Federation as a Service training

FaaS offer and User Interface

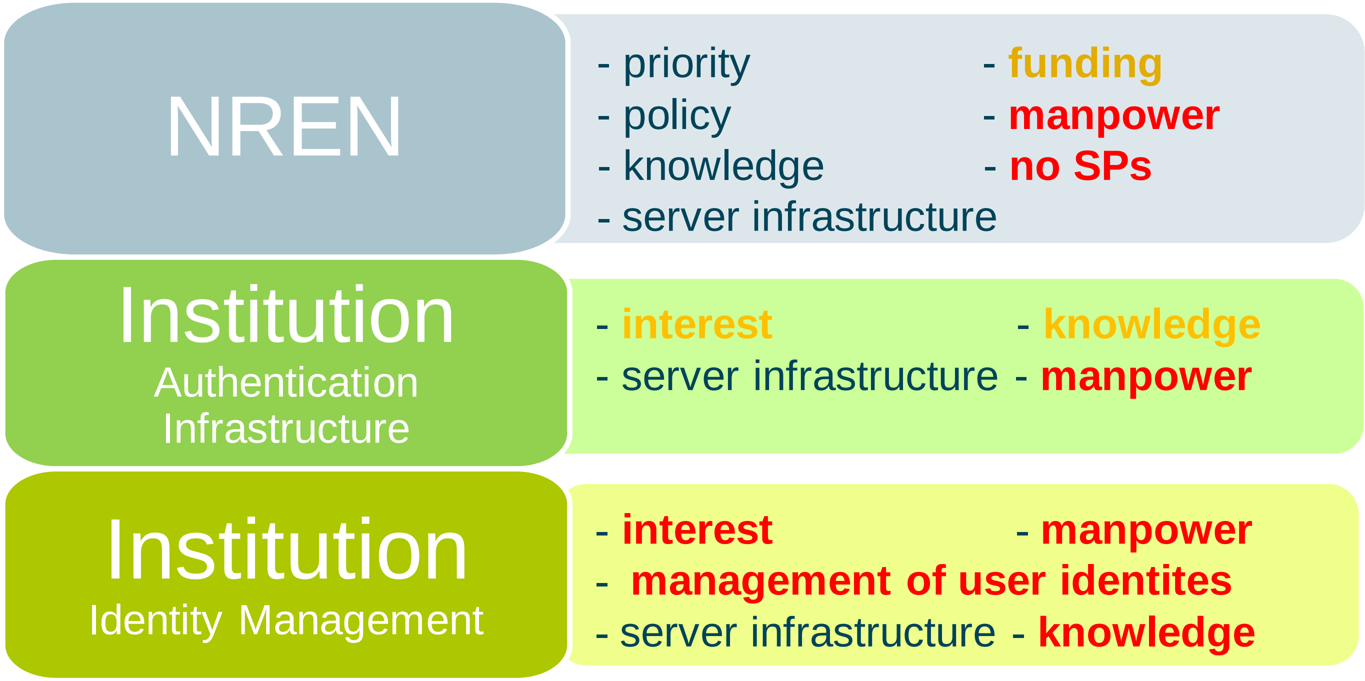
Vienna, 21-22th April 2015

Nebojša Ilić, Academic Network of Serbia Marina
Vermezović, Academic Network of Serbia

Innovation through participation

FaaS Business Case

- Half of GÉANT partners don’t have Identity federation



NREN

- priority
- policy
- knowledge
- server infrastructure
- **funding**
- **manpower**
- **no SPs**

Institution
Authentication Infrastructure

- **interest**
- server infrastructure
- **knowledge**
- **manpower**

Institution
Identity Management

- **interest**
- **manpower**
- **management of user identites**
- server infrastructure
- **knowledge**

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

FaaS Solution

- Enable Federation operators to easier perform tasks of registering entites and publishing federation metadata with 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

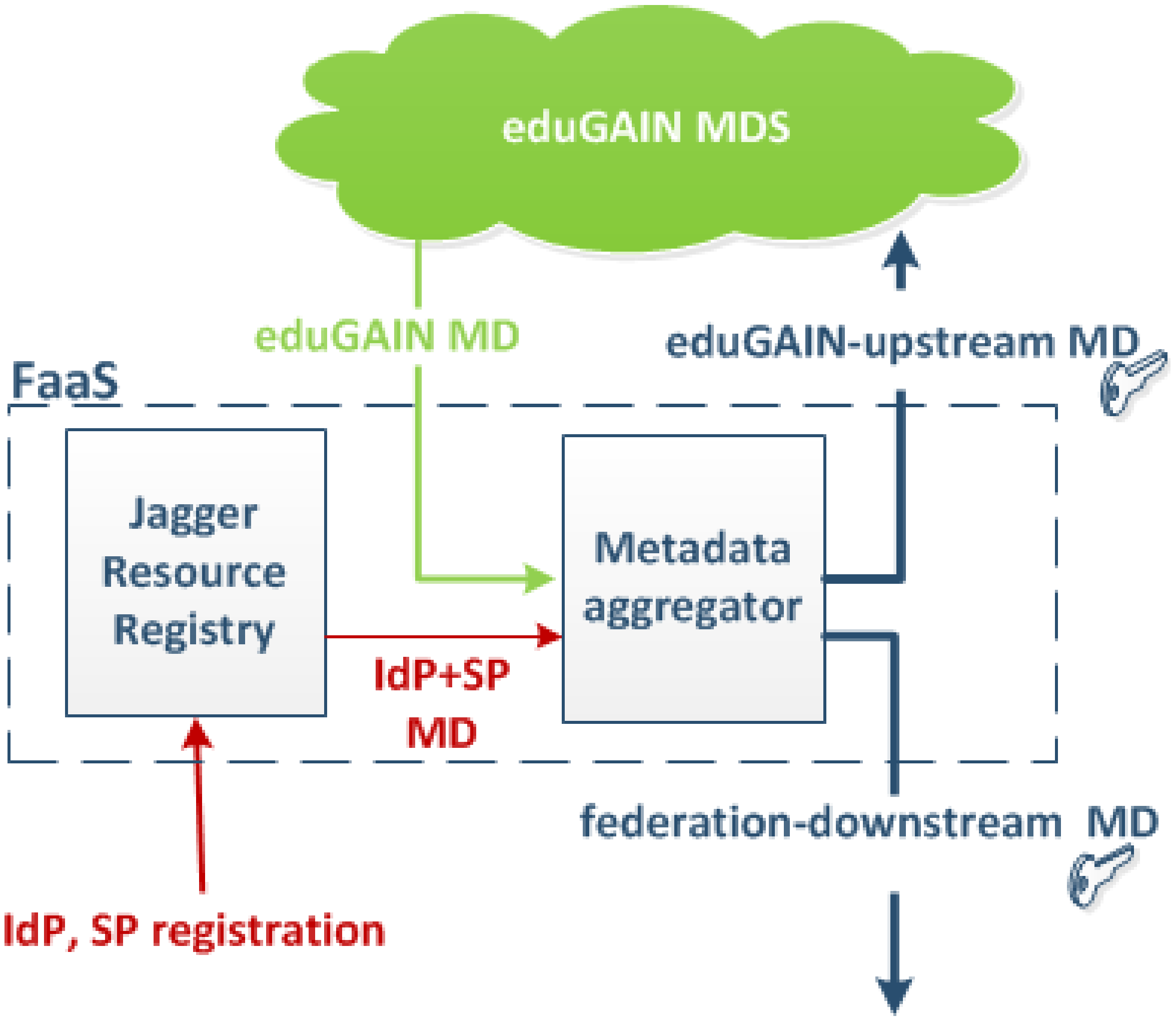
FaaS Software Stack

- FaaS is built by using community open source tools

- Each FaaS customer gets its own FaaS instance hosted and maintained 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

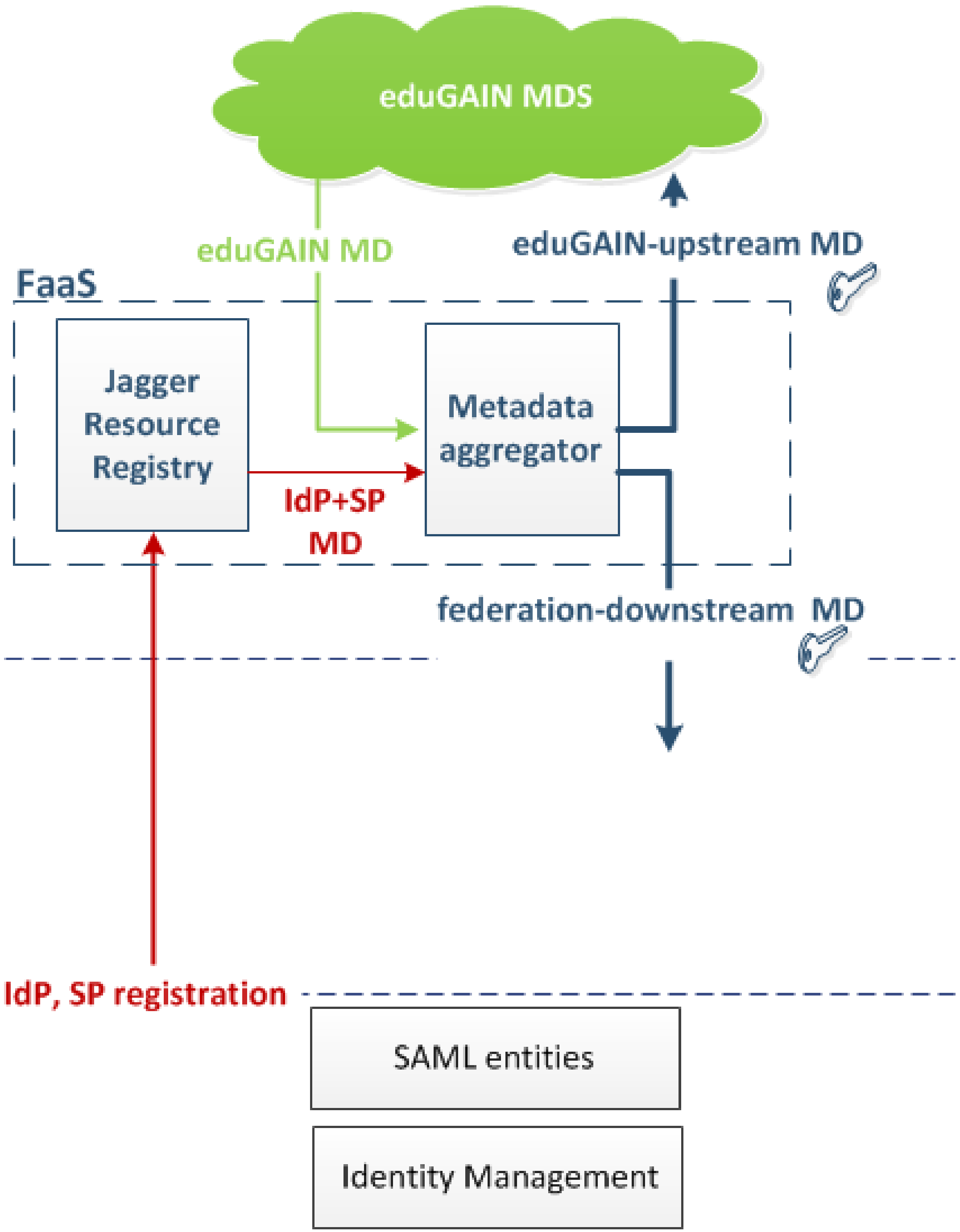
- Metadata aggregator is run:

- every 15 mins on full hour if there is change in any IdP/SP metadata or memership

- once a day at 01:00 am

	Administrative
eduGAIN	
GN3plus FaaS	- Managing the relationship with the Federation Operators – managing requests and registration for the service, organizing training and support, problem handling - 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
Institution	- Register through the Resource Registry - Management of the SAML entities - Identity Management

Technical



FaaS Jagger walktrough

- **DEMO** on the https://test.faas.geant.net
- **EXERCISE 1**: User Interface walkthrough

FaaS Jagger - Users, Roles, managing accounts

- FaaS UI user roles:
  - *Administrator – Federation operator, have full privileges*
  - *Member - SP/IdP owner, have privileges on their own SP/IdP*
  - *Guest – user that have logged in via federated access, but doesn't yet have any rights, can't see anything in the system*

- User can have local account created in the application by the Administrator

- **DEMO** in https://test.faas.geant.net

FaaS Jagger - Users, Roles, managing accounts

- User can login with local account
- If the users IdP is connected to the federation, user can login via federated account:
  - If the user doesn’t exist in local user database, his local account will be created with username == ePPN
  - If user exists in the local user database, then the federated identity will be linked to the local user account. Federated and local accounts are linked based on ePPN and username of local user
- **DEMO** in https://amres.faas.geant.net
- **EXERCISE 2**: Users, Roles and managing accounts

FaaS Jagger - Registering IdP,SP

- In order to join the federation, the IdP/SP owner needs to register entity metadata to the registry

- IdP/SP owner will have the XML metadata which is generated by the IdP/SP software and they simply need to register that metadata in the FaaS Jagger tool

- **DEMO** in https://test.faas.geant.net

- **EXERCISE 3**: Register basic sample IdP and SP

FaaS Jagger – Editing IdP,SP

- After registering an IdP/SP the entity owner can add or change existing metadata
- Adding some stuff to metadata requires approval by the Federation operator, such as adding Entity Categories
- **DEMO** in https://test.faas.geant.net
- **EXERCISE 4**: Edit registered IdP and SP metadata

FaaS Jagger – Federations

- There are two Federations that are registered in the FaaS Jagger:
  - NREN federation – which is your local NREN federation to which all IdPs and SPs will join. Metadata published at:

    https://server-name.faas.geant.net/md/federation-downstream

  - eduGAIN – GÉANT interfederation to which IdPs and SPs that want to interfederate will join. Metadata published at:

    https://server-name.faas.geant.net/md/eduGAIN-upstream

FaaS Jagger – Federations

- Several metadata fields are defined on the Federation level and then they appear in the metadata aggregates

- In the Entities descriptor:
  - *Name* and *publisher*- in the training instances set to base URL of registry application
- In the Entity descriptor:
  - *registrationAuthority* - in the training instances set to base URL of registry application
  - *registrationPolicy* – you can define Registration Policy in the Jagger, and then assing them to the entity

FaaS Jagger – Federations

- **DEMO** in https://test.faas.geant.net
- **EXERCISE 5**: Explore registered federations

FaaS Jagger - Joining NREN federation and eduGAIN

- Just registered IdP/SP is still not member of any federation and is not published in aggregated metadata. To do so, IdP/SP must explicitly join the federation in the FaaS Jagger.
- When IdP/SP have joined the NREN federation, its metadata is published in federation-downstream
- When IdP/SP have joined the eduGAIN its metadata is published in the eduGAIN-upstream
- **DEMO** in https://test.faas.geant.net
- **EXERCISE 6**: Join IdP and SP to NREN federation and to eduGAIN

FaaS Jagger - Management of registered IdP and SP

- Registry application allows certain management actions for the registered IdPs and SPs:
  - Changing the IdP/SP status: Lock/Unlock, Enable/Disable
  - Defining permissions on IdP/SP: read/write/manage permissions
  - Conforming to the Registration Policy

- **DEMO** in https://test.faas.geant.net

- **EXERCISE 7**: Management of registered IdP and SP

FaaS customization

- You can customize your FaaS instance:
  - Add your logo and tab title
  - Add your welcome page
  - Translate to your language
  - Define footer of notification email

- You can choose to have your instance available under your domain and under the name you choose, thus making the FaaS hosted tools have custom tailored look of your Identity federation and your community!

FaaS - how do I get the service ?

- FaaS offered at no additional cost for all GÉANT partners

- Get your own indenpendent instance nothing is shared except the signing key for metadata

- How to talk to us:
  - faas@geant.net – address to reach FaaS team - you should send the request for the service to this address
  - faas-discuss@geant.net – mailing list with all FaaS customers – used for general discussions, questions and notifications from FaaS team

- Show of hands of who is interested for the service ?