FaaS Toolbox and Basic Usage Workflow

The FaaS toolbox is built using Free/Libre/OpenSource software, with the two main components having been created by the academic community:

- Jagger Federation Registry is web application used for registering SAML IdP and SP metadata;
- pyFF SAML Metadata Appliance – short for *python Federation Feeder* is a simple, yet complete SAML metadata aggregator capable of doing HSM signing.

Federation Operator personnel and administrators of IdPs and SPs can register SAML entities into the federation registry application via a web UI. The web UI enables registration of SAML entities as simple as pasting the entity's metadata in a text box. The application then transforms raw SAML metadata into a rich UI that gives options to add or change a variety of additional data such as: metadata user interface elements, entity categories, etc. In this process, the Federation Operator personnel has the role to overlook and approve the registration (or make changes on behalf of the entity owners, if needed or requested).

After an entity has been registered it can become a member of both the local federation and eduGAIN. The administrator of the IdP/SP needs to add the entity as a "member" of local federation or eduGAIN in the registry application and the federation operator needs to approve it. Once the memebership is approved the entity will appear in the respective generated metadata streams.

The metadata aggregator used within FaaS is configured to consume eduGAIN metadata and registered local federation entities metadata and to produce two metadata streams:

- **Federation upstream** for publishing to eduGAIN. This metadata aggregate contains metadata from registered local federation entities, which in the registry application have chosen to *also* be published to eduGAIN;
- **Federation downstream** for publishing to Federation members. This metadata aggregate contains all of the registered local federation entities, which in federation registry application have chosen to be a member of local federation, and all entities from eduGAIN.

For creating the federation upstream and downstream metadata, the metadata aggregator is run:

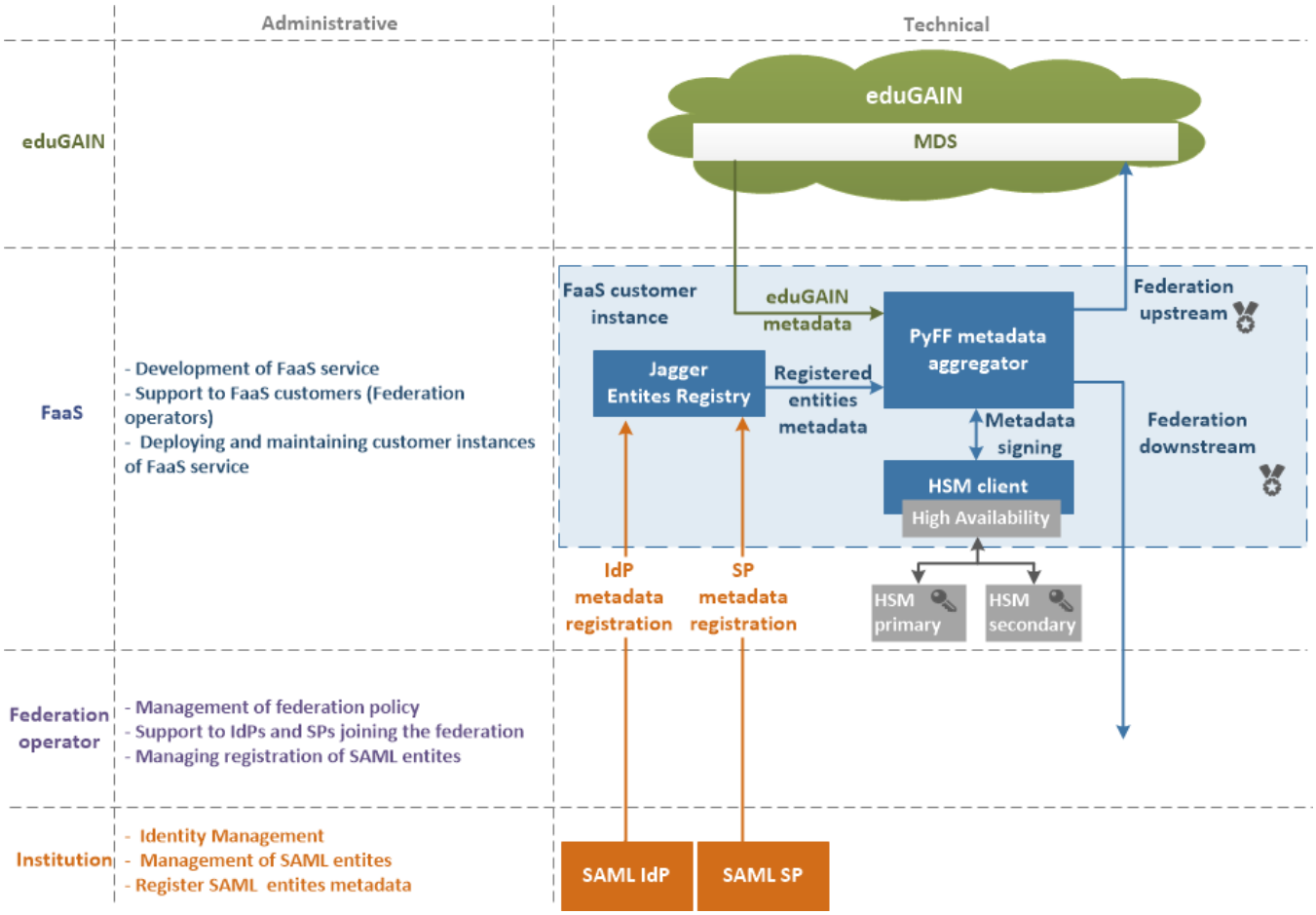
- regularly, once a day around 01:00 UTC, to keep the signed metadata "fresh" even without local changes occuring;
- on any change in registered SAML metadata, where the check for changes is performed every 10 minutes.

The metadata aggregator signs the metadata using an HSM - Hardware Security Module provided by NORDUnet. An HSM is a state of the art technology used for secure signing where the signing key is stored in hardware and not exposed to the operating system or application doing the signing.

There are two HSM partitions for all FaaS instances. Each partition is hosted on a different HSM appliance, located at different locations in Stockholm, Sweden. On each FaaS instance HA (High availability) group is defined and metadata aggregator is set to address its requests to the HA group instead of addressing its requests to any partitions directly. This approach provides:

- High availability - if one HSM appliance fails, the remaining appliance continue to provide the service;
- Load balancing - load spans over all HSM partitions which are members of the HA group.

A high level drawing of the FaaS toolbox architecture and administrative/technical responsibilites of the FaaS team, the Federation Operator and IDP/SP administrators is given in the diagram below.


Administrative
Technical
eduGAIN
eduGAIN
MDS
FaaS
- Development of FaaS service
- Support to FaaS customers (Federation operators)
- Deploying and maintaining customer instances of FaaS service
FaaS customer instance
eduGAIN metadata
PyFF metadata aggregator
Federation upstream
Jagger Entites Registry
Registered entities metadata
Metadata signing
Federation downstream
HSM client
High Availability
HSM primary
HSM secondary
IdP metadata registration
SP metadata registration
Federation operator
- Management of federation policy
- Support to IdPs and SPs joining the federation
- Managing registration of SAML entites
Institution
- Identity Management
- Management of SAML entites
- Register SAML entites metadata
SAML IdP
SAML SP