2021-07-23 R&S 2.0 Notes

Attendees
- Heather Flanagan
- Andrew Morgan
- Christos Kanellopoulos
- Jens Jensen
- Alan Buxey
- Scott Cantor
- Nicole Harris
- Alex Stuart
- Adam Snook

Pre-Reading
- Anonymous Authorization
- Pseudonymous Authorization
- comparison of attribute release information between each entity category

Working Draft
- Draft spec for R&S 2.0
- Personalized Authorization spec starter

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. 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
      i. We’ll resolve the need for information on the origin organization by adding guidance for the use for eduPersonScopedAffiliation
   j. DisplayName and Given/SN are required
2. Recap of consensus specific to the Personalized Authorization spec
   a. If schacHomeOrg is present, then it’s the value to be used; if not present, eduPersonScopedAffiliation should be used.
   b. 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.”
   c. The entity categories (Anonymous Authorization, Pseudonymous, and Personalized) are mutually exclusive
3. Reviewing the draft spec
   a. Normalizing organizational attributes between R&S, Anonymous, Pseudonymous Entity Categories
      i. From the 1 July 2021 call: Only Personalized requires a third-party review (similar to as R&S is today). The other entity categories can remain self-asserted since the risk is minimal.
      ii. From the 1 July 2021 call: The specs need to be consistent as they talk about how the attributes like affiliation and entitlement should be used.
      iii. From the 1 July 2021 call: The language around user identifiers for Pseudonymous and Personalized needs to be made consistent; those are the correct attributes, but the description needs to be made more clear.
   b. Clarifying entitlement
      i. From the 1 July 2021 call: It's not clear enough to say that this is the minimal bundle, but you might be able to get more.
      ii. From the 1 July 2021 call: The general principle is that if you want to have a frictionless interoperable experience and to meet minimization standards, don't do anything outside this bundle. But if your business needs require more, that's up to you and your responsibility.
      iii. From the 1 July 2021 call: If we're encouraging entitlement and not affiliation, then we should make sure that entitlement is in there.
      iv. From the 1 July 2021 call: The authorization story should be more consistent. We should also be consistent with what we say affiliation is for.
4. Discussion of subject-id as source for origin organization (if not resolved on the list)
   a. postponing pending coverage of Personalized Authorization and the other entity categories

Notes
1. Recap of consensus specific to the Personalized Authorization spec - no dissension in the ranks on these
Definition Statement for R&S

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.

<table>
<thead>
<tr>
<th>Areas questioned</th>
<th>Potential issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is R&amp;S focused on the requirements of the service or the organisational type</td>
<td>Issues with not having a definition of an R&amp;S / R&amp;E organisation and the fact that most organisations have business arms to R&amp;E structure</td>
</tr>
<tr>
<td>Should &quot;commercial&quot; services be allowed</td>
<td>No way to distinguish the nuance in commercial vs paid for</td>
</tr>
<tr>
<td>Should services that are contracted be allowed</td>
<td>Contracts are paid for things like collaborative wikis, having a contract does nothing to help the IdP administrator formulate an attribute release policy</td>
</tr>
<tr>
<td>Should &quot;management&quot; be dropped from the definition statement</td>
<td></td>
</tr>
<tr>
<td>Is this about translation of real world trust (need to collaborate with other humans) into the spec</td>
<td></td>
</tr>
<tr>
<td>Should services that are &quot;operated for&quot; IdPs be allowed (e.g. cloud infrastructure - geant.altassian.com vs wiki.geant.org)</td>
<td>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</td>
</tr>
<tr>
<td>Problem of only calling out e-journals in the existing spec</td>
<td>Better phrased as something like &quot;Service Provider MUST be able to prove that it has a legitimate need for the personal data in the attribute bundle.&quot; (positive rather than negative entry requirement).</td>
</tr>
</tbody>
</table>