SAML V2.0 Attribute Extensions Version 1.0

Committee Specification 01

4 August 2009

Specification URIs:

This Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-ext-cs-01.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-ext-cs-01.odt (Authoritative)

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-ext-cs-01.pdf

Previous Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-ext-cd-01.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-ext-cd-01.odt (Authoritative)

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-ext-cd-01.pdf

Latest Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-ext.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-ext.odt

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-ext.pdf

Technical Committee:

OASIS Security Services TC

Chair(s):

Hal Lockhart, BEA Systems, Inc.
Brian Campbell, Ping Identity Corporation

Editors:

Scott Cantor, Internet2

Declared XML Namespaces(s):

urn:oasis:names:tc:SAML:attributes:ext

Abstract:

This profile defines new XML attributes useful in extending the `<saml:Attribute>` element to communicate additional information about SAML attributes, their origin, rules for handling them, or any other kind of "meta-information" deemed interesting.

Status

This document was last revised or approved by the SSTC on the above date. The level of approval is also listed above. Check the current location noted above for possible later revisions of this document. This document is updated periodically on no particular schedule.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC by using the "Send A Comment" button on the TC's web page at 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 IPR section of the TC web page (http://www.oasis-open.org/committees/security/ipr.php).

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/security.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

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

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 OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

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' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on 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 implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

1 Introduction

Attribute extensions consist of XML attributes defined for inclusion in the various "attribute-extensible" elements in the SAML schema, as noted in section 7 of the SAML V2.0 core specification [SAML2Core].

This specification defines XML attributes for use within the `<saml:Attribute>` element to carry additional "meta-information" about a SAML attribute to a relying party. Such information is always considered optional and does not modify any of the normative processing rules defined by [SAML2Core].

1.1 Notation

This specification uses normative text.

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 [RFC2119]:

> …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.
```

Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

Prefix	XML Namespace	Comments
`saml:`	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAML2Core].
`attrext:`	urn:oasis:names:tc:SAML:attributes:ext	This is the namespace defined by this document and its accompanying schema [AttrExt-xsd].
`xsd:`	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [Schema1]. In schema listings, this is the default namespace and no prefix is shown.
`xsi:`	http://www.w3.org/2001/XMLSchema-instance	This is the XML Schema namespace for schema-related markup that appears in XML instances [Schema1].

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

1.2 Normative References

[AttrExt-xsd] OASIS Committee Draft 01, "SAML V2.0 Attribute Extension Schema", December 2008. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-ext.xsd

[RFC2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

[SAML2Core] OASIS Standard, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[Schema1] H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/. Note that this specification normatively references [Schema2], listed below.

[Schema2] Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/.

2 SAML V2.0 Attribute Extensions

2.1 Required Information

Identification: `urn:oasis:names:tc:SAML:attribute:ext`

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

Description: Given below.

Updates: None.

2.2 Profile Overview

This profile defines a set of optional XML attribute extensions that may appear in the `<saml:Attribute>` element to standardize the delivery of information found useful to SAML-enabled applications. As with all SAML extensions, these attributes are non-critical in nature, with no mandatory processing rules or intended impact on existing software or deployments.

Unless otherwise specified, these extension attributes should be understood to be composable, both with other extensions, and with any SAML profiles that make use of SAML attributes.

2.3 OriginalIssuer

The `OriginalIssuer` XML attribute identifies the entity that originally issued the containing SAML attribute and its values. It is analagous to the `<saml:Issuer>` element found in a SAML assertion, and allows the source of an attribute to be maintained for informational purposes across proxies/gateways, or in XML constructs other than SAML assertions.

The value of this attribute MUST be an entity identifier, per section 8.3.6 of [SAML2Core].

The following schema fragment defines the `OriginalIssuer` attribute:

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

2.3.1 Example

The example below shows a SAML attribute with an `OriginalIssuer` extension.

```
<saml:Attribute
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
       Name="urn:oid:2.5.4.42" FriendlyName="givenName"
      xmlns:ext="urn:oasis:names:tc:SAML:attribute:ext"
      ext:OriginalIssuer="https://idp.example.com/saml">
   <saml:AttributeValue xsi:type="xsd:string">Scott</saml:AttributeValue>
</saml:Attribute>
```

2.4 LastModified

The `LastModified` XML attribute indicates the date and time at which the containing SAML attribute's values were last modified, generally based on information kept at the attribute's ultimate source. See section 1.3.3 of [SAML2Core] for applicable rules on the use of date and time information in SAML constructs.

The following schema fragment defines the `LastModified` attribute:

```
<attribute name="LastModified" type="dateTime"/>
```

2.4.1 Example

The example below shows a SAML attribute with the `LastModified` extension.

```
<saml:Attribute
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
       Name="urn:oid:2.5.4.42" FriendlyName="givenName"
      xmlns:ext="urn:oasis:names:tc:SAML:attribute:ext"
      ext:LastModified="2008-10-31T12:46:02Z">
   <saml:AttributeValue xsi:type="xsd:string">Scott</saml:AttributeValue>
</saml:Attribute>
```

3 Conformance

3.0.1 SAML V2.0 Attribute Extensions

An asserting party can claim to support an extension attribute if it provides a means to include the XML attribute in the `<saml:Attribute>` information that it asserts.

A relying party can claim to support an extension attribute simply by demonstrating the ability to successfully process a `<saml:Attribute>` element that contains the XML attribute. Successful processing MAY consist of no changes to a relying party's behavior.

Appendix A. Acknowledgements

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

- George Fletcher, AOL
- Rob Philpott, EMC Corporation
- John Bradley, Individual
- Jeff Hodges, Individual
- Scott Cantor, Internet2
- Nate Klingenstein, Internet2
- Bob Morgan, Internet2
- Eric Tiffany, Liberty Alliance Project
- Tom Scavo, National Center for Supercomputing Applications (NCSA)
- Frederick Hirsch, Nokia Corporation
- Srinath Godavarthi, Nortel Networks Limited
- Paul Madsen, NTT Corporation
- Ari Kermaier, Oracle Corporation
- Hal Lockhart, Oracle Corporation
- Brian Campbell, Ping Identity Corporation
- Anil Saldhana, Red Hat
- Kent Spaulding, Skyworth TTG Holdings Limited
- Eve Maler, Sun Microsystems
- Emily Xu, Sun Microsystems
- Duane DeCouteau, Veterans Health Administration
- David Staggs, Veterans Health Administration

Appendix B. Revision History

- Draft 01.
- Draft 02, clarifed language in a couple of places.
- Committee Draft 01, CD edits.