Anonymous Access Entity Category

Overview

Research and Education Federations are invited to use the REFEDS Anonymous Access Entity Category with their members to support the release of attributes to Service Providers meeting the requirements described below.

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].

This definition is written in compliance with the Entity Category SAML Entity Metadata Attribute Types specification [RFC8409]; this specification may be extended to reference other protocol-specific formulations as circumstances warrant.

An FAQ for the Entity Category has been made available to help deployments [FAQ].

1. Definition

Candidates for the Anonymous Access Entity Category are Service Providers that offer a level of service based on proof of successful authentication. None of the attributes in this entity category are specifically intended to provide authorization information. See section 6. for a discussion of this use case.

By asserting this entity category, Service Providers are signaling that they do not wish to receive personalized data.

Identity Providers may indicate support for this Entity Category to facilitate discovery and improve the user experience at Service Providers. Self-assertion is the typical approach used, but this is not the only acceptable method.

2. Syntax

The following URI is used as the attribute value for the Entity Category and Entity Category Support attribute:

https://refeds.org/category/anonymous

3. Semantics (Se)

By asserting a Service Provider to be a member of this Entity Category, a registrar claims that:

- (Se1) The Service Provider has applied for membership in the Category and complies with this entity category's registration criteria.
- (Se2) The Service Provider's application for using the Anonymous Access Entity Category has been reviewed against the provided REFEDS [Guidelines] and approved by the registrar.

By registering for this Entity Category Attribute, a Service Provider has agreed to the registration criteria as defined in Section 4.

By asserting support for this Entity Category, Identity Providers are indicating that they will release attributes to Service Providers which also assert this category.

4. Registration Criteria (RC)

When a Service Provider's registrar (normally the Service Provider's home federation) registers the Service Provider in the Entity Category, the registrar MUST perform at least the following checks:

- (RC1) Ensure that the service meets the following technical requirements:
  - (RC1.1) The Service Provider provides an `<mdui:DisplayName>` and `<mdui:InformationURL>` in metadata. Including an English language version (i.e., xml:lang="en") is RECOMMENDED.
  - (RC1.2) The Service Provider provides one or more contacts in metadata.

These are the requirements to assert this entity category; any change MUST be reported by the Service Provider to the federation registrar. The federation registrar SHOULD remove the Entity Category if the Service Provider can no longer demonstrate compliance to these requirements.

5. Attribute Bundle

This Entity Category supports online services that need the affiliation and organization of the user to be provided. The attributes chosen represent a privacy baseline such that further minimization achieves no particular benefit. Thus, the minimal disclosure principle is already designed into the category.

The use of the `<md:RequestedAttribute>` mechanism supported by SAML metadata is outside the scope of this category and may co-exist with it in deployments as desired, subject to this specification's requirements being met.

5.1 Required Attributes

The *entity category attribute bundle* consists (abstractly) of the following data elements:

- *organization*
- *affiliation*

These abstract elements are bound to protocol-specific definitions in the following subsection(s) and additional bindings may be added in the future.

It is understood that not every subject can necessarily be associated with values for every attribute. For example, some users may have no formal affiliation with the issuing organization. In such cases, it is expected that those attribute(s) may not be provided. The designation that all these attributes are required is a general obligation and not specific to a given subject.

5.1.1 SAML 2.0

When SAML 2.0 is used, the following SAML Attributes make up the required attribute set defined abstractly above. In all cases, the defined `NameFormat` is `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`

- *organization* is defined to be:
  - `schacHomeOrganization` [SCHAC]
    - Attribute Name: `urn:oid:1.3.6.1.4.1.25178.1.2.9`
- *affiliation* is defined to be:
  - `eduPersonScopedAffiliation` [eduPerson]
    - Attribute Name: `urn:oid:1.3.6.1.4.1.5923.1.1.1.9`

The specific naming and format of the attributes above is guided by the [SAMLAttr] profile.

6. Authorization

None of the attributes defined in Section 5 are suitable for accurately signaling access authorization; signaling authorization is out of scope for this entity category. While they are often used as approximations, this inevitably denies access to authorized users and permits access to unauthorized users.

A companion document discussing the federated authorization problem and suggested practices can be found at [FederatedAuthorization].

7. Deployment Guidance for Service Providers

Service Providers SHOULD rely on the bundle of attributes defined in Section 5 but MAY ask for, or even require, other information as needed for additional purposes, via mechanisms that are outside the scope of this specification.

A common example would be a requirement for indicating authorization to access a service (see Section 6).

A Service Provider that conforms to this entity category would exhibit the following entity attribute in SAML metadata:

```
<mdattr:EntityAttributes
xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <saml:Attribute
      xmlns:saml="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">

<saml:AttributeValue>https://refeds.org/category/anonymous</saml:Attr
ibuteValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

8. Deployment Guidance for Identity Providers

An Identity Provider indicates support for this entity category by exhibiting the entity attribute in its metadata. Such an Identity Provider MUST, for a significant subset of its user population, release all required attributes in the bundle defined in Section 5 to all Service

Providers registered for this entity category, either automatically or subject to user consent or notification, without administrative involvement by any party. This is a tool to limit data release to services that do not wish to receive personalized attributes.

An Identity Provider that supports this entity category would exhibit the following entity attribute in SAML metadata:

```
<mdattr:EntityAttributes
xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <saml:Attribute
      xmlns:saml="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">

<saml:AttributeValue>http://refeds.org/category/anonymous</saml:Attri
buteValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

9. References

[BCP14] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997. Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017. <https://www.rfc-editor.org/info/bcp14>.

[eduPerson] REFEDS, “eduPerson,” https://refeds.org/specifications/eduperson.

[FAQ] REFEDS, “Anonymous Authorization,” wiki page, https://wiki.refeds.org/display/ENT/Anonymous+Authorization.

[FederatedAuthorization] REFEDS, “Federated Authorization Best Practices,” wiki page, https://wiki.refeds.org/display/GROUPS/Federated+Authorization+Best+Practices.

[Guidelines] REFEDS, “Requirements for Federations Operators Assessing Access-Related Entity Categories,” wiki page, https://wiki.refeds.org/display/ENT/Requirements+for+Federations+Operators+Assessing+Access-Related+Entity+Categories.

[RFC8409] Young, I., Ed., Johansson, L., and S. Cantor, "The Entity Category Security Assertion Markup Language (SAML) Attribute Types", RFC 8409, DOI 10.17487/RFC8409, August 2018, <https://www.rfc-editor.org/info/rfc8409>.

[SAMLAttr] Internet2 MACE Directory Working Group, “MACE-Dir SAML Attribute Profiles”, April 2008, https://refeds.org/wp-content/uploads/2022/02/internet2-mace-dir-saml-attributes-200804.pdf.

[SCHAC] “SCHema for ACademia,” REFEDS, https://refeds.org/specifications/schac.