2021-08-25 R&S 2.0 Notes

Attendees

- Jií Pavlík
- Heather Flanagan
- David St Pierre Bantz
- Pål Axelsson
- Björn Mattsson
- Andrew Morgan
- Scott Cantor
- Miroslav Milinovi
- Jens Jensen - STFC UKRI (from 15.30 UTC)

Regrets

- Alex Stuart
- Alan Buxey

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 for Personalized Authorization so far - **note that all changes will need to be validated via the consultation process**
    a. 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)
    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." (See 2021-07-01 R&S 2.0 Notes)
    c. The entity categories (Anonymous Authorization, Pseudonymous, and Personalized) are mutually exclusive (See 2021-07-01 R&S 2.0 Notes)
    d. We will use subject-id for this specification. (See 2021-08-10 R&S 2.0 Notes)
2. Reviewing the draft spec
    a. title of the category - this isn't about "Authorization" so maybe "Personalized Access" or "Personalized Entity Category"?
3. Start with section 6 of the draft; note this touches on the consensus we reached on an earlier call "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."

Notes

1. Recap of consensus for Personalized Authorization so far - **note that all changes will need to be validated via the consultation process**
    a. 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)
        i. this is more appropriate for the other entity categories; for Personalized, we're requiring schacHomeOrg and so this statement does not apply
    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." (See 2021-07-01 R&S 2.0 Notes)
    c. The entity categories (Anonymous Authorization, Pseudonymous, and Personalized) are mutually exclusive (See 2021-07-01 R&S 2.0 Notes)
    d. We will use subject-id for this specification. (See 2021-08-10 R&S 2.0 Notes)
2. Reviewing the draft spec
    a. title of the category - this isn't about "Authorization" so maybe "Personalized Access" or "Personalized Entity Category"?
        i. NO strong opinion, so we'll call it Personalized (poll divided fairly evenly)

3. Start with section 6 of the draft; note this touches on the consensus we reached on an earlier call "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."
    a. Scott Cantor and Andrew Morgan will work on revising section 6; keep the SHOULD/MAY construct, and work in at least an example of eduPersonEntitlement being something SPs might negotiate separately
4. Next steps
    a. Discuss proposals for section 6 and do a consensus call on the draft spec at our next call
    b. Target sending out for consultation the week of September 13; consultation to last for 4 weeks, which will overlap the REFEDS, CAMP, and ACAMP meetings
    c. During the consultation period for Personalized, we'll start work on harmonizing the Anonymous and Pseudonymous Authorization 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).