Metadata Specification

Version 1.0
(05 April 2012)

Metadata Specification

Information about the entities of the Federation is maintained in a signed XML document, called the federation metadata.

Metadata publishing rules

The metadata file is available both at http://metadata.eduid.hu/current/href.xml and https://metadata.eduid.hu/current/href.xml, however the unencrypted method is preferred. The file is stored on a highly available file server.

The metadata file is re-published every *4 hours* or whenever the entity information changes (eg. entities are added or modified). Entities are expected to refresh metadata information regularly, although the `cacheDuration` attribute is currently not in use (for interoperability reasons).

Trust in metadata

The information inside the metadata file must not be trusted after the date specified in the `validUntil` field of the topmost `EntitiesDescriptor` is expired. The expiration time is is set to **7 days** after the instant of the signature.

Verification of the metadata file

The contents of the metadata file must be trusted only if the signature of the Federation Operator can be validated.

The Federation Operator uses a self-signed certificate for signing the metadata file, therefore the signing key must be explicitly trusted. Properties of the signing certificate:

- DN: `C=HU, O=NIIF Institute, OU=eduID Federation Operator, CN=Metadata Signer/emailAddress=aai@niif.hu`
- MD5 fingerprint: `21:8C:BE:B4:D1:D6:12:C4:67:9F:16:FA:93:36:F6:A4`
- SHA1 fingerprint: `FE:AE:0B:E8:FB:59:ED:F7:CB:7F:69:DF:19:4F:8B:6D:C7:F6:96:66`
- Availability: from `Oct 5 08:18:46 2011 GMT` until `Sep 30 08:18:46 2031 GMT`

The certificate used for signing can be downloaded from https://metadata.eduid.hu/href-metadata-signer-2011.crt , which link should lead to a page without certificate warnings with most browsers. It is recommended to request the signing certificate from the Federation Operator by using some other verifiable transport as well (such as PGP-signed email).

Signing procedure

Information about the entities is retrieved from the Resource Registry by using strong server authentication. If the contents of the metadata changes, it is saved to a version control system and the 'diff' is sent to a public mailing list (href-metadata-changes)

The signing operation is done by a PIN-protected hardware token.

Signing key change or revocation

Changes of the signing key/certificate is always negotiated with the technical contacts of all federation entities.

Authenticating peer entities

It is recommended for all entities to use self-signed certificates, however, even if an entity uses a certificate signed by an external CA, it shall not be assumed that peers use any kind of PKI path validation or revocation checking.

Entity certificate change or revocation

An entity should change its signing certificate by allowing a time frame, when both the old and the new certificate is available in the metadata.

If an entity certificate is compromised, the Federation Operator must be notified immediately. The certificate is removed from the metadata and either replaced by a new one or the entity is removed from the metadata file. On such an incident, all technical contacts are notified to do an immediate metadata refresh to shorten the attack window.

Metadata extensions

Extension elements must be either interpreted according to their specification or ignored completely (while they are valid XML).

Non-federation metadata sets

The federation signing engine is able to produce files other than the federation metadata (called metadata sets). These files are available at https://metadata.eduid.hu/current/, all signed with the same credentials as the federation metadata, therefore it is easy to add them as an auxiliary metadata source.

- `href-test.xml`: staging federation metadata. Any federation member may register entities in this set.
- `href-edugain.xml`: entities that are **exported** to eduGAIN confederation. This file is consumed by eduGAIN MDS only. As eduGAIN follows an opt-in policy, only those entities are present in this set, whose administrators explicitly requested to be published in eduGAIN.
- `edugain.xml`: entities that are **imported** from eduGAIN confederation (minus Hungarian entities). If an entity wants to collaborate with eduGAIN entities from other federations, it needs to load this file.
- `<institution>.xml`: institution-specific metadata sets, which are maintained by the administrators of the institution. SPs inside this set are not required to be accepted by the federation, thus they are assumed to be used within the institution only.

Although an entity might appear in multiple sets, the entity information (including the entityID) must be the same across all sets. It is not allowed to register the same entity into multiple institution sets; the federation set must be used instead.

Metadata registration

Entity metadata management is performed by using Resource Registry, no direct editing is supported.

Depending on the access level, the following administrative tasks may be performed:

- *Federation administrators* are entitled to:
    - register new institutions
    - manage *Institutional Administrators*
    - manage Partner SPs
    - add or remove IdPs

        - manage production federation set and eduGAIN export set (see the section about metadata sets above)
- *Institutional Administrators* are entitled to:
    - register new SPs and place them to the institutional metadata and/or staging federation metadata sets
    - manage the SPs of the institution
    - request the inclusion of an SP to the federation metadata or the eduGAIN export from the Federation Operator
    - add or remove SP administrators
    - add or remove Privacy Administrators
    - manage the IdP(s) of the institution
- *SP administrators* are entitled to:
    - manage the SPs, which are assigned to them
- *Privacy Administrators* are entitled to:
    - manage attribute release rules of the IdP of the institution

Accordingly, all partner SP metadata management is performed by the Federation Operator, by the request of the Techical/Administrative Contact of the Partner.