2021-04-15 R&S 2.0 Notes

Attendees

- Christos Kanellopoulos
- Pål Axelsson
- Jiri Pavlik
- Miroslav Milinovi
- Alan Buxey
- Jon Agland
- Andrew Morgan
- Scott Cantor
- Nicole Harris
- David St Pierre Bantz
- Heather Flanagan

Regrets

- Markus
- Peter

Working Draft

- Draft spec for R&S 2.0

Agenda

1. Recap of consensus so far - **note that all changes will need to be validated via the consultation process**
   a. The FAQ will be revised to offer clarity on the term "affiliation" (see Research and Scholarship FAQ) and editorial changes made to the spec to make it more clear (see new draft spec for updated structure)
   b. eduPersonScopedAffiliation will become a required value
   c. R&S will require privacy statements
   d. Encouraging the use of eduPersonAssurance requires further discussion with the Assurance Working group
   e. subject-id should be listed as the new identifier
   f. R&S 1.3 and R&S 2.0 can co-exist; no migration detail will be included in the spec itself.
   g. ePPN and targeted ID to both be removed from R&S 2.0
   h. Information on OIDC requirements will be moved to R&S 2.1 (after the OIDF OIDCre working group has formal documentation in this space)
   i. eduPersonAssurance will be required, RAF recommended
2. Home Organization use case (Andrew Morgan and Christos Kanellopoulos)
3. Proposal to require DisplayName (Petersen)

Notes

1. Recap of consensus so far - **note that all changes will need to be validated via the consultation process**
   a. The FAQ will be revised to offer clarity on the term "affiliation" (see Research and Scholarship FAQ) and editorial changes made to the spec to make it more clear (see new draft spec for updated structure)
   b. eduPersonScopedAffiliation will become a required value
   c. R&S will require privacy statements
   d. subject-id should be listed as the new identifier
   e. R&S 1.3 and R&S 2.0 can co-exist; no migration detail will be included in the spec itself.
   f. ePPN and targeted ID to both be removed from R&S 2.0
   g. Information on OIDC requirements will be moved to R&S 2.1 (after the OIDF OIDCre working group has formal documentation in this space)
   h. eduPersonAssurance will be required, RAF recommended
2. Home Organization use case (Andrew Morgan and Christos Kanellopoulos)

   a. The general requirement is an attribute that identifies the home organization of the subject. In the absence of creating a new attribute, schacHomeOrg is a good fit because it is just a domain name, which makes it globally unique on the Internet and it is not directly tied to an entityID which does not map directly to a home organization (thank you, proxy servers). This turns into a basic identifier for where a user is from, which is important for the student mobility use case. An IdP would only be responsible for asserting its own home organization; this makes it a fixed value that an IdP would release for all its users.
      i. How is this different from scoped affiliation? There are cases where the scopes are not matching the home organization because of one IdP proxying for several organizations, or sub-units that will have their own home org but the scope of the parent organization. One could choose to derive home org from the scope, but that will require some assumptions that may not be accurate.
      ii. This may also be a use case for another value of affiliation.

      iii. Is this an attribute of the IdP or of the subject? It is not exactly an attribute of the subject. It is the name of the institution that's in the attribute of the user. It's about who I'm representing as an IdP (which makes it not about the subject). That will make it static most of the time, and it would possibly be easier to handle by defining a new value for eduPersonAffliation. If we define a value of "affiliate2", that value would be expected to appear only once and be clear in the profile.

      iv. In a typical model, this is actually pretty easy. But where it is more complicated, we need to figure out how to write the text that would help us predict what people will populate this value with. What do we do when it's a shared IdP and the IdP doesn't even know what the home org is?

      v. Another challenge here is that "home organization" isn't defined as a term itself in the SCHAC spec.

      vi. We're talking about two potential options here: introducing schacHomeOrg to R&S (which will be a lift since SCHAC isn't globally used), or adding a value to eduPersonScopedAffliation (which has its own lift).

      vii. We need to document what would happen in the more complex use cases (e.g., IdP that proxies other organizations) and how those would be handled.

         ☐ Miroslav Milinovi, Christos Kanellopoulos will write up complex use cases (or real world examples) to help describe what the IdP would assert when the IdP has several different organizations involved

      viii. It may help to consider home org to be defined as origin org.

      ix. It would also help if we offered (outside of R&S) more guidance on how to use things like subject-id to include student numbers or ERP identifiers

3. Proposal to require DisplayName (Petersen)

    a. To be covered on our next call