Kick-off call - 13 February 2020

Attendees:

Fredrik Domeij, Pål Axelsson, Alan Buxey, Andrew Morgan, Björn Mattsson, Shannon Roddy, Scott Cantor

Agenda:

1. Is the scope of work sufficiently clear?
2. Should this be expanded beyond SAML?
3. Administrivia: Thoughts on Chairs? Group name? Timeline?
4. Action items

Notes

Scope:

There is an errorURL in the specification for SAML that states that IdPs should have a URL with support information for usage. Would like to add more to that, to offer more granularity that will allow the user to have enough information to get to the right solution at the IdP. This would require a dynamic URL, since the answer might change depending on the error.

From the SWAMId perspective, we need to be able to inform users on different error types, and give the right home organization information on how to solve the problem.

- Example: you aren't using MFA, but it's required. Here's where you create an MFA at your institution
- Example: there aren't enough attributes to authorize your use
- Example: Your account does not reach a sufficient level of assurance, here's where you need to go to get appropriately verified

This requires changes on both the IdP and the SP. The exact error in the metadata contains all the information on how the user should proceed.

There's never been any real push to do more, or clarify the use of, errorURL. The idea is that if the IdP puts a tag in place, they will follow a common format with the appropriate information.

This is predicated on the SP having enough information on the different errors that can occur.

Most SPs are likely not going to care, and so will go only to the default URL.

InCommon looks like they will be including an errorURL requirement in the next revision of Baseline Expectations.

This isn't necessarily limited to SAML; none of the technologies have solved this, so we likely won't have any conflicts here.

Next step would be to lay out what the tags/errors need to be, and what the other fields would need to be. This should be done at the level of interfederation; local federations may require something more based on their own requirements. There are also privacy issues to consider (i.e., people want to see important captured and sent, but do not want it in URLs).

We need to be very sensitive to the backchannel model that could be seen as hiding sensitive data.

How can the appropriate information be offered by the IdP if the IdP doesn't know which user is having the error? Can this be handled differently by different IdPs? Can we scope these to purely the error without identifying the user at all?

When do we need to have a reasonable proposal complete? Should we tie this to the next round of Baseline Expectation? It's expected to go out for public comment in March 2020.

Is this something can be handled as a more centralized service by the federation? It could be. Either the individual IdP can host something in their service or CMS, or it could be centrally hosted by the federation. You could also have both, with the federation acting as a fallback.

Administrivia:

Fredrik Domeij willing to step up as Chair
Heather is a liaison to InCommon TAC and Pål is a member to CTAB and can send information in that direction

Action items

- [x] Heather Flanagan to create the mailing list creation - https://lists.refeds.org/sympa/info/error-handling
- [x] Heather Flanagan to create a Slack channel - #errorhandling
- [x] Heather Flanagan Meeting invites (same time, weekly) for 4 meetings - done
- [ ] Heather Flanagan Wiki organization