

2022-04-20 R&S 2.0 Notes

Attendees

- [Andrew Morgan](#)
- [Scott Cantor](#)
- [Jiri Pavlik](#)
- [Pål Axelsson](#)
- [Jens Jensen - STFC UKRI](#)
- [Heather Flanagan](#)
- [Alan Buxey](#)
- [Christos Kanellopoulos](#)
- [Martin Stanislav](#)
- [Marcus Hardt](#)

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

Agenda

- Verify WG Consensus items
- Review proposed changes to Anonymous and Pseudonymous ECs
 - Continue review of Pseudonymous at "Deployment Guidance for Service Providers"
- 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

- Pseudonymous Access
 - Significant work on 5.1; brought up some material from Deployment Guidance for IdPs, noted that two of the four attributes may not have values
 - ☐ [Heather Flanagan](#) will update Personalized with appropriate language from Pseudonymous
 - Suggestion that supporting documentation needs to explain how to handle situations like proxy services, IdPs of Last Resort. "Consider a user in the following situation ... Does that mean I am not supporting this EC?"

Moving back to Anonymous

- - Reminder about whether an SP can register more than one EC is an open question, because it is in conflict with 4.1 in Pseudonymous. It's technically possible but not required by policy. Personalized and Pseudonymous cannot be registered together, but Anonymous can work with Pseudonymous. If there's a contractual relationship, then none of this is relevant. This is about non-contractual scenarios, or where blanket contracts are in place. What about the reverse, when an IdP says they will only support one EC, and the SP wants to say "I want Personalized, but can live with Pseudonymous in order not to fail."

Next call:

- - May 4 @ 07:00 (same time slot) - will come back to Anonymous and the question about if/how to indicate whether an SP can indicate support for more than one of this family of ECs