

FaaS offer

WebSSO Identity federations in research and education are implemented by using the [SAML 2.0 standard](#). In SAML Identity federations, SPs and IdPs need to have information about each other, such as the communication endpoints, certificates and so forth, so that they can exchange authentication and authorization data. This information is described in [SAML metadata](#) (cf. [current specification with errata](#)). In order for SPs and IdPs to exchange their metadata in a scalable, secure and trustworthy manner the Federation Operator's role is to register SP's and IdP's metadata, validate it, aggregate and finally republish it as signed and trusted federation metadata. SPs and IdPs can then consume the federation metadata so that they learn about all of other entities in the federation (and beyond, see below).

Connecting Identity federations to each other is achieved by using the eduGAIN interfederation service. eduGAIN technology involves a "Metadata Distribution Service", which regularly retrieves and aggregates metadata from participating federations and makes this aggregated metadata available to them all again. It is again the Federation Operator's duty to exchange metadata between federation and eduGAIN by:

- publishing the local federation metadata to eduGAIN (federation upstream);
- consuming and republishing eduGAIN metadata to the federation members (federation downstream).

A Federation operator's responsibility is to perform these tasks in a secure and trustworthy manner. If performed manually, this work can be cumbersome and requires a steep learning curve which can present a big barrier for potential Federation operators.

FaaS offers a toolbox for simplified and secure management of Identity Federation metadata and for exchanging metadata with other federations via eduGAIN. The FaaS offer focuses on scalability, a friendly user interface and high security achieved by relying on an [HSM](#) for the protection of cryptographic keys. The toolbox is built using best-of-breed Free/Libre/OpenSource software and is provided as a hosted single tenant service, where each FaaS customer gets its own FaaS instance that can be localized and branded as desired.