How to configure login error messages for your SP

Introduction

When your online service stands behind a SAML Service Provider, it relies on a remote authentication service to authenticate end users accessing your application. If something goes wrong with the authentication process itself (lost password, Identity Provider down), the user will naturally ask for support at his home institution. On the other hand, if the authentication fails later in the workflow (Identity Provider not releasing required user attributes), it's up to the SP/application to provide the end user with appropriate error messages to help her fix the problem.

Note that this is not an eduGAIN specific issue, but eduGAIN makes problem fixing more complex because IdP and SP will stand in different countries, with possibly different federation organization and different federation rules.

A proper error message if user attributes are missing

That's a fairly common issue these days, because attribute release is not an industrialized process on Identity Providers end and out of the box IdP software will only release a very limited set of user attributes (session identifier and IdP identifier).

Most federated applications require a minimal set of user attributes from the end user's home organization Identity Provider: a user identifier (eduPersonPrincipalName, eduPersonTargetedId), the type of user (eduPersonAffiliation) or an authorization decision (eduPersonEntitlement). If these required attributes are missing in the IdP SAML response, the application/SP should provide the end user with an appropriate error message. The error message should mention:

- what went wrong,
- why,
- provide elements to help the user solve the issue.

A typical error message: **Access to service ABC failed because application is missing user profile informations from your home organization (University EFG) authentication service. These informations are required to perform access control. Missing informations are: attribute X, Y and Z. You should report this issue to your local authentication service admin (idp_admin@home.org).**

What the error message should not mention:

- federations, federated identities or AAI: end users are not aware of these concepts, that's infrastructure matter. All they know about is the target application and their home organization authentication service.
- Identity Provider, Service Provider, WAYF, Discovery Service: again, these are technical concepts the end user is not aware of,
- SAML, Shibboleth, simpleSAMLphp: end user also don't know about protocols and implementations.

Taking the above into account, the wiki page [How_to_configure_Shibboleth_SP_attribute_checker](https://wiki.shibboleth.net/confluence/display/SP_ATTRIBUTE_CHECKER) contains some useful instructions on how a Shibboleth Service Provider can be configured to not only show the user meaningful error message but also provide him an easy way to inform his Identity Provider administrator and ask him to ensure that attributes are released to the particular Service Provider.

Further more the linked page above also suggests to use a tracking image to log all cases of missing attributes in the web server log. This even works for multiple Service Providers and could thus be used by a community to collect and analyze data for "missing-attributes" cases centrally.

Error handling by the SP software

The SP software itself may raise errors if the authentication process fails.

Shibboleth SP provides configuration parameters to customize error pages with your own wording, custom logo, etc. the Shibboleth SPv2 or SPv3 documentation for further details.

Contextual error message by the federated application

In the error message example above, we include references to the Identity Provider name and IdP email contact. These informations can be found in eduGAIN metadata and are not provided by the SP by default. Shibboleth SPv2.5 or newer provides a way to extract this type of informations from eduGAIN metadata and make them available to the federated application.

- Related Shibboleth SPv3 documentation
- Related Shibboleth SPv2 documentation
- Detailed howto (in French)