Independent Submission
Request for Comments: 8409
Category: Informational
ISSN: 2070-1721

I. Young, Ed.
Independent
L. Johansson
SUNET
S. Cantor
Shibboleth Consortium

August 2018

The Entity Category Security Assertion Markup Language (SAML) Attribute Types

Abstract

This document describes two SAML entity attributes: one that can be used to assign category membership semantics to an entity and another for use in claiming interoperation with or support for entities in such categories.

This document is a product of the working group process of the Research and Education FEDerations (REFEDS) group.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8409.

Table of Contents

1. Introduction

This document describes a SAML attribute called the "entity category attribute". Values of this attribute represent entity types or categories. When used with the SAML V2.0 Metadata Extension for Entity Attributes [SAML2MetadataAttr], each such entity category attribute value represents a claim that the entity thus labeled meets the requirements of, and is asserted to be a member of, the indicated category.

These category membership claims MAY be used by a relying party to provision policy for release of attributes from an identity provider, to influence user interface decisions such as those related to identity provider discovery, or for any other purpose. In general, the intended uses of any claim of membership in a given category will depend on the details of the category's definition and will often be included as part of that definition.

Entity category attribute values are URIs. Therefore, this document does not specify a controlled vocabulary for assigning such values; they may be defined by any appropriate authority without any requirement for central registration. It is anticipated that other specifications may provide management and discovery mechanisms for entity category attribute values.

This document also describes a SAML attribute called the "entity category support attribute". This attribute contains URI values that represent claims that an entity supports and/or interoperates with entities in a given category or categories. These values, defined in conjunction with specific entity category attribute values, provide entities in a category with the means to identify peer entities that wish to interact with them in a fashion described by the category specification.

This document does not specify any values for either the entity category attribute or the entity category support attribute.

1.1. REFEDS Document Process

The Research and Education FEDerations [REFEDS] group is the voice that articulates the mutual needs of research and education identity federations worldwide. It aims to represent the requirements of research and education in the ever-growing space of access and identity management.

From time to time, REFEDS will publish a document in the RFC Series. Such documents will be published as part of the Independent Submission stream [RFC4844]; however, the REFEDS Working Group sign-off process will have been followed for these documents, as described in the REFEDS Participant's Agreement [REFEDS.agreement].

This document is a product of the REFEDS Working Group process.

2. Notation and Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The notation "@example" is used as a shorthand for an XML attribute with attribute name "example".

3. Entity Category Attribute

3.1. Syntax

Entity category attribute values MUST be URIs. Such values are also referred to as "category URIs" in this document.

It is RECOMMENDED that http:-scheme or https:-scheme URIs are used; it is further RECOMMENDED that a category URI resolves to a human-readable document defining the category.

Authorities defining entity categories MUST produce a specification of the entity category and SHOULD make arrangement for the category URI to resolve to the specification in human-readable form.

Authorities defining entity categories MAY use versioning of category URIs where appropriate; if versioning is used, each version of the specification of the entity category SHOULD clearly indicate the latest version of the category URI (and hence of the specification). The specification SHOULD include a description of how the authority defining the entity category implements governance for the specification if the specification is updated.

When used in SAML metadata or protocol elements, the entity category attribute MUST be encoded as a SAML 2.0 Attribute element with @NameFormat urn:oasis:names:tc:SAML:2.0:attrname-format:uri and @Name http://macedir.org/entity-category.

A SAML entity is associated with one or more categories by including the Attribute element described here in the entity's metadata through use of the metadata extension defined in [SAML2MetadataAttr]. In this extension, the Attribute element is contained within an mdattr:EntityAttributes element directly contained within an md:Extensions element directly contained within the entity's md:EntityDescriptor.

The meaning of the entity category attribute is not defined by this specification if it appears anywhere else within a metadata instance or within any other XML document.

If the entity category attribute appears more than once in the metadata for an entity, relying parties SHOULD interpret the combined set of associated attribute values as if they all appeared together within a single entity category attribute.

3.2. Semantics

The presence of the entity category attribute within an entity's entity attributes represents a series of claims (one for each attribute value) that the entity is a member of each named category. The precise semantics of such a claim depend on the definition of the category itself.

An entity may be claimed to be a member of more than one category. In this case, the entity is claimed to meet the requirements of each category independently unless otherwise specified by the category definitions themselves.

This document intentionally does not define "category", in order to leave the concept as general as possible. However, to be useful, category definitions SHOULD include the following as appropriate:

- A definition of the authorities who may validly assert membership in the category. While membership in some categories may be self-asserted informally by an entity's owner, others may need to be validated by third parties such as the entity's home federation or other registrar.
- A set of criteria by which an entity's membership in the category can be objectively assessed.
- A definition of the processes by which valid authorities may determine that an entity meets the category's membership criteria.
- A description of the anticipated uses for category membership by relying parties.

- A statement indicating the applicability or otherwise of membership of the entity category to different SAML role descriptors and any protocol support restrictions that may be relevant.

Entity categories SHOULD NOT be used to indicate the certification status of an entity regarding its conformance to the requirements of an identity assurance framework. The SAML extension defined in [SAML2IDAssuranceProfile] SHOULD be used for this purpose.

If significant changes are made to a category definition, the new version of the category SHOULD be represented by a different category URI so that the old and new versions can be distinguished by a relying party. It is for this reason that authorities defining entity categories MAY employ some form of versioning for category URIs. When versioning is used, each version of the entity category MUST be treated as a separate URI.

No ordering relation is defined for entity category attribute values. Entity category attribute values MUST be treated as opaque strings for the purpose of comparison. In particular, if the specification defining the entity category relies on versioning of the category URI, a relying party MUST NOT assume any particular ordering between different versions of the category URI. Any order between versions MUST be spelled out in the specification.

3.3. Entity Category Example

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="https://service.example.com/entity">
  <md:Extensions>
    <mdattr:EntityAttributes
      xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="http://macedir.org/entity-category">
        <AttributeValue
          >http://example.org/category/dog</AttributeValue>
        <AttributeValue>urn:oid:1.3.6.1.4.1.21829</AttributeValue>
      </Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
  ...
</md:EntityDescriptor>
```

4. Entity Category Support Attribute

4.1. Syntax

Entity category support attribute values MUST be URIs. Such values are also referred to as "category support URIs" in this document.

It is RECOMMENDED that http:-scheme or https:-scheme URLs are used; it is further RECOMMENDED that each such value resolves to a human-readable document defining the value's semantics.

A given category URI MAY be associated with multiple category support URIs in order to allow for multiple forms of support, participation, or interoperation with entities in the category. The authority defining the category URI and category support URIs MUST clearly describe the relationship between (all versions of) the category URI and (all versions of) the category support URIs as applicable in the entity category specification.

The entity category support attribute MUST be encoded as a SAML 2.0 Attribute element with @NameFormat urn:oasis:names:tc:SAML:2.0:attrname-format:uri and @Name http://macedir.org/entity-category-support.

Claims that a SAML entity implements support for one or more categories are represented by including the Attribute element described here in the entity's metadata through use of the metadata extension defined in [SAML2MetadataAttr]. In this extension, the Attribute element is contained within an mdattr:EntityAttributes element directly contained within an md:Extensions element directly contained within the entity's md:EntityDescriptor.

The meaning of the entity category support attribute is not defined by this specification if it appears anywhere else within a metadata instance or within any other XML document.

If the entity category support attribute appears more than once in the metadata for an entity, relying parties SHOULD interpret the combined set of associated attribute values as if they all appeared together within a single entity category support attribute.

4.2. Semantics

The presence of the entity category support attribute within an entity's entity attributes represents a series of claims (one for each attribute value) that the entity supports peer entities in a

category in a particular fashion. The precise semantics of such a claim depend on the definition of the category support URI itself. Category support claims will often be defined to be self-asserted.

An entity may be claimed to support more than one category. In this case, the entity is claimed to meet the support requirements of each category independently unless otherwise specified by the category definitions themselves.

This document intentionally does not define "support" for a category, in order to leave the concept as general as possible. It is assumed that entity category definitions MAY define one or more category support URIs signifying particular definitions for "support" by peers as motivated by use cases arising from the definition of the category itself.

A common case is expected to be the definition of a single category support URI whose value is identical to the category URI.

If significant changes are made to a category support definition, the new version SHOULD be represented by a different category support URI so that the old and new versions can be distinguished by a relying party. It is for this reason that authorities defining entity categories support MAY employ some form of versioning. When versioning is used, each version of the category support URI MUST be treated as a separate URI.

No ordering relation is defined for entity category support attribute values. Entity category support attribute values MUST be treated as opaque strings for the purpose of comparison. In particular, if the specification defining the category support URIs relies on versioning, a relying party MUST NOT assume any particular ordering between different versions of the category support URI. Any order between versions MUST be spelled out in the specification.

4.3. Entity Category Support Example

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="https://idp.example.edu/entity">
  <md:Extensions>
    <mdattr:EntityAttributes
      xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="http://macedir.org/entity-category-support">
        <AttributeValue
          >http://example.org/category/dog/basic</AttributeValue>
        <AttributeValue
          >http://example.org/category/dog/advanced</AttributeValue>
        <AttributeValue>urn:oid:1.3.6.1.4.1.21829</AttributeValue>
      </Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
  ...
</md:EntityDescriptor>
```

5. IANA Considerations

This document has no IANA actions.

6. Security Considerations

The presence of the entity category attribute within an entity's entity attributes represents a series of claims (one for each attribute value) that the entity is a member of the named categories. Before accepting and acting on such claims, any relying party needs to establish, at a level of assurance sufficient for the intended use, a chain of trust concluding that the claim is justified.

Some of the elements in such a chain of trust might include:

- The integrity of the metadata delivered to the relying party, for example, as assured by a digital signature.
- If the entity category attribute is carried within a signed assertion, the assertion itself must be evaluated.
- The policies and procedures of the immediate source of the metadata, in particular, any procedures the immediate source has with regard to aggregation of metadata from other sources.

- The policies and procedures implemented by agents along the publication path from the original metadata registrar. This may be determined by examination of the published procedures of each agent in turn or may be simplified if the entity metadata includes publication path metadata in mdrpi:PublicationPath elements as described in Section 2.3.1 of [SAML2MetadataRPI].

- The policies and procedures implemented by the original metadata registrar. The registrar's identity may be known implicitly or may be determined from the entity metadata if it includes an mdrpi:RegistrationInfo element and corresponding @registrationAuthority as described in Section 2.1.1 of [SAML2MetadataRPI].

- The definition of the category itself, in particular, any statements it makes about whether membership of the category may be self-asserted or may only be asserted by particular authorities.

Although entity category support attribute values will often be defined as self-asserted claims by the containing entity, the provenance of the metadata remains relevant to a relying party's decision to accept a claim of support as legitimate, and the specific definition of a support claim will influence the assurance required to act on it.

The conclusion that a claim of category membership or support is justified and should be acted upon may require a determination of the origin of the claim. This may not be necessary if the immediate source of the metadata is trusted to such an extent that the trust calculation is essentially delegated to it.

In many cases, a claim will be included in an entity's metadata by the original metadata registrar on behalf of the entity's owner, and the mdrpi:RegistrationInfo element's @registrationAuthority is available to carry the registrar's identity. However, any agent that is part of the chain of custody between the original registrar and the final relying party may have added, removed, or transformed claims according to local policy. For example, an agent charged with redistributing metadata may remove claims it regards as untrustworthy or add others that were not already present if they have value to its intended audience.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[SAML2MetadataAttr] Cantor, S., Ed., "SAML V2.0 Metadata Extension for Entity Attributes Version 1.0", August 2009, <http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr-cs-01.pdf>.

[SAML2MetadataRPI] La Joie, C., Ed., "SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0", April 2012, <http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.pdf>.

7.2. Informative References

[REFEDS] "Research and Education FEDerations (REFEDS) Group", <http://www.refeds.org/>.

[REFEDS.agreement] Research and Education Federations, "REFEDS Participant’s Agreement", <https://refeds.org/about/refeds-participants-agreement>.

[RFC4844] Daigle, L., Ed. and Internet Architecture Board, "The RFC Series and RFC Editor", RFC 4844, DOI 10.17487/RFC4844, July 2007, <https://www.rfc-editor.org/info/rfc4844>.

[SAML2IDAssuranceProfile] Morgan, RL., Ed., Madsen, P., Ed., and S. Cantor, Ed., "SAML V2.0 Identity Assurance Profiles Version 1.0", November 2010, <http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cs-01.pdf>.

Acknowledgements

This work has been a collaborative effort within the REFEDS and MACE-Dir communities. Special thanks to the following individuals (in no particular order):

- RL 'Bob' Morgan
- Ken Klingenstein
- Keith Hazelton
- Steven Olshansky
- Mikael Linden
- Nicole Harris
- Tom Scavo

Authors' Addresses

Ian A. Young (editor)
Independent

Email: ian@iay.org.uk

Leif Johansson
SUNET

Email: leifj@sunet.se

Scott Cantor
Shibboleth Consortium

Email: cantor.2@osu.edu