SAML V2.0 Metadata Extension for Entity Attributes Version 1.0

Committee Draft 01

6 February 2009

Specification URIs:

This Version:

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

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

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

Previous Version:

None

Latest Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.odt

http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.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:metadata:attribute

Abstract:

This profile defines an extension element for use in attaching SAML attributes to an `<md:EntityDescriptor>` or `<md:EntitiesDescriptor>` element, to communicate an arbitrary set of additional information about an entity in its metadata.

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

The SAML V2.0 metadata specification [SAML2Meta] includes the <md:Extensions> element in various places, including the <md:EntityDescriptor> and <md:EntitiesDescriptor> elements, for use in extending the specification by carrying externally defined content. This profile defines such an extension element, <mdattr:EntityAttributes>, as a container for one or more <saml:Attribute> or <saml:Assertion> elements. It allows an arbitrary set of attribute information to be carried within an entity's (or a group of entities') metadata to communicate additional information about that entity (or group) to a metadata consumer.

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].
md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace defined in the SAML V2.0 metadata specification [SAML2Meta].
mdattr:	urn:oasis:names:tc:SAML:metadata:attribute	This is the namespace defined by this document and its accompanying schema [MetaAttr-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

[MetaAttr-xsd] S. Cantor. SAML V2.0 Metadata Extension for Entity Attributes Schema. OASIS SSTC, November 2008. Document ID sstc-metadata-attr.xsd. See http://www.oasis-open.org/committees/security/.

[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.

[SAML2Meta] OASIS Standard, *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-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 Metadata Extension for Entity Attributes

2.1 Required Information

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

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

Description: Given below.

Updates: None.

2.2 Profile Overview

SAML deployments and SAML-enabled applications often make extensive use of the `<saml:Attribute>` element as a vehicle for carrying and consuming arbitrary structured information about assertion subjects. This profile defines a metadata extension element as a container for one or more such elements, or more generically for communicating a SAML attribute assertion. It allows attribute information to be carried within an entity's (or a group of entities') metadata to communicate additional information about that entity (or group) to a metadata consumer, much as an assertion can carry attributes about a subject.

In some SAML deployments, metadata is often maintained and signed by a third party federation operator, and this mechanism allows that operator to include extensible information (possibly signed by still another party) about the federation's member sites, such as their adherence to optional federation policies. Metadata consumers can then choose to process or ignore such information as they deem necessary.

This profiles defines no specific attributes to be communicated, but additional profiles might leverage it to do so.

2.3 Element <mdattr:EntityAttributes>

The `<mdattr:EntityAttributes>` element is a wrapper for one or more `<saml:Attribute>` or `<saml:Assertion>` elements. Assertions that appear MUST conform to the profile in section 2.4, and will contain only attribute statements. Relying parties MUST process assertions in accordance with the standard processing rules in [SAML2Core].

If this element is used within the `<md:Extensions>` element of an `<md:EntityDescriptor>` element, then it binds the enclosed SAML attributes (or the attributes within the enclosed assertions) to the enclosing entity.

If this element is used within the `<md:Extensions>` element of an `<md:EntitiesDescriptor>` element, then only `<saml:Attribute>` elements are to be used; `<saml:Assertion>` elements MUST NOT be included. The enclosed attributes are bound to each `<md:EntityDescriptor>` within the enclosing `<md:EntitiesDescriptor>` element.

The meaning of this element is undefined by this profile if it appears anywhere else within a metadata instance, or within any other XML document.

Finally, this element MUST NOT appear more than once within a given `<md:Extensions>` element.

The following schema fragment defines the `<mdattr:EntityAttributes>` element:

```
<element name="EntityAttributes" type="mdattr:EntityAttributesType"/>
<complexType name="EntityAttributesType">
  <choice maxOccurs="unbounded">
```

```
    <element ref="saml:Attribute"/>
    <element ref="saml:Assertion"/>
  </sequence>
</complexType>
```

2.4 Assertion Profile

All SAML assertions that appear in an `<mdattr:EntityAttributes>` element MUST conform to the following restrictions:

- The assertion's `<saml:Subject>` element MUST contain a `<saml:NameID>` element with a `Format` of `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`. The value of the `<saml:NameID>` MUST correspond to the `entityID` of the enclosing `<md:EntityDescriptor>` element.
- The assertion's subject element MUST NOT include any `<saml:SubjectConfirmation>` elements.
- One (and only one) `<saml:AttributeStatement>` element MUST be included. Other statement types MUST NOT be included.
- The assertion MUST be independently signed (rather than inheriting a signature from the metadata itelf).

Apart from the above constraints, any other legal assertion content MAY be included, including the `<saml:Conditions>` element and any conditions within it.

3 Conformance

3.0.1 SAML V2.0 Metadata Extension for Entity Attributes

A metadata producer conforms to this profile if it has the ability to produce extended metadata in accordance with section 2.

A metadata consumer conforms to this profile if it can consume extended metadata in accordance with section 2.

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:

- 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)
- Peter Davis, NeuStar, Inc.
- 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, add option for assertions, fix the schema and conformance sections.
- Committee Draft 01, CD edits.