2022-07-20 R&S 2.0 WG Notes

Attendees

- David St Pierre Bantz
- Heather Flanagan
- Marcus Hardt
- Nicole Harris
- Scott Cantor
- Andrew Morgan
- Jens Jensen - STFC UKRI
- Martin Stanislav

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

- Feedback from the community at REFEDS 44
    - Entity categories must be self-contained when it comes to the guidance around attribute release; they must not have dependencies on each other. Rather than tie the ECs together with the fallback mechanism we have been debating, it would be better to create a fourth EC with its own attribute bundle and associated guidance.
- Revising text for Personalized and Pseudonymous to remove the fallback text
- 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

- Feedback from the community at REFEDS 44
    - Entity categories must be self-contained when it comes to the guidance around attribute release; they must not have dependencies on each other. Rather than tie the ECs together with the fallback mechanism we have been debating, it would be better to create a fourth EC with its own attribute bundle and associated guidance.
    - Did the community think the fourth entity category was even useful? Should we still use it? It seems that the biggest constituency in Europe would see a combined EC as the same as Pseudonymous.
    - If we do this on its own, we will be able to see how well it does independent of others.
    - We can put these out to consultation separately, which will focus the conversations
    - Were there any questions about having these apply to most users? No, that is common text in ECs that this should apply to most, but it doesn't have to be all. The IdP still determines when (and to what users) to apply that tag and release the attributes.
    - Did people comment on pairwise being included? Yes, in that they noticed it and recognized we're shifting identifiers across the board.
    - Did people comment on how we are handling authorization? Not really
    - Does this impact if/whether SPs can request multiple ECs? What would the policy look like on the IdP side? If we let the SP request Pseudonymous and Personalized, then isn't that effectively the same as the fourth EC?
        - the argument is that if you get one set of attributes you get a different level of service (see May 4 notes); though we've also tried to back away from that with the combined EC
        - The IdP can publish multiple, but the SP needs to only publish one IF we create that fourth EC.
        - This is a question more for federations; that doesn't get described in the EC specs themselves

    - We need the REFEDS Guidelines doc to help explain how these ECs do/don't relate to each other and what federations should consider when supporting them. We will need to add something to the Anonymous to make sure to point to the guidelines since those guidelines will include more than just how federations should review requests
        - Some concern that this will be so complicated to deploy that the fourth EC is just too much
        - We should be really simple on how to support these ECs and avoid "if/then/else" structures in the guidelines
        - It needs to be simple enough that SPs are clear on what they are asking for and why, clear for IdPs on what to support and why, and clear for federations as to what they will support
        - Normally do not incude supporting material in the consultation, so we don't have to have these guidelines done before then
- Revising text for Personalized and Pseudonymous to remove the fallback text
    - Heather will work on the text
    - Group to think about what we need to call the fourth EC
- 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."
    - Heather wants to prioritize the discussion of this before we go out to consultation