Personalized Entity Category

Overview

Research and Education Federations are invited to use the REFEDS Personalized 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 [EntityCatTypes]; 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 Personalized Entity Category are Service Providers that have a proven need to receive a small set of personally identifiable information about their users in order to effectively provide their service to the user or to enable the user to signal their identity to other users within the service. The Service Provider must be able to effectively demonstrate this need to their registrar and demonstrate their compliance with regulatory requirements concerning personal data through a published Privacy Notice.

Identity Providers may indicate support for Service Providers in 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.

The following sections detail the requirements for both Service Providers and Identity Providers, in category membership and support respectively.

2. Syntax

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

https://refeds.org/category/personalized

3. Semantics

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

- 3.1 The Service Provider has applied for membership in the Category and complies with this entity category's registration criteria.
- 3.2 The Service Provider's application for using the Personalized Entity Category has been reviewed against the provided REFEDS guidelines [TBD] and approved by the registrar.

In possessing the Entity Category Attribute with the above value, a Service Provider claims that it will not use attributes for purposes that fall outside of the service definition as presented at the time of registration to its users and referred to in metadata and will support this statement within their published Privacy Notice.

In possessing the Entity Category Support Attribute with the above value, an Identity Provider claims that it will release attributes to approved Service Providers as outlined in the "Identity Provider Requirements" section below.

4. Registration Criteria

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:

- 4.1 The service has a proven and documented need for the personally identifiable information that forms the attribute bundle for this entity category.
- 4.2 The Service Provider has committed to data minimisation and will not use the attributes for purposes other than as described in their application.
- 4.3 Ensure that the service meets the following technical requirements:
    - 4.3.1 The Service Provider deployment supports SAML V2.0.
    - 4.3.2 The Service Provider claims to refresh federation metadata at least daily.
    - 4.3.3 The Service Provider provides an `<mdui:DisplayName>`, `<mdui:InformationURL>`, and `<mdui:PrivacyStatementURL>` in metadata. Including an English language version (i.e., xml:lang="en") is RECOMMENDED.
    - 4.3.4 The Service Provider provides one or more contacts in metadata.

5. Attribute Bundle

The mechanism by which this entity category provides for consistent attribute release is through the definition of a set of commonly supported and consumed attributes typically required for effective use of personalized services. 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 required data elements:

- *organization*
- *shared user identifier*
- *person name*
- *email address*
- *affiliation*
- *assurance*

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

With regard to assurance, the REFEDS Assurance Framework [REFEDSAF] is REQUIRED as a source of values, but other frameworks and their values are permitted. Note that Identity Providers are not expected or required to alter their business processes or to assert any particular assurance levels for their subjects, but rather are required to communicate what they can provide.

The requirement to support the REFEDS Assurance Framework implies that at least one value, 'https://refeds.org/assurance' MUST be supplied, but no others are specifically required unless the IdP deems them to be applicable..

Any or all of these required attributes may be absent under specific conditions.

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`
- *shared user identifier* is defined to be:
  - `subject-id` [SAMLSubId]
    - Attribute Name: `urn:oasis:names:tc:SAML:attribute:subject-id`
- *person name* is defined to be all of:
  - `displayName` [eduPerson]
    - Attribute Name: `urn:oid:2.16.840.1.113730.3.1.241`
  - `givenName` [eduPerson]
    - Attribute Name: `urn:oid:2.5.4.42`
  - `sn` [eduPerson]
    - Attribute Name: `urn:oid:2.5.4.4`
- *email address* is defined to be:
  - `mail` [eduPerson]
    - Attribute Name: `urn:oid:0.9.2342.19200300.100.1.3`
- *affiliation* is defined to be:
  - `eduPersonScopedAffiliation` [eduPerson]
    - Attribute Name: `urn:oid:1.3.6.1.4.1.5923.1.1.1.9`
- *assurance* is defined to be:
  - `eduPersonAssurance` [eduPerson]
    - Attribute Name: `urn:oid:1.3.6.1.4.1.5923.1.1.1.11`

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

6. Deployment Guidance for Service Providers

Service Providers SHOULD rely on the bundle of attributes defined in Section 5 for personalization on behalf of the subject, 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, for which the use of eduPersonEntitlement [eduPerson] is a typical pattern.

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

An entity attribute for SPs that conform to this entity category:

```
<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>http://refeds.org/category/personalized</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

7. 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 tagged Service Providers, either automatically or subject to user consent or notification, without administrative involvement by any party.

However, excepting the `subject-id` attribute, it is understood that not every subject can necessarily be associated with values for every attribute. For example, some may have no formal affiliation with the issuing organization, or carry no assurance designation; some may even lack a given or family name for personal or cultural reasons. 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.

With regard to the *assurance* requirement, Identity Providers are not expected or required to alter their business processes or to provide any particular assurance level for their subjects, but rather are required to communicate what they do provide, or other applicable information as appropriate.

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

An entity attribute for IdPs that support this entity category:

```
<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/personalized</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

8. References

[TBD] *Will be developed post-consultation and may be similar to https://wiki.refeds.org/pages/viewpage.action?pageId=57147646.*

[eduPerson] eduPerson and eduOrg Object Classes, January 2021, https://refeds.org/eduperson.

[EntityCatTypes] 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>.

[FAQ] *Will be developed post-consultation.*

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

[SAMLAttr] Internet2 MACE Directory Working Group, “MACE-Dir SAML Attribute Profiles”, April 2008, https://shibboleth.net/documents/internet2-mace-dir-saml-attributes-200804.pdf.

[SAML2SubjId] OASIS Committee Specification, SAMLV2.0 Subject Identifier Attributes Profile Version 1.0, January 2019, https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.odt.

[SCHAC] SCHAC (SCHema for ACademia), April 2015, https://wiki.refeds.org/display/STAN/SCHAC.