Error Handling WG Notes - 27 February 2020

Attendees

- Fredrik Domeij
- Alan Buxey
- Andrew Morgan
- Nicole Roy
- Scott Cantor
- Heather Flanagan
- Björn Mattsson

Agenda

Working Document - Use Cases and Errors

1. Discuss any additional error states
    a. Criteria: "Do we think that (most) IdP's are willing to write a support page for users for this error?"
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

1. Discuss any additional error states
    a. Criteria: "Do we think that (most) IdP's are willing to write a support page for users for this error?"
    b. "attribute value too large" and "bad attribute value" and various of the SAML status error codes might be useful
        i. Bad attribute value: if an SP is using some of the new attributes, but those attributes (e.g., subjectID) seem to be in conflict with other data in the system (two identical subject identifiers for separate users)
        ii. What on the list is actionable? What do you want the user to be in the middle of resolving? Note that another perfectly valid action is to simply indicate “We've logged the issue; someone will be in touch [with the IdP]”. Since the SP doesn't know what the IdP will want to do, the SP can't tell the IdP to do any particular thing.
        iii. Perhaps we just need a generic “catch all” case for everything not otherwise covered with only contact information to the IdP? Note that it's only the IdP knows who the right contact is at any given institution.
        iv. What is our benchmark? Options include:
            1. If the error must be something actionable by the user, then we should not include any generic information.
            2. If the IdP has told the SP that the IdP wants the error handled a certain way, then that's what we want to see in the error code; this may not be something the user can act on.
        v. If all the IdPs will respond to a particular condition in a particular way, is that a reasonable response that will fit into this proposal? Will the SPs be happy with the outcome they get in reporting those issues to the IdP? The SP should be the ones driving the SPs satisfaction with the UX in implementing this proposal.
    c. **Consensus: If the common use case for a given error is not something the user can do something about, or is something not related to the specific user, something that can be handled behind the scenes by the technical contacts of the SP/IdP, then it out of scope for this WG.**
        i. bad attribute value and value too large (as discussed on list) are out of scope
        ii. MISSING_ATTRIBUTES, AUTHZ_FAILURE, and REQ_AUTHN_CONTEXT are all in scope. “You are not authorized to access this content. If you think you should be able to access this content, please contact your IdP (using the errorUrl, possible with different url:s for different errors, provided by the IdP in metadata."
        iii. AUTHN_TOO_OLD (probably a FORCE_AUTHN error) might be out of scope; this is more an IdP error than anything the user can do something with other than start over, or at least not likely something that has to do with the user data at the IdP or something the user is doing wrong.
        iv. SCOPE - in practice, the software that understands scope tends to drop and filter out the info, so it's indistinguishable from not receiving it. This will look most like a bad attribute value. Out of scope.
        v. SAML states
            - [ ] Scott Cantor to review the SAML states and report to the list if any of them might be reasonable for us to consider as a common error state
2. Next steps
    a. Next call, 5 March - usual time. Will discuss the Scope error state and Additional Fields
    b. Reminder: Call on 12 March will have the DST insanity where Europe switches before the US