Consultation Response call - 18 June 2020

Attendees

- Fredrik Domeij
- Pål Axelsson (HKR)
- Scott Cantor
- Alan Buxey
- Andrew Morgan
- Niels van Dijk
- Heather Flanagan
- Björn

Consultation Feedback and Responses

- Consultation: Error Handling

Working Specification Document

- https://docs.google.com/document/d/1FQh2SLuxFlF4g9ARvMnXZxOlq4o4NXnNPJnRaC0ic6g/edit

Notes

- The current specification, for one scenario it works very well - when there is no logical or reasonable way for a user to do anything other than wait for the IdP resolves whatever needs to be done (or tells them it can't be resolved).
- For another scenario, however, where research service providers or proxies, there might be a number of ways for a user to continue to use the SP regardless of whether they could use the initial IdP. The best scenario is that the user continues to use their home institution, but if that doesn't work for whatever reason (and it could be any number of reasons), the SPs probably have a number of other ways for the user to log in. For example: The proxy at CERN offers 4 different ways to log in to their services, though the probably allow different qualities of services. We should allow the user the ability to return to some location offered by the SP that supports an alternate way to authenticate (or to something that doesn't require authentication at all).
- Users should not get stuck in holes if not needed. We should also stay away from making authZ decisions on behalf of the SP. If we support a fallback URL, the IdP can present better information to the user as informed by the SP.
- This is not currently how any other protocol works. Anything involving callback URLs mean you have to handle callback redirectors (would require intelligence on the IdP side to watch for this). Maybe we could use an SP errorURL? If you do want the experience of multiple options for the user, then offer a link that the user can click on to report the error to the IdP.
- We could pass the same transaction context back to the SP in real-time to support of the above.

Consensus: keep the protocol simple for now. If we see in a year a strong need for extending, we will do that. What we have will not preclude those potential future additions. Explain in the text a bit more about what the SP can do (Fredrik has already added this to the text)