY refer to

Line 673

A token assertion MAY carry a sp:IncludeToken attribute that requires that the token be included in the message

Line 684

then references to that token are REQUIRED to contain all the specified reference types.

Line 691

Any token assertion MAY also carry an OPTIONAL sp:Issuer element

Line 696

Any token assertion MAY also carry an OPTIONAL sp:IssuerName element.

Line 703

While both sp:Issuer and sp:IssuerName elements are OPTIONAL they are also mutually exclusive

Line 706

Any token assertion MAY also carry an OPTIONAL wst:Claims element

Line 710

This element indicates the REQUIRED claims that the security token MUST contain in order to satisfy the requirements of the token assertion.

Line 713

Individual token assertions MAY further limit what claims MAY be specified for that specific token assertion.

Line 716

As long as the union of all tokens in the received message contains the REQUIRED set of claims from REQUIRED token issuers the message is valid according to the receiver's policy.

Line 736

This boolean property specifies whether derived keys SHOULD be used as defined in WS-SecureConversation

Line 900

Note: The IssuedToken MAY or MAY NOT be associated with key material and such key material MAY be symmetric or asymmetric.

Line 902

Services MAY also include information in the sp:RequestSecurityTokenTemplate element

Line 1180

then either the sp:SecureConversationToken or the sp:IssuedToken assertion SHOULD be used instead

Line 1187

Because this token is issued by the target service and MAY NOT have a separate port

Line 1379

the sp:IssuedToken assertion SHOULD be used instead

Line 1451

the sp:IssuedToken assertion SHOULD be used instead

Line 1597

This property specifies the algorithm suite REQUIRED for performing cryptographic operations with symmetric or asymmetric key based security tokens.

Line 1635

This property indicates the order in which integrity and confidentiality are applied to the message, in cases where both integrity and confidentiality are REQUIRED

Line 1639

This boolean property specifies whether the signature MUST be encrypted.

Line 1641

The primary signature element is NOT REQUIRED to be encrypted if the value is 'true'

Line 1646

This boolean property specifies whether signatures MUST cover the token used to generate that signature.

Line 1650

It is RECOMMENDED that assertions that define values for this property apply to [Endpoint Policy Subject].

Line 1653

This boolean property specifies whether signature digests over the SOAP body and SOAP headers MUST only cover the entire body and entire header elements.

Line 1661

It is RECOMMENDED that assertions that define values for this property apply to [Endpoint Policy Subject].

Line 1674

then it SHOULD appear before the ds:Signature and xenc:ReferenceList elements

Line 1700

then it SHOULD appear before the ds:Signature and xenc:ReferenceList elements

Line 1719

However, the xenc:ReferenceList is NOT REQUIRED to appear before independently encrypted tokens such as the xenc:EncryptedKey token as defined in WSS

Line 2133

Additional tokens MAY be specified to augment the claims

Line 2134

This section defines seven properties related to supporting token requirements which MAY be referenced by a Security Binding

Line 2145

Supporting tokens MAY be specified at a different scope than the binding assertion

Line 2148

the sender SHOULD merge the requirements by including all tokens

Line 2152

all the tokens SHOULD sign and encrypt the various message parts

Line 2161

To illustrate the different ways that supporting tokens MAY be bound to the message

Line 2165

Even before any supporting tokens are added, each binding requires that the message is signed using a token satisfying the REQUIRED usage for that binding

Line 2171

Note: if REQUIRED, the initiator MAY also include in the Security header the token used as the basis for the message signature (Sig1), not shown in the diagram

Line 2178

Supporting tokens are included in the security header and MAY OPTIONALLY include additional message parts to sign and/or encrypt

Line 2229

Signed tokens are included in the “message signature” as defined above and MAY OPTIONALLY include additional message parts to sign and/or encrypt

Line 2283

produced from the message signature and MAY OPTIONALLY include

Line 2339

This assertion MAY OPTIONALLY include additional message parts to sign and/or encrypt

Line 2345

If transport security is used, the token (Tok2) is included in the Security header and the signature (Sig2) SHOULD cover the message timestamp as illustrated below

Line 2485

There are several OPTIONAL aspects to the WSS: SOAP Message Security specification

Line 2496

a token MAY be referenced using different mechanisms

Line 2551

This boolean property specifies whether wsse11:SignatureConfirmation elements SHOULD be used

Line 2634

These assertions relate to interactions with a Security Token Service and MAY augment the behaviors defined by

Line 2649

A challenge issued by the server MAY increase the number of messages exchanged by the client and service

Line 2656

This boolean property indicates whether client entropy is REQUIRED to be used as key material for a requested proof token. A value of 'true' indicates that client entropy is REQUIRED. A value of 'false' indicates that client entropy is NOT REQUIRED

Line 2661

This boolean property indicates whether server entropy is REQUIRED to be used as key material for a requested proof token. A value of 'true' indicates that server entropy is REQUIRED. A value of 'false' indicates that server entropy is NOT REQUIRED

Line 2881

Policy MAY be embedded inside an Issued Token assertion, or acquired out-of-band. There MAY be an explicit trust relationship between the Server and the STS. There MUST be a trust relationship between the Client and the STS.

Line 2885

client-specific parameters that MUST be understood

Line 2898

The Client MAY augment or replace the contents of the RST

Line 2902

The Issued Token Policy Assertion contains elements which MUST be understood by the Client. The assertion contains one element which contains a list of arbitrary elements which SHOULD be sent along to the STS

Line 2908

All items are OPTIONAL , since the Server and STS MAY already have a pre-arranged relationship

Line 3808

A wsse:UsernameToken MAY be encrypted when a transport binding is not being used

2.2 Section 2 Security Policy Model

Added after line 288

Parameters defined by this specification represent additional information for engaging behaviors that do not need to participate in matching. When multiple security policy assertions of the same type with parameters present occur in the same policy alternative the parameters should be treated as a union. Note that a service may choose to accept messages that do not match its policy.

2.3 Section 4.2.3 ContentEncryptedElements Assertion

Added after line 593

If no attribute is provided, then XPath 1.0 is assumed.

2.4 Section 5.1.1 Token Inclusion Values

The schema had token inclusion values defined that did not match the values defined in the specification. The following schema fragment was corrected.

Original, incorrect, schema fragment

```
  <xs:simpleType name="IncludeTokenType">
    <xs:restriction base="xs:anyURI" >
      <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-
trust/200702/ws-securitypolicy/IncludeToken/Never" />
      <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-
trust/200702/ws-securitypolicy/IncludeToken/Once" />
      <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-
trust/200702/ws-securitypolicy/IncludeToken/AlwaysToRecipient" />
      <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-
trust/200702/ws-securitypolicy/IncludeToken/AlwaysToInitiator" />
      <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-
trust/200702/ws-securitypolicy/IncludeToken/Always" />
    </xs:restriction>
  </xs:simpleType>
```

Updated, correct, schema fragment

```
  <xs:simpleType name="IncludeTokenType">
    <xs:restriction base="xs:anyURI" >
      <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never" />
      <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Once" />
      <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient" />
      <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToInitiator" />
      <xs:enumeration value="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Always" />
    </xs:restriction>
  </xs:simpleType>
```

2.5 Section 5.4.7 SecureConversationToken Assertion

Line 1282 changed

<sp:SC10SecurityContextToken />

to

<sp:SC13SecurityContextToken />

2.6 Section 6.4 [Signature Protection] Property

Lines 1640-1642 changed

The primary signature element is not required to be encrypted if the value is ‘true’ when there is nothing else in the message that is encrypted.

to

The primary signature element is not required to be encrypted if the value is ‘true’ when there is nothing in the message that is covered by this signature that is encrypted.

2.7 Section 6.7 [Security Header Layout] Property

Line 1665 table contents changed

wsse:Timestamp

to

wsu:Timestamp

2.8 Section 7.5 AsymmetricBinding Assertion

Line 2097 changed

The specified token populates the [Recipient Signature Token] property and is used for the message signature from Recipient to recipient.

to

The specified token populates the [Recipient Signature Token] property and is used for the message signature from recipient to the initiator.

Lines 2103 changed

The specified token populates the [Recipient Encryption Token] property and is used for the message encryption from recipient to Recipient.

to

The specified token populates the [Recipient Encryption Token] property and is used for the message encryption from initiator to recipient.

2.9 Section 10.1 Trust13 Assertion

Line 2720 changed

sp:Trust10

to

sp:Trust13

3 Normative Errors

None.

4 References

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

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

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