The Entity Category SAML Entity Metadata Attribute Types
draft-young-entity-category-00

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 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

Copyright Notice

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

Table of Contents

1. Introduction and Motivation

   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 by an entity to support and/or interoperate 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.

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.

1.1. 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].

2. Entity Category Attribute

2.1. 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.

2.2. 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.

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:

o 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.

o A set of criteria by which an entity's membership in the category
   can be objectively assessed.

o A definition of the processes by which valid authorities may
   determine that an entity meets the category's membership criteria.

o A description of the anticipated uses for category membership by
   relying parties.

If significant changes are made to a category definition, the new
version of the category SHOULD be represented by a different category
URI.

Entity category attribute value URIs MUST be treated as opaque
strings.

2.3. 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>
```

3. Entity Category Support Attribute

3.1. 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.

A SAML entity claims a form of support for entities in 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 support
attribute is undefined by this specification if it appears anywhere
else within a metadata instance, or within any other XML document.

3.2. 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.

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.

Entity category support attribute value URIs MUST be treated as
opaque strings.

3.3. 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>
```

4. IANA Considerations

   This memo includes no request to IANA.

5. 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:

   o The integrity of the metadata delivered to the relying party, as
      for example assured by a digital signature.

   o If the entity category attribute is carried within a signed
      assertion, the assertion itself must be evaluated.

   o The procedures and policies of the immediate source of the
      metadata; in particular, any procedures the immediate source has
      with regard to aggregation of metadata from other sources.

   o 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 as described in the
      [SAML2MetadataDRI] extension.

   o The policies and procedures implemented by the original metadata
      registrar.

   o 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.

6. References

6.1. 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>.

[SAML2MetadataDRI]
            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>.

6.2. Informative References

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

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

[RFC4844]   Daigle, L. Internet Architecture Board, "The RFC Series
            and RFC Editor", RFC 4844, July 2007.

Appendix A. Acknowledgements

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

o RL 'Bob' Morgan

o Ken Klingenstein

o Keith Hazelton

o Steven Olshansky

o Mikael Linden

o Nicole Harris

o Ian A. Young

o Tom Scavo

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

B.1. 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
NORDUNet

EMail: leifj@sunet.se

Scott Cantor
Internet2

EMail: cantor.2@osu.edu