Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 2, 2016

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

May 31, 2016

The Entity Category SAML Attribute Types
draft-young-entity-category-04

Abstract

This document describes a SAML entity attribute which can be used to assign category membership semantics to an entity, and a second attribute for use in claiming interoperation with or support for entities in such categories.

This document is a product of the Research and Education Federations (REFEDS) Working Group process.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 2, 2016.

carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction

This document describes a SAML attribute, referred to here as the "entity category attribute", values of which 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 labelled 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, and this document does not specify a controlled vocabulary. Category URIs may therefore 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.

A second SAML attribute, referred to here as the "entity category support attribute", contains URI values which 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 values, provide entities in a category with the means to identify peer entities that wish to interact with them in category-specific fashion.

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

1.1. REFEDS Document Process

The Research and Education Federations group ([REFEDS]) 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 wish to publish a document in the Internet RFC series. Such documents will be published as part of the RFC 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", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [BCP14].

3. Entity Category Attribute

3.1. Syntax

Entity category attribute values MUST be URIs. It is RECOMMENDED that http:-scheme or https:-scheme URLs are used, and further

RECOMMENDED that each such value resolves to a human-readable document defining the category.

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 [SAML2MetadataAttr] metadata extension, in which 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 undefined by this specification if it appears anywhere else within a metadata instance, or within any other XML document.

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

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.

The definition of the concept of a category is intentionally not addressed in this document, in order to leave it 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 [SAML2IDAssuranceProfile] extension 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.

No ordering relation is defined over entity category value URIs. Entity category attribute value URIs MUST be treated as opaque strings for the purpose of comparison.

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. It is RECOMMENDED that http:-scheme or https:-scheme URLs are used, and further RECOMMENDED that each such value resolves to a human-readable document defining the value's semantics. A given entity category value MAY be associated with multiple support values in order to allow for multiple forms of support, participation, or interoperation with entities in the category.

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 [SAML2MetadataAttr] metadata extension, in which 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 undefined by this specification if it appears anywhere else within a metadata instance, or within any other XML document.

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

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 identifier 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.

The definition of the concept of "support" for a category is intentionally not addressed in this document, in order to leave it as general as possible. It is assumed that entity category definitions MAY define one or more support values 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 support

value whose URI is identical to that defined for the category itself.

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.

No ordering relation is defined over entity category value URIs. Entity category attribute value URIs MUST be treated as opaque strings for the purpose of comparison.

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 memo includes no request to IANA.

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, as for example 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 either 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 [SAML2MetadataRPI] section 2.3.1.

- 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 attribute as described in [SAML2MetadataRPI] section 2.1.1.

- 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 attribute 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 which were not already present if they have value to its intended audience.

7. References

7.1. Normative References

[BCP14] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[SAML2MetadataAttr] Cantor, S., Ed., "SAML V2.0 Metadata Extension for Entity Attributes", August 2009, <http://wiki.oasis-open.org/security/SAML2MetadataAttr>.

[SAML2MetadataRPI] La Joie, C., Ed., "SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0", April 2012, <http://wiki.oasis-open.org/security/SAML2MetadataDRI>.

7.2. Informative References

[REFEDS] Research and Education Federations, "REFEDS Home Page", <http://www.refeds.org/>.

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

[RFC4844] Daigle, L. and Internet Architecture Board, "The RFC

Series and RFC Editor", RFC 4844, July 2007.

[SAML2IDAssuranceProfile]
Morgan, RL., Ed., Madsen, P., Ed., and S. Cantor, Ed., "SAML V2.0 Identity Assurance Profiles Version 1.0", November 2010, <https://wiki.oasis-open.org/security/SAML2IDAssuranceProfile>.

Appendix A. Acknowledgements

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

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

Appendix B. Change Log (to be removed by RFC Editor before publication)

B.1. Since draft-young-entity-category-03

Additional improvements in response to IETF Gen-Art review:

- Section 3.2: additional SHOULD language recommending that category definitions include applicability information for particular SAML role descriptors.
- Section 3.2: added an informative reference to [SAML2IDAssuranceProfile] and language recommending its use over entity categories where appropriate.

B.2. Since draft-young-entity-category-02

Fix link to the REFEDS Participant's Agreement [REFEDS.agreement].

Clarifications in response to IETF Gen-Art review:

- Section 1: make explicit the fact that we don't specify any values of either attribute in this document.

- Section 3.1, Section 4.1: clarify that it is possible for attribute values to appear within multiple Attribute elements, and that this SHOULD be regarded as equivalent to combining them within a single Attribute element.

- Section 3.2, Section 4.2: clarify the expectation that categories are independent unless their definitions say otherwise.

- Section 3.2, Section 4.2: 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*.

- Section 3.2, Section 4.2: *No ordering relation is defined over entity category value URIs.* Entity category attribute value URIs MUST be treated as opaque strings *for the purpose of comparison*.

B.3. Since draft-young-entity-category-01

Changes from REFEDS consultation process:

1. Simplify title from "The Entity Category SAML Entity Metadata Attribute Types" to "The Entity Category SAML Attribute Types".

2. Clarify the use of [SAML2MetadataRPI] in Section 6 by indicating the elements and attributes to be used, and the sections of [SAML2MetadataRPI] in which they are defined.

3. Remove any implication that category and category support claims are necessarily being made "by" the entity itself.

4. Clarify that the origin of a category membership or support claim may not always be the original registrar.

Grammar fix in Abstract.

Change the reference anchor for the SAML [SAML2MetadataRPI] extension, as it now more commonly known as RPI than its original DRI abbreviation.

B.4. Since draft-young-entity-category-00

Update affiliations for Leif Johansson and Scott Cantor.

Remove authors from acknowledgements.

Reorganize some of the introductory boilerplate sections.

B.5. Since draft-macedir-entity-category

Adopted as base for draft-young-entity-category-00.

Changed ipr from "pre5378Trust200902" to "trust200902" and submission type from IETF to independent.

Designate Ian Young as editor for this version. Set more general affiliation.

Modernised reference to RFC 2119 [BCP14] and moved that reference to the introduction.

Adjusted layout of examples so that they don't exceed the RFC standard line length.

Minor typographical nits but (intentionally) no substantive content changes.

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