eduGAIN

the inter-federation service
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.

March 2021:
- 71 Active Federations
- 7 Candidate Federations
- 7417 entities
Where were we 10 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](http://www.edugain.org)
  - Pre-pilot phase: Croatia, Czech Republic, Finland, Germany, Poland and Switzerland
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 over 70 participant federations connecting more than 7,000 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. |
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 straightforward 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.
The size of the MD aggregate (centrally distributed MD aggregate file) to manage eduGAIN is getting increasingly large and unpractical to handle.

A new protocol (MDQ) has been developed to implement Dynamic Metadata Query to avoid the need for storing the whole chunk of eduGAIN MD in memory or on file.

MDQ protocol is a lightweight REST-like, HTTP-based protocol for requesting and providing MD.

MQD also relies on EntityID.
- EntityID becomes part of the request URL.
- An example implementation of MDQ server is PyFF (pyff.io) - implementing an MDX MDQ protocol server.
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.
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.
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:

[https://mds.edugain.org/edugain-v1.xml](https://mds.edugain.org/edugain-v1.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)**
Role of Federation Operators

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 Baseline Expectations

- To improve the interoperation among entities, the eduGAIN community is currently working in the definition of Baseline Expectations for eduGAIN, classifying them in three groups:
  - BE for Identity Providers
  - BE for Service Providers
  - BE for Federation Operators

- [https://wiki.refeds.org/display/GROUPS/Baseline+Expectations+Working+Group](https://wiki.refeds.org/display/GROUPS/Baseline+Expectations+Working+Group)

- The outcome of the work of the Baseline Expectations working group might imply new rules for participating to eduGAIN, or new requirements, aimed at improving the user experience, ensuring interoperability, and improve the overall health of the eduGAIN Metadata
eduGAIN

Technical Operations

Federation as a Service

Support
Security Incident Response

Development

KPIs
99% Metadata Service Availability
+15% Membership

2019
February
March
April
May
June

eduGAIN All-hands meeting - Rome
eduGAIN Steering Group meeting
OpenID Foundation workshop (IIW)
TNC19

eduGAIN Metadata New validation service
eduGAIN policy and operation documents
eduGAIN certificate renewal
eduGAIN TRUSTful certificate deployment

70 Identity Federations
4044 Identity Providers
3116 Service Providers

GÉANT PMC
REFEDS Production Federation Map
eduGAIN Federation Map

- **Participants**
- **Voting-only**
- **Candidate**
GLAD webinar on Attribute Release

“Successful Attribute Release and eduGAIN IdP Health Check” – life after the webinar

https://learning.geant.org
Examples of benefits of eduGAIN for Research Communities:

• Examples of Research and User communities who benefit from eduGAIN
  • The LIGO/Virgo international gravitational waves research community implemented an AAI pilot on eduGAIN within the AARC project providing a central IdP/SP proxy connecting their IdPs to the services.
    • This would allow LSC and Virgo members to use their institutional credentials to access LSC resources directly.
    • https://wiki.geant.org/display/AARC/LSC+Ligo+Scientific+Collaboration
  • The GARR Cloud dashboard made available to eduGAIN users by configuring the Openstack Keystone Identity service as an eduGAIN service provider
  • CILogon: accessing X.509 based e-infrastructures using eduGAIN
LIGO-Virgo
CILogon (https://cilogon.org) enables federated access to Cyberinfrastructure (CI). CILogon provides a gateway from campus SAML authentication to X.509.
Thank you

mario.reale@geant.org

www.geant.org