# Pseudonymous 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 Pseudonymous 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/pseudonymous.


- Implementation Guidance
  - Relationship to other Resource Access Entity Categories
    - For Service Providers
    - For Identity Providers
  - Identity Provider Configuration
- Deprecated Pseudononymous Targeted Identifiers
  - eduPersonTargetedID
  - NameID


# Implementation Guidance

## Relationship to other Resource Access Entity Categories

### For Service Providers

By asserting participation in an Entity Category, a service provider (SP) is signaling to identity providers its minimally requited 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 Authorization 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:

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 Entity Categories.

## Identity Provider Configuration

To properly support the Pseudonymous Authorization 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.

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:

1. Prepare SP-specific attribute release rules, using the Pseudonymous Authorization category as a template.
2. 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>
<!-- 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>
```

## 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. 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.