2022-05-25 R&S 2.0 Notes

Attendees

- Andrew Morgan
- Scott Cantor
- Pål Axelsson
- Heather Flanagan
- Christos Kanellopoulos
- Björn Mattsson
- Jií Pavlík
- 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

Agenda

- Review text re: requiring a graceful failover from Personalized to Pseudonymous, and consider what that means for the data minimization statement
- 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

- Scott captured what Christos was looking for in IdP guidance
    - Some debate on whether this should be a SHOULD rather than a MAY. How would this be handled? Filter policies should be able to take care of this for the IdP.
    - This does make it difficult to figure out from an SP what they should expect to receive.
- Pal's proposal requires registering both categories, which Scott's proposal doesn't.
    - If the IdP reads that a service may do both of them, they won't do that by default because they will insist on minimization.
    - We're not saying send more data to pseudonymous, we're saying send less data to pseudonymous. If you say pseudonymous as a service, that's "all I need to operate is pseudonymous (e.g., pairwise)" If you say personalized as a service, that's "you nominally want personalized and a public IP, but you can function with less and you'd like services to fall back to that if that's what you're comfortable with." Mechanically, how we do it is the question.
    - Concern that Pal's text may still lead to confusion.
    - The problem with both ways of doing this is the increase in complexity to the ECs. Will that result in less uptake or better uptake?
    - There will be questions from both IdP and SPs - should we leave this to SPs to take care of users, or should we drive users to consent? What is the recommended default?
    - Consent is problematic because of different laws; we need to leave that out of the document. Whatever the default is may well depend on your jurisdiction.
    - Regarding the complexity, that's not as much a problem as ambiguity.
    - This isn't a technical problem (of complexity or even ambiguity) it's a data protection problem. If you have a data minimization focused DPO, they will release the minimum and nothing else. They may not understand that we're saying it's ok to give less.
    - What's written in pseudonymous is already true today in that as an IdP operator I can add attributes at my discretion. How do we write this such that people are more comfortable? By providing sample release policies.
    - In Pal's proposal, it doesn't explain what the IdP is supposed to do (though that is implied). It's a warning that the SP won't know what to expect to receive.
- Poll - Where do we include text regarding a graceful fallback to Pseudonymous?
    - Only what's been proposed in Personalized
    - Only what's been proposed in Pseudonymous (14%; 1/7)

    - Something in both ECs (86%; 6/7)
    - Need more info
- Regarding both suggestions, one is written more towards SPs, the other more towards IdP.
    - Maybe have the guidance in SP section for Personalized, and in the IdP section for Pseudonymous.
    - In an IdP that supports Personalized, and the SP requests both, if we say respond with Personalized, that goes against data minimization. If you are doing both and you give the less of the two, you may not get full service for the users. It's up to the IdP to decide if that's acceptable; all the power is given to the IdP.
    - If the SP can decide if it requires less data, it can assert that. So that much is up to the SP, not the IdP.
    - You could split the SP category on the Personalized side, one that's personalized, the other that's personalized with a fallback; that would provide a very clean signal to the IdP. But by doing that, you're communicating under GDPR that you don't actually need Personalized and so you'll only get Pseudonymous.
      If we take minimization text out of Personalized (which we have to do if we go ahead with this fallback option) that will result in Pseudonymous.
    - If an SP says they support Personalized, it means they need to personalize access for the user. There may be compensating controls involved. Can we include text that allow for that in Personalized? And in Pseudonymous, say that IdP MAY release more info if the SP has compensating controls in place. (The IdP would need to assume that the SP has compensating controls.)
      In both cases, the SP gets a stable identifier that enables personalization to be done, either by what the IdP is releasing or what the SP collects later. So, what we're talking about is the name and email attributes that are different between the two ECs.
    - If the SP is telling the IdP Personalized, then that has to imply they really need the person's official email and official name, and maybe they need subject ID and not pairwise ID.
    - For the SP use case, if they get all the info from the IdP, then registration can happen with no other intervention. If they don't get all the information, there are additional steps required (e.g., email verification, institutional authorization/validation) which raises the cost of operation for the SP. The service will be personalized at the end regardless of what attributes they receive from the IdP.
    - Are we trying to overoptimize for a user case where user verification and validation are required, either within the federated authentication flow or as additional actions? One argument is that in Europe, this kind of verification and validation are becoming more generally required. Another argument is that SPs do not actually require this on the larger scale. Group is disagreeing with mostly anecdotal understanding of what's really happening. Christos can speak to research communities, Heather speaking more to scholarly publishing.
    - What we have in Pseudonymous is reasonably clear, but having the justification on the Personalized is still proving tricky. An IdP will not read Personalized info in the Pseudonymous EC, but they also don't really need to. It's a "if you even see this other thing, do this instead" If you're not doing personalized
- Homework - group to consider what and where text should go in Personalized, and should consider how to clarify Pseudonymous to help reduce confusion and ambiguity.