2022-05-04 R&S 2.0 Notes

Attendees

- Andrew Morgan
- Scott Cantor
- Pål Axelsson
- Jens Jensen - STFC UKRI
- Heather Flanagan
- Christos Kanellopoulos
- Martin Stanislav
- Marcus Hardt
- David St Pierre Bantz
- Björn Mattsson

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

Agenda

- Review proposed changes to Anonymous and Personalized
    - Walkthrough Anonymous and the question about if/how to indicate whether an SP can indicate support for more than one of this family of ECs
    - Review updates to Personalized that were based on changes to Pseudonymous
- Review initial draft for authorization (Scott C's action item from last 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."

Notes

- Review proposed changes to Anonymous and Personalized
    - Walkthrough Anonymous and the question about if/how to indicate whether an SP can indicate support for more than one of this family of ECs
    - Review updates to Personalized that were based on changes to Pseudonymous
    - Focus on Section 5 of Personalized and whether that first paragraph must match Pseudonymous or not. Particularly of note, the sentence "The attributes chosen represent a privacy baseline such that further minimization achieves no particular benefit." is what makes it impossible for a site to request both Pseudonymous and Personalized; they are mutually exclusive given this statement.
        - If a service is running that could function with Pseudonymous, but would have value-add if Personalized, then that's an argument as to why to use both. It's not then a minimization argument, it's a usability argument.
        - Could we change "achieves no particular benefit" to "achieves no particular benefit for applicable service behaviors"?
        - Can an IdP send both pairwise and subject? They are separate attributes so both could be sent; it's up to the SP as to how to consume them.
        - It is possible to set a policy that sets the preferences for one EC over another (e.g., if an SP asserts both Anonymous and Pseudonymous, then Anonymous wins)
        - Group consensus: SPs should be allowed to request multiple ECs.
        - This will make configuration more challenging for IdPs.
        - FAQ will need to include what to do when asserting multiple categories, so SPs know what to expect.
        - What would make Christos happy is if there was language to denote that if I, as an SP, request personalized but the IdP supports up to pseudonymous the IdP should use that instead of just nothing.
        - By making ECs composable, we are giving some IdPs and SPs in some regions a footgun. That is a valid concern, but it is out of scope for what we write in the spec.

        - Note that metadata cannot, according to the spec, be ordered such that if an SP wants to assert multiple that automatic failover works. The IdP can set the policy to prefer one EC over another, but SPs cannot do that.
    - Heather to post a question to the list to ask SPs how they envision these three categories combine (or not combine) for their services.
- Review initial draft for authorization (Scott C's action item from last 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."