Web Services Security
XrML Token Binding

Working Draft 01, 20 September 2002

Document identifier:
WSS-XrML-01

Location:
TBD

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

Contributors:

TBD – Revise this list to include WSS TC contributors

Phillip Hallam-Baker, VeriSign
Maryann Hondo, IBM
Chris Kaler, Microsoft
Hiroshi Maruyama, IBM
Anthony Nadalin, IBM
Nataraj Nagaratnam, IBM
Hemma Prafullchandra, VeriSign
John Shewchuk, Microsoft

Abstract:
This document describes how to use eXternsible Rights Markup Language (XrML) licenses with the **Error! Hyperlink reference not valid.** specification.

Status:
This is an interim draft. Please send comments to the editors.

Committee members should send comments on this specification to the mailto:wss@lists.oasis-open.org list. Others should subscribe to and send comments to the wss-comment@lists.oasis-open.org list. To subscribe, visit http://lists.oasis-open.org/ob/adm.pl.

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 Security Services TC web page (http://www.oasis-open.org/who/intellectualproperty.shtml).

Table of Contents

1 Introduction 4
1.1 Goals and Requirements 4
1.1.1 Requirements 4
1.1.2 Non-Goals 4
2 Notations and Terminology 5
2.1 Notational Conventions 5
2.2 Namespaces 5
2.3 Terminology 5
3 Usage 7
3.1 Processing Model 7
3.2 Attaching Security Tokens 7
3.3 Identifying and Referencing Security Tokens 7
3.4 Proof-of-Possession of Security Tokens 8
3.5 Error Codes 9
3.6 Threat Model and Countermeasures 9
4 Acknowledgements 10
5 References 11
Appendix A: Revision History 12
Appendix B: Notices 13

1 Introduction

The WS-Security specification proposes a standard set of SOAP extensions that can be used when building secure Web services to implement message level integrity and confidentiality. This specification describes the use of eXternsible Rights Markup Language (XrML) licenses with respect to the **Error! Hyperlink reference not valid.** specification.

Note that Section 1 is non-normative.

1.1 Goals and Requirements

The goal of this specification is to define the use of SAML assertions in the context of WS-Security including for the purpose of securing SOAP message exchanges.

The requirements to be satisfied by this specification are listed below.

1.1.1 Requirements

TBS

- ?

1.1.2 Non-Goals

The following topics are outside the scope of this document:

- ? TBS

2 Notations and Terminology

This section specifies the notations, namespaces, and terminology used in this specification.

2.1 Notational Conventions

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119.

Namespace URIs (of the general form "some-URI") represent some application-dependent or context-dependent URI as defined in RFC2396.

This specification is designed to work with the general SOAP message structure and message processing model, and should be applicable to any version of SOAP. The current SOAP 1.2 namespace URI is used herein to provide detailed examples, but there is no intention to limit the applicability of this specification to a single version of SOAP.

Readers are presumed to be familiar with the terms in the Internet Security Glossary.

2.2 Namespaces

The XML namespace URIs that MUST be used by implementations of this specification are as follows (note that different elements in this specification are from different namespaces):

```
http://schemas.xmlsoap.org/ws/2002/xx/secext
http://schemas.xmlsoap.org/ws/2002/xx/utility
```

The following namespaces are used in this document:

Prefix	Namespace
S	http://www.w3.org/2001/12/soap-envelope
ds	http://www.w3.org/2000/09/xmldsig#
xenc	http://www.w3.org/2001/04/xmlenc#
wsse	http://schemas.xmlsoap.org/ws/2002/xx/secext
wsu	http://schemas.xmlsoap.org/ws/2002/xx/utility
xrml	http://www.xrml.org/schema/2001/11/xrml2core

2.3 Terminology

This specification employs the terminology defined in the WS-Security Core Specification.

Defined below are the basic definitions for additional terminology used in this specification.

91 [TBS]

3 Usage

This section describes the profile (specific mechanisms and procedures) for the SAML binding of WS-Security.

Identification: urn:oasis:names:tc:WSS:1.0:bindings:WSS-XrML-binding

Contact information: TBD

Description: Given below.

Updates: None.

3.1 Processing Model

The processing model for WS-Security with XrML licenses is no different from that of WS-Security with other token formats as described in WS-Security.

3.2 Attaching Security Tokens

XrML licenses are attached to SOAP messages using WS-Security by placing the license element inside the <wsse:Security> header. The following example illustrates a SOAP message with an XrML license token.

```
<S:Envelope xmlns:S="...">
    <S:Header>
        <wsse:Security xmlns:wsse="...">
            <xrml:license xmlns:xrml="...">
                ...
            </xrml:license>
            ...
        </wsse:Security>
    </S:Header>
    <S:Body>
        ...
    </S:Body>
</S:Envelope>
```

3.3 Identifying and Referencing Security Tokens

The WS-Security specification defines the *wsu:Id* attribute as the common mechanism for referencing security tokens by "Id" (the specification describes the reasons for this). Since the XrML specification does not allow attribute extensibility on the <xrml:license> element, this specification defines a separate mechanism for referencing licenses. The XrML specification allows licenses to be named using a URI with the *licenseId* attribute. Consequently, this specification defines the global namespace qualifier attribute *xmltok:RefType* for use with the <wsse:Reference> element (used within a <wsse:SecurityTokenReference> element). Using this attribute, references can specify the type of token desired thereby allowing the token-specific matching rules to be processed. Specifically, when the

xmktok:RefType attribute's value is "xrml:license", then the *URI* attribute refers to an <xrml:license> element whose *licenseId* attribute is specified by the URI attribute.

The following example illustrates a message with an XML Signature that references an XrML token.

```
<S:Envelope xmlns:S="...">
    <S:Header>
        <wsse:Security xmlns:wsse="...">
            <xrml:license xmlns:xrml="..."
                          licenseId="urn:SecurityToken-ef375268"/>

                ...
            </xrml:license>
            <ds:Signature xmlns:ds="...">
                ...
                <ds:KeyInfo>
                   <wsse:SecurityTokenReference>
                     <wsse:Reference URI="urn:SecurityToken-ef375268"
                                    xmltok:RefType="xrml:license"
                                    xmlns:xmltok="..."/>
                   </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
            ...
        </wsse:Security>
    </S:Header>
    <S:Body>
        ...
    </S:Body>
</S:Envelope>
```

3.4 Proof-of-Possession of Security Tokens

As previously stated, the WS-Security specification does not dictate how subject confirmation must be performed. As well, the XrML specification allows for multiple types of confirmation. If a secure transport is not used, it is strongly RECOMMENDED that a key-based confirmation mechanism be used.

Any processor of XrML security tokens MUST conform to the required validation and processing rules defined in the XrML specification.

The following table illustrates how several different confirmation mechanisms are processed:

Mechanism	**RECOMMENDED Processing Rules**
<xrml:keyHolder>	The sender (the subject) includes an XML Signature that can be verified with the key information in the referenced security token.
<xrml:allPrincipals>	The sender (the subject) includes an XML Signature that can be verified. An implementation MAY choose to not require

	principals to "authenticate".

3.5 Error Codes

When using XrML licenses, it is RECOMMENDED to use the error codes defined in the WS-Security specification. However, implementations MAY use custom errors, defined in private namespaces if they desire. Care should be taken not to introduce security vulnerabilities in the errors returned.

3.6 Threat Model and Countermeasures

The use of XrML licenses with WS-Security introduces no new threats beyond those identified for XrML or WS-Security with other types of security tokens.

Message alteration and eavesdropping can be addressed by using the integrity and confidentiality mechanisms described in WS-Security. Replay attacks can be addressed by using of message timestamps and caching, as well as other application-specific tracking mechanisms. For XrML licenses ownership is verified by use of keys, man-in-the-middle attacks are generally mitigated.

It is strongly RECOMMENDED that all relevant and immutable message data be signed.

It should be noted that transport-level security MAY be used to protect the message and the security token.

In order to *trust* XML based tokens, they SHOULD be signed using the mechanisms outlined in WS-Security. This allows readers of XML Tokens to be certain that the tokens have not been forged or altered in any way. It is strongly RECOMMENDED that the `<xrml:license>` elements be signed (either within the token, as part of the message, or both).

4 Acknowledgements

This specification was developed as a result of joint work of many individuals from the WSS TC including:

TBD

5 References

[DIGSIG] Informational RFC 2828, "Internet Security Glossary," May 2000.

[KEYWORDS] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, Harvard University, March 1997

[SAMLBind] Oasis Committee Specification 01, P. Mishra (Editor) Bindings and Profiles for the OASIS *Security Assertion Markup Language (SAML)*, May 2002.

[SAMLCore] Oasis Committee Specification 01, P. Hallem-Baker, and E. Maler, (Editors), *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)*, May 2002.

[SAMLReqs] OASIS Committee Consensus Draft, D. Platt, Evan Prodromou (Editors), SAML Requirements and Use Cases, OASIS, December 2001.

[SAMLSecure] OASIS Committee Specification 01, C. McLaren (Editor), Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) , May 2002.

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

W3C Working Draft, Nilo Mitra (Editor), SOAP Version 1.2 Part 0: Primer, June 2002.

W3C Working Draft, SOAP Version 1.2 Part 1: Messaging Framework, Martin Gudgin, Marc Hadley, Noah Mendelsohn, Jean-Jacques Moreau, Henrik Frystyk Nielsen (Editors), June 2002.

W3C Working Draft, Martin Gudgin, Marc Hadley, Noah Mendelsohn, Jean-Jacques Moreau, Henrik Frystyk Nielsen (Editors), SOAP Version 1.2 Part 2: Adjuncts, June 2002.

[URI] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax," RFC 2396, MIT/LCS, U.C. Irvine, Xerox Corporation, August 1998.

[WS-Security] TBS – point to the OASIS core draft

[XML-ns] W3C Recommendation, "Namespaces in XML," 14 January 1999.

[XML Signature] W3C Recommendation, "XML Signature Syntax and Processing," 12 February 2002.

[XML Token] Contribution to the WSS TC**,** Chris Kaler (Editor), WS-Security Profile for XML-based Tokens, August 2002.

232 # Appendix A: Revision History

Rev	Date	What
01	19-Sep-02	Initial draft produced by extracting SAML related content from [XML token]

233

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 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.