Preparing an SP for Interfederation

Considerations for exposing a SAML Service Provider to users and institutions registered with *other* Identity Federations via Interfederation arrangements (such as eduGAIN).

Access control

No assumptions should be made about the provenance or quality of identities from federated or interfederated IDPs *based purely on successful authentication at a SAML IDP*. If your service should only be available to certain user groups (e.g. students, faculty or staff at academic institutions) be sure to enforce this via explicit access control configuration based on attributes sent by the SAML IDP.

> Do not assume that anyone/anything that can authenticate at an institutional SAML IDP is necessarily a member in good standing of that institution.

That avoids any surprises with regard to account issuing practices at other institutions or IDPs.

Metadata

Load SAML Metadata that *also* (i..e, in addition to eduID.at member SPs) includes entities known via Interfederation agreements, such as eduGAIN:

> **eduID.at Metadata for Interfederation**
>
> `http://eduid.at/md/aconet-interfed.xml`

As always, **use the provided Metadata Verification Key to make sure the metadata is authentic and hasn't been tampered with**.

For the Shibboleth SP check out the complete configuration examples provided.

Operational aspects

The interfederation-enabled SAML 2.0 Metadata document (see above) is much larger (1-2 orders of magnitude) than the one only containing entities covered by the eduID.at policies. So make sure the machine your SAML SP implementation runs on has sufficient memory (RAM) available. xmldsig-signature validation on these large documents may also take significant CPU resources (relevant when updating metadata every few hours or every day), but adding more CPU cores to a machine will not typically speed up this process significantly as it cannot be parallelised.

The Shibboleth SP software in particular has an issue *only* affecting its *first start*, when no previously downloaded, validated and cached metadata is available locally. The Shibboleth wiki provides some ways of dealing with that (e.g. by adding a configuration snippet that disables systemd's process start timeout). Also manually starting `shibd` before (re-)restarting it via the service manager (systemd or otherwise) should take care of that issue.
Be sure to follow our configuration examples, particularly with regards to the `verifyBackup="false"` setting on the Signature MetadataFilter.

IDP Discovery

In order to log in to a federated service the subject needs to be able to select the IDP they want to log in with/from. The most useful and obvious way to do this is by presenting the subject with a user interface to select/find their organisation by name.

Manually managing lists of Identity Providers users may log in from does not scale, is not sufficiently dynamic (IDPs' names and/or logos may change over time) and may also not provide a proper user experience. It will therefore be necessary to deploy or utilise some kind of IDP discovery service.
(The eduID.at Demo SP currently demonstrates use of 3 different IDP discovery interfaces. A real production service would of course not do this.)

External discovery services

You can always make use of one of the central "fallback" discovery interface provided by ACOnet or Seamless Access.

> Using an external discovery service is *not recommended* as it sends users away from the service (which may be seen as disrupting the access process) and may confuse users due to different designs at the Service Provider, the central IDP Discovery Service and again at the Identity Provider. On the plus side, external discovery services usually implement the relevant specifications and may have performed usability testing of their interfaces which may not be the case (or may be too much work when done properly) for home-grown/ad-hoc implementations.

See Discovery Services for more, including references to Seamless Access.

Prepare for missing attributes from IDPs

Consider handling any access errors due to missing attributes as gracefully as possible. That includes giving precise instructions to the subject on what failed, why and what to do about it. Using information from SAML metadata support or technical contact data for the IDP should be offered, see this example from the eduGAIN Wiki for a demonstration.

Notify ACOnet

To make your Service Provider available to subjects from other interfederated institutions contact ACOnet in order for your entity to become visible to eduGAIN (and from there to other eduGAIN-participating federations and institutions).