Anonymous Authorization

This guidance is for v1 of this specification ONLY. Please refer to:Anonymous, Pseudonymous and Personalized Access FAQ for the most up-to-date version of supporting material.

The Anonymous Authorization Entity Category can be found on the REFEDS website and text from the website should be used as the authoritative source: https://refeds.org/category/anonymous.

Implementation Guidance

Guidance for Federation Operators

Requirements for Federations Operators Assessing Access-Related Entity Categories. Please note the "Registration Criteria" section for each entity category.

Relationship to other Entity Categories

For Service Providers

By asserting participation in an Entity Category, a service provider (SP) is signaling to identity providers its minimally 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 Entity Category. For example, an SP entity asserting Anonymous Authorization 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:

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

For Identity Providers

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

Identity Provider Configuration

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

All of the attributes permitted in the Anonymous 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 authorization attribute release may require an underlying agreement between the IdP organization and the SP organization. To accommodate these nuances, an IdP may adopt one of the following configuration strategies:

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

The following example illustrates a possible Anonymous 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 user identifiers from being released:

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

  <!-- In this example, the IdP by default releases ePPN and ePTID.
       This configuration overrides those defaults and blocks
       their release. -->
  <AttributeRule attributeID="eduPersonPrincipalName">
    <DenyValueRule xsi:type="ANY"/>
  </AttributeRule>
  <AttributeRule attributeID="eduPersonTargetedID">
    <DenyValueRule xsi:type="ANY"/>
  </AttributeRule>

<!-- Release attributes defined in the Anonymous Authorization
      category -->
  <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>
```