Error Handling WG Notes - 20 February 2020

Attendees

- Fredrik Domeij
- Andrew Morgan
- Pål Axelsson
- Scott Cantor
- Nicole Roy
- Heather Flanagan

Agenda

1. Consideration of the proposal from ACAMP - https://bit.ly/2rOYgl1
2. Working Document
3. Review of possible error states
4. Discussion on what other information may be needed

Notes

Consideration of the proposal from ACAMP - https://bit.ly/2rOYgl1

- Best Practice around Error Handling

From ACAMP Notes

Best Practice around Error Handling

Service Providers have needs from authentication, could be any number from, for example, the following:

- A successful authentication
- Specific attributes (e.g. eppn, email, name, affiliation, entitlements)
- Minimal assurance (e.g. RAF Medium, SWAMID Identity Assurance 2)
- MFA authentication (e.g. Refeds MFA, SWAMID Person-Proofed Multi-Factor)
- Step-up authentication (forceAuthn)

In case any of this fail during authentication, Service Providers often have nothing they can do about it, except for asking the user to retry the authentication. There needs to be a way for Service Providers to point the user in the right direction if the authentication is not complete, from the perspective of the Service Provider.

The errorURL is meant to be used for this. The defined expected information that should be presented to the user at the errorURL is however somewhat narrow in regard of this:

https://kantarainitiative.github.io/SAMLprofiles/saml2int.html#_metadata_and_trust_management

[SDP-MD12]

An IdP's metadata MUST include the errorURL attribute on its <md:IDPSSODescriptor> element. The content of the errorURL attribute MUST be an https URL resolving to an HTML page.

The errorURL HTML page should be suitable for referral by SPs if they receive insufficient attributes from the IdP to successfully authenticate or authorize the user's access. The page should provide information targeted at the end user explaining how to contact the operator of the IdP to request addition of the necessary attributes to the assertions.

https://kantarainitiative.github.io/SAMLprofiles/saml2int.html#_web_browser_sso

[SDP-SP12]

If a successful authentication response lacks sufficient or appropriate SAML Attributes (including subject identifiers) for successful SP operation, the SP MUST display a meaningful status message to the user. This message MUST direct the user to appropriate support resources offered by the SP or, alternatively, to the errorURL attribute in an IdP's metadata.

There are many reasons an SP may be unable or choose not to provide service to a user based on an given authentication response. IdPs failing to release the necessary SAML Attributes is the most prevalent interoperability issue encountered in larger, general purpose federations, which is why this scenario is singled out here.

We need a best-practice for the information expected at the errorURL and a way to point users to specific, common, parts of the errorURL.

    - We should not leave errorURL in unless we had more specific language about how to guide people on what to do. The language that's in there now pre-date what was discussed at ACAMP; it was not really modified based on current level of interest.
    - One group in the room advocated using a back-channel protocol for error reporting rather than front-channel. What, if anything, would be gained by that? What do we need to know about that possible path forward?
        - It would (probably) be more complicated to do something via back-channel.
        - You can give a lot more information via a back-channel than via a URL, and that's a privacy concern
    - The things we could point to in the OIDC protocol as comparison points do not seem appropriate comparisons. Would like to have someone more familiar with OAuth and OIDC to chime in on this.
    - Can we focus on what the application can figure out as an error state, that the SP or IdP doesn't actually have to know?
    - What happens if an IdP cannot handle an authN context class, and it just returns that info. Encryption signing errors would be another example. SAML has some ways to handle those errors in the protocol, but it's not for the end-user.
        - It's not a problem if we also include conditions that are captured in the protocol which we have status codes for. Let's carve out a condition for the AuthN context issue, such that if the IdP sends the error, if the SP wants to point the user back to the IdP with that information, they can.

- Syntax of errorURL

Adapted from ACAMP notes

Syntax of errorURL

errorURL is added in the IDPSSODescriptor tag:

<md:IDPSSODescriptor errorURL="https://www.bth.se/login-problems.html">

There is only one errorURL per IdP. The ID could be used as a query-string to the errorURL, or more generic, at TAG in the errorURL can be replaced by any of the ID:s in the definitions above. Examples:

UMU: https://www.servicedesk.umu.se/faq/idp-error.php?error=TAG
KAU: https://www.kau.se/support/idp-error/TAG.html
LIU: https://www.liu.se/idp-error.html#TAG
BTH: https://www.bth.se/login-problems.html

I.e. it is up to the IdP to optionally include the TAG in the errorURL. IdP:s are expected to handle unknown (new) TAG values appropriately. TAG includes only [A-Z0-9_].

For example, if a user has logged in to an SP from KAU and the SP is with missing attributes, it should point the user to the url https://www.kau.se/support/idp-error/MISSING_ATTRIBUTES.html

--

Saml-metadata-2.0-os

errorURL [Optional]

Optional URI attribute that specifies a location to direct a user for problem resolution and additional support related to this role.

--

- MISSING_ATTRIBUTES (could be a scope issue)
- AUTHORIZATION_FAILURE
- AUTHN_TOO_OLD
- REQ_AUTHN_CONTEXT

- Are we trying to distinguish (via TAG or some string) between an errorURL that is appropriate to use for an action, versus just a pointer to a page? Alternatively, we could add a flag to the metadata. We could also add several errorURLs for each type of error..
- How would we make this extensible to support future use cases?
- We are not trying to create an exhaustive set
    - A good possible design goal: do not change more than we have to to make this all work
    - What namespace/schema does errorURL come from? It's part of the core SAML metadata schema. Since errorURL is undefined, we still have room to work. They would just be prefixed.
    - This protocol may require a query string.
    - Consensus - we'll start with what's described in the ACAMP document

Additional fields that will be required

- Transaction ID

- ...

The most common case might be the missing attributes; we do not want to pass back the list of missing attributes, we want to provide a link to “what to do about missing attributes”. In this case, we could be more specific, but it may be of limited value. If there is some generally useful thing to do, though, it will eventually find its way into code.

Possible error states:

- MISSING_ATTRIBUTES
- AUTHORIZATION_FAILURE (e.g., entitlement, assurance)
- REQ_AUTHN_CONTEXT (i.e., requested authentication class issue)
- AUTHN_TOO_OLD (i.e., time sense authentication is too large)
- SCOPE (needs further discussion, detected and filtered by at least Shib SP, not distinguished from MISSING_ATTRIBUTES by the application behind the SP in the proxy case)

Next steps: update Working Document; wrap up possible error states; consider any additional fields that will be required -- focus on what different information pages the IdP:s want to have! the error codes should be mapped one-to-one with that