Metadata

ACOnet publishes several SAML 2.0 Metadata documents, some of which are documented below.

Signature Validation required for any Metadata consumption

All use of SAML Metadata published by ACOnet requires verification of the cryptographic signature (xmldsig) on that metadata against the published Metadata Signing Key. Trust in any information contained in SAML Metadata published by ACOnet should **only** be derived from a valid signature with that key, **not** based on the URL the metadata is downloaded from.

Production

Service Providers only providing services to ACOnet participants can use this limited Metadata document, which only contains entities registered with ACOnet (i.e., those accounted for by formal ACOnet Identity Federation members who are bound by the ACOnet Identity Federation Policy):

Entities registered with ACOnet

`https://eduid.at/md/aconet-registered.xml`

Federation members who should use this limited Metadata document:

- Service Providers registering individually with every Identity Federation, such as internationally acting e-resource providers
- Service Providers which (by the "nature" of their service; e.g. target market or legal status) are limited to subjects from eduID.at member institutions.

All other Federation members will want to make use of the Interfederation-enabled Metadata document, which contains all eduID.at member institutions *as well as* any SAML entities known via Interfederation agreements, such as eduGAIN. Those interfederated entities are bound by the policies of their respective Registrars or Home Federations.

Entities registered with ACOnet plus Interfederation Entities

`https://eduid.at/md/aconet-interfed.xml`

Federation members who should use this Metadata document include:

- Service Providers registered with ACOnet also offering their services via Interfederation, as well as
- **All Identity Providers registered with ACOnet**, including but not limited to those participating in Interfederation.
  (Only SPs will be relevant to an IDP and communication with SPs is best managed via attribute release policies, not metadata exclusion.)

Metadata validity and refresh

Currently eduID.at Metadata is being signed daily (or more often) and validity (`validUntil`) is being set to +14 days in the future each time. That means consumers of this metadata will need to refresh (download and evaluate signature) eduID.at metadata *at least* every 14 days, which a correctly configured software should do automatically. (Note that this validity window may be shortened further in the future without prior notice.)

Consumers of eduID.at Metadata, i.e., SAML IDPs and SPs (and potentially SAML IDP Discovery Services) **should refresh eduID.at metadata at least once a day**, but may do so more often. The example Metadata Providers in this documentation are set to a 4-hour refresh (i.e., re-downloading and evaluating the eduID.at SAML metadata 6 times a day – or less often *if* it can be established on the HTTP layer that the metadata hasn't changed), shortening the time it takes for software to learn of new, changed or removed entities.

The example Metadata Filters in this set of documentation are using a maximum validity of 28 days, i.e., software configured that way would reject SAML metadata that (a) does not have any upper limit in its validity, and (b) where validity exceeds 28 days in the future. This allows metadata consumers to protect themselfs from overly large "windows of opportunity".