Error Handling Service

InCommon Federated Error Handling Service

The goal of Federated Error Handling is to provide a better user experience in those situations where an IdP provides an SP with insufficient information (attributes) to make an access control decision. Federated Error Handling makes use of the Error Handling URL in IdP metadata.

The InCommon Federation operates a centralized *Federated Error Handling Service* that SPs can use to generate simple but effective error pages for the end user. The Error Handling Service offers a simplified mechanism for obtaining the `errorURL` value from metadata or delegating the handling of the "missing attribute" error condition if the set of IdPs is a strict subset of InCommon members.

Note that this Error Handling Service is deployed on the same production infrastructure that hosts InCommon metadata and the InCommon Discovery Service. All of these services are available 24x7 with manual failover to a redundant hot spare in the event of an outage.

Using the Service

The InCommon Federated Error Handling Service can be used by SPs in a couple of different ways. In general, if the user arrives at the SP with insufficient attributes, the SP redirects the user to the Error Handling Service with the entity ID of the user's IdP. Depending on other information in the redirect:

1. The Service will display an SP-branded error page to the user, with a link to the public Error Handling URL for the given IdP.
2. The Service will determine the Error Handling URL for the given IdP and return it to the SP for further processing, presumably so that the SP can roll its own error handler.

See examples of each case in the next section.

Requesting the Service

The URL prefix to the Error Handling Service is:

```
https://ds.incommon.org/FEH/sp-error.html...
```

The full URL includes a query string with the following syntax:

Any given request **must** contain exactly one of the `return` or `sp_entityID` parameters in the query string. The `idp_entityID` parameter **should** be included as well, otherwise the result will be completely predictable (and not very useful).

Case 1. If both the `sp_entityID` and `idp_entityID` parameters are included in the query string, the Error Handling Service constructs a simple SP-branded error page from user interface elements in SP metadata. A link to the IdP's Error Handling URL is included in the body of the error page and the user is encouraged to visit this page at the IdP for further instructions.

Example 1: https://ds.incommon.org/FEH/sp-error.html?sp_entityID=https%3A%2F%2Fcilogon.org%2Fshibboleth&idp_entityID=urn%3Amace%3Aincommon%3Aosu.edu

Case 2. If both the `return` and `idp_entityID` parameters are included in the query string, the Error Handling Service will determine the Error Handling URL (`errorURL`) of the given IdP and then redirect the client to the `return` URL with the `errorURL` included in the query string. If the IdP has no `errorURL` in metadata, the client is simply redirected to the `return` URL without any additional information.

Example 2: https://ds.incommon.org/FEH/sp-error.html?return=http%3A%2F%2Fwww.incommon.org%2F%3Ffoo%3Dbar&idp_entityID=urn%3Amace%3Aincommon%3Aosu.edu

Visit the Federated Error Handling (FEH) Service home page to determine the service URLs for arbitrary parameter values.

Service Integration

At the very end of the SAML Web Browser SSO flow, since the user has a security context, the application can enforce whatever access control policy is in effect. How the security context is exposed to the application depends on the SAML software in use. A common technique is to expose user attributes via server variables or HTTP headers. In that case, the application itself checks to see if the required attributes are present. If so, the request is satisfied; otherwise an access control error occurs.

At this point, the application can redirect the user to the Federated Error Handling Service if it can determine the entity ID of the user's IdP. Assuming the IdP entity ID is included as part of the security context (and therefore exposed along with other attributes), the application code can formulate a redirect URL with the required query string (see above).

Alternatively, the web server may be configured to enforce access control rules. In that case, the server is responsible for redirecting the user to the Federated Error Handling Service, but the idea is the same: upon error, redirect the user with the appropriate information in the redirect URL and let the Federated Error Handling Service do the rest.

Shibboleth Notes

In the case of Shibboleth Service Provider software, applications or protected scripts have access to the identity provider's entityID via the `Shib-Identity-Provider` variable/header. Other information in the IdP's metadata, such as the `errorURL`, user interface extensions, and contact information, are not easily accessible except by parsing the metadata directly. The Federated Error Handling Service offers a simplified mechanism for obtaining the `errorURL` value from metadata.

To integrate a Shibboleth SP with the Federated Error Handling Service, follow the error-handling instructions in the Shib wiki carefully.