2022-09-08 R&S 2.0 Notes

Attendees

- Heather Flanagan
- Björn Mattsson
- Pål Axelsson
- Andrew Morgan
- Jií Pavlík
- Scott Cantor
- Nicole Harris
- Alan Buxey
- David St Pierre Bantz
- Jens Jensen - STFC UKRI

Pre-reading

- Anonymous Access Draft
- Pseudonymous Access Draft
- Personalized Access Draft
- 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 Anonymous that Section 4 that requires proof while leaving in wording that requires documentation for Registration Requirements - 24 January 2022
- We will remove the technical requirements for SAML2 and metadata refresh - 7 April 2022
- Pseudonymous is done (modulo any changes identified as we work through personalized) - 20 April 2022
- Federations should allow SPs to request multiple ECs - 4 May 2022
    - Consensus on this revised in light of expectation to keep ECs distinct and to create a fourth EC that allows a modified fallback mechanism (if these attributes cannot be released, then release these others) - 20 July 2022

Agenda

- Review revised text for Personalized and Pseudonymous
- Review initial draft for authorization - 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."

Notes

- Review revised text for Personalized and Pseudonymous
    - Group agreed that, modulo some formatting changes, the documents are ready for consultation. Heather to sort the details.
- Review initial draft for authorization - 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."
    - expect contention
    - suggested maybe additional examples covering faculty, staff members?
        - should be SP specific for each eduPersonEntitlement; in practice, it's unlikely you'll be able to avoid doing that. The dominant use case is that roles and privs do not overlap between services. It's easier to start with unique and work backwards to shared; every new service will be considered unique to start, and Grouper is often used to facilitate when there are common policies behind those entitlements
        - It would be nice to have a research project as a use case (if we can find one that's willing to be shared)
    - Maybe be worth noting that issues with categorizing entitlements is similar to issues with categorizing affiliation; should use some more text there.
    - This is ready for consultation
- Next steps - after the consultation for the ECs and the best practice doc, we'll start on the fourth EC to address the fallback option use case