SAML XPath Attribute Profile

OASIS Draft, 15 August 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 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 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 Introduction

XML documents describing a user can map 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 focuses on referencing parts of identity data services accessible via Liberty Alliance Data services template [DST].

1.1 Notation

This specification uses normative text to define an extension to the SAML V2.0 metadata specification. The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in [RFC 2119] :

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

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

```
Listings of XML schemas appear like this.
```

```
Example code listings appear like this.
```

2 XPath Attribute Profile

This section defines a profile for XPath named SAML v2 attributes.

~~XML documents describing a user can map 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 focuses on referencing parts of identity data services accessible via Liberty Alliance Data services template [DST].~~

2.1 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

2.2 SAML attribute naming

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

An Attribute Authority MAY constrain the allowable XPath expressions. Attribute Authorities MAY~~can constrain the allowable XPath expressions. Attribute Authorities can~~ publish the allowable XPath expressions in metadata [SAMLMeta] by enumerating each allowed expression.

2.3 Profile-Specific XML Attributes

Implementation MUST use the `xmlns` attribute to qualify prefixes found in the XPath attributes. This attribute can reside anywhere in the document within the scope of an XPath SAMLAttribute~~must use the `xmlns` attribute to qualify prefixes found in the XPath attributes. This attribute can reside anywhere within the document~~.

The attribute `ResourceIndicator` MAY specify the URI of a specific document. If the `Subject` element and `XPath` attribute (including any associated namespace declarations) do not uniquely identify a resource, then `ResourceIndicator` attribute MAY~~can specify the URI of a specific document. If the `Subject` element and `XPath` attribute (including any associated namespace declarations) do not uniquely identify a resource, then `ResourceIndicator` attribute can~~ identify the resource to which the XPath should apply.

Schema for `ResourceIndicator` attribute follows:

```
<attribute name="ResourceIndicator" type="anyURI"/>
```

2.4 Interoperability

Since implementations and configurations may support different subsets of XPath attributes, the following sections provide rules to achieve some level of~~Implementations and configurations might only support a subset of XPath attributes. Implementation must follow the following guidelines to achieve~~ interoperability.

Text Nodes

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

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 MUST~~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 Liberty service requires support of the XPath expression of "`/pp:PP/pp:LegalIdentity/pp:LegalName`", then implementations of this profile must~~should~~ support the value of "`/pp:PP/pp:LegalIdentity/pp:LegalName/text()`".

2.5 Examples

Personal Profile Example:

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

Resource Indicator Example:

```
<saml:Attribute Name="/r:Resume/r:PreviousEmployement/r:Employeer/text()"
NameFormat="http://www.w3.org/TR/1999/RECXPath-199911169"
xpath:ResourceIndicator="http://oasis-open.org/~jdoe/resume.xml”
xmlns:r="urn:oasis:names:sample:resume"
xmlns:xpath="urn:oasis:names:tc:SAML:profiles:attribute:XPath"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
   <saml:AttributeValue>Acme, Incorporated</saml:AttributeValue>
   <saml:AttributeValue>Local Grocery Company</saml:AttributeValue>
</saml:Attribute>
```

3 References

[RFC 2119]	S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.
[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

4 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

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.
4	07/05/05	Cameron Morris	Added text to make ResourceIndicator optional. Added text to describe the need to qualify namespace prefixes in XPath attribute names.
4	08/15/05	Cameron Morris	Added the normative wording of MUST, MAY, SHOULD... Fixed wording on the scope of where xmlns attributes should be placed. Added Schema for ResourceIndicator
~~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.~~
~~4~~	~~07/05/05~~	~~Cameron Morris~~	~~Added text to make ResourceIndicator optional. Added text to describe the need to qualify namespace prefixes in XPath attribute names.~~

~~Rev~~	~~Date~~	~~By Whom~~	~~What~~

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.

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

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