2021-12-09 R&S 2.0 Notes

Attendees

- Pål Axelsson
- Björn Mattsson
- Alex Stuart
- Andrew Morgan
- Scott Cantor
- Jií Pavlík
- David St Pierre Bantz
- Heather Flanagan
- Alan Buxey

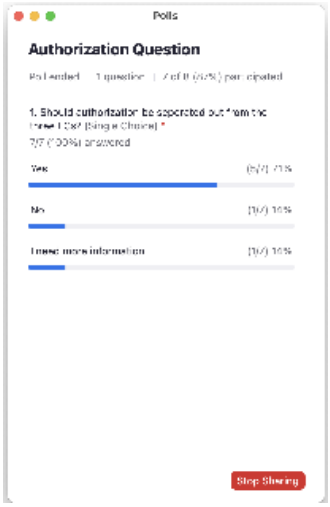
Pre-reading

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

Agenda

- Feedback from SeamlessAccess Contract Language WG on the Anonymous and Pseudonymous ECs
- Discussing potential changes to harmonize with the Personalized Access EC

Notes

- Feedback from the SeamlessAccess Contract Language group has been added in a box in each draft.
- If we work against the assumption that these should be harmonized, need to make sure we have consensus on which direction the harmonization should run. If we re-write according to the same rules, rather than adjust piecemeal, that might be more effective.
- One big difference in the doc is how they handle organization. There was a lot of discussion, and Personalized did something different because it does not require affiliation.
- An entity category sets rules for attribute release; allowing several alternatives for any specific use defeats the purpose of standardization.
- The way entitlement is referred to, if we make it consistent with Personalized, will also result in changes. Entitlement is not in personalized at all.
- Should affiliation be required in Anonymous if it uses affiliation and organization?
- These are not authorization specs; they are authentication and identification specs. If we are talking about authorization, we need to be consistent across all three ECs.
- If you want to require eduPersonEntitlement for use with authorization, you need to be more specific about values.
    - Should not bake the registry into the document
    - Entitlement has a security implication; entitlement is a general concept; releasing entitlement cannot be done per SP, it would be general and released to all SPs
    - 

- For anonymous, the default identification is organization-wide. Whether that's sufficient for authorization is dependent on the service. In a sense, this ends up being just a replacement for IP address authorization. We already decided that we won't prevent people from using affiliation for authorization decisions, though we will tell them they shouldn't. The goal is to be consistent across all three ECs, so we should stick with what we decided in Personalized.

- If we take away authorization from the ECs, we need to provide guidance for how to do authorization properly
  - Should this be prescriptive guidance or descriptive guidance? Prescriptive would be something like how to specifically use common-lib-terms; Descriptive would have the library/common-lib-term as an example
  - It will often be a business problem to get entitlement populated with whatever values the SP might expect to see. Authorization may require SP-specific knowledge, sometimes it may be IdP-specific knowledge.
  - Given the range of possibilities, the document must be descriptive because it will need to talk about when and why IdP specific authorization would work (e.g., common-lib-terms) and when and why it wouldn't and SP-specific authorization should happen. Current thought is to have this be a living doc that may refer to the registry and be updated as we learn more about existing and valid use cases for how authorization is handled in the world. There are entitlements that are highly generic; there are others that are highly specific. Here's where to find highly generic that you should use when general interop is required. If you have other use cases, consider adding to the registry. (Don't reinvent wheels.)
- Action items:
  - [ ] Scott Cantor to take a first pass at writing up a descriptive doc for entitlement
  - [ ] Pål Axelsson to take a first pass at updating the anonymous and pseudonymous specs with what we have in personalized