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).

1 XPath Attribute Profile

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

1.1 Required Information

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

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

Description: Given below.

Updates: NA

1.2 SAML attribute naming

The `NameFormat` XML attribute in `Attribute` elements must be **http://www.w3.org/TR/1999/REC-XPath-19991116.** This indicates that the format of `Name` conforms to the XPath specification.

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

1.3 Profile-Specific XML Attributes

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

1.4 Interoperability

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

Text Nodes

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

Liberty Alliance Data Services Template

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

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

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

1.5 Example

Personal Profile Example

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

2 References

[SSTC] **"*OASIS Security Services Technical Committee*". See http://www.oasis-open.org/committees/security/**

[SAMLv2.0] **OASIS Security Services Technical Committee, "*Security Assertion Markup Language (SAML) Version 2.0 Specification Set*". OASIS Standard, 15 Mar 2005. Available at http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip**

[SAMLv2Core] **S. Cantor et al., "*Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*". OASIS, March 2005. Document ID saml-core-2.0-os. Available at http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf**

[SAMLMeta] **S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-metadata-2.0-os. See http://www.oasis-open.org/committees/security/.**

[XML] **Bray, T., Paoli, J., Sperberg-McQueen, C.M. and E. Maler, François Yergeau, "*Extensible Markup Language (XML) 1.0 (Third Edition)*", World Wide Web Consortium Recommendation REC-xml, Feb 2004, Available at http://www.w3.org/TR/REC-xml/**

[XPath] **J. Clark and S. DeRose, World Wide Web Consortium Recommendation, 16 Nov 1999. Available at** http://www.w3.org/TR/1999/REC-XPath-19991116

[LAP] **"*Liberty Alliance Project*". See http://www.projectliberty.org/**

[DST] **J. Kainulainen et al., *"Liberty ID-WSF Data Services Template Specification"*. Available at http://projectliberty.org/specs/liberty-idwsf-dst-v1.0.pdf**

[PP] **Sampo Kellomäki et al., *"Liberty ID-SIS Personal Profile Service Specification"*. Available at http://projectliberty.org/specs/liberty-idsis-pp-v1.0.pdf**

[EP] **Sampo Kellomäki et al., "*Liberty ID-SIS Employee Profile Service Specification".* Available at http://projectliberty.org/specs/liberty-idsis-ep-v1.0.pdf**

3 Acknowledgments

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

- TBD

112 # 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

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.