2021-07-01 R&S 2.0 Notes

Attendees

- Heather Flanagan
- David St Pierre Bantz
- Scott Cantor
- Maarten Kremers
- Miroslav Milinovi
- Nicole Harris
- Jií Pavlík
- Björn Mattsson@BTH
- Alan Buxey

Pre-Reading

- Anonymous Authorization
- Pseudonymous Authorization

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. Normalizing organizational attributes between R&S, Anonymous, Pseudonymous Entity Categories
    a. 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

Notes

1. Normalizing organizational attributes between R&S, Anonymous, Pseudonymous Entity Categories
    a. Nicole has created a comparison of attribute release information between each entity category
    b. Why is OrgDN included at all? It's not clear what's actually required. Do we have to express home org in all cases? If the SP needs to know what organization a user is coming from because of a subscription model, then they really should be using the entitlement data and not the organization. Still under debate: should entitlement require registration? The original concern was that a free-for-all of support for entitlement was too hard to support. Alternatively, though, these are generally pairwise. Suggest we limit the scope regarding the interoperability of the entity category.
    c. If home org is required in all cases, we should be clear as to why that information should be used and how it is not an entitlement. Maybe "if schacHomeOrg is present, then it's the value to be used; if not present, eduPersonScopedAffiliation should be used."
    d. eduPersonOrgDN is an X.509 structure; the value in the directory is formally defined, whereas the scope we use are domains. If you put the scope in the OrgDN, then you have a broken OrgDN.
    e. If we normalize on schacHomeOrg, that can just be a string passed as per config in the IdP; it does not have to be set in a directory
        i. Poll: Should we default to schacHomeOrg for all three entity categories? Yes 75% (6); No 13% (1); Need More Info 13% (1)
        ii. No - if we require schacHomeOrg exclusively, will limit adoption. ScopedAffiliation is so much more commonly supported.
        iii. **Consensus: if schacHomeOrg is present, then it's the value to be used; if not present, eduPersonScopedAffiliation should be used.**
    f. If we remove entitlements from the attribute bundle, are SPs even allowed to ask for an entitlement attribute given "Service Providers SHOULD limit their data requirements to the bundle of attributes defined in Section 4."? The purpose of this is to say that the IdP is not guaranteed to give you anything else, not that you can't ask for anything else. Entitlement needs to be described better; even limiting to

common-lib-terms is not sufficient for all cases. eduPersonEntitlement may also be more than one value….. that sentence reads like it can only be one
        i. Need to write up language in the new proposal that would transfer across to the other, minus the entitlement part.
        ii. Poll: Should we adopt the text 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." Yes for all three 63% (5); Yes for Pseudonymous and Personalized only 25% (2); No, too open 13% (1)
            1. It's not clear enough to say that this is the minimal bundle, but you might be able to get more.
            2. 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.
            3. If we're encouraging entitlement and not affiliation, then we should make sure that entitlement is in there.
            4. The authorization story should be more consistent. We should also be consistent with what we say affiliation is for.
    g. The entitlements registry is only for globally recognized values, not any and all values possible
    h. The categories are mutually exclusive; an SP can't publish in metadata that they want all three. They'll have to pick what works for the majority of their use cases, and otherwise negotiate for additional attributes where needed.
    i. 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.
    j. The specs need to be consistent as they talk about how the attributes like affiliation and entitlement should be used.
    k. 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.
2. Next step
    a. Heather will draft changes to the personalized entity category, highlighting where we think that language should be used in the other entity categories
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

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).