Preparing an IDP for Interfederation

Considerations for eduID.at SAML Identity Providers for use with services registered with *other* Identity Federations via Interfederation arrangements (such as eduGAIN).

Identity Provider Best Practices

You will find that nothing here is specific to Interfederation participation, i.e. *all* IDPs in eduID.at should be configured like this.

eduID.at Identity Providers also participating in eduGAIN

(All eduID.at IDPs should participate in eduGAIN.)

`https://eduid.at/entities/idp/edugain`

Rationale

Only by (also) participating in Interfederation will you be able to support your academic constituency in providing them with secured access to the resources they need. For example E-Research or Student Mobility cannot happen without international collaboration and shared, properly managed access to scientific tools or administrative applications. Cf. the FIM4R (Federated Identity Management for Research Collaborations) paper.

Metadata

All IDPs in eduID.at should load SAML Metadata that also includes entities known via Interfederation agreements, such as eduGAIN. This metadata set alone is sufficient for all eduID.at Federation and Interfederation purposes, so can replace any previously used one:

eduID.at Metadata for Interfederation

`https://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.

Make attributes available

Adjust the IDP configuration to lookup and/or generate any missing attributes. You'll find copy/paste-able examples for all of those in our IDP 4 Attribute resolution documentation.

Every eduID.at-registered IDP should be able to produce at least the following attributes:

- Name attributes
  - displayName (`urn:oid:2.16.840.1.113730.3.1.241`)
  - givenName (`urn:oid:2.5.4.42`)
  - sn/surname (`urn:oid:2.5.4.4`)
- Identifiers
  - SAML Subject-ID (`urn:oasis:names:tc:SAML:attribute:subject-id`)
  - SAML Pairwise-ID (`urn:oasis:names:tc:SAML:attribute:pairwise-id`)
  - SAML2 persistent NameID (`urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`)
  - eduPersonPrincipalName (`urn:oid:1.3.6.1.4.1.5923.1.1.1.6`)
  - mail (`urn:oid:0.9.2342.19200300.100.1.3`)
  - European Student Identifier by means of specific `schacPersonalUniqueCode` attribute values, where applicable (tertiary education students)
- Authorization / Org data
  - eduPersonScopedAffiliation (`urn:oid:1.3.6.1.4.1.5923.1.1.1.9`)
  - eduPersonEntitlement (`urn:oid:1.3.6.1.4.1.5923.1.1.1.7`)
  - schacHomeOrganization (`urn:oid:1.3.6.1.4.1.25178.1.2.9`)

Attribute release

Extend your existing IDP attribute release configuration to make use of Service Categories, to enable scalable *and* controlled attribute release.

The use of the provided Service Categories to automate attribute release as much as possible is **recommended for all eduID.at IDPs**, especially those also participating in eduGAIN.

Be sure to test your attribute release rules with the eduGAIN Attribute Release Check!

> There are more useful tests available in our Testing an IDP documentation.

Notify ACOnet

To make your Identity Provider usable with services registered in other federations contact ACOnet in order for your entity to become visible to those services.

If you added support for Service Categories-based attribute release (which is strongly recommended) please also notify ACOnet about which ones you support, so this can be documented in your Identity Provider's SAML Metadata. Signalling the support for a given Service Category allows services relying on attributes defined in such Service Categories to automatically filter which IDPs to make available for login. By only listing IDPs that claim to support a given Service Category chances of successful logins (and hence of a proper user experience) for subjects coming from those Identity Providers are greatly enhanced! Conversely, IDPs *not* announcing support for any of the popular Service Categories (i.e., those giving the Service Providers *no* indication that necessary attributes will be released) might sometimes find themselves unable to access some of these services, even if the IDP would release the needed attributes.