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

<table>
<thead>
<tr>
<th>Line Number</th>
<th>Current Text</th>
<th>Proposed Text / Query / Suggestion</th>
<th>Proposer</th>
<th>+1 (add your name here if you agree with the proposal)</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>79-81</td>
<td>The R&amp;S registration criterias is fuzy and have given unpredictability in a service fulfills a the criteria or not when you look over federation boundairies. It's better to have a clear definition of what you mean in the document.</td>
<td>Pål Axelson, SWAMID</td>
<td>The consultation copy had an incorrect link to InCommon's R&amp;S registration practice. That has been corrected. In addition, a summary of the practice has also been brought into this document.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 of 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 manual informed decisions for entities.

Mike Grady, Unicon
Albert Wu (internet2.edu)

Added additional IdP guidance: see Volume II: Deployment Guidance for Identity Providers, Part III.

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.

James Basney (bross.edu)

We agree that this is a great idea. TAC has charted the Federation Readiness Check WG to work on just this.

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 SP) 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 SP software such as the Shibboleth SP and SimpleSAMLphp.

Michael Grady (unicorn.net)

+1. FIM4L would appreciate clarifying whether the categories are mutually exclusive.

The intent of the guidance is to require an InCommon-registered SP to choose at most one of the three Access entity categories. An InCommon-registered SP should not simultaneously be a part of more than one Access entity category. Volume II: Deployment Guidance: For Service Providers has been updated to reflect this detail. In addition, a ticket is being filed with Federation Manager team to update the tool to enforce this restriction. Because the REFEDS specifications themselves do not prohibit an SP from registering in multiple categories, added Volume II: Deployment Guidance: For Identity Providers: Part IV: Prioritizing attribute release when an SP belongs to multiple Access entity categories to address interactions with SPs from other eduGAIN member federations.

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/1qL6q7K9h9xVvV2kCvGzJUm-xcvoE5s_x5gC3vFHCg/view#u=y=sharing

Michael Grady (unicorn.net)

Thank you. We will incorporate these examples in the final wiki documentation.

Common uses of this category include anonymous access to licensed content where the service wishes to allow the user to save settings.

FIM4L WG

Thank you. We have updated the guidance with the suggested text.

See Also

- Trust and Identity Consultations Home
- InCommon Working Groups Home