

Entity-Categories Home

- [Categories in Use](#)
- [Purpose](#)
- [Introduction](#)
- [Rationale](#)
- [Supporting Material](#)
- [Guidance on Attribute Release](#)

Categories in Use

REFEDS currently recommends the following entity categories:

- [Research and Scholarship](#)
- [GEANT Data protection Code of Conduct](#) (version 2)
- [Hide From Discovery](#)
- [Anonymous Access](#)
- [Pseudonymous Access](#)
- [Personalized Access](#)

Purpose

Entity Categories group federation entities that share common criteria. The intent is that all entities in a given entity category are obliged to conform to the characteristics set out in the definition of that category.

While Entity Categories have multiple potential uses, they were initially conceived as a way to facilitate IdP decisions to release a defined set of attributes to SPs without the need for detailed local review for each SP. The decision by the IdP would instead be based on the criteria detailed in each SP entity category specification. Categories were also conceived for IdPs to indicate support for the SP categories; SPs would use this information to tailor discovery and other aspects of the user experience.

Federations make use of both a SAML entity attribute which can be used to assert category membership for an entity (typically by SPs), and a second attribute for use in claiming interoperation with or support for entities in such categories (typically by IdPs).

Introduction

The Entity Category attribute can be expressed as a SAML attribute. When used with the [SAML V2.0 Metadata Extension for Entity Attributes](#) each such entity category attribute value represents a claim that the entity thus labelled meets the requirements of, and is asserted to be a member of, the indicated category. These category membership claims MAY be used by a relying party to provision policy for release of attributes from an identity provider, to influence user interface decisions such as those related to identity provider discovery, or for any other purpose. In general, the intended uses of any claim of membership in a given category will depend on the details of the category's definition, and will often be included as part of that definition.

Entity category attribute values are URIs, and this document does not specify a controlled vocabulary. Category URIs may therefore be defined by any appropriate authority without any requirement for central registration. It is anticipated that other specifications may provide management and discovery mechanisms for entity category attribute values.

A second SAML attribute, the "entity category support attribute", contains URI values which represent claims by an entity to support and/or interoperate with entities in a given category or categories. These values, defined in conjunction with specific entity category values, provide entities in a category with the means to identify peer entities that wish to interact with them in category-specific fashion.

This introductory text is adapted from the [MACE-DIR Entity Category proposal](#).

Rationale

A growing number of Service Providers (SPs) are joining federations. As is the standard practice in the higher education and research world, it is essential for users to be recognisable when using certain services: name, email, institutional affiliation are often needed by the SP. Unfortunately, the default Attribute Release Policies in place at most campus Identity Providers (IdPs) do not share any information with these sites without local review of the SP's purpose, governing policy, and operational practices. This approach is simply not scalable to the thousands of campus IdPs and thousands of SPs. It is already a serious problem for the big virtual organizations and research labs; the hoped-for explosion of smaller collaboration sites housed in academic departments will not succeed with federation without a scalable solution. It is also essential that the justification for the requested release has been examined to meet data release requirements.

All federation SPs are already bound by a set of practices governing how they manage and use personal attributes. Entity Categories define additional set criteria that are designed to facilitate IdP policy decisions to release a controlled set of low-risk attributes to SPs without local review for each SP, based on the criteria detailed in each entity category specification.

IdPs can simplify the management of their Attribute Release Policies by taking advantage of entity categories. With a one-time addition to their default release policies they can specify a set of attributes to release to all SPs that are in a specific category. This policy would apply to SPs that are added to the category in the future, without the IdP administrator having to make any changes.

Entity Category support currently varies per federation. Please contact your home federation, or [REFEDS](#), to discuss further.

Supporting Material

- [Entity Category FAQ for Federation](#)
- [Research and Scholarship FAQ](#)
- [Data Protection Code of Conduct](#) wiki space
- [Anonymous, Pseudonymous and Personalized Access FAQ](#)

Guidance on Attribute Release

- [Guidance on justification for attribute release for RandS](#)
- [Requirements for Federations Operators Assessing Access-Related Entity Categories](#)

Recent space activity



[Teun Fransen](#)

[Anonymous, Pseudonymous and Personalized Access FAQ](#) updated
Nov 21, 2023 [view change](#)

[Nicole Harris](#)

[Anonymous, Pseudonymous and Personalized Access FAQ](#) updated
Mar 01, 2023 [view change](#)



[Thomas Lenggenhager](#)

[Anonymous, Pseudonymous and Personalized Access FAQ](#) updated
Mar 01, 2023 [view change](#)

[Nicole Harris](#)

[Personalized](#) updated Feb 28, 2023 [view change](#)
[Anonymous Authorization](#) updated Feb 28, 2023 [view change](#)

Space contributors

- [Teun Fransen](#) (157 days ago)
- [Nicole Harris](#) (422 days ago)
- [Thomas Lenggenhager](#) (422 days ago)
- [Heather Flanagan](#) (571 days ago)
- [Andrew Cormack](#) (861 days ago)
- ...