2022-01-24 R&S 2.0 Notes

Attendees

- Heather Flanagan
- Andrew Morgan
- David St Pierre Bantz
- Björn Mattsson
- Scott Cantor
- Jií Pavlík
- Christos Kanellopoulos
- Rob Smith (OpenAthens)
- Kevin Morooney
- Jens Jensen

Pre-reading

- Anonymous Access Draft
- Pseudonymous Access Draft
- Personalized Access Entity Category (zenodo copy)
- Federated Authorization Best Practices

WG Consensus

- The Anonymous Access, Pseudonymous Access, and Personalized Access Entity Categories shall be harmonized based on the decisions made around Personalized Access.
- Authorization guidance shall be split out into a separate, descriptive paper and not be part of any of the entity categories.
- The names should be “Access Entity Category” not “Authorization Entity Category” - 10 January 2022
- We will not include assurance requirements to the Anonymous Access Entity Category - 10 January 2022
- We will take out wording in Section 4 that requires proof while leaving in wording that requires documentation for Registration Requirements - 24 January 2022

Agenda

- Verify WG Consensus items
- Review proposed changes to Anonymous and Pseudonymous ECs
- Review initial draft for authorization (Scott C’s action item from last call) - Federated Authorization Best Practices

Notes

- Verified WG Consensus items
- Review proposed changes to Anonymous and Pseudonymous ECs (Pål’s action item from last call)
  - Should Anonymous Access require registration? Should there at least be validation within the federation regarding the registration of the SP? Because we took out the R&S-ness, it’s not clear how the registrar is going to validate any of the requirements; we’ve taken out the requirement that requires human judgement. This is a policy requirement on the federation that the registration process that all entity categories are validated. Beyond checking that the elements exist, what can be validated?
    - One option is that the federation operator checks that requested attributes are described in the privacy policy; though this is far from common practice at the moment – it would at least show that the SP has thought about why attributes are needed.
    - Should the Anonymous Access EC Registration Requirements keep section 4.1? 4, yes; 5, no; 1, need more info. The “need more info” is that the desire for review is there, but the pragmatic view is that the registrar can’t consistently do it. One consideration is that it’s important to at least ask the question so that there is some indication of best effort that some (minimal) care was put into this.
    - Consensus on the rewording to take out “proven” from the registration requirements
  - Concern that schacHomeOrganization doesn’t allow for finer-grained organizational information; it’s the scope of the IdP. An IdP can have multiple scopes, though.
  - Pål to match up Pseudonymous and Personalized EC’s based on changes made to Anonymous
- Review initial draft for authorization (Scott C’s action item from previous call) - Federated Authorization Best Practices
  - “I think it’s important that a service that requires only the former but can do the latter be able to assert both. We should take care to author the changes to both of them to ensure that’s sensible. It shouldn’t worded so strictly that you have to pick only one.”
  - To be discussed next call