



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 eXtensible 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>).

30 **Table of Contents**

31 1 Introduction 4

32 1.1 Goals and Requirements 4

33 1.1.1 Requirements 4

34 1.1.2 Non-Goals 4

35 2 Notations and Terminology..... 5

36 2.1 Notational Conventions..... 5

37 2.2 Namespaces 5

38 2.3 Terminology 5

39 3 Usage 7

40 3.1 Processing Model..... 7

41 3.2 Attaching Security Tokens 7

42 3.3 Identifying and Referencing Security Tokens 7

43 3.4 Proof-of-Possession of Security Tokens..... 8

44 3.5 Error Codes 9

45 3.6 Threat Model and Countermeasures 9

46 4 Acknowledgements10

47 5 References11

48 Appendix A: Revision History.....12

49 Appendix B: Notices13

50

51 **1 Introduction**

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

56 Note that Section 1 is non-normative.

57 **1.1 Goals and Requirements**

58 The goal of this specification is to define the use of SAML assertions in the context of [WS-](#)
59 [Security](#) including for the purpose of securing [SOAP](#) message exchanges.

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

61 **1.1.1 Requirements**

62 TBS

63 ?

64 **1.1.2 Non-Goals**

65 The following topics are outside the scope of this document:

66 ? TBS

67

68 2 Notations and Terminology

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

70 2.1 Notational Conventions

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

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

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

80 Readers are presumed to be familiar with the terms in the [Internet Security Glossary](#).

81 2.2 Namespaces

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

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

86 The following namespaces are used in this document:

87

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

88 2.3 Terminology

89 This specification employs the terminology defined in the [WS-Security](#) Core Specification.

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

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

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

135 The following example illustrates a message with an [XML Signature](#) that references
 136 an XrML token.

```

137 <S:Envelope xmlns:S="...">
138   <S:Header>
139     <wsse:Security xmlns:wsse="...">
140       <xrml:license xmlns:xrml="..."
141         licenseId="urn:SecurityToken-ef375268" />
142       ...
143     </xrml:license>
144     <ds:Signature xmlns:ds="...">
145       ...
146       <ds:KeyInfo>
147         <wsse:SecurityTokenReference>
148           <wsse:Reference URI="urn:SecurityToken-ef375268"
149             xmktok:RefType="xrml:license"
150             xmlns:xmktok="..." />
151         </wsse:SecurityTokenReference>
152       </ds:KeyInfo>
153     </ds:Signature>
154     ...
155   </wsse:Security>
156 </S:Header>
157 <S:Body>
158   ...
159 </S:Body>
160 </S:Envelope>
161
162
  
```

163 3.4 Proof-of-Possession of Security Tokens

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

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

170 The following table illustrates how several different confirmation mechanisms are
 171 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".
--	-------------------------------

172 **3.5 Error Codes**

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

177 **3.6 Threat Model and Countermeasures**

178 The use of XrML licenses with [WS-Security](#) introduces no new threats beyond those
179 identified for XrML or WS-Security with other types of security tokens.

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

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

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

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

194 **4 Acknowledgements**

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

197 TBD

5 References

- 198
- 199 **[DIGSIG]** Informational RFC 2828, "[Internet Security Glossary](#)," May 2000.
- 200 **[KEYWORDS]** S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels,"
201 [RFC 2119](#), Harvard University, March 1997
- 202 **[SAMLBind]** Oasis Committee Specification 01, P. Mishra (Editor) [Bindings and](#)
203 [Profiles for the OASIS Security Assertion Markup Language \(SAML\)](#),
204 May 2002.
- 205 **[SAMLCore]** Oasis Committee Specification 01, P. Hallem-Baker, and E. Maler,
206 (Editors), [Assertions and Protocol for the OASIS Security Assertion](#)
207 [Markup Language \(SAML\)](#), May 2002.
- 208 **[SAMLReqs]** OASIS Committee Consensus Draft, D. Platt, Evan Prodromou (Editors),
209 [SAML Requirements and Use Cases](#), OASIS, December 2001.
- 210 **[SAMLSecure]** OASIS Committee Specification 01, C. McLaren (Editor), [Security and](#)
211 [Privacy Considerations for the OASIS Security Assertion Markup](#)
212 [Language \(SAML\)](#) , May 2002.
- 213 **[SOAP]** W3C Note, "[SOAP: Simple Object Access Protocol 1.1](#)," 08 May 2000.
- 214 W3C Working Draft, Nilo Mitra (Editor), [SOAP Version 1.2 Part 0: Primer](#),
215 June 2002.
- 216 W3C Working Draft, [SOAP Version 1.2 Part 1: Messaging Framework](#),
217 Martin Gudgin, Marc Hadley, Noah Mendelsohn, Jean-Jacques Moreau,
218 Henrik Frystyk Nielsen (Editors), June 2002.
- 219 W3C Working Draft, Martin Gudgin, Marc Hadley, Noah Mendelsohn,
220 Jean-Jacques Moreau, Henrik Frystyk Nielsen (Editors), [SOAP Version](#)
221 [1.2 Part 2: Adjuncts](#), June 2002.
- 222 **[URI]** T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers
223 (URI): Generic Syntax," [RFC 2396](#), MIT/LCS, U.C. Irvine, Xerox
224 Corporation, August 1998.
- 225 **[WS-Security]** TBS – point to the OASIS core draft
- 226 **[XML-ns]** W3C Recommendation, "[Namespaces in XML](#)," 14 January 1999.
- 227 **[XML Signature]** W3C Recommendation, "[XML Signature Syntax and Processing](#)," 12
228 February 2002.
- 229 **[XML Token]** Contribution to the WSS TC, Chris Kaler (Editor),
230 WS-Security Profile for XML-based Tokens, August 2002.
- 231

232

Appendix A: Revision History

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

233

234 **Appendix B: Notices**

235 OASIS takes no position regarding the validity or scope of any intellectual property or other rights
236 that might be claimed to pertain to the implementation or use of the technology described in this
237 document or the extent to which any license under such rights might or might not be available;
238 neither does it represent that it has made any effort to identify any such rights. Information on
239 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS
240 website. Copies of claims of rights made available for publication and any assurances of licenses
241 to be made available, or the result of an attempt made to obtain a general license or permission
242 for the use of such proprietary rights by implementors or users of this specification, can be
243 obtained from the OASIS Executive Director.

244 OASIS invites any interested party to bring to its attention any copyrights, patents or patent
245 applications, or other proprietary rights which may cover technology that may be required to
246 implement this specification. Please address the information to the OASIS Executive Director.

247 Copyright © OASIS Open 2002. *All Rights Reserved.*

248 This document and translations of it may be copied and furnished to others, and derivative works
249 that comment on or otherwise explain it or assist in its implementation may be prepared, copied,
250 published and distributed, in whole or in part, without restriction of any kind, provided that the
251 above copyright notice and this paragraph are included on all such copies and derivative works.
252 However, this document itself does not be modified in any way, such as by removing the
253 copyright notice or references to OASIS, except as needed for the purpose of developing OASIS
254 specifications, in which case the procedures for copyrights defined in the OASIS Intellectual
255 Property Rights document must be followed, or as required to translate it into languages other
256 than English.

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

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

264