Error Handling WG Notes - 5 March 2020

Attendees

- Alan Buxey
- Fredrik Domeij
- Pål Axelsson (HKR)
- Scott Cantor
- Andrew Morgan
- Shannon Roddy
- Heather Flanagan

Regrets

- Nicole Roy
- Björn Mattsson

Agenda

Working Document - Use Cases and Errors

1. SAML error states
2. Additional fields (focus on what different information pages the IdP's want to have; the error codes should be mapped one-to-one with that)
3. Next steps

Notes

Working Document - Use Cases and Errors

- See updates to the page

Reviewed proposed criteria for what should be included on the list of errors to be handled

- These are reasonable, as long as we allow for changes if a particular use case requires it

SAML error states (and others we should consider)

- Scott did his review and most SAML error codes are not likely candidates for the first round of work

  - AUTHN_FAILED - There are many circumstances where an IdP will send that status, but it's usually when authentication is misconfigured
- Should also consider a catch-all error code for "GENERIC" circumstances where the IdP itself wants to get involved

Additional fields (focus on what different information pages the IdP's want to have; the error codes should be mapped one-to-one with that)

- What information do we need to pass in the error URL to make it useful? What is the minimal set of information we can define?

  - A transaction identifier - un-encoded (probably) fine; if yes, then URL encoding is not needed
  - A timestamp (EPOCH, 64 bit)
- Note that where they show in the URL indicates whether or not they need to be encoded. If certain tags have to be in the query string, that changes whether they have to be encoded or not.

  - EntityID might be the only value we should have encoded
- See proposed examples in the Working Document

Other considerations

- SWAMID will set up a sample system to demo response pages for the five value types
- Do any of the error states need more information that would help the IdP respond/react more quickly? We still need to be careful not to share information like what attributes are missing, etc., but if there's anything that will allow the IdP to act without having to contact the SP would be good.

  - If IdP should contact SP, signal that?
  - If the SP has non-sensitive information that might be useful, signal that? (e.g., please support R&S)

    - Do these break the guideline for this to be user information?

Next steps

- Next call to discuss any remaining technical requirements, and figure out how to document all this for community consideration; also look at demo system that SWAMID will probably have ready by then