Pseudonymous Authorization Resource Access Entity Category

Overview

All Identity Providers and Service Providers are invited to use the Pseudonymous Authorization Resource Access Entity Category (RAEC) 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 RAEC are Service Providers that grant service access based on proof of successful authentication, which make authorization decisions based on *affiliation* and *entitlement*, 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.

For the purposes of this document, a *user attribute* is an attribute that reveals or may reveal a person’s identity, personal characteristics, contact information, or affiliation/role/access authorization.

For the purposes of this document, *affiliation* refers to the organizational association between the user and their home institution, by means of employment, membership, enrollment in an educational program, etc. *Entitlement* means the right of the user to access a given resource at the Service Provider by meeting a set of criteria that have been agreed between a given IdP and a given SP, for example by means of, but not limited to, a contractual arrangement. Entitlements are typically evaluated by mapping a set of user attributes against the terms of the agreement. In the federated authentication context, entitlements may be evaluated on the IdP side, in which case the IdP performs the attribute mapping and asserts the result by passing an agreed entitlement attribute with an agreed value to the SP, or they may be evaluated on the SP

side, in which case it is necessary for the IdP to pass all necessary attributes for evaluation of the entitlement to the SP during the authentication transaction.

N.B. This specification relates only to personal data passed between the IdP and the SP and does not relate to any personal data requested directly from the end-user or their browser, potentially via a consent flow.

N.B. This specification details the default configuration and does not restrict additional entity categories or attributes to be requested or exchanged as a result of bilateral arrangements

2. Syntax

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

https://example.org/category/psuedonymous

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 definition as presented at the time of registration to its users and referred to 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 that need the affiliation and entitlement of the user to be verified. 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*

Optional:

- *Affiliation type (for reporting purposes)*
- *Metrics code (for reporting purposes)*

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

Preference order	**Attribute**	**Example values**	**Comments**
1	eduPersonEntitlement	`urn:mace:dir:entitlement:common-lib-terms`	Applies when entitlements are evaluated on the IdP side
2	isMemberOf	`https://fed.example.org/sig-mobile-wg`	Applies when the SP uses group membership/affiliation to determine service entitlement
3	memberOf	`XBLU-RXS-BL`	Applies when the SP uses group membership/affiliation to determine service entitlement

Note: The IdP SHOULD take care to return only entitlement data which is relevant to the specific SP to avoid the potential for deanonymization.

Where *a pairwise user identifier* is a long-lived, non-reassignable, uni-directional identifier defined as a SAML pairwise subject identifier [SAML2SubjId]. At the time of this writing, other deprecated identifiers are still in common use; see Annex II for more information. Service Providers SHOULD consider supporting these legacy identifiers until broad adoption of the new profile has taken place. Identity Providers are advised to move to the new pairwise identifiers as soon as practicable.

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>KRBODPWQQDMG2PL3CCDIJ4A576XRLYBX@example.org</saml2:AttributeValue> </saml2:Attribute>	

Where *affiliation type* SHOULD be:

Preference order	Attribute	Example values	Comments
1	eduPersonScopedAffiliation	member@example.org	Affiliation type is indicated by the left-hand side of eduPersonScopedAffiliation The left component is one of the values from the eduPersonAffiliation controlled vocabulary, which specifies the person's relationship(s) to the institution in broad categories

And where *metrics code* SHOULD be a mutually agreed attribute and value upon code to allow for granular usage reporting, cost reallocation, targeted invoicing, etc., between an SP and IdP.

“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, but MAY negotiate for additional data in a bilateral agreement as required via mechanisms that are outside the scope of this specification.

Service Providers MUST commit to following the principles of the GEANT Data Protection Code of Conduct, and when supported by their federation assert this in metadata [DPCoCo].

The service provider MUST NOT assert the Authentication Only RAEC, Anonymous Authorization RAEC, or Research and Scholarship attribute release bundle entity categories if it asserts this entity category, and the SP MUST NOT request any of the attributes described in those entity categories from the IdP through other mechanisms unless bilateral arrangements are in place.

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-authorization</saml:Attribute
Value>
  </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

[AnonRAEC] “Anonymous Authorization Entity Category” - citation TBD

[PseudRAEC] “Pseudonymous Authorization Entity Category” - citation TBD

[R&S] “Research and Scholarship Entity Category,” REFEDS, https://refeds.org/category/research-and-scholarship.

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

[DPCoCo] “Data Protection Code of Conduct Home,” GEANT, https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home.

[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>.

[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 2019, https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/cs01/saml-subject-id-attr-v1.0-cs01.html.

[SCHAC] “Schema for ACademia,” REFEDS, https://wiki.refeds.org/display/STAN/SCHAC.

Annex I - Implementation Guidance

Relationship to other Resource Access Entity Categories

For Service Providers

By asserting participation in a Resource Access Entity Category, a service provider (SP) is signaling to identity providers its minimally acceptable (required?) user attribute bundle to successfully grant the user access. Particularly when publishing the SP's SAML metadata in a federation, each unique SP SAML entity SHOULD assert at most one Resource Access Entity Category. For example, an SP entity asserting Authentication Only category SHOULD NOT simultaneously assert the Pseudonymous Authorization category. Doing so sends conflicting messages.

If a service needs to accommodate different resource access schemes due to contractual differences, the configuration SHOULD be handled in one of the following ways:

a. Express the difference in a separate entity metadata with a different entity ID;
b. Negotiate and configure the attribute release agreement bi-laterally, outside the scope of the Resource Access Entity Categories.

For Identity Providers

An Identity Provider (IdP) SHOULD simultaneously support all Resource Access entity categories.

Identity Provider Configuration

To properly support the Pseudonymous Authorization Resource Access category, in addition to releasing those attributes permitted by the Pseudonymous Authorization category, an Identity Provider (IdP) MUST take care to block any user attribute not permitted by the Pseudonymous Authorization category from being released to an SP asserting this category unless bilateral arrangements are in place.

A *user attribute* is an attribute that reveals or may reveal a person's identity, personal characteristics, contact information, or affiliation/role/access authorization.

Most of the attributes permitted in the Pseudonymous Authorization category are multi-valued attributes. When configuring release, an IdP SHOULD only release values applicable to the SP the user is accessing. Further, configuring attribute release may require an underlying contract

between the IdP organization and the SP organization. To accommodate these nuances, an IdP may adopt one of the following configuration strategies:

a. Prepare SP-specific attribute release rules, using the Pseudonymous Authorization category as a template.
b. Create a release rule for the Pseudonymous Authorization category; use regular expression within the rule to filter values by SP.

The following example illustrates a possible Pseudonymous Authorization category template for the Shibboleth Identity Provider's attribute filter policy (attribute-filter.xml). This template permits the release of attributes defined in this category to the named SP entity while explicitly blocks other user attribute released by default from being released:

```
<AttributeFilterPolicy id="refedsPseudonymousCategoryTemplate">
  <PolicyRequirementRule xsi:type="Requester"
      value="https://sp.example.org"/>

  <!-- In this example, the IdP by default releases email.
       This configuration overrides those defaults and blocks
       their release. -->
  <AttributeRule attributeID="mail">
    <DenyValueRule xsi:type="ANY"/>
  </AttributeRule>
 <!-- Release attributes defined in the Pseudonymous Authorization
      category -->
  <AttributeRule attributeID="samlPairwiseID">
    <PermitValueRule xsi:type="ANY"/>
  </AttributeRule>
  <AttributeRule attributeID="eduPersonScopedAffiliation">
    <PermitValueRule xsi:type="ANY"/>
  </AttributeRule>
  <AttributeRule attributeID="eduPersonOrgDN">
    <PermitValueRule xsi:type="ANY"/>
  </AttributeRule>

  <!-- Release entitlement values defined by MACE-DIR as well as those
       specific to example.org's demo service -->
  <AttributeRule attributeID="eduPersonEntitlement">
    <PermitValueRule xsi:type="OR">
```

```
      <Rule xsi:type="ValueRegex"
            regex="^urn:mace:example.org:demoservice:.*$" />
      <Rule xsi:type="ValueRegex"
            regex="^urn:mace:dir:entitlement:.*$" />
    </PermitValueRule>
  </AttributeRule>

</AttributeFilterPolicy>
```

Annex II - Deprecated Pseudononymous Targeted Identifiers

This section documents various pseudonymous, targeted identifiers that are still in common use today. While we encourage organizations to transition away from these as much as possible, we recognize they may still need to be used for the purposes of sharing a pseudonymous identifier during a federated authentication workflow.

eduPersonTargetedID

From the eduPerson (202001) specification:
NOTE: eduPersonTargetedID is DEPRECATED and will be marked as obsolete in a future version of this specification. Its equivalent definition in SAML 2.0 has been replaced by a new specification for standard Subject Identifier attributes [https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html], one of which ("urn:oasis:names:tc:SAML:attribute:pairwise-id") is a direct replacement for this identifier with a simpler syntax and safer comparison rules. Existing use of this attribute in SAML 1.1 or SAML 2.0 should be phased out in favor of the new Subject Identifier attributes."

NameID

This Attribute is a direct replacement for the `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` NameID Format defined in SAML [SAML2SubjId]. There are obvious syntactic differences, in a deliberate attempt at simplification. The XML syntax and data "triple" are replaced with a simpler id/scope pair encoded into a string, and the awkward use of a pair of URIs to qualify the value is replaced with a simpler, shorter, and more flexible approach that more easily emulates the email address syntax required by many applications, and decouples identifier scoping from SAML entity naming.