

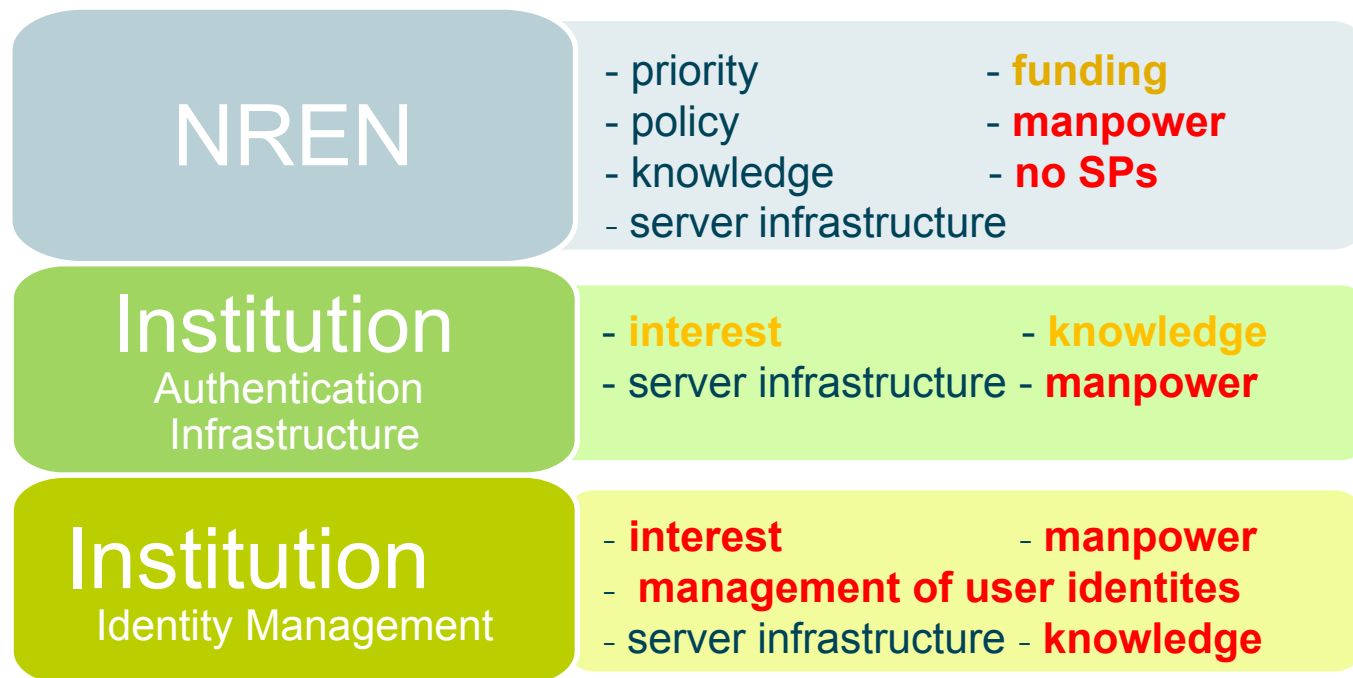
Federation as a Service training FaaS Jagger UI

Belgrade, 22-23th October 2014

Nebojša Ilić, Academic Network of Serbia

Marina Vermezović, Academic Network of Serbia

- Half of GÉANT partners don't have Identity federation



- Concept: Lower the technology barrier for deployment of Identity federation for NRENs
- FaaS provides tools to efficiently manage Identity federation metadata and connect to eduGAIN!

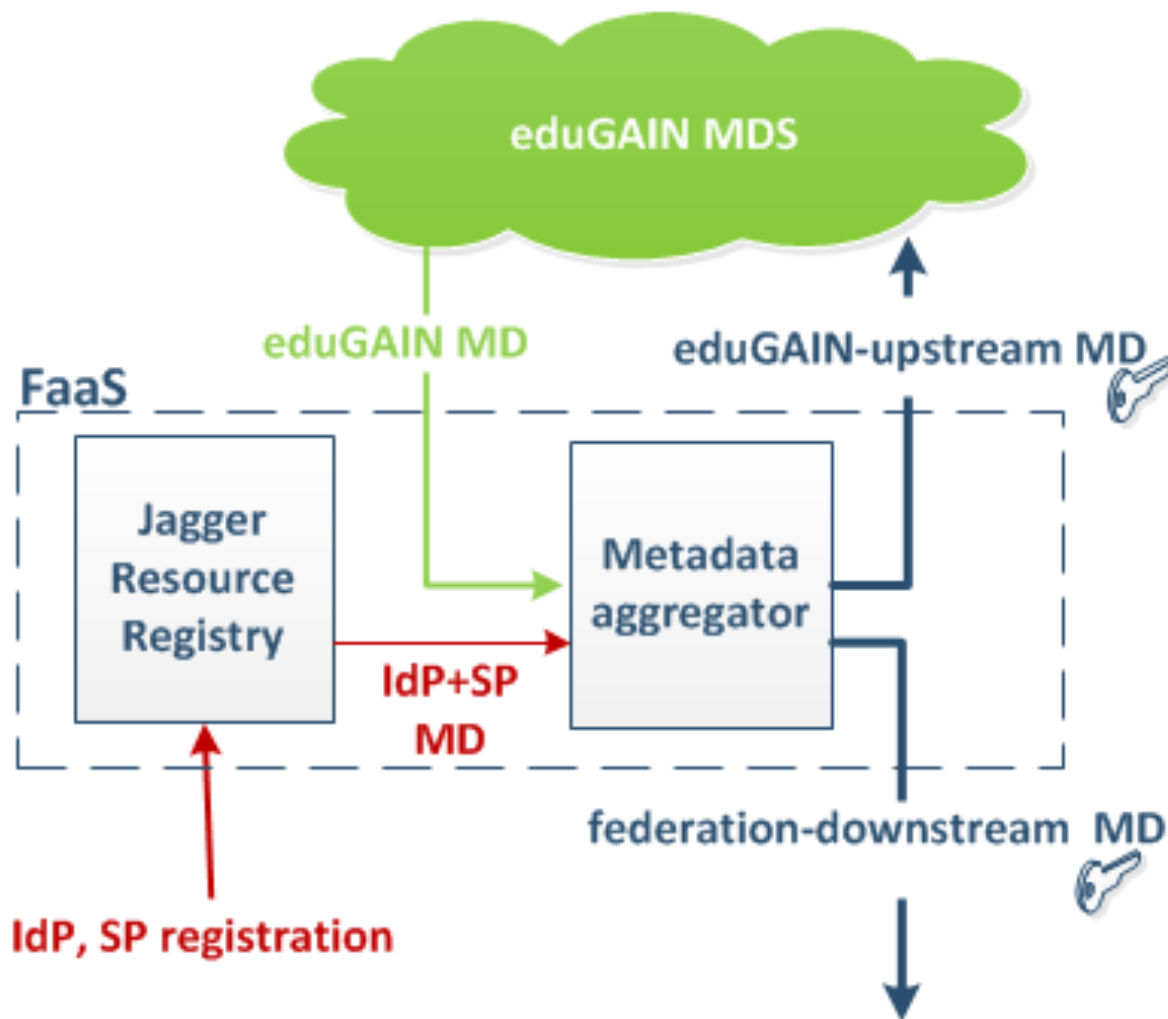
- Enable Federation operators to easier perform tasks of registering entites and publishing metadata (metadata Registry):
 - Registration of IdP and SP entities metadata
 - Validate metadata
 - Enrich entities metadata
 - Aggregate metadata
 - Sign metadata
 - Republishing interfederation metadata in local federation
 - Publish local federation entities that want to interfederate
- Why?
 - Gets too cumbersome to do this manually, use tools for automatization!
 - Important to perform securely and trustworthy

- FaaS is built by using community open source tools
- Each FaaS customer gets its own FaaS instance hosted by GÉANT with following tools:
 - Resource Registry for registering entites metadata – using HEANET Jagger RR tool [1]
 - Metadata Aggregation and Signing – using pyFF [2] and HSM
 - Central Backup Discovery service

[1] <http://jagger.heanet.ie/>

[2] <https://pythonhosted.org/pyFF/>

FaaS – How does it work?



- **eduGAIN-upstream** contains all NREN IdP/SPs that have joined eduGAIN
- **federation-downstream** contains all NREN IdP/SPs that have joined NREN federation + complete eduGAIN metadata
- Metadata aggregator is run:
 - every 15 mins on full hour if there is change in any IdP/SP metadata or membership
 - once a day at 01:00 am

Administrative

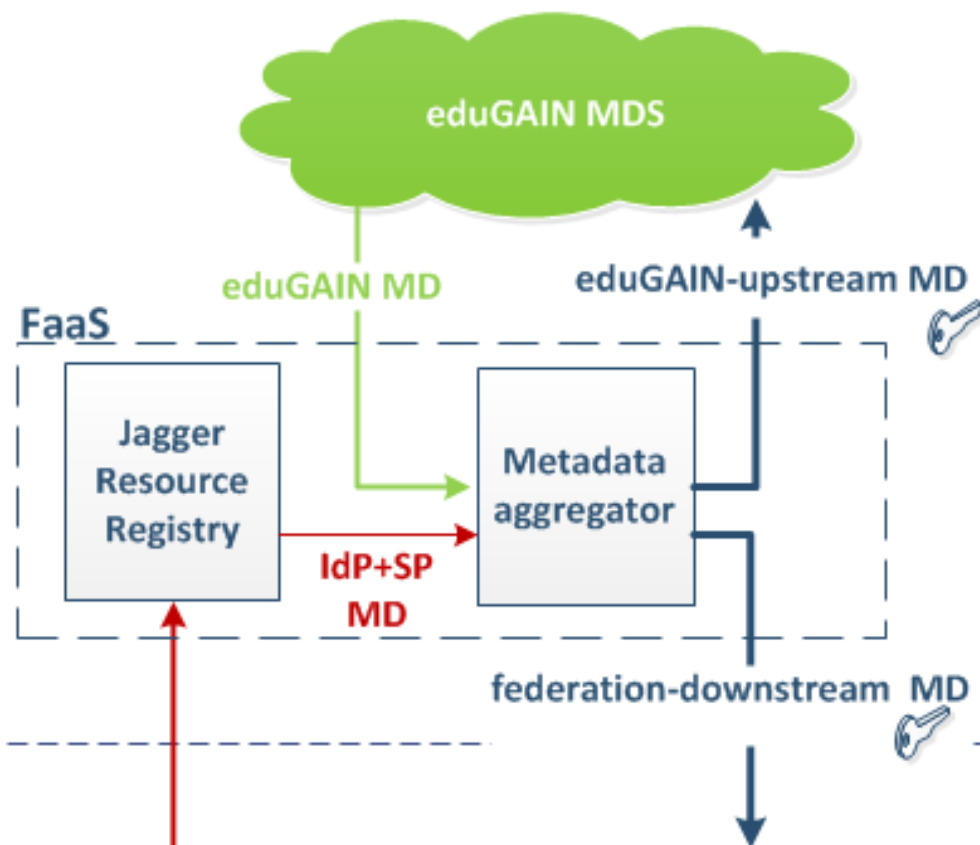
Technical

eduGAIN

- Managing the relationship with the Federation Operators – managing requests and registration for the service, organizing training and support, problem handling

GN3plus FaaS

- Service management and operations – provision and deprovision of the service, maintaining and upgrading of the service instances



Federation operator

- Management of the federation policy
- Managing the relationship with the institutions - managing requests for joining, auditing and approving registration to the federation, providing support and communications
- Managing the registration of the institution and their SAML entities via Resource Registry

IdP, SP registration

Institution

- Register through the Resource Registry
- Management of the SAML entities
- Identity Management

