# Anonymous, Pseudonymous and Personalized Access FAQ

## Anonymous , Pseudonymous and Personalized Access Entity Categories FAQ



## General Information

### Where are the official definitions for Anonymous Access and Pseudonymous Acess and Personalized Access Entity Categories?

The formal, approved definitions

https://refeds.org/category/anonymous

https://refeds.org/category/pseudonymous

https://refeds.org/category/personalized

(Note that the URI values of the REFEDS entity attribute resolve to the appropriate specification)

### What is the differences between version 1 and version 2 of these Entity Categories?

The main differences should be noted:

| Entity Category | Changes v1 to v2 |
|---|---|
| Anonymous | • Change of name from "authorization" to access to better reflect the intent of the process<br>• Clarity on authorization processes<br>• Removal of support for eduPersonOrgDN<br>• Removal of support for entitlement |
| Pseudonymous | • Change of name from "authorization" to access to better reflect the intent of the process<br>• Clarity on authoriztion processes<br>• Removal of support for eduPersonOrgDN<br>• Removal of support for entitlement |
| Personalized | • Improvement in compliance process<br>• Clarity on authorization processes |

### Why does this enable me to release personal data?

These entity categories typically allow for release of data under the **legitimate interests justification** within GDPR, but can also be applied with **contractual interests** and **consent** models. With these categories, the Federation Operator carries out a lightweight review of the Service Provider to ensure they have a legitimate interest in asserting the entity category. This process models good practice from GDPR and the balance test proposed by the Article29 Working Party (now the European Data Protection Board). This creates scalability within our environment: IdPs have been reluctant to release attributes due to the lack of resource to do full assessments and lack of clarity as to who should be responsible. It also builds on the trust model created in the federation environment to build scalability of trust.

### Why do you call these "access" and not "authorization"?

There's more detail about this in our authorization guidelines: Federated Authorization Best Practices. Determining whether someone is fully authorized to use a service is complex and depends on the relationship between all the players in the transaction. These categories more simply describe that a person has been given the ability to **access** a service.

### What do I do if I think a Service Provider is misusing any of these entity categories?

In the first instance, please contact the Federation Operator of the federation that the entity is registered with. If this is not successful, please reach out to the REFEDS Steering Committee at contact@refeds.org.

### Are SPs allowed to request additional attributes other than those defined in these entity categories?

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 group of attributes are designed to meet a common privacy baseline, so release of further personally identifiable attributes should in general not be necessary unless bespoke information is need for a service. Other, non-personal, attributes may be required for specific service needs.

### Will I definitely get the attributes requested?

Release of data from organisations is governed by data protection laws that provide a variety of mechanisms to ensure that people and organisations have choice over the data that is released. There may however be legitimate reasons for attributes not be release (e.g. user consent, data not available for all users in IDM systems etc.). SPs are encouraged to consider providing helpful error message screens where this may impact service provision.

### Are attributes single or multi-valued?

Service Providers should reference the eduPerson specification for details on values that may be received per attribute, but in general terms:

- pairwise-id, subject-id, displayName are single-valued.
- givenName + sn, email address, eduPersonScopedAffiliation can be mutli-valued.

## For IdP Operators

### Which attributes have to be released?

| Entity Category | Attributes |
|---|---|
| Anonymous Access (v2) | • schacHomeOrganization<br>• eduPersonScopedAffiliation |
| Pseudonymous Access (v2) | • schacHomeOrganization<br>• pairwise-id<br>• eduPersonScopedAffiliation<br>• eduPersonAssurance |
| Personalized Access (v2) | • schacHomeOrganization<br>• subject-id<br>• displayName<br>• givenName<br>• sn<br>• mail<br>• eduPersonScopedAffiliation<br>• eduPersonAssurance |

### How do I configure an IdP to release attributes to SPs?

To release attributes to all current and future R&S SPs with a one-time configuration, an IdP leverages entity attributes (instead of entity IDs). Thus the configuration steps documented in the R&S IdP Config topic require Shibboleth IdP v2.3.4 or later, which fully supports using entity attributes in SP metadata as part of an attribute release filter policy. No other SAML IdP software is known to support entity attributes at this time.

IdPs are broadly taking one of two approaches to releasing attributes to R&S SPs:

- Configure an IdP to Release a Fixed Subset of R&S Attributes. This releases the same subset to every R&S SP.
- Configure an IdP to Release a Dynamic Subset of R&S Attributes. This releases a different subset to each R&S SP based on the `<md:RequestedAttribute>` elements in SP metadata.