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).

Table of Contents

1 Introduction

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

1.1 Notation

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

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.
```

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

2 XPath Attribute Profile

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

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: N/A

Extends: N/A

2.2 Motivating Use Case

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

2.3 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 V1.0 specification.

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

2.4 Profile-Specific XML Attributes

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

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

The schema for the `ResourceIndicator` attribute follows:

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

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

2.5 Interoperability

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

2.5.1 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 contain slash-separated, absolute paths. However, some documents might not allow the enumeration of all text nodes in metadata, simply because the arbitrary structure of these documents.

2.5.2 Liberty Alliance Data Services Template

The Data Services Template, defined by the Liberty Alliance, recommends that conforming implementations use XPath to query documents or services related to an identity. Several of these services, such as the Employee Profile Service [EP] and the Personal Profile Service [PP], define a minimum set of XPaths a service must allow. This defines one interoperable set of XPath expressions implementations must support. Similarly, implementations that map these documents to attributes of this profile MUST 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 support the value of "`/pp:PP/pp:LegalIdentity/pp:LegalName/text()`".

3 Examples

Following are some examples of this attribute profile.

3.1 Personal Profile Text Node

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

```
<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>
```

3.2 Resource Indicator

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

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

3.3 XML-Structured Attribute Value

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

```
<saml:Attribute Name="/r:Resume/r:PreviousEmployment/r:Employer"
NameFormat="http://www.w3.org/TR/1999/RECXPath-199911169"
xpattr:ResourceIndicator="http://example.com/~jdoe/resume.xml”
xmlns:r="urn:oasis:names:sample:resume"
xmlns:xpattr="urn:oasis:names:tc:SAML:profiles:attribute:XPath"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
   <saml:AttributeValue>
      <r:Employer current=”true”>Acme, Incorporated</r:Employer>
   </saml:AttributeValue>
   <saml:AttributeValue>
      <r:Employer current=”false”>Local Grocery</r:Employer>
   </saml:AttributeValue>
</saml:Attribute>
```

4 References

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

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

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

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

[RFC3280] *The TLS Protocol Version 1.0*, http://www.ietf.org/rfc/rfc3280.txt

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

[XPathV10] J. Clark and S. DeRose, World Wide Web Consortium Recommendation, 16 Nov 1999. http://www.w3.org/TR/1999/REC-XPath-19991116.

A. Acknowledgments

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

- Conor P. Cahill, AOL, Inc.
- Hal Lockhart, BEA Systems, Inc
- Thomas Wisniewski, Entrust
- Irving Reid, Hewlett-Packard Company
- Guy Denton, IBM
- Heather Hinton, IBM
- Anthony Nadalin, IBM
- Scott Cantor, Internet2
- RL “Bob” Morgan, Internet2
- John Hughes, Individual
- Nick Ragouzis, Individual
- Frederick Hirsch, Nokia
- Senthil Sengodan, Nokia
- Abbie Barbir, Nortel
- Cameron Morris, Novell
- Paul Madsen, NTT USA
- Ari Kermaier, Oracle
- Vamsi Motukuru, Oracle
- Brian Campbell, Ping Identity
- Darren Platt, Ping Identity
- Prateek Mishra, Principal Identity
- Rob Philpott, RSA Security
- Jahan Moreh, Sigaba
- Eve Maler, Sun Microsystems
- Emily Xu, Sun Microsystems
- Mike Beach, The Boeing Company
- Greg Whitehead, Trustgenix
- David Staggs, Veteran's Health Admin

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

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.