



SAML XPath Attribute Profile

Committee Draft, 30 August 2005

Document identifier:

sstc-saml-xpath-attribute-profile-cd-01

Location:

http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

Editor:

Cameron Morris, Novell

Contributors:

Conor P. Cahill, AOL, Inc.
Rich Salz, DataPower
Scott Cantor, Internet2
John Kemp, Nokia
Lloyd Burch, Novell
Greg Whitehead, Trustgenix
Robert Aarts, Trustgenix
Anne Anderson, Sun Microsystems
Eve Maler, Sun Microsystems

Abstract:

This document defines an attribute profile for SAML V2.0 using XPath V1.0 for attribute names. It lets SAML attribute authorities map XML documents, associated with a user, into SAML attributes. In particular, this profile enables attribute authorities to map Liberty Alliance data services into SAML attributes. XPath attributes can then be queried, asserted, and published in metadata.

Status:

This is a **Committee Draft** approved by the Security Services Technical Committee on 30 August 2005.

Committee members should submit comments and potential errata to the security-services@lists.oasis-open.org list. Others should submit them to the security-services-comment@lists.oasis-open.org list (to post, you must subscribe; to subscribe, send a message to security-services-comment-request@lists.oasis-open.org with "subscribe" in the body) or use other OASIS-supported means of submitting comments. The committee will publish vetted errata on the Security Services TC web page (<http://www.oasis-open.org/committees/security/>).

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 web page for the Security Services TC (<http://www.oasis-open.org/committees/security/ipr.php>).

40 **Table of Contents**

41 1 Introduction..... 3

42 1.1 Notation..... 3

43 2 XPath Attribute Profile..... 4

44 2.1 Required Information..... 4

45 2.2 Motivating Use Case 4

46 2.3 SAML Attribute Naming..... 4

47 2.4 Profile-Specific XML Attributes..... 4

48 2.5 Interoperability..... 5

49 2.5.1 Text Nodes..... 5

50 2.5.2 Liberty Alliance Data Services Template..... 5

51 3 Examples..... 6

52 3.1 Personal Profile Text Node..... 6

53 3.2 Resource Indicator..... 6

54 3.3 XML-Structured Attribute Value..... 6

55 4 References..... 7

56

57 1 Introduction

58 This document defines an attribute profile for SAML V2.0 using XPath V1.0 for attribute names.

59 1.1 Notation

60 This specification uses normative text to describe the use of SAML attribute queries and assertions.

61 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
62 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as
63 described in [RFC 2119] :

64 ...they MUST only be used where it is actually required for interoperation or to limit behavior
65 which has potential for causing harm (e.g., limiting retransmissions)...

66 These keywords are thus capitalized when used to unambiguously specify requirements over protocol and
67 application features and behavior that affect the interoperability and security of implementations. When
68 these words are not capitalized, they are meant in their natural-language sense.

69 `Listings of XML schemas appear like this.`

70

71 `Example code listings appear like this.`

72 This specification uses the following typographical conventions in text: `<SAMLElement>`,
73 `<ns:ForeignElement>`, `Attribute`, **Datatype**, `OtherKeyword`.

74 2 XPath Attribute Profile

75 This document defines a profile for SAML V2.0 attributes using XPath V1.0 for attribute names and XPath
76 query results as attribute values.

77 2.1 Required Information

78 **Identification:** urn:oasis:names:tc:SAML:profiles:attribute:XPath

79 **Contact information:** security-services-comment@lists.oasis-open.org

80 **Description:** Given below.

81 **Updates:** N/A

82 **Extends:** N/A

83 2.2 Motivating Use Case

84 SAML V2.0 [SAMLCore] attribute authorities may have available XML documents and web services that
85 describe a user, such as services that implement the Data Services Template [DST] as defined by the
86 Liberty Alliance [LAP]. The attribute authority uses XPath V1.0 [XPathV10] to extract information out of
87 XML and place the information in assertions as attribute values. The XPath expression itself names the
88 attribute. The attribute authority configures XPath attributes that it will assert. Attribute requesters discover
89 possible XPath attributes via metadata [SAMLMeta].

90 2.3 SAML Attribute Naming

91 The `NameFormat` XML attribute in `<Attribute>` elements MUST be [http://www.w3.org/TR/1999/REC-](http://www.w3.org/TR/1999/REC-XPath-19991116)
92 [XPath-19991116](http://www.w3.org/TR/1999/REC-XPath-19991116). This indicates that the format of `Name` conforms to the XPath V1.0 specification.

93 An attribute authority MAY constrain the allowable XPath expressions. Attribute authorities MAY publish
94 the allowable XPath expressions in metadata by enumerating each allowed expression.

95 2.4 Profile-Specific XML Attributes

96 An `<Attribute>` with an XPath formatted name MUST have, within its scope, namespace declarations
97 (`xmlns:*`) for all prefixes used in the XPath.

98 The attribute `ResourceIndicator` MAY appear in `<Attribute>` to specify the URI of a specific
99 document. This attribute applies when the `<Subject>` element and the XPath expression do not uniquely
100 identify to which resource the XPath should apply. An `<Attribute>` without `ResourceIndicator`
101 implies that the attribute authority can uniquely identify the resource to which the XPath applies with the
102 `<Subject>` and XPath expression.

103 The schema for the `ResourceIndicator` attribute follows:

```
104 <schema  
105   targetNamespace="urn:oasis:names:tc:SAML:profiles:attribute:XPath"  
106   xmlns="http://www.w3.org/2001/XMLSchema"  
107   elementFormDefault="unqualified"  
108   attributeFormDefault="unqualified"  
109   blockDefault="substitution"  
110   version="2.0">  
111   <annotation>  
112     <documentation>  
113       Document identifier: draft-saml-xpath-attribute-profile  
114       Location: http://docs.oasis-open.org/security/saml
```

```
115         Revision history:
116             Version 1 (May, 2005):
117                 Custom schema for the XPath attribute profile.
118         </documentation>
119     </annotation>
120     <attribute name="ResourceIndicator" type="anyURI"/>
121 </schema>
```

122 **2.5 Interoperability**

123 Since implementations and configurations may support different subsets of XPath attributes, the following
124 sections provide rules to achieve some level of interoperability.

125 **2.5.1 Text Nodes**

126 To encourage interoperability, supported XPaths SHOULD include all possible text nodes. This helps
127 requesting parties since they do not need to parse an asserted attribute value. XPaths to these leaf nodes
128 MUST contain slash-separated, absolute paths. However, some documents might not allow the
129 enumeration of all text nodes in metadata, simply because the arbitrary structure of these documents.

130 **2.5.2 Liberty Alliance Data Services Template**

131 The Data Services Template, defined by the Liberty Alliance, recommends that conforming
132 implementations use XPath to query documents or services related to an identity. Several of these
133 services, such as the Employee Profile Service [EP] and the Personal Profile Service [PP], define a
134 minimum set of XPaths a service must allow. This defines one interoperable set of XPath expressions
135 implementations must support. Similarly, implementations that map these documents to attributes of this
136 profile MUST allow queries for the text nodes of the XPaths defined by these data services. Note, that
137 these services usually list the elements that directly contain text nodes.

138 For example, if the Liberty service requires support of the XPath expression of
139 `"/pp:PP/pp:LegalIdentity/pp:LegalName"`, then implementations of this profile must support the
140 value of `"/pp:PP/pp:LegalIdentity/pp:LegalName/text ()"`.

141 3 Examples

142 Following are some examples of this attribute profile.

143 3.1 Personal Profile Text Node

144 This example shows an attribute named with an XPath that identifies the Liberty Personal Profile
145 <LegalName> element's text content as the attribute value of interest; the attribute name is the XPath
146 that leads to the relevant text node.

```
147 <saml:Attribute  
148   Name="/pp:PP/pp:LegalIdentity/pp:LegalName/text()" "  
149   NameFormat="http://www.w3.org/TR/1999/RECXPath-199911169"  
150   xmlns:pp="urn:liberty:id-sis-pp:2003-08"  
151   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">  
152   <saml:AttributeValue>John Q. Doe</saml:AttributeValue>  
153   <saml:AttributeValue>John Quincy Doe</saml:AttributeValue>  
154 </saml:Attribute>
```

155 3.2 Resource Indicator

156 This example shows the use of the optional ResourceIndicator defined by this profile.

```
157 <saml:Attribute  
158   Name="/r:Resume/r:PreviousEmployment/r:Employer/text()" "  
159   NameFormat="http://www.w3.org/TR/1999/RECXPath-199911169"  
160   xpathtr:ResourceIndicator="http://example.com/~jdoe/resume.xml"  
161   xmlns:r="urn:oasis:names:sample:resume"  
162   xmlns:xpathtr="urn:oasis:names:tc:SAML:profiles:attribute:XPath"  
163   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">  
164   <saml:AttributeValue>Acme, Inc.</saml:AttributeValue>  
165   <saml:AttributeValue>Local Grocery</saml:AttributeValue>  
166 </saml:Attribute>
```

167 3.3 XML-Structured Attribute Value

168 This example shows an attribute value that contains XML-structured content, rather than just text. The
169 attribute name does not include a specification of a text node.

```
170 <saml:Attribute Name="/r:Resume/r:PreviousEmployment/r:Employer"  
171   NameFormat="http://www.w3.org/TR/1999/RECXPath-199911169"  
172   xpathtr:ResourceIndicator="http://example.com/~jdoe/resume.xml"  
173   xmlns:r="urn:oasis:names:sample:resume"  
174   xmlns:xpathtr="urn:oasis:names:tc:SAML:profiles:attribute:XPath"  
175   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">  
176   <saml:AttributeValue>  
177     <r:Employer current="true">Acme, Incorporated</r:Employer>  
178   </saml:AttributeValue>  
179   <saml:AttributeValue>  
180     <r:Employer current="false">Local Grocery</r:Employer>  
181   </saml:AttributeValue>  
182 </saml:Attribute>
```

183 4 References

- 184 **[DST]** J. Kainulainen et al., *Liberty ID-WSF Data Services Template Specification*.
185 Available at <http://projectliberty.org/specs/liberty-idwsf-dst-v1.0.pdf>.
- 186 **[EP]** Sampo Kellomäki et al., *Liberty ID-SIS Employee Profile Service Specification*.
187 Available at <http://projectliberty.org/specs/liberty-idsis-ep-v1.0.pdf>.
- 188 **[LAP]** Liberty Alliance Project. See <http://www.projectliberty.org/>.
- 189 **[PP]** Sampo Kellomäki et al., *Liberty ID-SIS Personal Profile Service Specification*.
190 Available at <http://projectliberty.org/specs/liberty-idsis-pp-v1.0.pdf>.
- 191 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
192 RFC 2119, March 1997. See <http://www.ietf.org/rfc/rfc2119.txt>.
- 193 **[RFC3280]** *The TLS Protocol Version 1.0*, <http://www.ietf.org/rfc/rfc3280.txt>
- 194 **[SAMLCore]** S. Cantor et al., *Assertions and Protocols for the OASIS Security Assertion
195 Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID
196 saml-core-2.0-os. See [http://docs.oasis-open.org/security/saml/v2.0/saml-core-
197 2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf).
- 198 **[SAMLMeta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language
199 (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-metadata-2.0-
200 os. See <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.
- 201 **[XPathV10]** J. Clark and S. DeRose, World Wide Web Consortium Recommendation, 16 Nov
202 1999. <http://www.w3.org/TR/1999/REC-XPath-19991116>.
- 203

204 A. Acknowledgments

205 The editor would like to acknowledge the contributions of the OASIS Security Services Technical
206 Committee, whose voting members at the time of publication were:

- 207 • Conor P. Cahill, AOL, Inc.
- 208 • Hal Lockhart, BEA Systems, Inc
- 209 • Thomas Wisniewski, Entrust
- 210 • Irving Reid, Hewlett-Packard Company
- 211 • Guy Denton, IBM
- 212 • Heather Hinton, IBM
- 213 • Anthony Nadalin, IBM
- 214 • Scott Cantor, Internet2
- 215 • RL "Bob" Morgan, Internet2
- 216 • John Hughes, Individual
- 217 • Nick Ragouzis, Individual
- 218 • Frederick Hirsch, Nokia
- 219 • Senthil Sengodan, Nokia
- 220 • Abbie Barbir, Nortel
- 221 • Cameron Morris, Novell
- 222 • Paul Madsen, NTT USA
- 223 • Ari Kermaier, Oracle
- 224 • Vamsi Motukuru, Oracle
- 225 • Brian Campbell, Ping Identity
- 226 • Darren Platt, Ping Identity
- 227 • Prateek Mishra, Principal Identity
- 228 • Rob Philpott, RSA Security
- 229 • Jahan Moreh, Sigaba
- 230 • Eve Maler, Sun Microsystems
- 231 • Emily Xu, Sun Microsystems
- 232 • Mike Beach, The Boeing Company
- 233 • Greg Whitehead, Trustgenix
- 234 • David Staggs, Veteran's Health Admin

235 The editor also wishes to acknowledge Doug Earl and Stuart Jensen of Novell for their contributions to this
236 specification.

B. Notices

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

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

249 **Copyright © OASIS Open 2005. All Rights Reserved.**

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

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

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