REFEDS

Entity Category Updates

REFEDS 44

Problem Statement

- *The current definition of who can be tagged with R&S ("Candidates for the Research and Scholarship (R&S) Category are Service Providers that are operated for the purpose of supporting research and scholarship interaction, collaboration or management, at least in part.") is being interpreted differently by different groups.*

- *Requirements that are not specifically in the specification are being applied by federations, creating an uneven use of the specification*.

Sample of the Challenges

- Is R&S focused on the requirements of the service or the organisational type?
  - Issues with not having a definition of an R&S / R&E organisation and the fact that most organisations have business arms to R&E structure
- Should "commercial" services be allowed?
  - No way to distinguish the nuance in commercial vs paid for
- Should services that are contracted be allowed?
  - Contracts are paid for things like collaborative wikis, having a contract does nothing to help the IdP administrator formulate an attribute release policy
- Should services that are "operated for" IdPs be allowed (e.g., cloud infrastructure - geant.altassian.com vs wiki.geant.org)?
  - Who is registering the entity, which challenges are there with registering cloud entities, how do you determine the difference between a private / community-based approach vs just having an account in a commercial environment

So Let’s Make It About The Attributes

“Candidates for the **Personalized Entity Category** are Service Providers that have a proven need to receive a **small set of personally identifiable information** about their users in order to effectively provide their service to the user or to enable the user to signal their identity to other users within the service.”

Anonymous Access

schacHomeOrganization
eduPersonScopedAffiliation

Pseudonymous Access

schacHomeOrganization
pairwise-id
eduPersonScopedAffiliation
eduPersonAssurance

Personalized Access

schacHomeOrganization
subject-id
displayName
givenName
Sn
Mail
eduPersonScopedAffiliation
eduPersonAssurance

Key Points of WG Consensus (Part 1)

- If schacHomeOrg is present, then it's the value to be used; if not present, eduPersonScopedAffiliation should be used. (See 2021-07-01 R&S 2.0 Notes)
  - this is more appropriate for the other entity categories; for Personalized, we're requiring schacHomeOrg and so this statement does not apply
- We will adopt the following from R&S 1.3: "Service Providers SHOULD limit their data requirements to the bundle of attributes defined in Section 5, but MAY negotiate for additional data as required via mechanisms that are outside the scope of this specification." (See 2021-07-01 R&S 2.0 Notes)
- The entity categories (Anonymous Authorization, Pseudonymous, and Personalized) are mutually exclusive (See 2021-07-01 R&S 2.0 Notes)
- We will use subject-id for this specification. (See 2021-08-10 R&S 2.0 Notes)

Key Points of WG Consensus (Part 2)

- The Anonymous Access, Pseudonymous Access, and Personalized Access Entity Categories shall be harmonized based on the decisions made around Personalized Access.
- Authorization guidance shall be split out into a separate, descriptive paper and not be part of any of the entity categories.
- The names should be "Access Entity Category" not "Authorization Entity Category" - 10 January 2022
- We will not include assurance requirements to the Anonymous Access Entity Category - 10 January 2022
- We will take out wording in Anonymous that Section 4 that requires proof while leaving in wording that requires documentation for Registration Requirements - 24 January 2022
- We will remove the technical requirements for SAML2 and metadata refresh - 7 April 2022
- Federations should allow SPs to request multiple ECs - 4 May 2022

Still to resolve…

- Practicalities of a graceful fallback mechanism OR a fourth EC
  - If the SP should only request **Personalized**, and if the IdP only supports **Pseudonymous**, the IdP will respond with Pseudonymous even if the request is for Personalized. The SP will present a different (lesser) level of service if it can't get Personalized, thus resolving the concern that the SP cannot operate with less than Personalized.
- Review initial draft for authorization - Federated Authorization Best Practices