2021-06-10 R&S 2.0 Notes

Attendees

- Nicole Harris
- Alan Buxey
- Alex Stuart
- Pål Axelsson
- Mischa Salle
- Miroslav Milinovi
- Scott Cantor
- Jií Pavlík
- Björn Mattsson@BTH
- Heather Flanagan

Working Draft

- Draft spec for R&S 2.0
- "Identifiable User" 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. Definition Statement for R&S
    a. Review new alternative to R&S 2.0
3. Discussion of subject-id as source for origin organization (if not resolved on the list)
4. Solicitation of volunteers to focus on supporting documentation
5. Normalizing organizational attributes between R&S, Anonymous, Pseudonymous Entity Categories

Notes

1. Definition Statement for R&S
    a. Review new alternative to R&S 2.0
    b. Poll: Which entity category should we focus on: R&S 2.0 (3 people, 33%), Identifiable User (5 people, 56%), Both, I Need More Information (1 person, 11%)
    c. The proposal to call this Personalized Authorization seems to resonate.
    d. We could layer on the concept of R&S to Personalized Authorization.
    e. Personalized Authorization is an entirely different approach that let's us avoid the unsolvable issue of defining what R&S means in all federations. Instead, we're focusing on whether the SP needs the attributes, regardless of whatever R&S means. People don't release data just because of the type of service; there are other considerations regarding what country they are in, what they need it for, etc.
    f. R&S may be easier to promote because it is well known.
    g. Reminder that for assurance, you have to say what you're doing (which may be nothing). The big change in R&S 2.0 is actually subject-id.
    h. All the difficult questions for Personalized Authorization are around marketing and politics, not technical merit.
    i. Does CoCo fit into this realm of entity categories? It's just a different way of asking for the same kind of data. The only thing we can monitor and check is the privacy URL. This entity category doesn't help make a sensible decision about the attribute bundle.
    j. Should we do a pre-consultation effort? It might not be clear until we have cleaned up the text and removed R&S. Need to frame it and present it as an extension of the other entity categories. The consultation will be something of a unit for the whole bundle.
    k. We have also proposed some structured language around R&S to offer guidance to fed ops on when and how to apply it. In either category, fed ops would need to actively opt into this. We want to get to the point where there is an understanding that there is a fed ops process. This is in supporting material, not in the spec itself. We can move to get community buy in on this right now.
2. Normalizing organizational attributes between R&S, Anonymous, Pseudonymous Entity Categories
    a. Particularly regarding how organizations are identified, we need to determine if consistency across all the entity categories is possible (it is definitely desirable)

    b. Homework: working group members need to read through the other entity categories so we can discuss them in conjunction with Personalized Authorization. If we want to propose changes to those specs in favor of the work done in this working group, that's ok.
3. 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
4. Solicitation of volunteers to focus on supporting documentation
    a. postponing until we have WG consensus on spec

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.

Areas questioned	**Potential issues**
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 "management" be dropped from the definition statement	
Is this about translation of real world trust (need to collaborate with other humans) into the spec	
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
Problem of only calling out e-journals in the existing spec	Better phrased as something like "Service Provider MUST be able to prove that it has a legitimate need for the personal data in the attribute bundle." (positive rather than negative entry requirement).