

Ubuntunet Identity Federation Training

eduGAIN introduction

Slides v1.4

eduGAIN

the inter-federation service



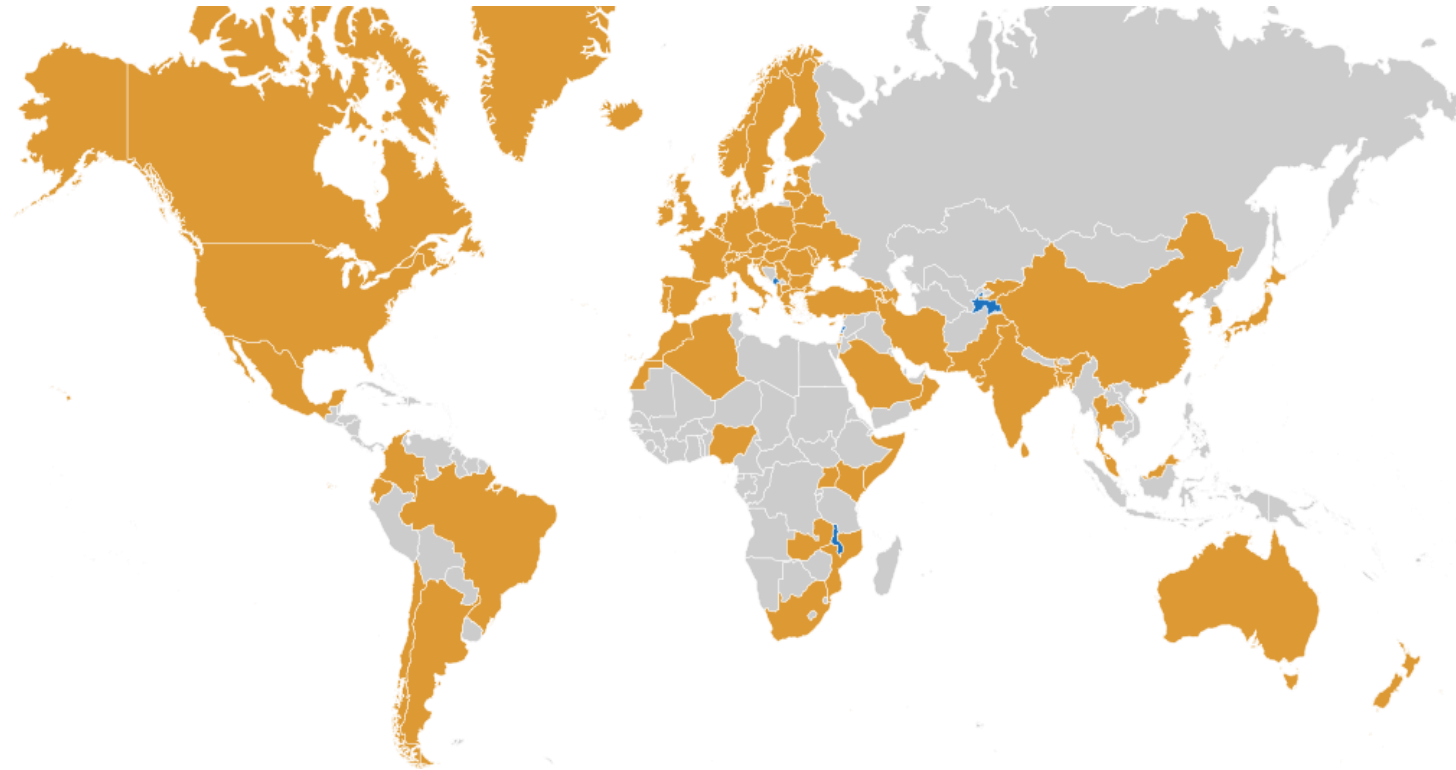
eduGAIN

Enabling secure Single Sign On services to global research and educational resources



Federated identities enable users to access a wide range of services using their account managed by their 'home' institution

- Improves access / Improves security / Reduces management overhead and costs.



January 2024:
* 79 Active Federations
* 6 Candidate Federations
* 9100 entities

Where were we 14 years ago (2010) ?

EduGAIN



- Project by GÉANT
 - Based on SAML
 - It's not a Federation, it's a service to connect Federations
 - www.edugain.org
- 
- A map of Europe with several countries highlighted in green, representing the pre-pilot phase of the EduGAIN project. The highlighted countries are Finland, Germany, Poland, and Switzerland. Croatia and the Czech Republic are also mentioned in the text but not highlighted on the map.
- Pre-pilot phase:
Croatia, Czech Republic, Finland, Germany, Poland and Switzerland

What is eduGAIN?

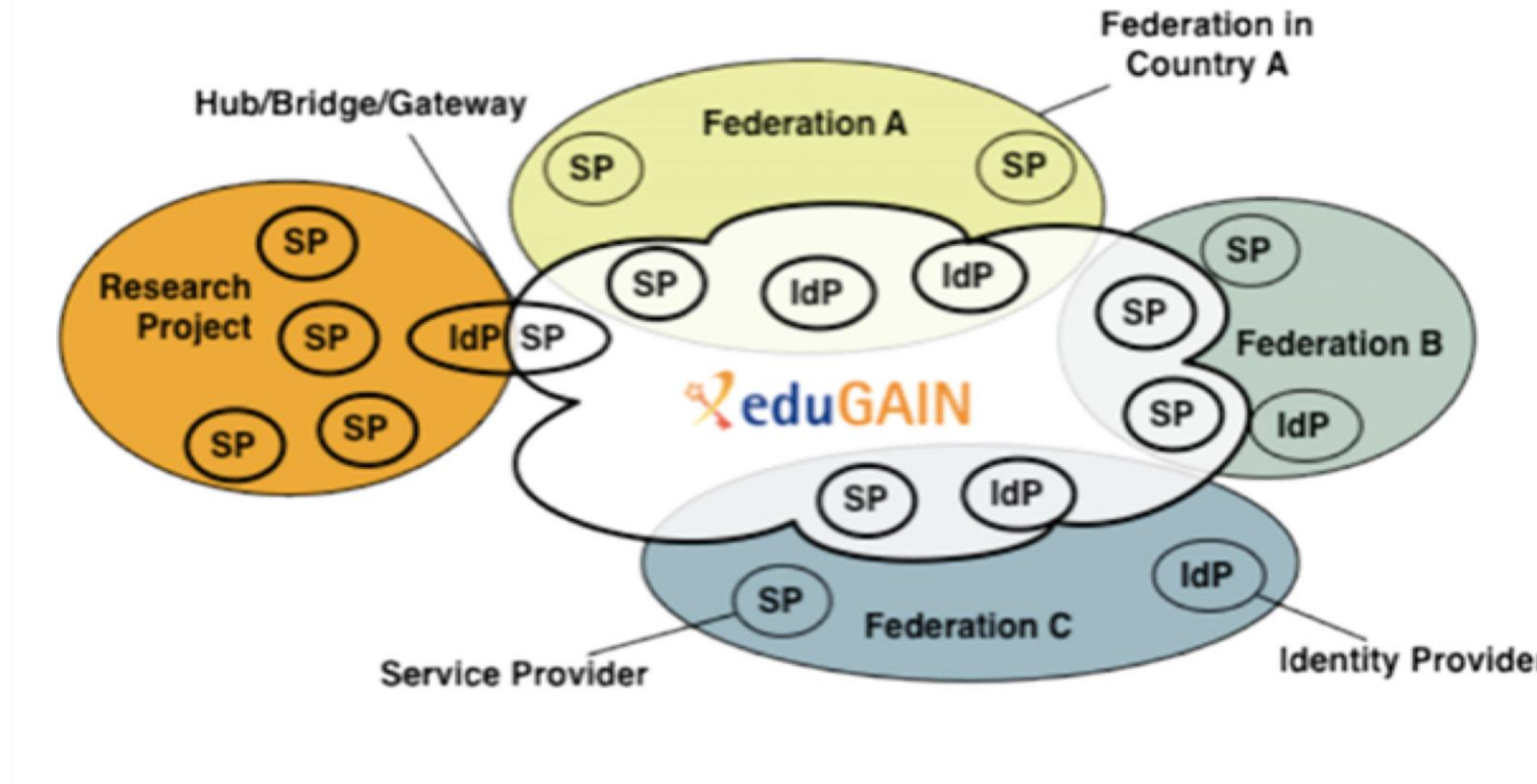


You might have heard that:

- *eduGAIN provides an efficient, flexible way for participating federations, and their affiliated users and services, to **interconnect***
- *The eduGAIN Interfederation service is intended to **enable the trustworthy exchange of information related to identity, authentication and authorisation** between the member federations*
- *eduGAIN **allows students and researchers to securely access a world of educational resources** using a single sign-on*
- *But...*

..... What is it ?

The big picture about eduGAIN



The **eduGAIN inter-federation** service connects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN comprises around 80 participant federations connecting more than 9,000 Identity and Service Providers.

Who benefits from eduGAIN?



Federations

- More services for your users – enables them to access services from different federations.
- Lower administration costs – thanks to easier technical integration.
- Saves time - no need to make bilateral agreements with other federations.
- Trustworthy - secure collaboration and exchange of information.

Service providers

- Grow your audience - offer services to a greater number of users.
- Lower costs per user - your audience grows without increasing the demand for passwords and user support.

Identity providers

- Offer more to your users - enables access to a wider range of services than are available locally or nationally.
- No extra administrative burden - if you are already participating in a federation with Web Single Sign On set up.

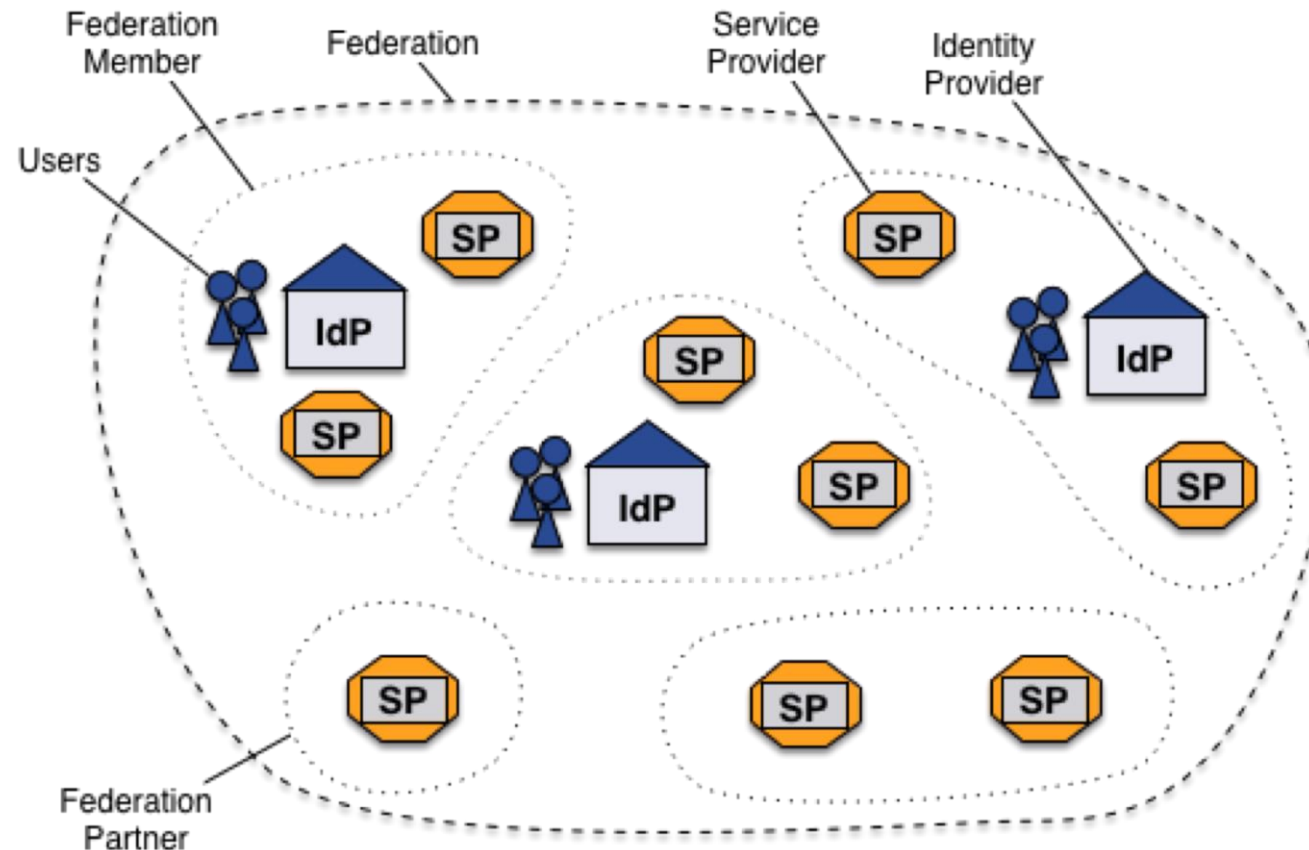
Identity holders (students, researchers, educators, campus administrators)

- Access a wider range of services than are available nationally or locally.
- One digital identity and password for all services connected through eduGAIN.
- eduGAIN is 'invisible' to you so you can access services without extra effort.

Identity Federation

Identity Federation

An identity federation (or just federation) is a collection of organizations that agree to interoperate under a certain rule set. This rule set typically consists of **legal frameworks**, **policies** and **technical profiles** and standards. It provides the necessary **trust** and **security** to exchange home organizations' **identity** information to **access services** within the federation.



Identity Providers, Service Providers and Discovery Service



Identity Provider

The system component that authenticates a user (e.g. with username and passwords) and issues identity assertions on behalf of the user who wants to access a service protected by a Service Provider.

Service Provider

The system component that evaluates identity assertions from an Identity Provider and uses the information from the assertion for controlling access to protected services.

Discovery Service

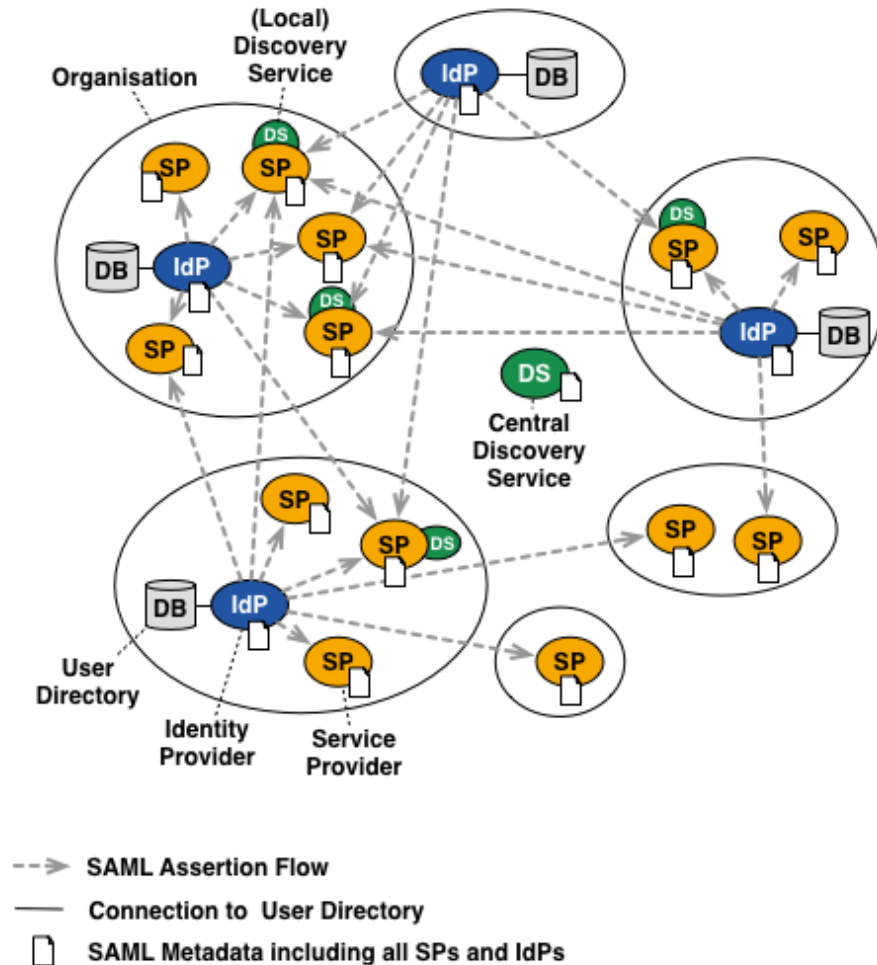
The Discovery Service service, also known as "Where Are You From (WAYF)" service, lets the user choose his home institution from a list and then redirects the user to the login page of the selected institution for authentication.

Full Mesh Federations

Full mesh federations are the most common and straight forward to implement federations because **everything is distributed** and there is **no need for a central component** that has to be protected specifically against failover (that duty is distributed as well).

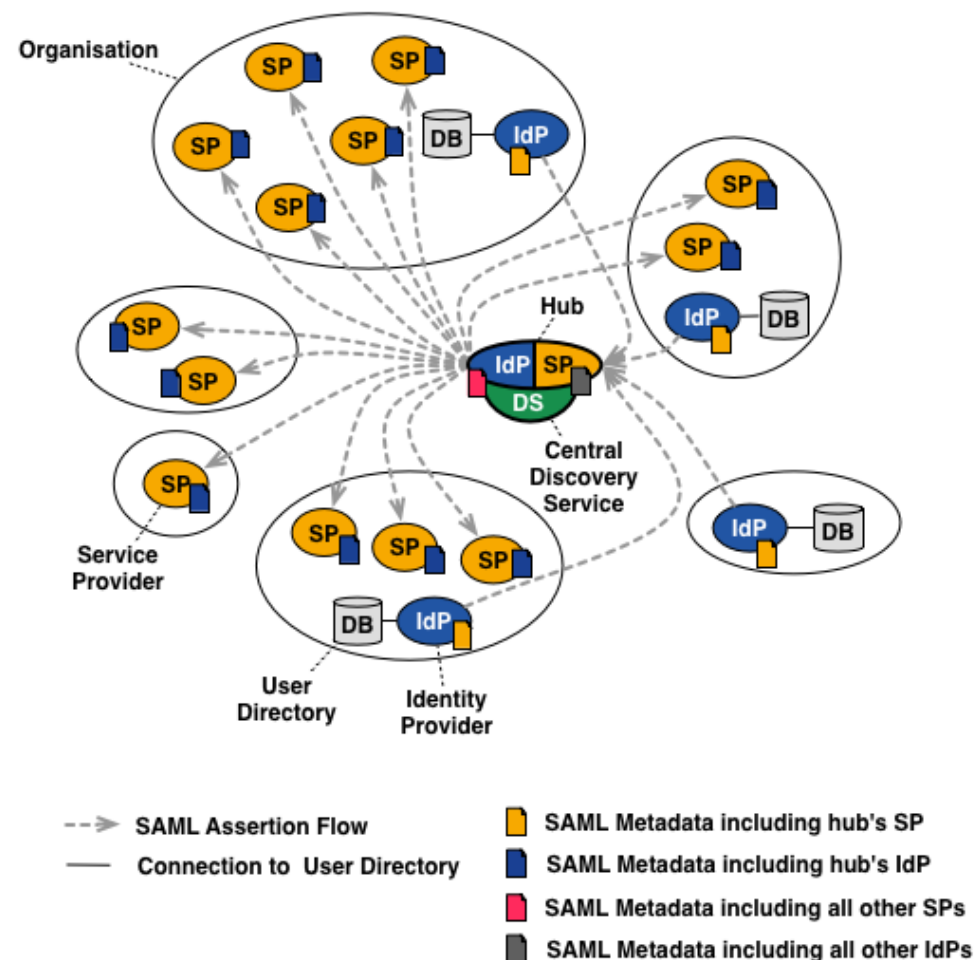
Every organisation in mesh federations (IdP) connected to a local user data **operates their own Identity Provider** base and an arbitrary number of Service Providers (SP).

All these **entities are listed in a centrally distributed SAML metadata file**, which is consumed by all entities.

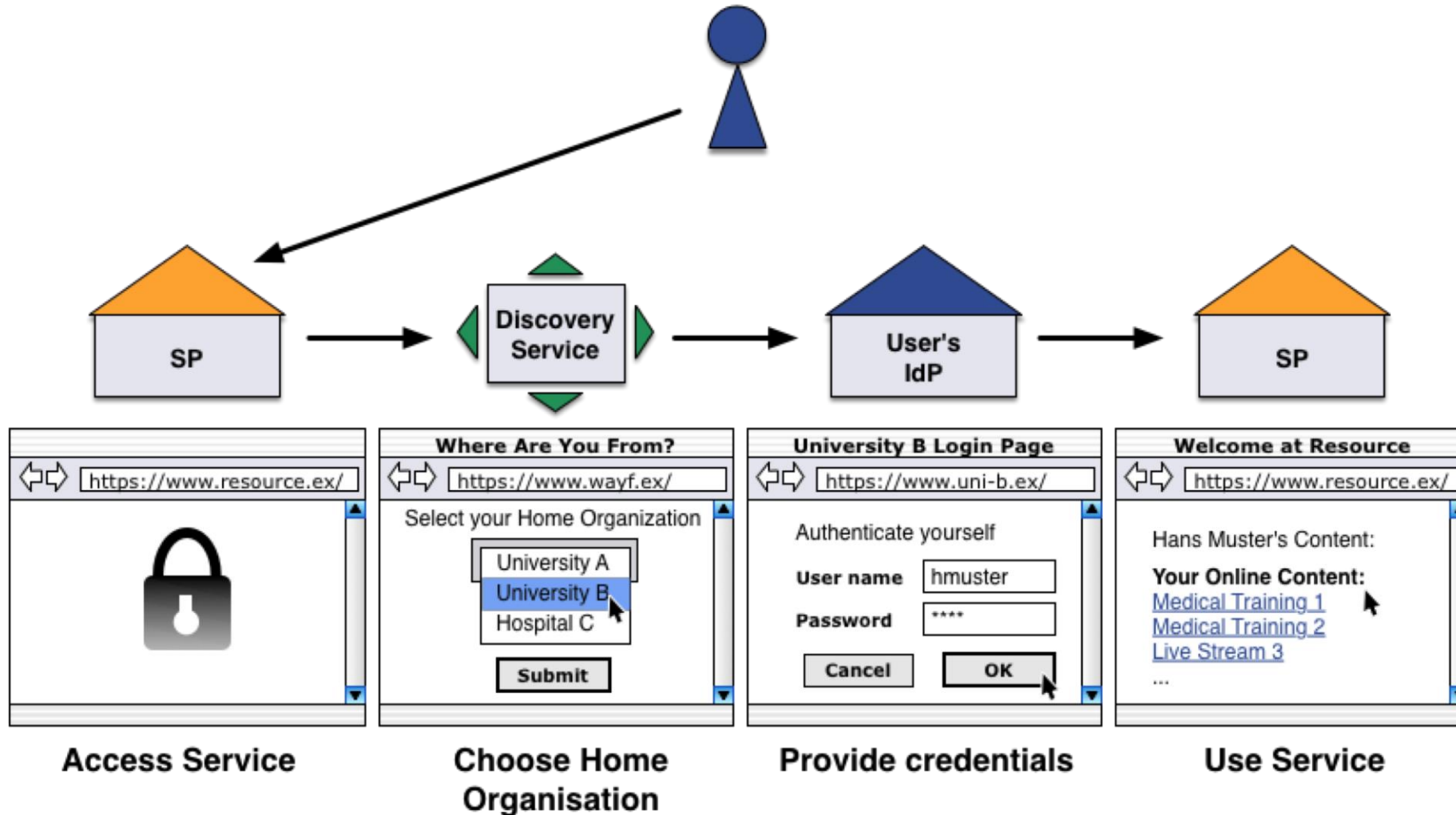


Hub and Spoke Federations

- Hub & Spoke federations with distributed login rely on a central hub or proxy via which all SAML assertions are sent.
- The hub **serves as a Service Provider** versus the Identity Providers and **as an Identity Provider** versus the Service Providers in the federation.
- **Each organisation still operates their own Identity Provider** connected to a local user database but the Identity Provider only needs metadata of the hub.
- Vice versa the **Service Providers only need metadata for the hub.**
- On the hub there is a central Discovery Service for all users.
- Because the hub is a single-point of failure, it has to be carefully secured and protected. ¹¹ | www.geant.org



A simple flow



Entities, metadata and Identity Federation

Entities register metadata

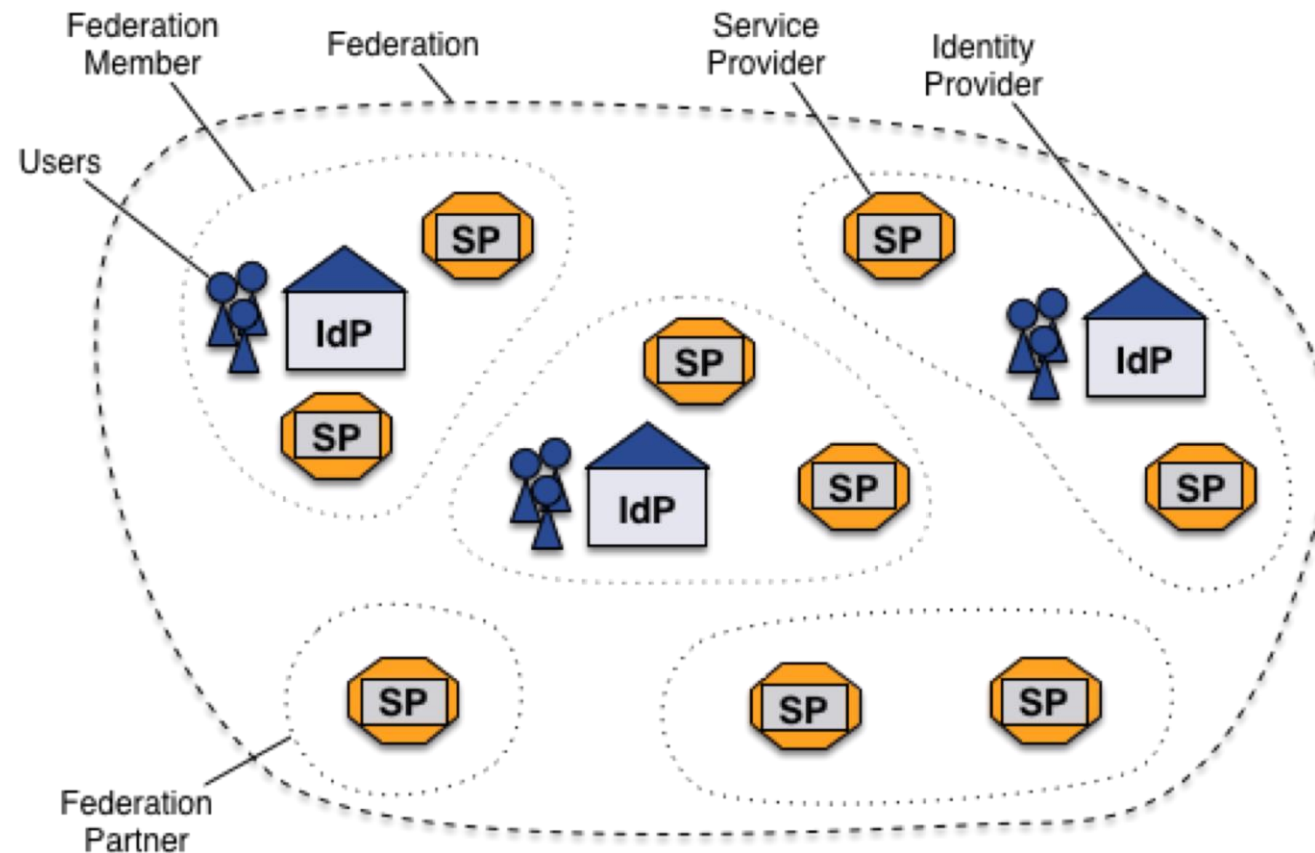
Participating Entities register their metadata into the Federation

The Federation feed

The Federation validates and aggregates all the entities' metadata creating one or more federation feed

Signing & Distribution

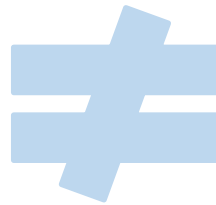
The Federation feed(s) is signed with the Federation key and distributed through an MDS (Metadata Distribution System)



Confederation vs Interfederation

Confederation

often implies common rules for all federations and/or their members, i.e., common rules for every HO/IDP and SP.

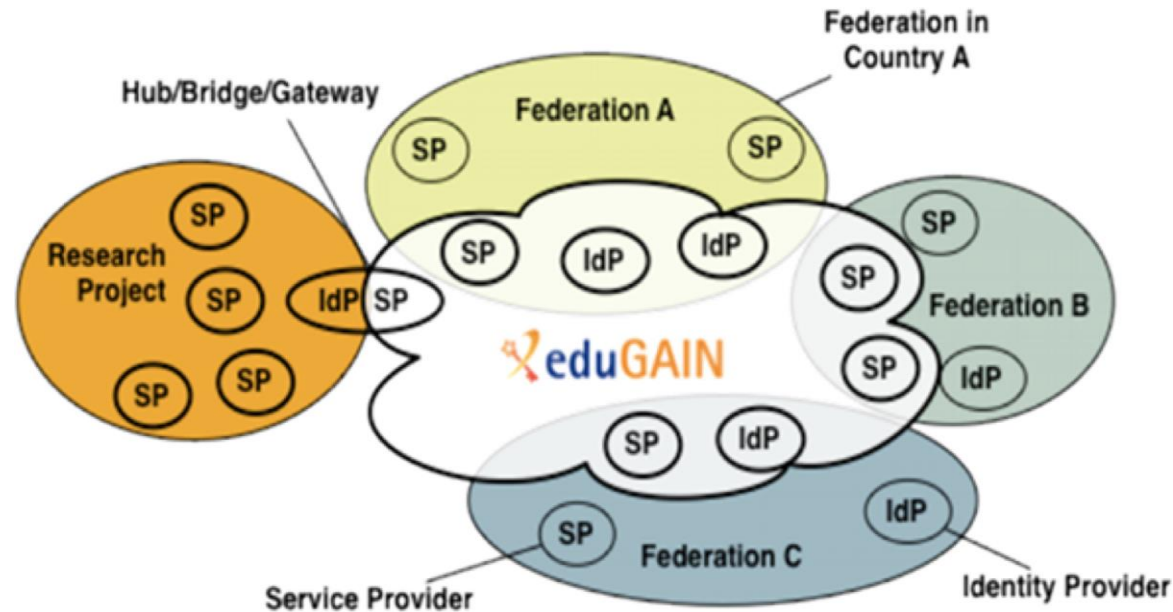


Interfederation

inter-connects federations without establishing One Rule To Bind Them All

Today we refer to eduGAIN as an Interfederation service.

What does eduGAIN do?



eduGAIN mediates the exchange of SAML Metadata describing IDPs and SPs – between participating federations (plus a bit of policy).

eduGAIN MDS, how does it work?

Federations' upstream feed

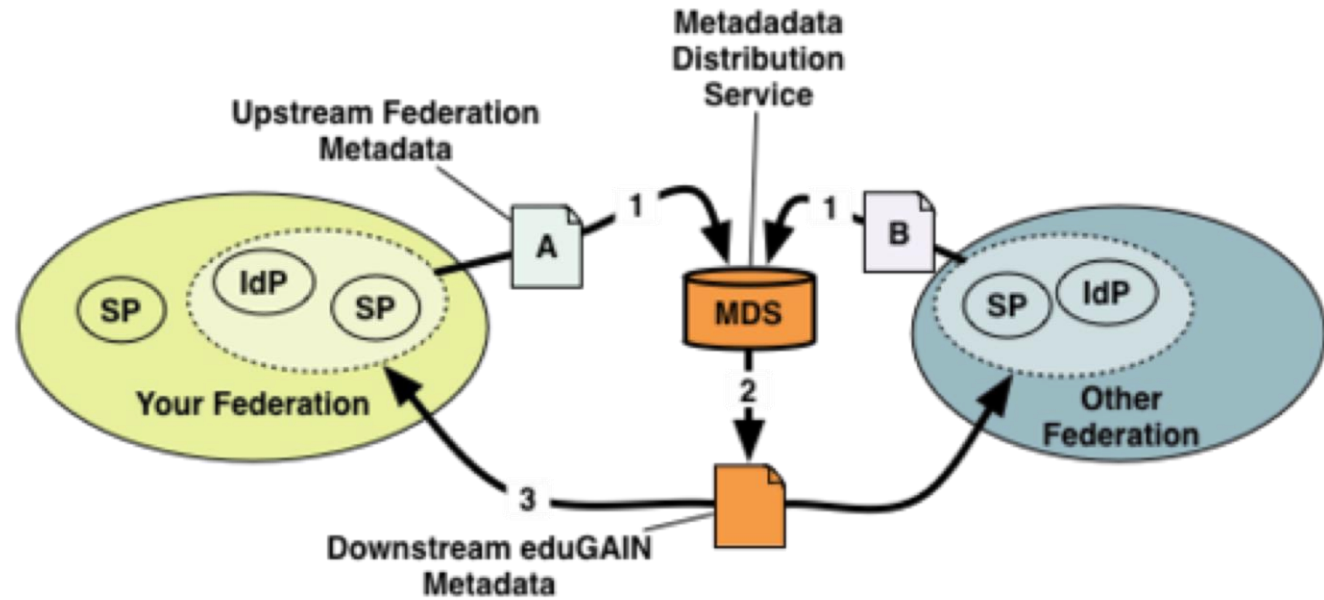
Participating Federations provide a metadata aggregate of entities to be exported to eduGAIN

The eduGAIN feed

Federations' metadata aggregates are picked up, validated and aggregated in the so called eduGAIN feed




Signing & Distribution

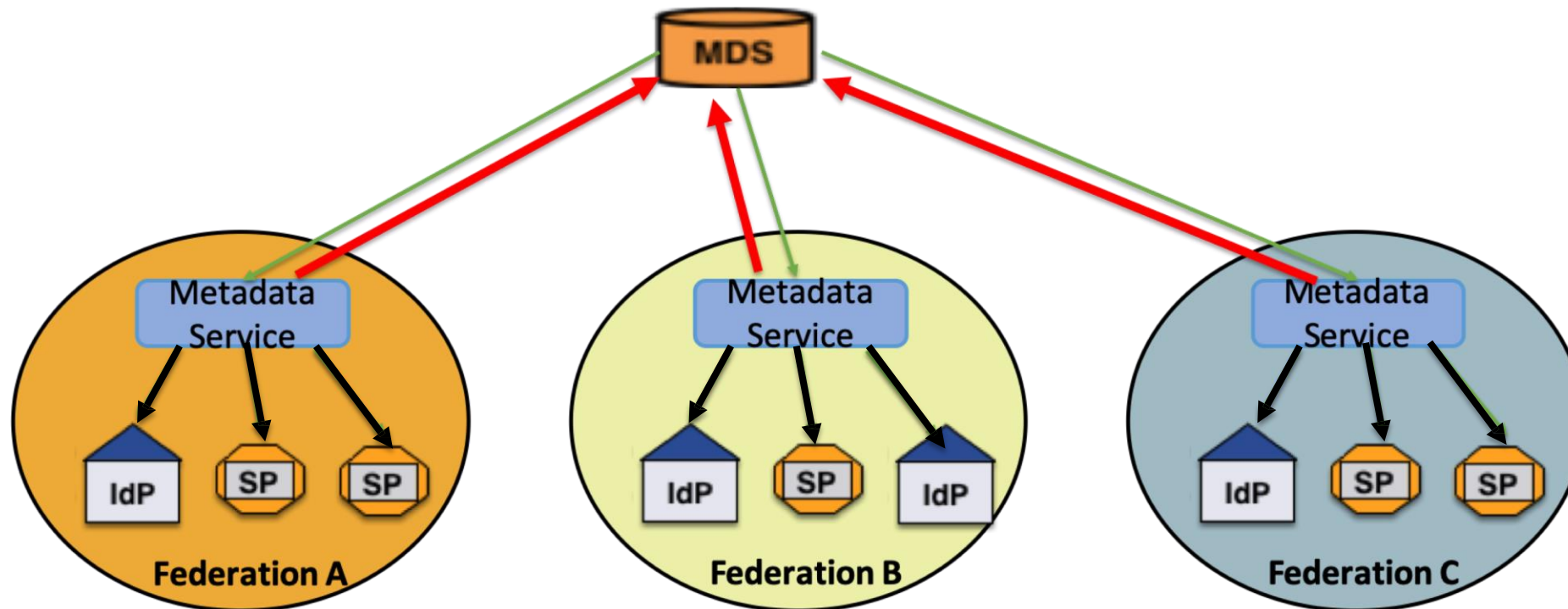
The eduGAIN feed is signed with the eduGAIN key and distributed through the eduGAIN MDS:



<http://mds.edugain.org/edugain-v2.xml>

eduGAIN Metadata flow

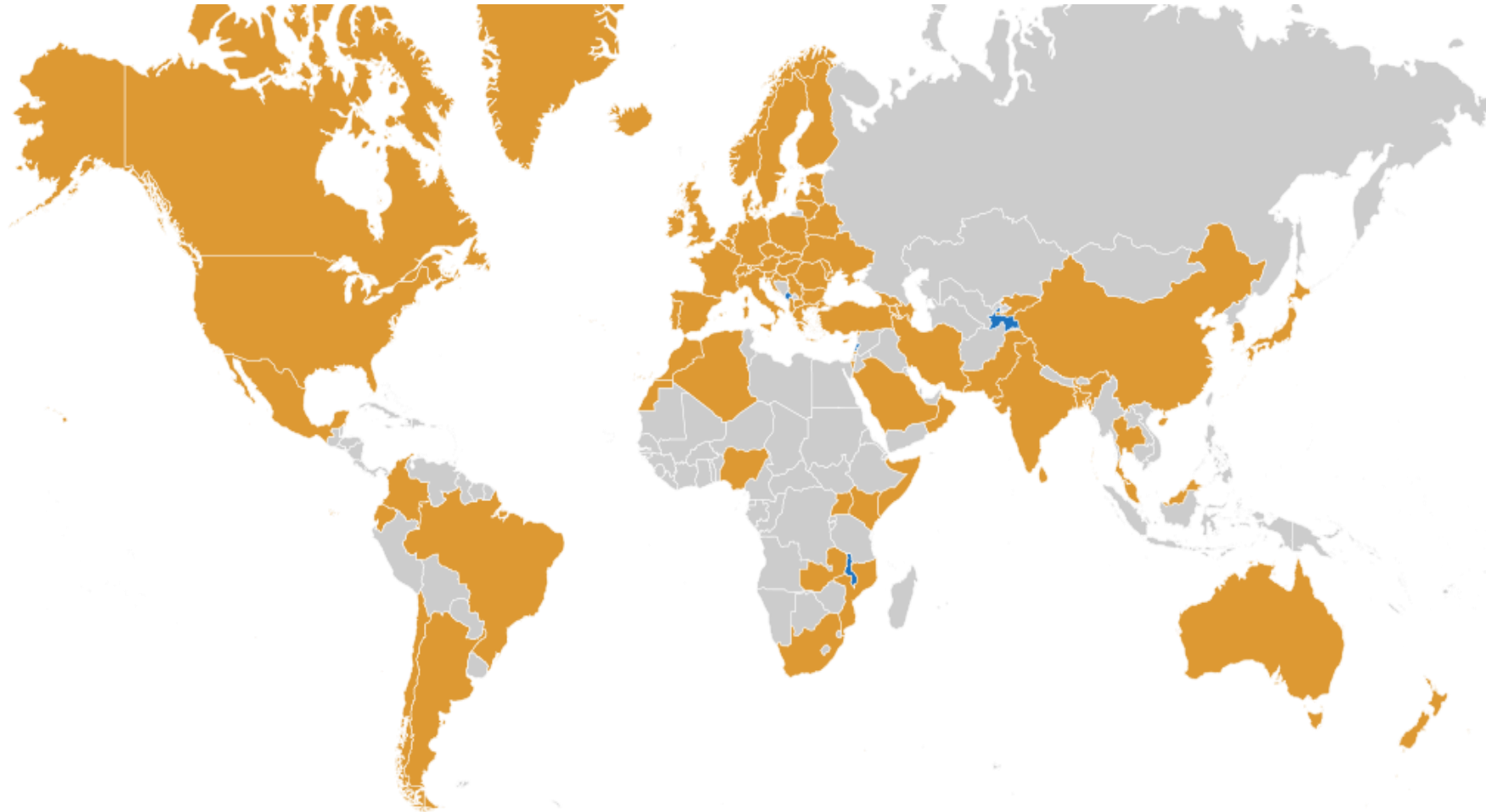
-  Upstream flows produced by Federations for eduGAIN MDS
 -  Downstream flows produced eduGAIN MDS for Federations
 -  Downstream flows produced by Federations for their community
- eduGAIN Metadata Service (MDS)**



A federation Operator is an organization that operates an identity federation.

- **Operation typically includes at minimum:**
 - Collecting, processing and republishing federation metadata
 - Common policies and legal frameworks that all federation participants adhere to
 - Guidelines and deployment instructions to operate services in the federation
 - Helpdesk to assist with deploying services and debugging issues
- **Many federations also offer:**
 - A central Discovery Service/WAYF service
 - A guest Identity Provider for users that don't have accounts at participating organisations
 - A test infrastructure and test service
 - Hosted Identity Providers
 - Workshops and Trainings

eduGAIN Federation Map





To provide an open, innovative and trusted information infrastructure for the European knowledge economy and to the benefit of society worldwide

Thank you

katarina.simonovic@amres.ac.rs

www.geant.org



© GÉANT Association
As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-2019).