The consultation process and review by the Schema Editorial Board resulted in two major areas of concern: first, that the entity categories were attempting more than one thing at a time (access control and metrics), and second that IdPs would find it impossible to scale support for entitlements across all the different SPs without a controlled vocabulary or a common attribute value format.

The proposal from the Schema Board is to remove the requirements for metrics and entitlement entirely. Entitlements may be added back in after work is completed to create the necessary controlled vocabulary or attribute value format.

In addition, other supporting material that offers advice and how-to guidance must be moved to a supporting document (such as a wiki page) and not included in the specification itself.

Anonymous Authorization Entity Category

Overview

All Identity Providers and Service Providers are invited to use the Anonymous Authorization Entity Category with their members to support 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 Anonymous Authorization Entity Category are Service Providers that grant service access based on proof of successful authentication, which make authorization decisions based on *affiliation,* and which do not require any additional user attributes.

Example Service Providers may include (but are not limited to) services such as licensed e-resource providers, retailers, vendors, platform providers, services providing access to research data sets, and collaborative tools and services such as wikis, project, and grant management tools that require enough information to make authorization decisions based on affiliation.

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

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 defined in the Service Provider’s privacy statement in metadata as defined in the SAML V2.0 Metadata Extensions [MDUI].

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.

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 the effective use of online 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 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.

The *Anonymous Authorization attribute bundle* consists (abstractly) of the following data elements:

Required:

- *Organization*
- *Entitlement*

Where *Organization* MUST 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. SPs MAY use the left hand side as a basis for implementing access control and/or reporting policies
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.

“Order of preference" in the above tables refers both to the choice the IdP SHOULD make about which attributes to release 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 are guided by the protocol in use. For SAML 2.0 the [SAMLInt] profile MUST be used. This specification may be extended to reference other protocol-specific formulations as circumstances warrant.

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

5. Service Provider Requirements

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

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

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

An entity attribute for SPs that conform to Anonymous Authorization:

```
<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/anonymous/
    </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 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 Anonymous 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://refeds.org/category/anonymous
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

7. References

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

[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 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.