2022-05-18 R&S 2.0 Notes

Attendees

- Andrew Morgan
- Scott Cantor
- Pål Axelsson
- Heather Flanagan
- Christos Kanellopoulos
- Marcus Hardt
- Björn Mattsson
- Martin Stanislav

Regrets

- Alan Buxey

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
        - 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. Note consensus from 4 May 2022 call re: allowing SPs to request multiple ECs.
        - Note responses from SPs:
            - Meshna (Elsevier) on list: "I think an SP should signal the lowest possible category it needs. Anything else would require additional explanation / negotiation and in my eyes that's in conflict with the purpose of categories."
            - Alan (myUniDays) on list: they will only use Psuedonymous, but adds that multi-tiered services may want different levels of personalization, but being able to distinguish in the moment of a user logging in is problematic
            - Participants in SeamlessAccess Contract Language Working Group suggest we look at the original proposals that included implementation details. (SeamlessAccess Pseudonymous, Anonymous Authorization)
    - 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
    - If the SPs are going to just ask for additional information directly after getting what they can from the EC, what's the point of allowing multiple ECs?
    - Coming back to why an SP would want to request multiple ECs - it is about allowing graceful failures.
        - Note that the identifiers are different across Pseudonymous and Personalized, and so this doesn't necessarily qualify as a graceful failure from more to less.
    - Ebsco's SP currently supports the equivalent to all three ECs based on the privacy preferences of the user and the IdP

    - If you support multiple ECs, the result of what comes back to the SP will be very hard to predict. We may be making the problem worse instead of better. From a true GDPR perspective, should use Pseudonymous directly in support of data minimization. The extremes (Anonymous and Personalized) are reasonably well defined, the question does come with Pseudonymous.
    - This is the same issue between "Required" and "Optional" attributes - no one actually knows how to handle that, and usually just drop the optional.
    - Is the solution a fourth category? We are looking at a specific scenario that is fairly well defined: "we want this but will accept this" and we could write a category specifically to capture this.
    - Maybe add language who do not support personalized and get a request from an SP that does; suggest that the IdP should not fail, but instead should have different default behavior. This happens with NameID policies (though that's a problem with the NameID spec).
    - Should we create a fourth entity category to resolve optional attribute requests? Poll - Yes (3); No (1); I would rather update Pseudonymous (0); I need more information (3)
        - No - this would just extend the problem as it still does not offer guidance as to what to use and when.
        - If GDPR is the primary motivator, then again need to choose the lesser of the two categories.
        - We could also change Personalized to allow for two bundles, and in the GDPR case get the lesser of two bundles, but then any service that ask for Personalized may receive Pseudonymous information, even if that's not what they can use. To avoid that, need to allow multiple ECs.
    - If we only update Pseudonymous to say "If an SP supports personalized but an IdP supports pseudonymous, the IdP MUST respond with the pseudo bundle." But feedback this won't work because the participants don't look at that cross configuration as per policy, and that if an SP is expecting subjectID they won't be able to handle pairwiseID.
    - Are we trying to put every SP into one of these categories? Maybe some SPs just don't work with these ECs. But this might also be a common enough scenario that we should address it to avoid problems down the road.
    - If we say "if an SP supports personalized but an IdP supports pseudonymous, the IdP MUST respond with the pseudo bundle." then the statement "The attributes chosen represent a privacy baseline such that further minimization achieves no particular benefit." needs to come out of Personalized
    - In some cases, a service may be able to function with less, but the user will have a worse experience. The support side is clearer than the IdP side.
    - **For our next call: WG members will add proposed text to both Psudeonymous and Personalized to see if we can come to consensus on where and how to clarify the need for failover information while addressing data minimization concerns.**
- 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."