ΤΑΥΤΟΠΟΊΗΣΗ ΚΑΙ ΕΞΟΥΣΙΟΔΌΤΗΣΗ ΓΙΑ ΤΗ ΔΙΕΘΝΉ ΕΡΕΥΝΗΤΙΚΉ ΣΥΝΕΡΓΑΣΊΑ

Νικόλας Λιαμπότης

Federated Identity Management (FIM) for Research

- Access services using **identities from their Home Organizations** when available.
- Secure integration of **guest identity solutions** and **support for stronger authentication** mechanisms when needed.
- **Access** to the various services should be granted **based on the role(s)** the users have in the collaboration.
- Users should have **one persistent identity** across all community services when needed.
- **Ease of use for users and service providers**. The complexity of multiple IdPs/Federations/Attribute Authorities/ - technologies should be hidden.

Initial challenges

Attribute Release	Attribute Aggregation	User Friendliness	SP Friendliness
Persistent Unique Id	Credential translation	Credential Delegation	User Managed Information
Levels of Assurance	Guest users	Step-up AuthN	Best Practices
Community based AuthZ	Non-web-browser	Social & e-Gov IDs	Incident Response

AARC project in a nutshell

- EC-funded project
  - AARC (2015-2017),
  - AARC2 started in Apr 2017 and will end in 2019
- 25 Partners: NRENs, research and e-Infrastructure providers as equal partners
  - Focus on enabling FIM for eScience
- https://aarc-project.eu/

Watch the AARC video to find out more

https://www.youtube.com/watch?v=Xpwb6BNxNW4

What AARC wants to achieve?

Improve adoption of FIM – Promote FIM key aspects, leverage identity providers outside the academic boundaries and deliver training

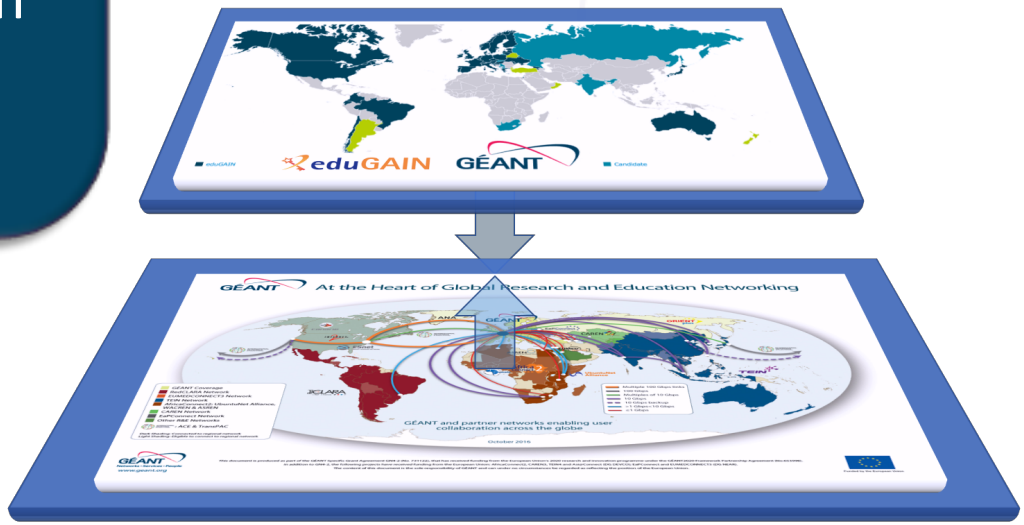
Address eScience requirements – Deliver a blueprint architecture and a number of building blocks to meet eScience requirements.

Offer support for global policies – Work on and sponsor the development of key policy frameworks that aim to add additional 'flavours' to edu

Make results sustainable – Pilot results in production environments and ensure that pilots operations and, security and policy frameworks rest with r/e-infrastructures.

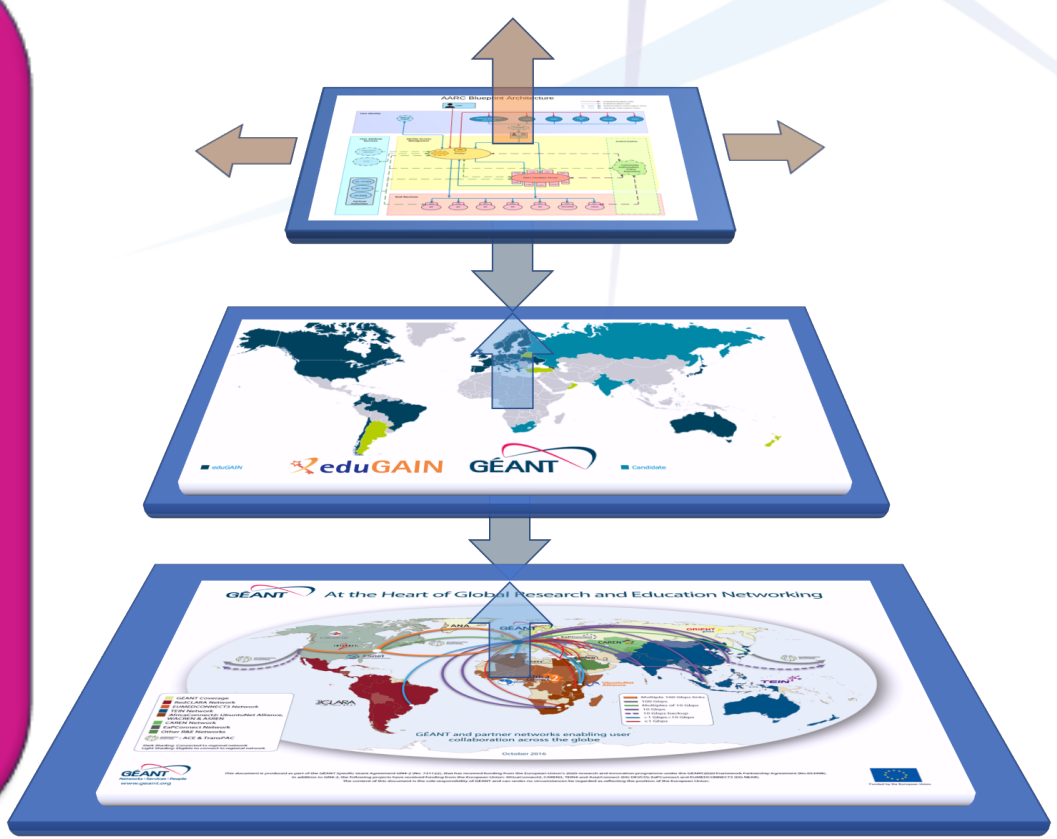
eduGAIN – A global network of academic identities

- Allows researchers to use ONE digital identity to access MANY services and resources available in eduGAIN
- Access to resources based on the user's affiliation
  - AuthZ done by resources

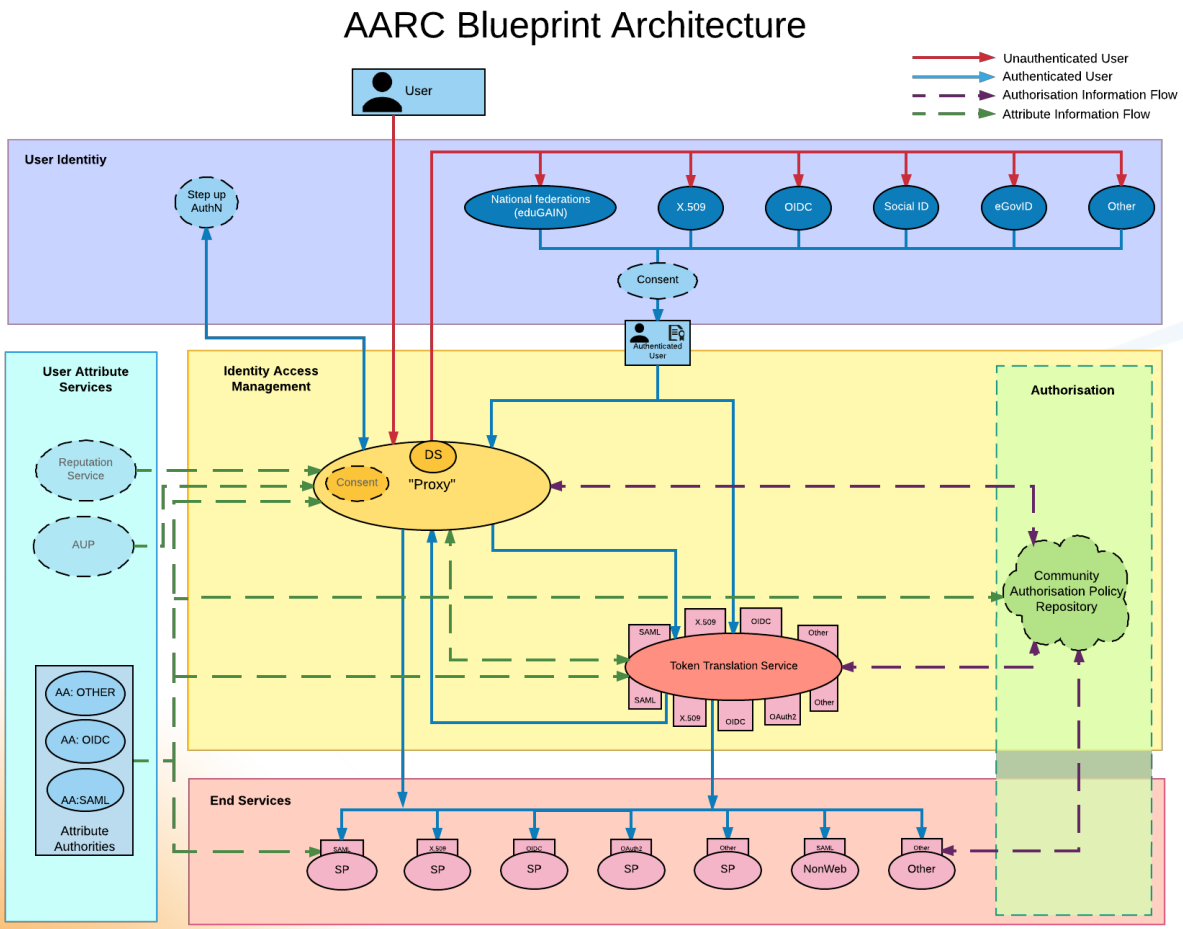


AARC – Enabling an ecosystem of solutions on top of eduGAIN

- A Blueprint **Architecture** for authentication and authorization
  - A set of architectural and policy building blocks on top of eduGAIN
- eduGAIN and the Identity Federations
  - A solid foundation for federated access in Research and Education



AARC Blueprint Architecture



- **User Identities** – services which provide electronic identities that can be used by users participating in International Research Collaborations
- **Identity Access Management** – defines an administrative, policy and technical boundary between the internal/external services and resources.
- **Authorization** – contains elements to controls the many ways users can access to services and resources.
- **End-services** – where the external services interact with the other elements of the AAI

https://aarc-project.eu/architecture

AARC Guidelines & Best Practices

- Uniform representation of unique user identifiers

```
<uid>@<scope>
```

- Standardised way of expressing group membership & role information

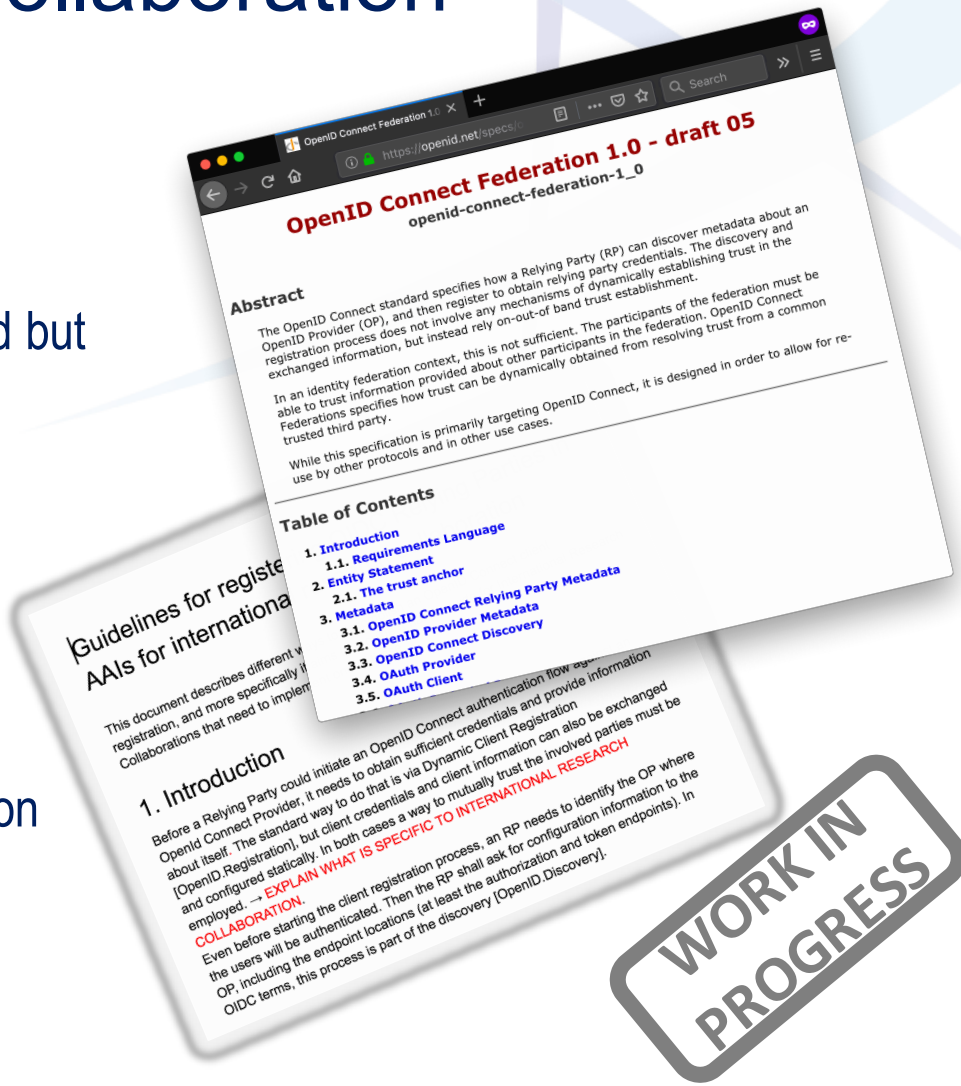
```
<NAMESPACE>:group:<GROUP>[:<SUBGROUP>*][:role=<ROLE>]#<AUTHORITY>
```

- Non-web-browser-based access (e.g. SSH/SFTP or HTTP APIs via OAuth2 tokens and X.509 certs)
- Delegation (e.g. via token exchange)
- Security Incident Response Trust Framework for Federated Identity (Sirtfi)
- Evaluation and combination of assurance information

OpenID Connect for Research Collaboration

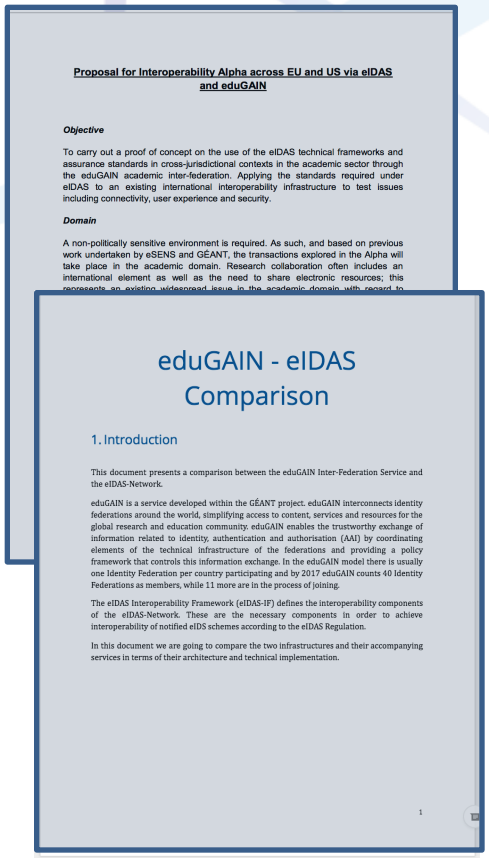
- Challenges:
  - Automatic registration is not a trusted approach
  - Approval-based approaches are trusted but cannot scale

- Goal: **"Scalable"** and **"Trusted"** dynamic registration mechanism for OIDC clients:
  - OAuth 2.0 protected dynamic registration
  - OpenID Connect Federation



eIDAS for Research Collaboration

- **2016-07 – 1st meeting in Brussels between AARC, GN4 and eIDAS Reps**
  - Investigate the possibility of an interoperation pilot between eduGAIN and eIDAS
- **2016-09 – 2nd meeting in London (AARC, GN4, Internet2, eIDAS Reps)**
  - Draft proposal for an interoperability pilot between
  - 3 Use cases:
    1. authenticate to eduGAIN service with eIDAS eID
    2. authentication to an eduGAIN service where a higher LoA is required
    3. Study the case of cross-border attribute provision between universities
- **2016-10 – eduGAIN Steering Group**
  - Plans for internal analysis and recommendation on the interoperation scenarios
- **2017-01 – Reprioritization of eIDAS goals**
  - Pilots suspended until CEF/eIDAS can allocate the needed resources
- **2017-05 – eduGAIN – eIDAS Gap Analysis & Interoperability proposal**



Proposal for Interoperability Alpha across EU and US via eIDAS and eduGAIN

Objective

To carry out a proof of concept on the use of the eIDAS technical frameworks and assurance standards in cross-jurisdictional contexts in the academic sector through the eduGAIN academic inter-federation. Applying the standards required under eIDAS to an existing international interoperability infrastructure to test issues including connectivity, user experience and security.

Domain

A non-politically sensitive environment is required. As such, and based on previous work undertaken by eSENS and GÉANT, the transactions explored in the Alpha will take place in the academic domain. Research collaboration often includes an international element as well as the need to share electronic resources; this

eduGAIN - eIDAS Comparison

1. Introduction

This document presents a comparison between the eduGAIN Inter-Federation Service and the eIDAS-Network.

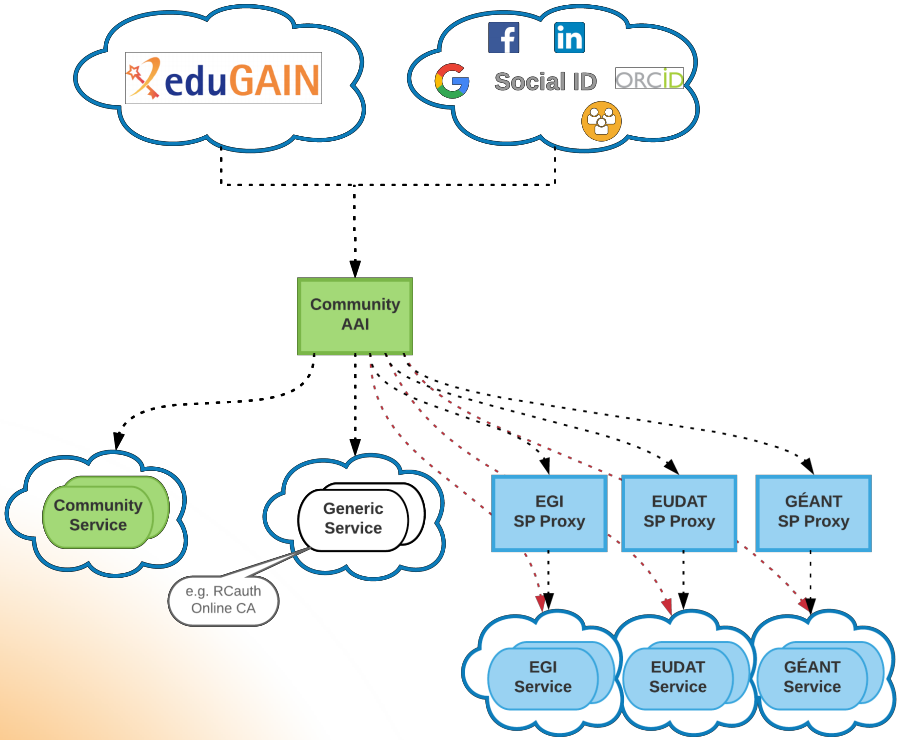
eduGAIN is a service developed within the GÉANT project. eduGAIN interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation (AAI) by coordinating elements of the technical infrastructure of the federations and providing a policy framework that controls this information exchange. In the eduGAIN model there is usually one Identity Federation per country participating and by 2017 eduGAIN counts 40 Identity Federations as members, while 11 more are in the process of joining.

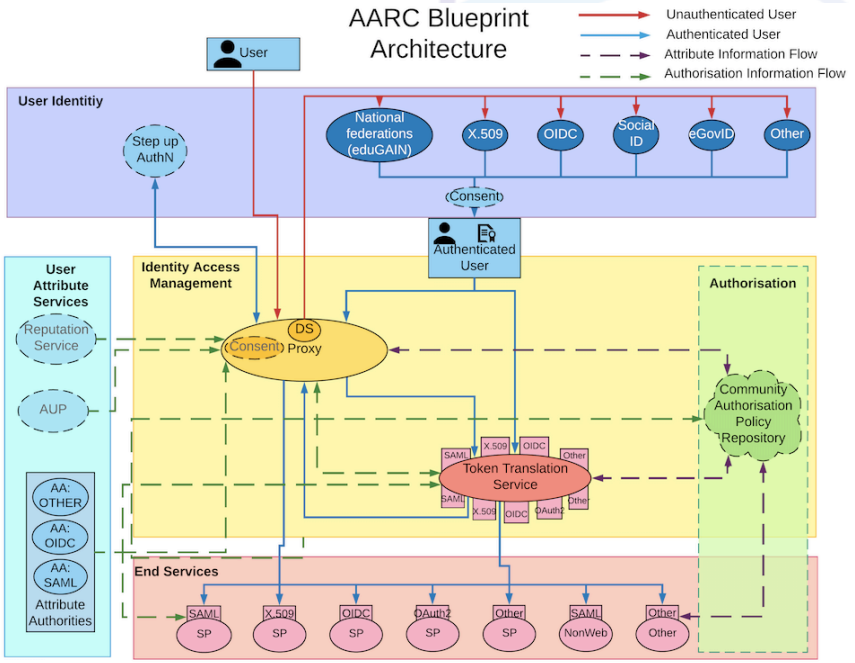
The eIDAS Interoperability Framework (eIDAS-IF) defines the interoperability components of the eIDAS-Network. These are the necessary components in order to achieve interoperability of notified eIDS schemes according to the eIDAS Regulation.

In this document we are going to compare the two infrastructures and their accompanying services in terms of their architecture and technical implementation.

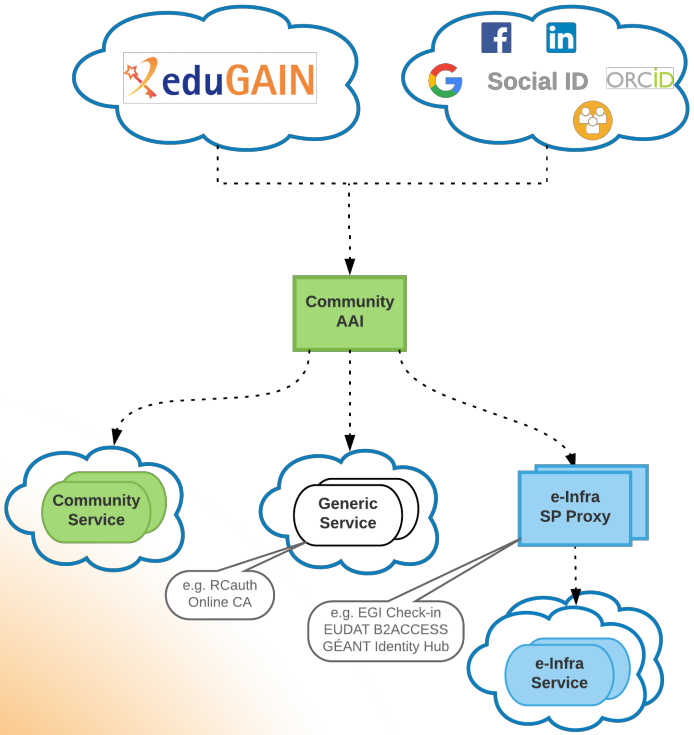
1

Community-first AARC BPA approach for the European Open Science Cloud



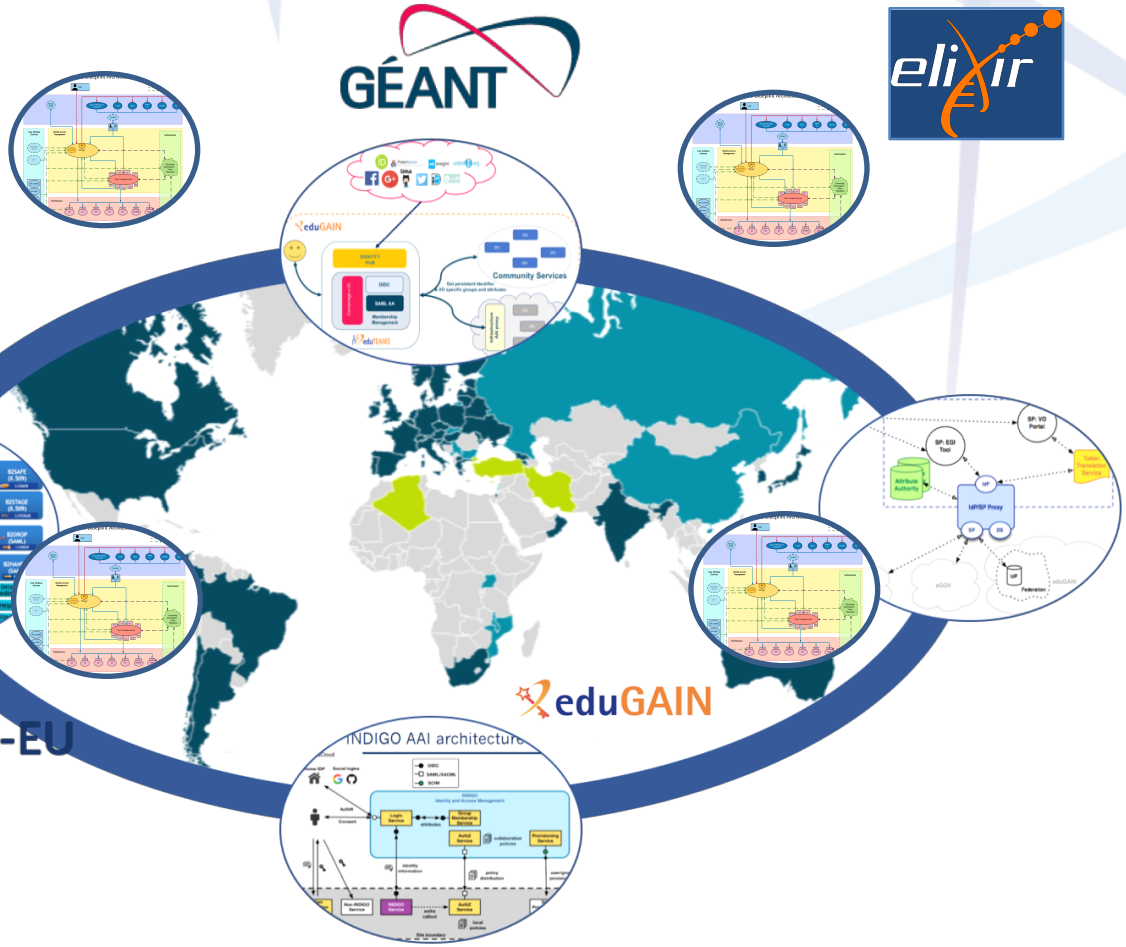


Community-first AARC BPA approach for the European Open Science Cloud



- Researchers sign in using their institutional (eduGAIN), social or community-managed IdP via their Research Community AAI
- Community-specific services are connected to a single Community AAI
- Generic services (e.g. RCauth.eu Online CA) can be connected to more than one Community AAI proxies
- e-Infra services are connected to a single e-infra SP proxy service gateway, e.g. B2ACCESS, Check-in, Identity Hub, etc

AARC BPA Implementations



EUDAT

DARIAH-EU

EGI

INDIGO - DataCloud
Better Software for Better Science