

Working Document - Use Cases and Errors

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 interederation; 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).

From the [SAML2-INT Spec](#):

[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.

Errors in the OAuth 2 world

<https://www.oauth.com/oauth2-servers/server-side-apps/possible-errors/>

Criteria

Do we think that (most) IdP's are willing to write a support page for users for this error?

Is the underlying problem something related to the user that he or she can do anything about by using generic information provided by the IdP?

Errors not directly related to the user should not be included in the errorUrl use case, they should be logged by the SP and handled by the SP in direct contact with the IdP.

Possible Error States

Replace all (och only first?) occurrences of ERRORURL-tags

Field: ERRORURL_CODE

error state	Typically caught by	Notes
MISSING_ATTRIBUTES	Application	In scope
AUTHENTICATION_FAILURE	Service Provider	In scope (e.g. requested authentication class issue)
AUTHORIZATION_FAILURE	Application	In scope (e.g., entitlement, assurance)
OTHER_ERROR	Application	Last resort error, should probable include contact information to the IdP's "user support"
AUTHN_TOO_OLD		Out of scope for the WG
SCOPE		Out of scope for the WG

Optional Additional Fields

additional field	Syntax	Notes
ERRORURL_TS	Numbers	Seconds since 1970 (Unix epoch seconds since 1970 UTC)
ERRORURL_RP	URL encoded	https%3A%2F%2Fsome-sp.domain.com%2Fshibboleth-sp
ERRORURL_TID	URL encoded	Whatever the SP needs to understand what the IdP is talking about (e.g. some transaction id) – IF_THE_IDP_IS_TO_CONTACT_THE_SP_PLEASE_PROVIDE_THIS
ERRORURL_CTX	URL encoded	Useful context information for the IdP (e.g. Please support R&S) – POSSIBLE_SOME_INFORMATION_USEFUL_FOR_THE_IDP not be meant to be presented to the user

<https://support.umu.se/IdP-support.html>

https://wiki.swamid.se/IdP-support/ERRORURL_CODE

[https://www.kau.se/support/idp-error/ERRORURL_CODE.html?](https://www.kau.se/support/idp-error/ERRORURL_CODE.html?timestamp=ERRORURL_TS&transaction_id=ERRORURL_TID&remote_service_provider_entityid=ERRORURL_RP&extra_information=ERRORURL_INFC)

[timestamp=ERRORURL_TS&transaction_id=ERRORURL_TID&remote_service_provider_entityid=ERRORURL_RP&extra_information=ERRORURL_INFC](https://www.kau.se/support/idp-error/ERRORURL_CODE.html?timestamp=ERRORURL_TS&transaction_id=ERRORURL_TID&remote_service_provider_entityid=ERRORURL_RP&extra_information=ERRORURL_INFC)

https://www.kau.se/support/idp-error/ERRORURL_CODE.html?ts=ERRORURL_TS&tid=ERRORURL_TID&rp=ERRORURL_RP

https://www.servicedesk.umu.se/faq/idp-error.php?error=ERRORURL_CODE×tamp=ERRORURL_TS&transaction_id=ERRORURL_TID