


consultation-refeds-access-ec-deployment-guidance

 **Community Review**

This consultation is closed.

The document editors are reviewing and drafting responses to the consultation feedback.

Background

In 2023, REFEDS published the latest revisions of three attribute release entity categories designed to facilitate privacy-preserving, standard, and streamlined user information release in federated transactions. These are Anonymous Access, Pseudonymous Access, and Personalized Access categories. Together, we refer to them as the REFEDS Access Entity Categories.

The InCommon Federation (InCommon) wishes to encourage the widespread adoption of these categories when requesting and releasing user information in federated transactions. To that end, the InCommon Technical Advisory Committee's SAM2Int/Entity Category Deployment Guidance Working Group has produced a series of deployment guidance to help the InCommon Federation community adopt the REFEDS Access Entity Categories.

This is a Three-in-One Document

The Working Group produced materials organized in three loosely-connected volumes:

1. Understanding the REFEDS Access Entity Categories;
2. Deployment Guidance for InCommon Participants;
3. Working with Required Attributes;

They are compiled together in a single document to facilitate community review. In their final published format, the topics will be parsed into a series of web articles cross-linked among each other.

More are Coming

We are aware that the InCommon community will likely need additional detailed guidance, for example, around migration strategies. A new TAC working group is forming to develop these additional materials. We welcome your input and participation. Please note your interest in the Feedback Log below.

Document for Review / Consultation

The PDF for the consultation is available:

- [inc-refeds-access-ec-deployment-guide-consultation-20240321.pdf](#)

All comments should be made added to the Feedback Log below. Comments posted to other channels will not be included in the consultation review.

Participants are invited:

- to consider the proposed deployment guidance to the REFEDS Access Entity Categories

This consultation opens on April 1, 2024 and closes on April 30, 2024 at 5PM PDT.

Feedback Log

Line Number	Current Text	Proposed Text / Query / Suggestion	Proposer	+1 (add your name here if you agree with the proposal)	Action
79-81		The R&S registration criterias is fuzy and have given unpredictability in a service fulfills a the criteria or not when you look over federation boundararies. It's better to have a clear defintion of what you mean in the document.	Pål Axelsson, SWAMID		

117-119	Whether you support the automatic release mechanism required by the REFEDS entity categories or not, you can at least use these templates to standardize attribute release to individual SPs.	It states automatic release is required by the entity categories but that is not true. In personalized it's stated "An Identity Provider indicates support for this entity category by exhibiting the entity attribute in its metadata. Such an Identity Provider MUST, for a significant subset of its user population, release all required attributes in the bundle defined in Section 5 to all tagged Service Providers, either automatically or subject to user consent or notification, without administrative involvement by any party.". This means that those identity providers expressing support in metadata must do automatic release but if you don't express support in metadata you can still release attributes based on for example an manual informed decisions for entities.	Pål Axelsson, SWAMID		
93 - 103		Wherever you put it, the advice for the anonymous category needs to include a warning about existing attribute release policies in the IdP. Because I've worked with institutions that release something like the R&S bundle to ALL InCommon (or even all InCommon MDQ sourced) services, or even, in some cases, to ALL SPs for which the IdP has metadata. And it is not uncommon (no pun intended) for the current maintainer of that IdP to not even realize that. And, even if you then configure support for Anonymous tagged services, unless you explicitly DENY the already greater set (many of which will be personally identifying), you will then be releasing attributes to an Anonymous service that you should not be. (I also think this is why explicit advice on how to easily test what you are releasing after adding support for the profile will be critical, including identifying a service that is "tagged" for this profile and how to see what your IdP would then send.)	Mike Grady, Unicon	Albert Wu (internet2.edu)	
455, 470-476	staff@dentistry.acme.edu, staff@nursing.acme.edu	The guidance in this document about defining scope values for "e.g., school/college within a university" conflicts with the guidance at Scope that "Multiple scopes should not be used to distinguish multiple subgroups of users within a single security domain." I think InCommon should continue to recommend against registration of multiple scope values for a single entity, to avoid added complexity and to maintain consistency with current guidance.	James Basney (illinois.edu)		
		Can InCommon or REFEDS run simple SPs that IDP operators can use for testing their implementation of the Access Entity Categories? I'm thinking of a page that displays the attributes and values released to the SP. This relates to Mike Grady's comment regarding overlapping attributes release policies.	Andy Morgan, Oregon State University		
120-123		Based on what one can see at this link: https://incommon.org/custom/federation/info/all-entity-categories.html#SPs it would appear that these entity categories are NOT mutually exclusive. I.e. An SP could be tagged with all three of these new categories. Assuming that interpretation is right (originally I assumed an SP would have one and only one of these categories), then deployment guidance will need to include a discussion of whether your configuration "prefers" the most privacy preserving category supported, rather than choosing the most permissive (e.g. personalized). The configuration gets more complex (at least for the Shibboleth IdP) to support default release for all 3 of these categories, but to favor the most restrictive (privacy preserving one). Most definitely will need sample config for federation supporting IdP software such as the Shibboleth IdP and SimpleSAMLphp.	Michael Grady (unicon.net)	+1. FIM4L would appreciate clarifying whether the categories are mutually exclusive.	
		Here is an example of more specific documentation that I think will be needed for at least IdP operators wanting to implement these profiles: https://docs.google.com/document/d/1qEle7K2Npx_VvVK2CVgG3Um-xicsQs_x5gzCSvsFHCg/view?usp=sharing	Michael Grady (unicon.net)		
89-90	Common uses of this category include anonymous access to licensed content where the service wishes to allow the user to save settings.	Common uses of this category include anonymized access to licensed content (library, online journals, etc) where the service wishes to allow the user to save settings. Many prefer the Pseudonymous Access Category because of the stable identifier which enables non personal identifiable user profiles. In general, anonymous category would increase privacy. More on this may be found in the Recommendations for libraries document of FIM4L, https://zenodo.org/records/7313371	FIM4L WG		

See Also

- [Trust and Identity Consultations Home](#)
- [InCommon Working Groups Home](#)