Web Services Security:

SOAP Message Security 1.0

(WS-Security 2004)

Errata 1.0

Committee Draft 200512, December 2005

Document identifier:

{*WSS: SOAP Message Security* }-{*1.0*} (Word) (PDF)

Document Location:

http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0-errata-004

Errata Location:

http://www.oasis-open.org/committees/wss

Editors:

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

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 OASIS Standard Version 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
327	Timestamp ValueType needs to be clarified
328	Errata on STR transform
256	STR attributes are not protected
264	Post review period comments: Errors in WSS core and username/x.509 profile examples.
290	Inconsistency in the KeyIdentifier encoding type default between core and SAML
444	Request to remove the WS-Security 1.0 errata from WSS page or fix it

2 Typographical Errors

2.1 Section 7.1 SecurityTokenReference Element

Delete the following line (652):

This optional attribute is used to type the usage of the `<wsse:SecurityToken>`.

and replace it with:

This optional attribute is used to type the usage of the `<wsse:SecurityTokenReference>`.

3 Normative Errors

3.1 Section 2.2 Namespaces

Delete lines 185-188:
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

Add the following after line 198:
Notice – The schema http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd MUST be updated, the update is to change the reference http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd to http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd

URI fragments defined in WSS: SOAP Message Security 1.0 are relative to a base URI of `http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0`

3.2 Section 4.2 Id Schema

Delete line 421:
namespace} is "`http://www.w3.org/2001/XMLSchema`" and which {name} is "Id."
and replace it with:
namespace} is "`http://www.w3.org/2001/XMLSchema`" and which {type} is "ID."

3.3 Section 5 Security Header

Delete the line 495:
The receiver must generate a fault if unable to interpret or process security tokens
and replace it with:
The receiver MUST generate a fault if unable to interpret or process security tokens

3.4 Section 7.1 SecurityTokenReference Element

Delete line 634:
If a <wsse:SecurityTokenReference> is used outside of the <wsse:Security> header
and replace it with:
If a <wsse:SecurityTokenReference> is used outside of the security header processing

3.5 Section 7.2 KeyIdentifiers

Add after line 735:
The <wsse:KeyIdentifier> element is only allowed inside a <wsse:SecurityTokenReference> element.

3.6 Section 7.3 Key Identifiers

Delete table at line 761

URI	Description
#Base64Binary	XML Schema base 64 encoding (default)

And replace with

URI	Description
#Base64Binary	XML Schema base 64 encoding

Delete the following line
"encoded. For example, a hash value may be encoded using base 64 encoding (the default)."
and replace it with
"encoded. For example, a hash value may be encoded using base 64 encoding".

3.7 Section 7.4 Embedded Reference

Schema shows ValueType attribute but no wsu:Id attribute in the schema. The ValueType should be replaced with a wsu:Id.

Add after line 769:
The `<wsse:Embedded>` element is only allowed inside a
`<wsse:SecurityTokenReference>` element.

3.8 Section 8.1 Algorithms

Delete URI in table (line 863):
http://www.w3.org/TR/2003/NOTE-soap12-n11n-20030328/
and replace it with:
http://www.w3.org/TR/soap12-n11n/

3.9 Section 8.3 Signing Tokens

Delete lines 1293 and 1294
"instants that specify leap seconds. If, however, other time types are used, then the `ValueType` attribute (described below) MUST be specified to indicate the data type of the time format."
and replace it with
"instants that specify leap seconds."

4 Non-Normative Errors

4.1 Section 3.4 Examples

Delete lines 305-308:

```
(005)    <xxx:CustomToken wsu:Id="MyID"
                xmlns:xxx="http://fabrikam123/token">
(006)          FHUIORv...
(007)    </xxx:CustomToken>
```

and replace it with:

```
(005)    <wsse:BinarySecurityToken ValueType="
http://fabrikam123#CustomToken "
     EncodingType="...#Base64Binary" wsu:Id=" MyID ">
(006)          FHUIORv...
(007)    </wsse:BinarySecurityToken>
```

4.2 Section 6.2.1 Username

Delete line 532:
A string label for this security token.
and replace it with:
A string label for this security token. The wsu:Id allow for an open attribute model.

4.3 Section 6.3.2 Encoding Binary Security Tokens

Delete the following lines (606-612):
When a <wsse:BinarySecurityToken> is included in a signature—that is, it is referenced from a <ds:Signature> element--care should be taken so that the canonicalization algorithm (e.g., Exclusive XML Canonicalization [EXC-C14N]) does not allow unauthorized replacement of namespace prefixes of the QNames used in the attribute or element values. In particular, it is RECOMMENDED that these namespace prefixes be declared within the <wsse:BinarySecurityToken> element if this token does not carry the validating key (and consequently it is not cryptographically bound to the signature).

No replacement text is needed. QNames have been replaced by URIs.

4.4 Section 7.3 Key Identifiers

Delete the following line (757-760):
"/wsse:SecurityTokenReference/wsse:KeyIdentifier/@EncodingType
The optional `EncodingType` attribute is used to indicate, using a URI, the encoding format of the `KeyIdentifier` (`#Base64Binary`). The base values defined in this specification are used (Note that URI fragments are relative to this document's URI):"
and replace it with:
"/wsse:SecurityTokenReference/wsse:KeyIdentifier/@EncodingType
The optional `EncodingType` attribute is used to indicate, using a URI, the encoding format of the `KeyIdentifier` (`#Base64Binary`). This specification defines the EncodingType URI values appearing in the following table. A token specific profile MAY define additional token specific EncodingType URI values. A

KeyIdentifier MUST include an EncodingType attribute when its ValueType is not sufficient to identify its encoding type.”

4.5 Section 8.3 Signing Tokens

Delete the following lines (1034-1036)”
"The transform takes a single mandatory parameter, a <ds:CanonicalizationMethod> element, which is used to serialize the input node set."
and replace it with:
"The transform takes a single mandatory parameter, a <ds:CanonicalizationMethod> element, which is used to serialize the output node set."

4.6 Section 11 Extended Example

Delete lines 1392-1396

```
(015)             <ds:KeyInfo>
(016)                <wsse:KeyIdentifier
                         EncodingType="...#Base64Binary"
                     ValueType="...#X509v3">MIGfMa0GCSq...
(017)                </wsse:KeyIdentifier>
(018)             </ds:KeyInfo>
```

and replace it with

```
(015)             <ds:KeyInfo>
                       <wsse:SecurityTokenReference>
(016)                        <wsse:KeyIdentifier
                                   EncodingType="...#Base64Binary"
                             ValueType="...#X509v3">MIGfMa0GCSq...
(017)                        </wsse:KeyIdentifier>
                       </wsse:SecurityTokenRefernece>
(018)             </ds:KeyInfo>
```

5 Clarifications

5.1 Section 8.3 Signing Tokens

Signing a SecurityTokenReference (STR) provides authentication and integrity protection of only the STR and not the referenced security token (ST). If signing the ST is the intended behavior, the STR Dereference Transform (STRDT) may be used which replaces the STR with the ST for digest computation, effectively protecting the ST and not the STR. If protecting both the ST and the STR is desired, you may sign the STR twice, once using the STRDT and once not using the STRDT.

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

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	0919/04	Updated per comments on list
4	10/01/04	Updated per comments on list
5	12/07/05	Issue 444

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.