Metadata Registration Practice Statement

Version: 1.0

(27/09/2011)

aai@niif.hu

Common Practices

All IdP, SP and RRA [1] administrators connect via https and authenticate via eduID to the Resource Registry, where the original information gets administrated which is later used for generating the federation metadata.

In addition, before the federation operator publishes metadata dedicated for interfederation, an institution has first to declare that its processes are ready for interfederation. Only then the federation operator will be able to declare that their respective entity is also technically ready to participate in interfederation.

Practices on Identity Provider Registration

An IdP registering to the federation needs to be manually approved by the Members' Board. Such approval requires:

- a completed membership service agreement signed by official representative(s) of the newly participating institution
- elements and attributes to be registered must use a domain name of that institution

Subsequent changes to these elements and attributes do not require re-approval by the federation operator. Only, administrators appointed specifically by that institution can modify the IdP specific information.

Practices on Service Provider Registration

Each SP must be manually approved by an RRA Administrator in order to be registered with the federation. RRA Administrators must be from the institution on whose behalf the SP gets registered.

It is the duty of the RRA Administrator to review and approve all the details provided by the SP administrator. In addition, an RRA Administrator can reject changes or further modify details of an SP before approving it.

After approving the details about a new SP, the user who requested to register it becomes its first SP administrator. An SP administrator can transfer the administration right to further users. Only users with administrator rights for a specific SP are able to modify its elements and attributes. Such changes require re-approval by an RRA Administrator.

Additional Rules for Federation Partner Service Providers

A signed Federation Partner Agreement is required before a Federation Partner SP can register with the federation. Federation Partner SPs are always approved by a Federation Operator.

Practices regarding metadata modifications

In eduID, no metadata gets modified because the federation operator generates it on behalf of all entities.

The source for generating metadata is the Resource Registry. The details of a registering entity are entered manually by providing the necessary information. Alternatively, a wizard will parse existing entity metadata to gather as many details as possible in order to facilitate the registration.

The IdP/SP administrator also has to supply non-technical information like descriptions or support contacts. All technical and non-technical information is stored as decomposed items in a database. To generate federation metadata, information from that database gets composed into SAML metadata format.

All entites in the Resource Registry could be in one or more metadata-sets. Beside the federation metadata there are metadata-sets with generated metadata files for each institution and for edugain.

---

[1] RRA Administrator = Resource Registration Authority Administrator A role assigned to one or more persons to act on behalf of the institution which signed the federation service agreement. An RRA Administrator has to review and approve new and changed SPs belonging to or sponsored by the institution before such an SP gets loaded into federation metadata.