Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 29, 2012

I. Young
UKf
L. Johansson, Ed.
NDN
March 28, 2012

The Entity Category SAML Entity Metadata Attribute Type draft-macedir-entity-attribute-00.xml

Abstract

This document describes a SAML entity attribute which can be used to assign category membership semantics to an entity.

Requirements Language

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** [RFC2119].

Status of this Memo

This Internet-Draft will expire on September 29, 2012.

Copyright Notice

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.

2. 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.

3. 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:

- 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.

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.

4. 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>
```

5. 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
- Ian A. Young
- Tom Scavo

6. IANA Considerations

This memo includes no request to IANA.

7. 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 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.
- 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.
- The policies and procedures implemented by the original metadata registrar.
- 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.

8. Normative References

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[SAML2MetadataAttr]	Cantor, S., Ed., “SAML V2.0 Metadata Extension for Entity Attributes,” August 2009 (PDF).
[SAML2MetadataDRI]	La Joie, C., Ed., “SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0.”

Authors' Addresses

Ian A. Young
UK Access Management Federation for Education and Research

Email: **ian@iay.org.uk**

Leif Johansson (editor)
NORDUNet
Email: **leifj@sunet.se**