REFEDS Entity Category: Pseudonymous Authorization
v.1 published 15 March 2021

Overview

All Identity Providers and Service Providers are invited to use the Pseudonymous Authorization Entity Category to manage the release of attributes to Service Providers meeting the requirements described below.

The keywords "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].

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.

1. Definition

Candidates for the Pseudonymous Authorization Entity Category are Service Providers that grant service access based on proof of successful authentication, and which offer personalization based on a pseudonymous user identifier and which do not require any other user attributes. These service providers do not qualify for the REFEDS Research and Scholarship Entity Category [R&S].

Example Service Providers may include (but are not limited to) services that support research and scholarship such as licensed e-resource providers, retailers, vendors, platform providers to support access to online content, inter-library loan services, services providing access to research data sets, and collaborative tools and services such as wikis, project, and grant management tools that require some personal information about users to work effectively.

2. Syntax

The following URI is used as the attribute value for the Entity Category and Entity Category Support attribute:
https://refeds.org/category/pseudonymous

3. Semantics

By asserting that it is a member of this Entity Category, a Service Provider claims that it will not use attributes for purposes that fall outside of the Service Provider's privacy statement as listed in the privacystatementurl in metadata.

Identity Providers may indicate support for Service Providers in this category by asserting the Entity Category Support Attribute with the above value; self-

assertion is the typical approach used.

By asserting this attribute, Identity Providers are indicating that they will release attributes to Service Providers which also assert this category as outlined in the "Service Provider Requirements" section below either by default or only for Service Providers they have an agreement with. They may need to consult with other departments within their organization to verify the relationship with the Service Provider.

4. 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 personalizable services. The attributes chosen represent a privacy baseline such that further minimization achieves no particular benefit. Thus, the minimal disclosure principle is designed into this 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.

The Pseudonymous Authorization attribute bundle consists (abstractly) of the following required data elements:

Required:

- *Organizational identifier*
- *Entitlement data*
- *Pseudonymous pairwise user identifier*

Where *Organization* SHOULD be one of the following, in order of preference:

Preference order	Attribute	Example values	Comments
1	eduPersonScopedAffiliation	`member@example.org`	Organization is indicated by the right-hand side of eduPersonScopedAffiliation. This right-hand side syntax of eduPersonScopedAffiliation intentionally matches that used for the right-hand side values for eduPersonPrincipalName. The "scope" portion MUST be the administrative domain to which the affiliation applies.
2	eduPersonOrgDN	`ou=Potions,o=Hogwarts,dc=hsww,dc=wiz`	The distinguished name (DN) of the directory entry representing the institution with which the

			person is associated.
3	schacHomeOrganization	example.edu	Specifies a person´s home organization using the domain name of the organization. Issuers of schacHomeOrganization attribute values via SAML are strongly encouraged to publish matching shibmd:Scope elements as part of their IDP's SAML metadata.

Note that the Organization concept explicitly specifically indicates the affiliation of the user independently of the IdP entity ID. With the use of a hub or consortia-based IdP, IdP entity ID does not necessarily represent the organization of the user.

Where *entitlement data* MUST use a registered value in the eduPersonEntitlement namespace [ePEregistry]:

Attribute	**Example values**	**Comments**
eduPersonEntitlement	urn:mace:dir:entitlement:common-lib-terms	Applies when entitlements are evaluated on the IdP side

Where *a pairwise user identifier* is a long-lived, non-reassignable, uni-directional identifier defined as a SAML pairwise subject identifier [SAML2SubjId].

Preference order	**Attribute**	**Example values**	**Comments**
1	samlPairwiseID	<saml2:Attribute FriendlyName="samlPairwiseID" Name="urn:oasis:names:tc:SAML:attribute:pairwise-id" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" ><saml2:AttributeValue>KRBODPWQQDMG2PL3CCDIJ4A576XR	

		LYBX@example.org</saml2:AttributeValue> </saml2:Attribute>	

"Order of preference" in the above tables refers both to the choice the IdP SHOULD make about which attributes to send in case they have multiple available to choose from, and to the order in which the SP SHOULD use the attributes in case they receive multiple from the IdP.

Many of the above attributes are defined or referenced in the [eduPerson] specification or in the [SCHAC] specification. The specific naming and format of these attributes is guided by the protocol in use. For SAML 2.0 the [SAML2Int] profile MUST be used. This specification may be extended to reference other protocol-specific formulations as circumstances warrant.

5. Service Provider Requirements

Service Providers SHOULD limit their data requirements to the bundle of attributes defined in Section 4.

ServiceProviders MUST provide at least one mdui:PrivacyStatementURLvalue [MDUI].

Service Providers are strongly encouraged to support all of the specified alternatives for the *pairwise user identifier* attribute described in Section 4 to maximize interoperability. Failure to do so will result in problems even when working exclusively with Identity Providers that claim support for the category.

A Service Provider that conforms to the Pseudonymous Authorization Entity Category would exhibit the following entity attribute in SAML metadata:

An entity attribute for SPs that conform to the Pseudonymous Authorization 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/pseudonymous</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

6. Identity Provider Requirements

By asserting this attribute, Identity Providers are indicating that they are able to support this entity category. They MAY release the attribute bundle defined in section 4 to all Service Providers which assert this category by default, or only for Service Providers which assert the entity category and with which they have an

agreement.

An entity attribute for IdPs that support the Pseudonymous Authorization 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://example.org/category/pseudonymous-authorization
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

7. References

[eduPerson] "eduPerson," REFEDS, https://refeds.org/eduperson.

[ePEregistry] "eduPersonRegistry Information," REFEDS, https://wiki.refeds.org/display/STAN/eduPerson+Registry+Information.

[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>.

[MDUI] Cantor, Scott et al. "SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0", March 2005, <https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/os/sstc-saml-metadata-ui-v1.0-os.html>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[SAML2Int] "SAML V2.0 Deployment Profile for Federation Interoperability," Kantara Initiative, 9 December 2019, https://kantarainitiative.github.io/SAMLprofiles/saml2int.html.

[SAML2SubjId] "SAML V2.0 Subject Identifier Attributes Profile Version 1.0," OASIS, 19 January