Error Handling WG Notes - 21 May 2020

Attendees

- Heather Flanagan
- Pål Axelsson
- Andrew Morgan
- Scott Cantor
- Fredrik Domeij
- Alan Buxey

Notes

- Consultation feedback review

Comment 1 - disagree with complicating the protocol. If there's a need of the SP to maintain control of the user, suggest the SP open a new window. Note that the user is already blocked, which is why this error protocol exists. We send the user back tot the IdP because the SP cannot do anything further - there is no reasonable way to continue from the SP's perspective.

- Regarding abuse opportunities, we need to worry about open redirects. There's nothing signed here to prevent abuse. That precludes putting the error page with your IdP. You don't want an open redirector off your IdP.
- Scott to take the action to add Proposed additional text to the spec: If the SP prefers to maintain control over the user interface then opening a new window would be the preferred way to handle this.

Comment 2 - the friendly name is under the control of the IdP; if the SP passes that back then the IdP will be well positioned to handle this. If the SP creates a new name, that might create more problems than it solves The alternative would be to put in more language specific to every protocol. We could be more specific with attribute names to include the protocol, and direct away from friendly names. It will be longer names that humans can't read because they will be OIDs. Since this is originally expected to be human readable, there is some conflict about whether using OIDs would actually be better (more precise, less human clear).

- Consensus: Lack of precision is intended to make this protocol agnostic. No change

Comment 3 and 4 - Some attributes are used for authorization, and missing them means you have no authorization. The SP doesn't always know if it's a problem of missing attributes or if the user is actually not authorized (the missing attributes may be intentional). But not all missing attributes will result in authorization failure issues (e.g., authorization is rarely if ever done on name attributes).

- One suggestion - remove AUTHORIZATION_FAILURE entirely
- If we modify the definition for MISSING_ATTRIBUTE and change it to ATTRIBUTE_FAILURE, that could cover all cases
- Maybe replace MISSING_ATTRIBUTE with "identification failure" (or "personalization failure") "authorization failure" and "authentication failure? We still have a fall back if the use case doesn't apply to one of these three.
- Also suggest we reorder the error codes, so it goes in order of "authentication failure" then "authorization failure" then others
- Action: Scott will rename MISSING_ATTRIBUTE to identification failure and we'll discuss further on the next call

Next call: Thursday, 28 May, usual time; will discuss remaining comments. A separate call will be scheduled to discuss responses with the community