



SAML XPath Attribute Profile

OASIS Draft, 23 May 2005

Document identifier:

draft-saml-xpath-attribute-profile

Location:

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

Editors:

TBD

Contributors:

TBD

Abstract:

This profiles the use of SAML attributes for using XPath URI's as attribute names. This lets XML documents, associated with a user, be mapped into a set of SAML attributes. In particular, this lets Liberty Alliance data services be mapped into SAML attributes. These attributes can then be published in metadata, queried and asserted.

Status:

This is a Draft.

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>).

29 1 XPath Attribute Profile

30 XML documents describing a user can be mapped arbitrarily into SAML attributes [SAMLv2Core]. This
31 profile defines how to use XPath [XPath] as a means to map these documents into SAML attributes.
32 XPath defines a compact URI structure to reference parts, and query for parts, of an XML Document.
33 This profile is particularly focused on referencing parts of identity data services accessible via Liberty
34 Alliance Data services template [DST].

35 1.1 Required Information

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

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

38 **Description:** Given below.

39 **Updates:** NA

40 1.2 SAML attribute naming

41 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)
42 **XPath-19991116**. This indicates that the format of `Name` conforms to the XPath specification.

43 The allowable XPath expressions can be constrained by an Attribute Authority. Constraints to allowable
44 XPath expressions can be published in metadata [SAMLMeta] by enumerating each allowed expression.

45 1.3 Profile-Specific XML Attributes

46 The `ResourceIndicator` attribute indicates to which the document the XPath expression applies. The
47 `ResourceIndicator` can specify either an actual document URI or a document schema URI. A
48 schema URI implies that the attribute authority must locate a document or service that both applies to the
49 user and conforms to the schema indicated.

50 1.4 Interoperability

51 Implementations and configurations can, and probably will, only support a subset of XPath attributes. In
52 order to achieve interoperability some guidelines should be followed.

53 Text Nodes

54 To encourage interoperability, it is recommended that supported XPaths include all possible text nodes.
55 XPaths to these leaf nodes should be slash separated, absolute paths. However, enumerating these text
56 nodes in metadata may not always be possible, because the structure of these documents can be
57 arbitrary. Support for text nodes is encouraged because requesting parties do not need to parse the
58 resulting values.

59 Liberty Alliance Data Services Template

60 The data services template, defined by Liberty Alliance [LAP], recommends that conforming
61 implementation use XPath to query documents or services related to an identity. Several of these
62 services [EP][PP] define a minimum set of XPaths a service must allow. This defines one inter-operable

63 set for all implementations. Similarly, implementations that map these documents to attributes of this
64 profile should allow queries for the text nodes of the XPaths defined by these data services. Note, that
65 these services usually list the elements that directly contain text nodes.

66 For example, if the XPath value `"/PP/LegalIdentity/LegalName"` is required by a Liberty service
67 then `"/PP/LegalIdentity/LegalName/text ()"` should be supported by implementation of this
68 profile.

69 **1.5 Example**

70 **Personal Profile Example**

```
71 <saml:Attribute NameFormat="http://www.w3.org/TR/1999/REC-XPath-19991116"  
72     Name="/PP/LegalIdentity/LegalName/text ()"  
73     DocumentType="urn:liberty:id-sis-pp:2003_08">  
74 <saml:AttributeValue xsi:type="xs:string">John Q. Doe</saml:AttributeValue>  
75 </saml:Attribute>
```

2 References

76

- 77 [SSTC] “OASIS Security Services Technical Committee”. See
78 <http://www.oasis-open.org/committees/security/>
- 79 [SAMLv2.0] OASIS Security Services Technical Committee, “Security Assertion
80 Markup Language (SAML) Version 2.0 Specification Set”. OASIS
81 Standard, 15 Mar 2005. Available at [http://docs.oasis-
82 open.org/security/saml/v2.0/saml-2.0-os.zip](http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip)
- 83 [SAMLv2Core] S. Cantor et al., “Assertions and Protocols for the OASIS Security
84 Assertion Markup Language (SAML) V2.0”. OASIS, March 2005.
85 Document ID saml-core-2.0-os. Available at [http://docs.oasis-
86 open.org/security/saml/v2.0/saml-core-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)
- 87 [SAMLv2Meta] S. Cantor et al. *Metadata for the OASIS Security Assertion Markup
88 Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID
89 saml-metadata-2.0-os. See [http://www.oasis-
90 open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 91 [XML] Bray, T., Paoli, J., Sperberg-McQueen, C.M. and E. Maler, François
92 Yergeau, “Extensible Markup Language (XML) 1.0 (Third Edition)”,
93 World Wide Web Consortium Recommendation REC-xml, Feb 2004,
94 Available at <http://www.w3.org/TR/REC-xml/>
- 95 [XPath] J. Clark and S. DeRose, World Wide Web Consortium
96 Recommendation, 16 Nov 1999. Available at
97 <http://www.w3.org/TR/1999/REC-XPath-19991116>
- 98 [LAP] “Liberty Alliance Project”. See <http://www.projectliberty.org/>
- 99 [DST] J. Kainulainen et al., “Liberty ID-WSF Data Services Template
100 Specification”. Available at [http://projectliberty.org/specs/liberty-
101 idwsf-dst-v1.0.pdf](http://projectliberty.org/specs/liberty-idwsf-dst-v1.0.pdf)
- 102 [PP] Sampo Kellomäki et al., “Liberty ID-SIS Personal Profile Service
103 Specification”. Available at [http://projectliberty.org/specs/liberty-
104 idsis-pp-v1.0.pdf](http://projectliberty.org/specs/liberty-idsis-pp-v1.0.pdf)
- 105 [EP] Sampo Kellomäki et al., “Liberty ID-SIS Employee Profile Service
106 Specification”. Available at [http://projectliberty.org/specs/liberty-
107 idsis-ep-v1.0.pdf](http://projectliberty.org/specs/liberty-idsis-ep-v1.0.pdf)

108 **3 Acknowledgments**

109 The editors would like to acknowledge the contributions of the OASIS Security Services Technical
110 Committee, whose voting members at the time of publication were:

- 111 • TBD

A. Revision History

Rev	Date	By Whom	What
0	03/30/05	Cameron Morris	First draft
1	04/14/05	Cameron Morris	Added Interoperability text, Added XPath URL as the NameFormat, and changed ServiceType to DocumentType
2	05/03/05	Cameron Morris	Added text addressing Robert Aarts comments concerning text nodes
3	05/23/05	Cameron Morris	Renamed DocumentType to ResourceIndicator. Extended definition of ResourceIndicator to allow pointing to specific XML documents. Renamed document and document urn.

B. Notices

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

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

125 **Copyright © OASIS Open 2003-2005. All Rights Reserved.**

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

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

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

140 JavaScript is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and
141 other countries.