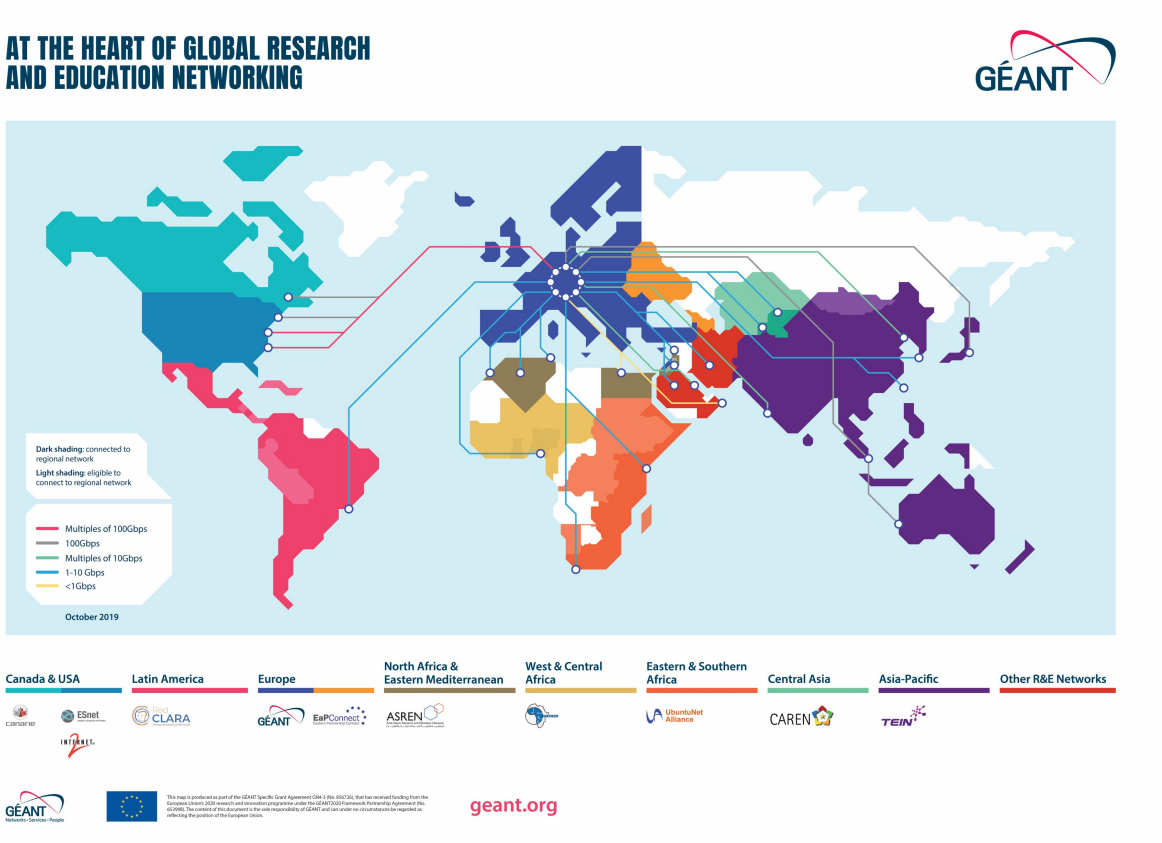
Conferenza GARR 2026
La forma del cambiamento

Authentication and Authorisation services in a changing world

Klaas Wierenga
GÉANT

GÉANT


AT THE HEART OF GLOBAL RESEARCH AND EDUCATION NETWORKING
GÉANT
Dark shading: connected to regional network
Light shading: eligible to connect to regional network
Multiples of 100Gbps
100Gbps
Multiples of 10Gbps
1-10 Gbps
<1Gbps
October 2019
Canada & USA
Latin America
Europe
North Africa & Eastern Mediterranean
West & Central Africa
Eastern & Southern Africa
Central Asia
Asia-Pacific
Other R&E Networks
geant.org


REY
OSL
HEL
STO
TAR
RIG
KAU
COP
DUB
COR
LON
AMS
HAM
BER
POZ
BRU
FRA
PRA
LUX
KIE
PAR
GEN
VIE
BRA
BUD
CHI
LJU
ZAG
BUC
MAR
MIL
BEL
SOF
BIL
POR
LIS
SIN
MAD
POD
SKO
IST
THE
TIR
ATH
NIC
VAL
TEL
Fibre
Spectrum
Connected Regional Network
Leased Capacity
March 2025

The challenge

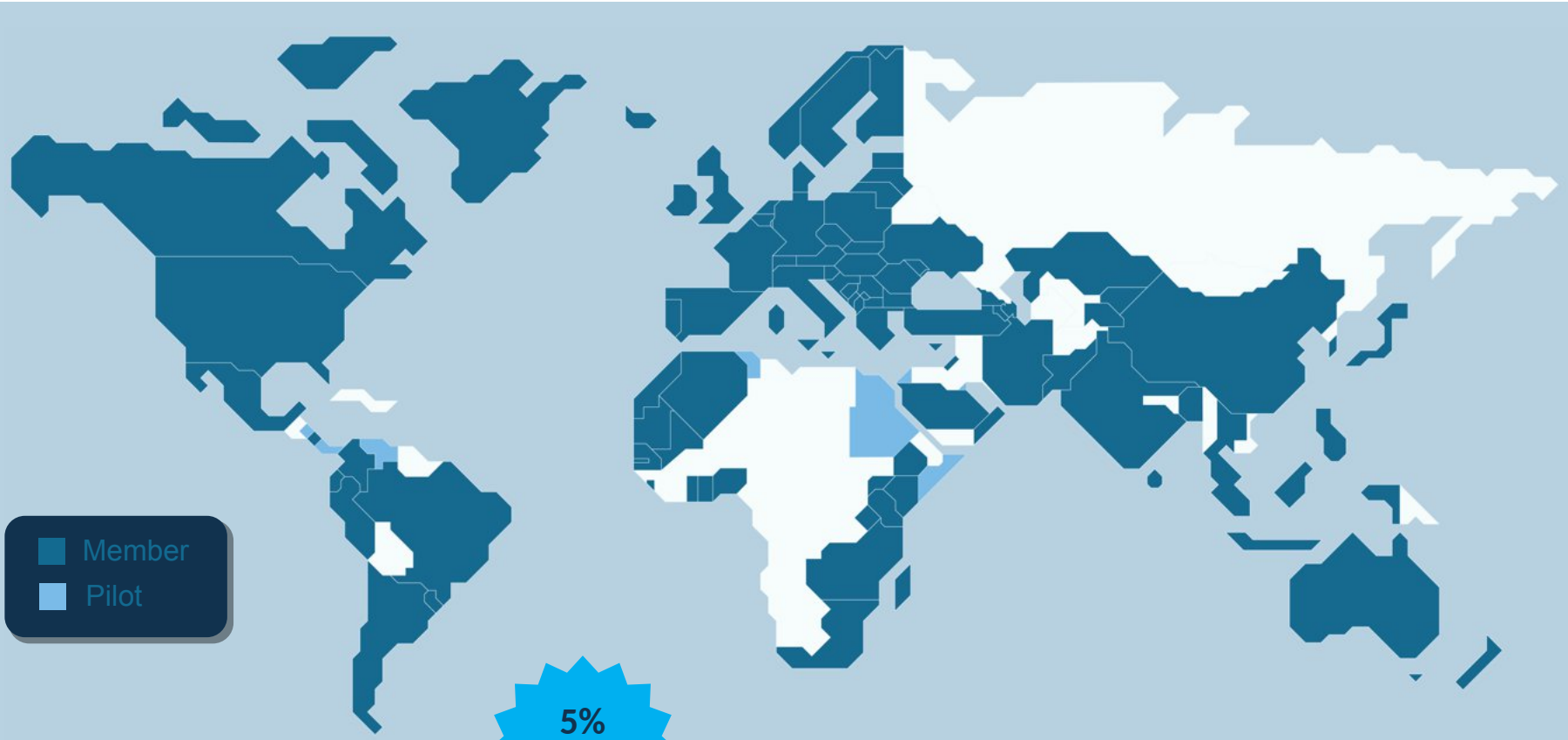
The only real problem for the Internet is scaling!

Mike O'Dell


Trust does not scale!
Taylor Swift


eduroam
RENU
I have signed up for
eduroam! Have you?

eduroam



9.2 BILLION TIMES

#love2eduroam

eduroam

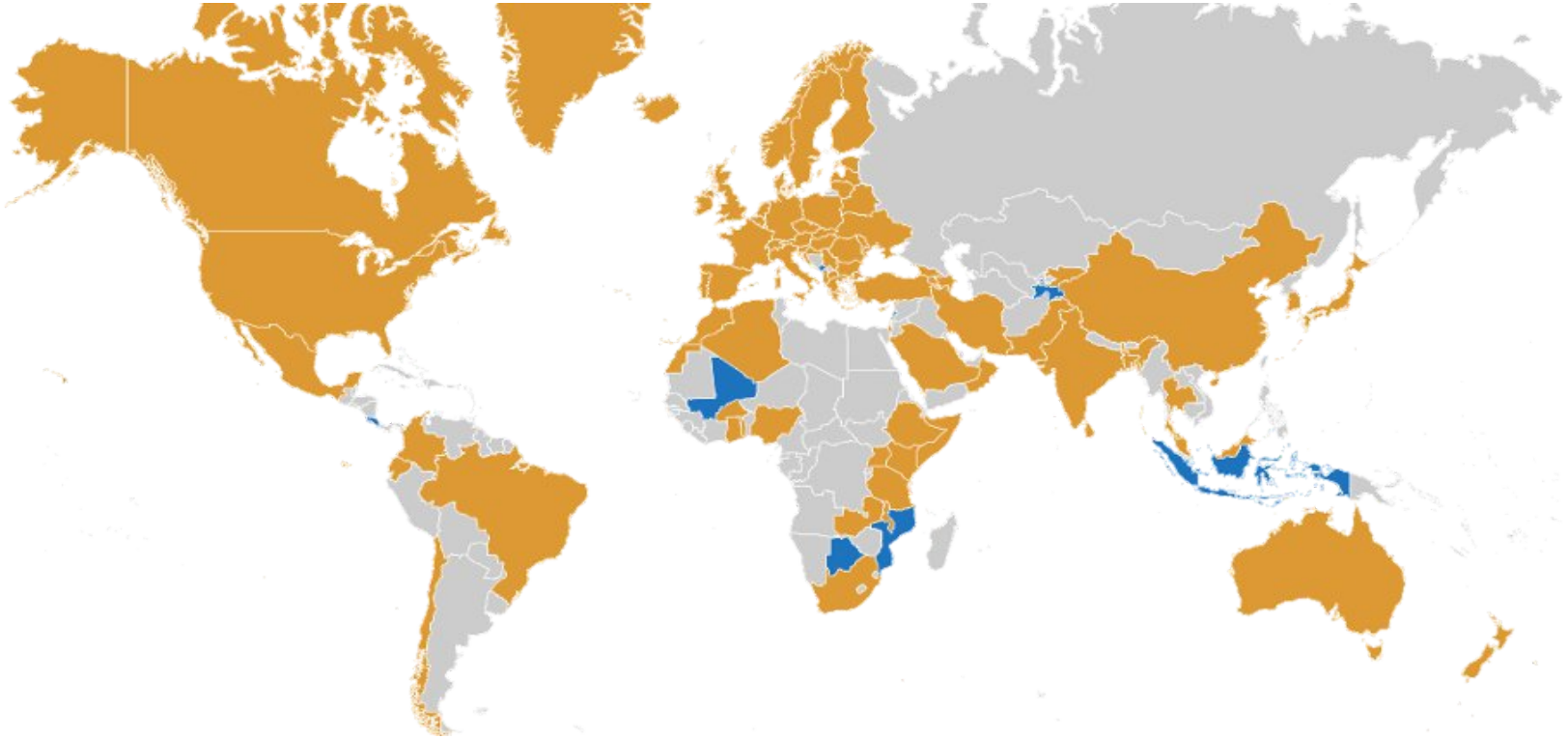
5% growth

>106	10,500+	44,600+	25,000,000+
Countries	Institutions	Service Locations	Authentications per day

Identity federations

A common identity layer

eduGAIN



83
Identity Federations

214 M users

6340
Identity Providers

3984
Service Providers

10s of M weekly AuthN

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.

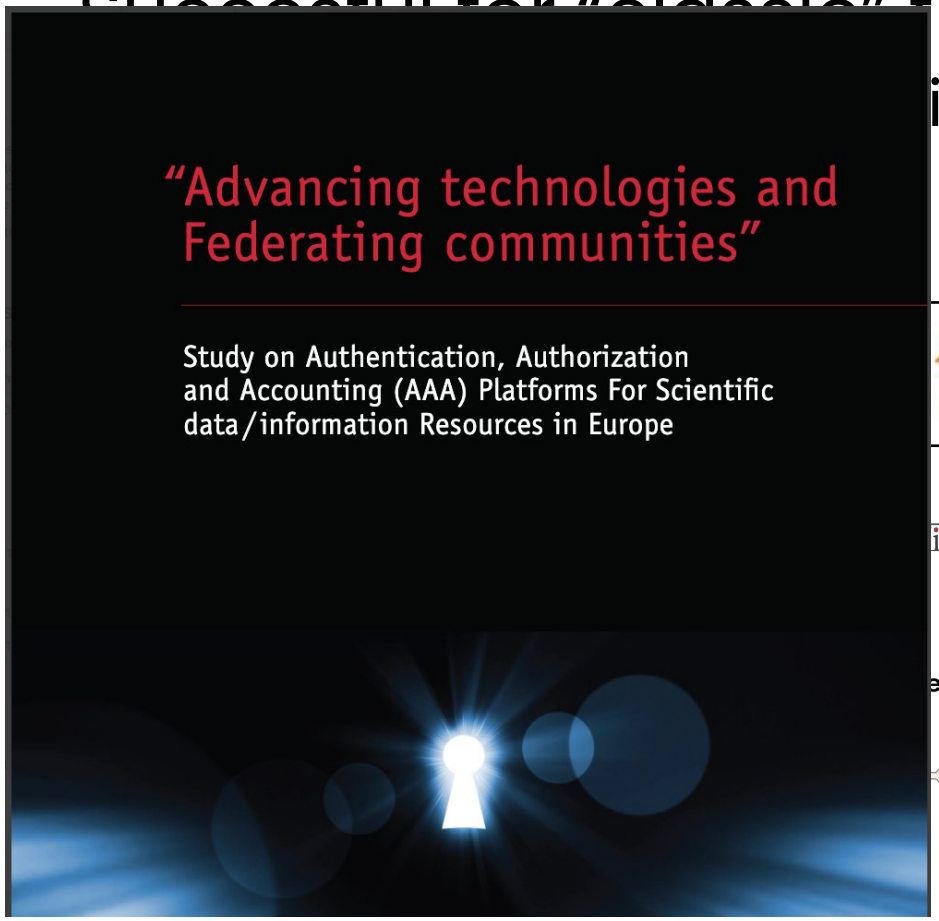
Trouble in paradise – threat to NREN relevance

Succesful for “classic” flow

- student – university – identity federation – service provider

Trouble in paradise – threat to NREN relevance

- Successful for "classic" flow
- identity f



Federated Identity Management for Research Collaborations

Paper Type: Research paper

Date of this version: 28 August 2013

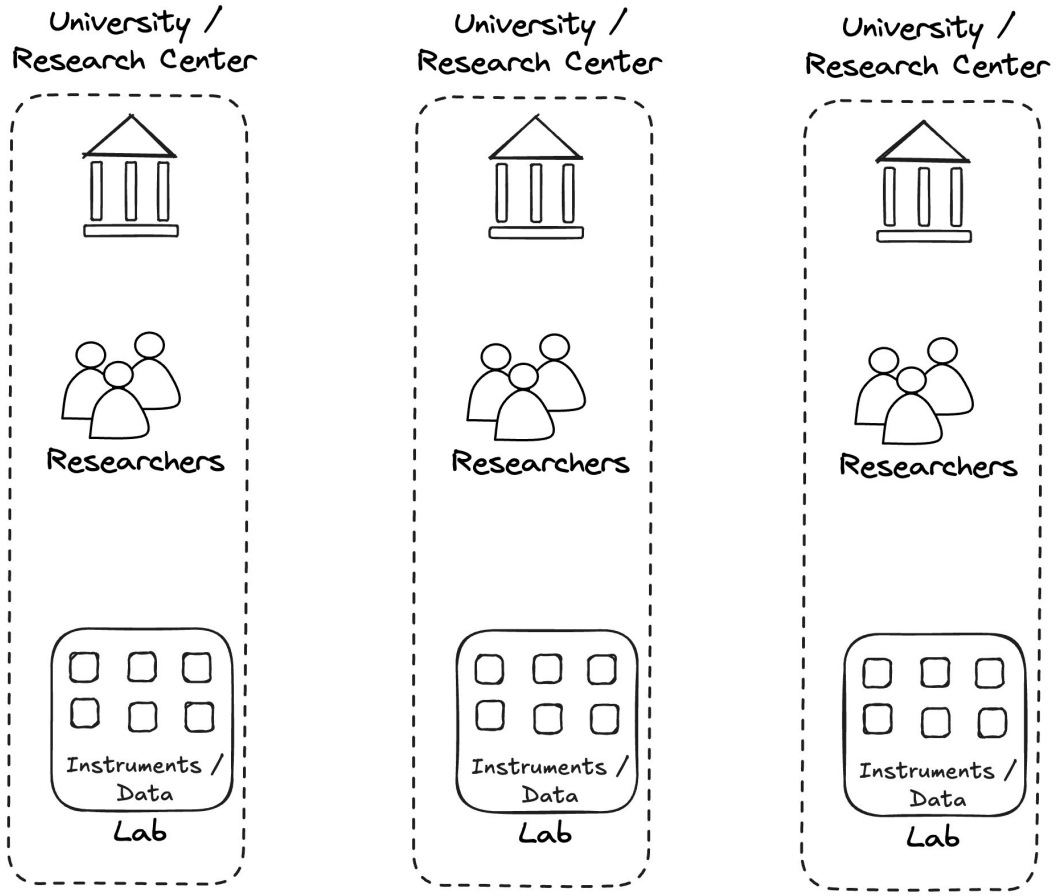
Abstract

Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

A number of laboratories including national and regional research organizations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries.

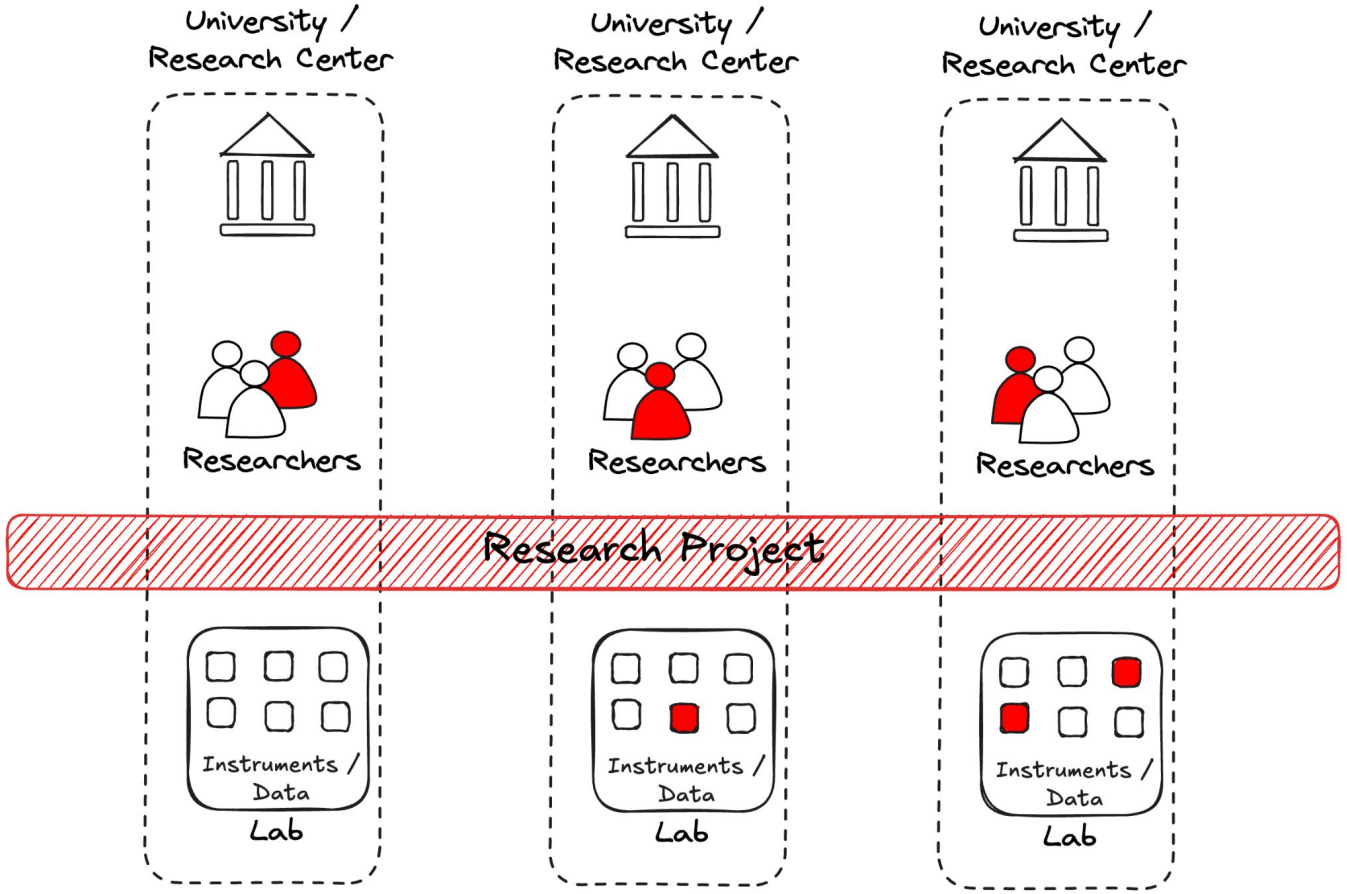
Driven by these needs, representatives from a variety of research communities, including photon/neutron facilities, social science & humanities, high-energy physics, atmospheric science, bioinformatics and fusion energy, have come together to discuss how to address these issues with the objective to define a common policy and trust framework for Identity Management based on existing structures, federations and technologies.

This paper will describe the needs of the research communities, the status of the activities in the FIM domain and



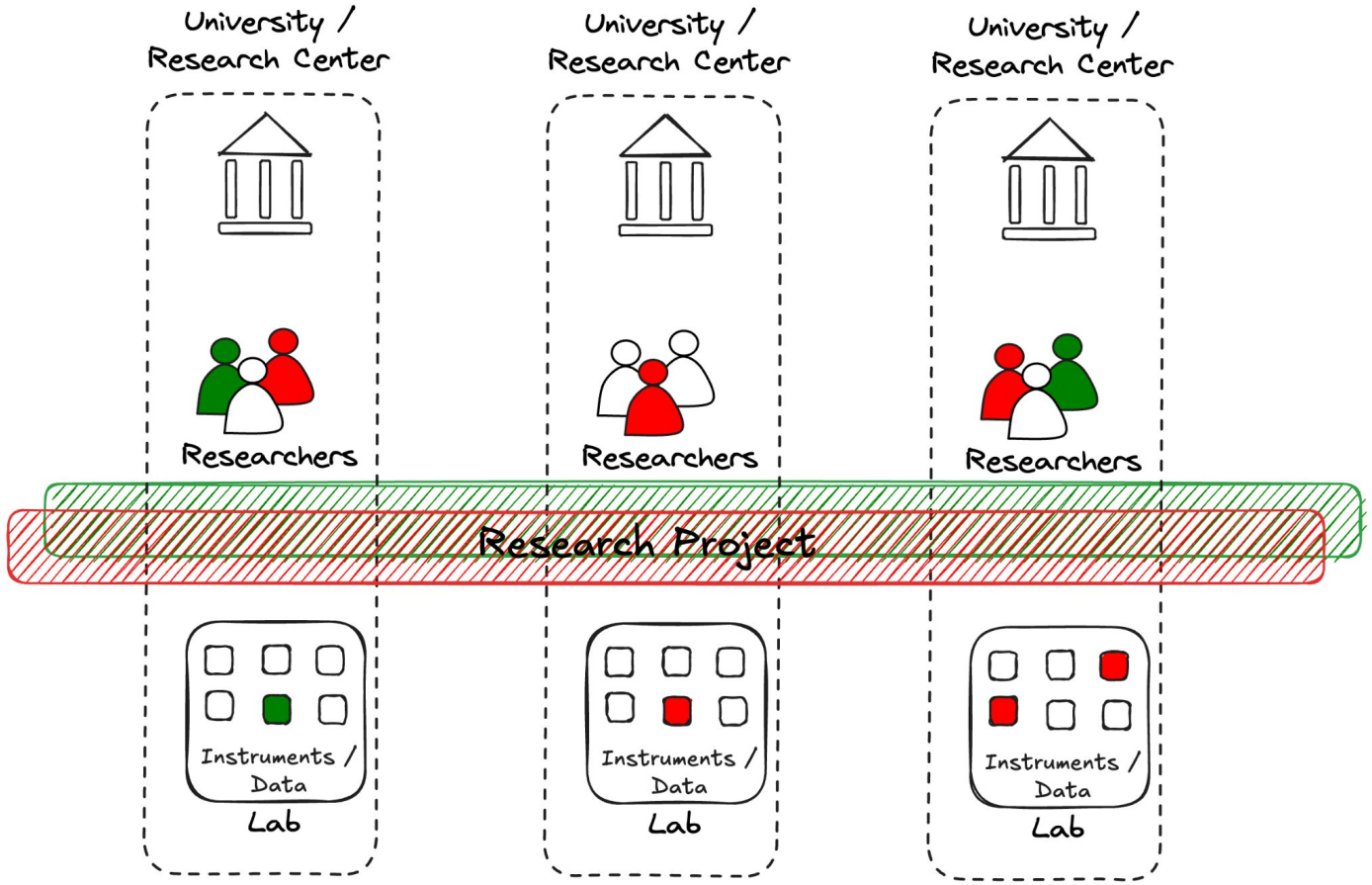
Starting point

- Researchers conducting research at their home organisation
- Access to data / instruments at the home laboratories based on their organisational / lab identity / permissions.



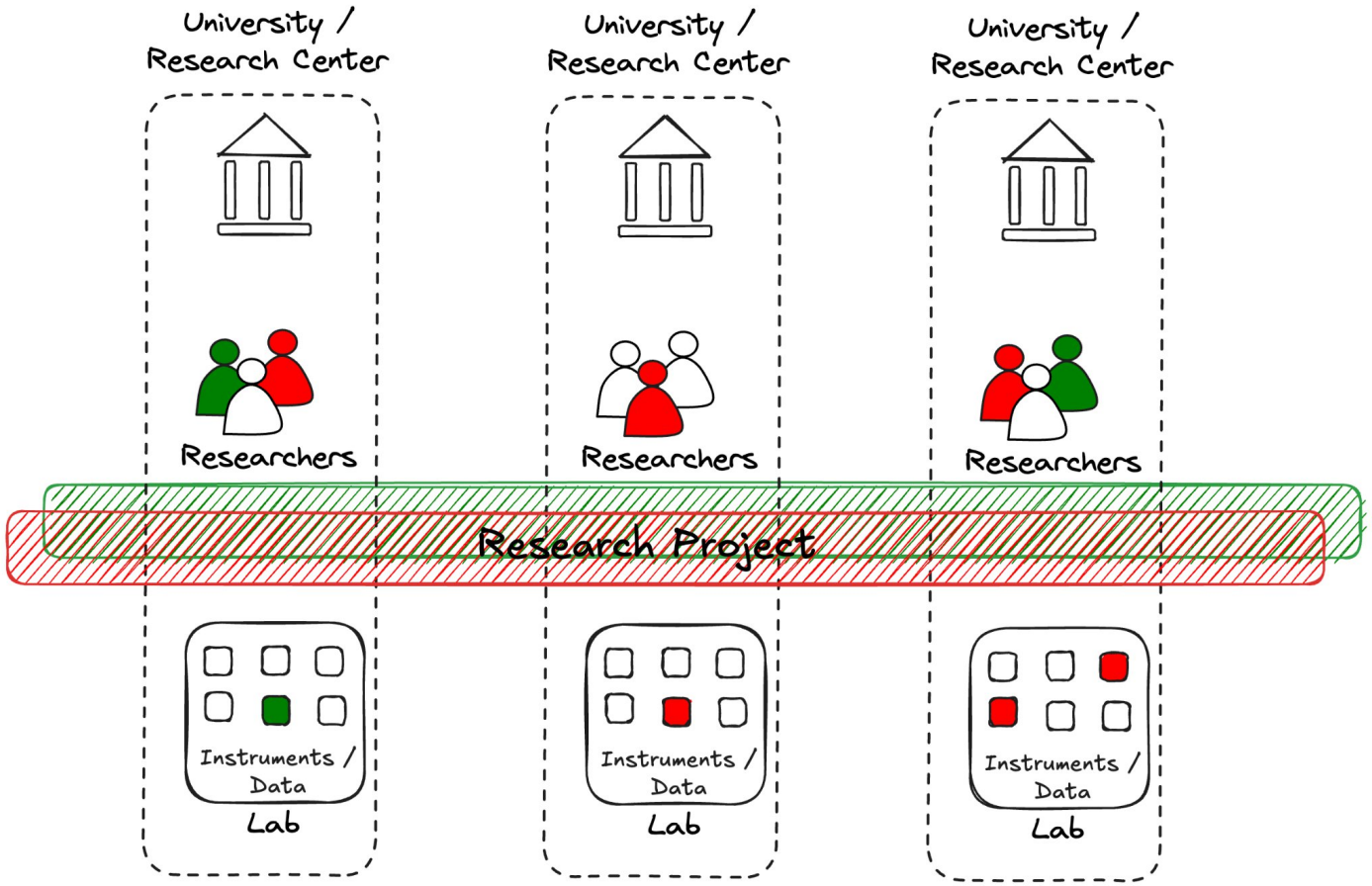
Research Collaboration

- Researchers coming together from multiple organisations to collaborate on research projects.
- Access to data / instruments across organisational boundaries
- Access based based on the role they have in the collaboration.



Research Collaboration

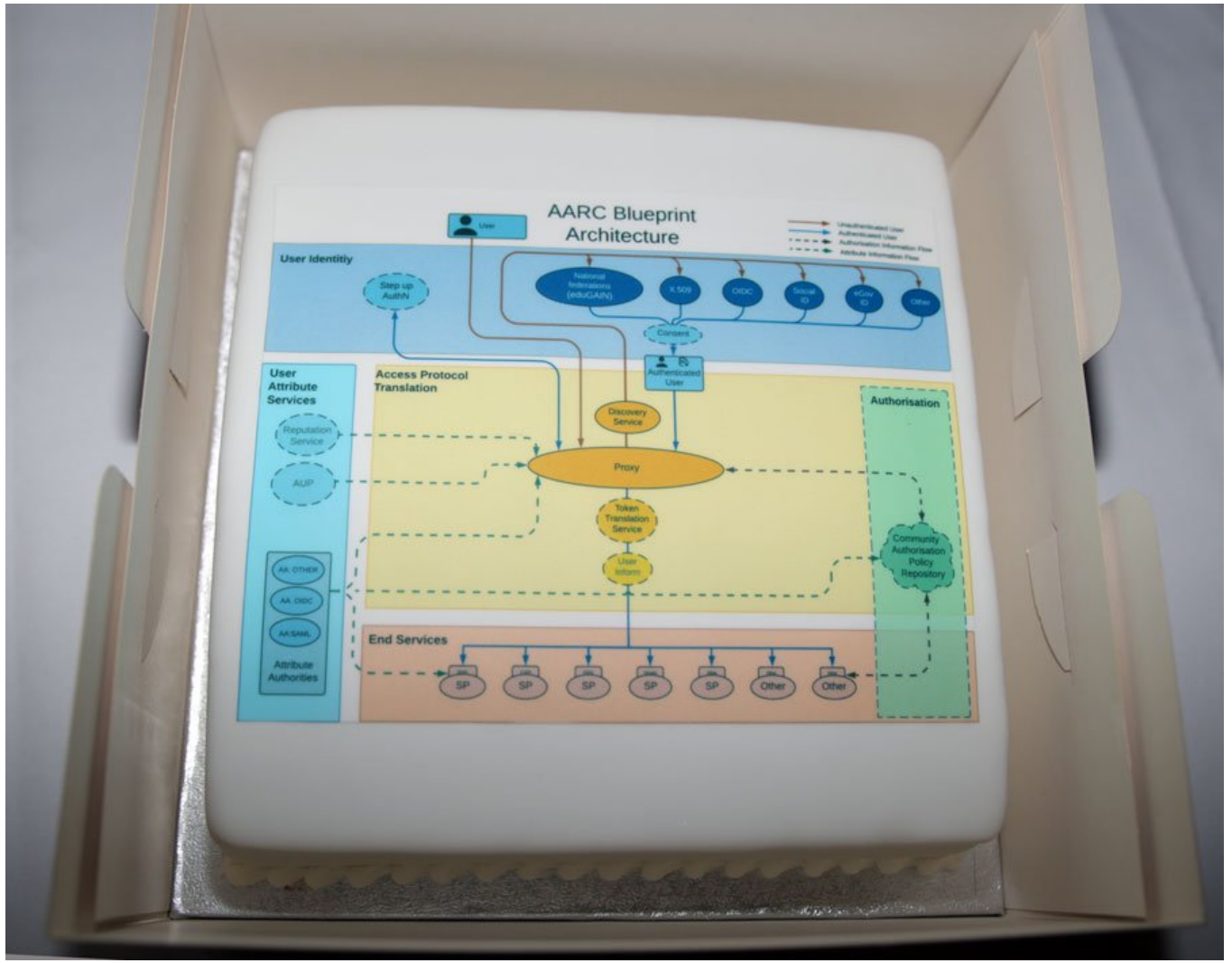
- Researchers coming together from multiple organisations to collaborate on research projects.
- Access to data / instruments across organisational boundaries
- Access based based on the role they have in the collaboration.



Challenges

- How can we identify the researchers from their home organisation?
- How do we know in which collaboration a researcher is member of?
- How do we know what is the role of a researcher in a research collaboration?
- How do we know which services / instruments / data sets can a users access?

AARC BPA to the rescue!



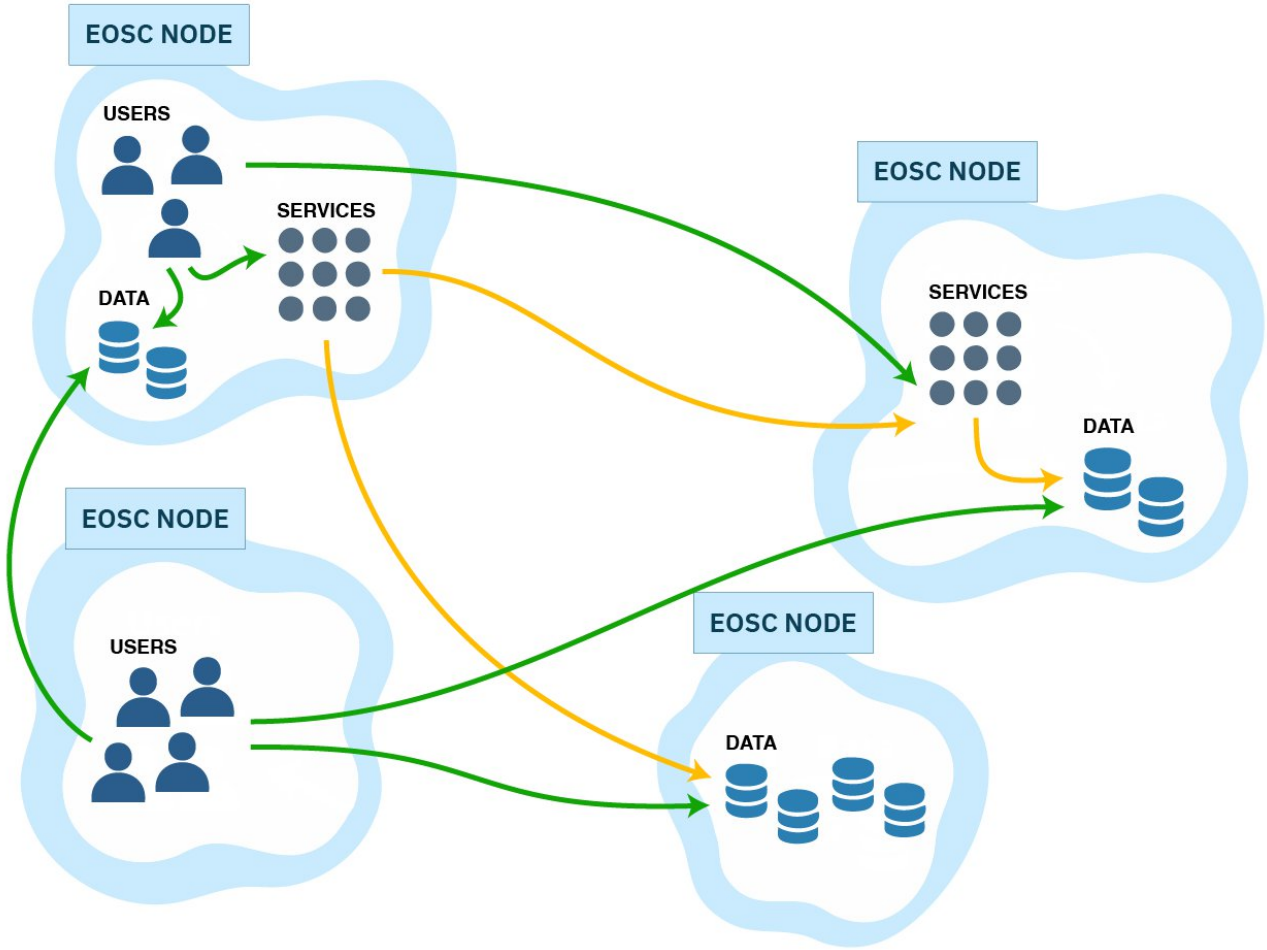
But wait….

The same architectural pattern (the AARC Blueprint Architecture), using proxies, turns out to be very useful for

- EOSC
- EuroHPC Federation Platform
- Erasmus Without Paper / University Alliances
- EUDI Wallets

- Transition to OpenID Connect
- Transition to OpenID Federation

European Open Science Cloud



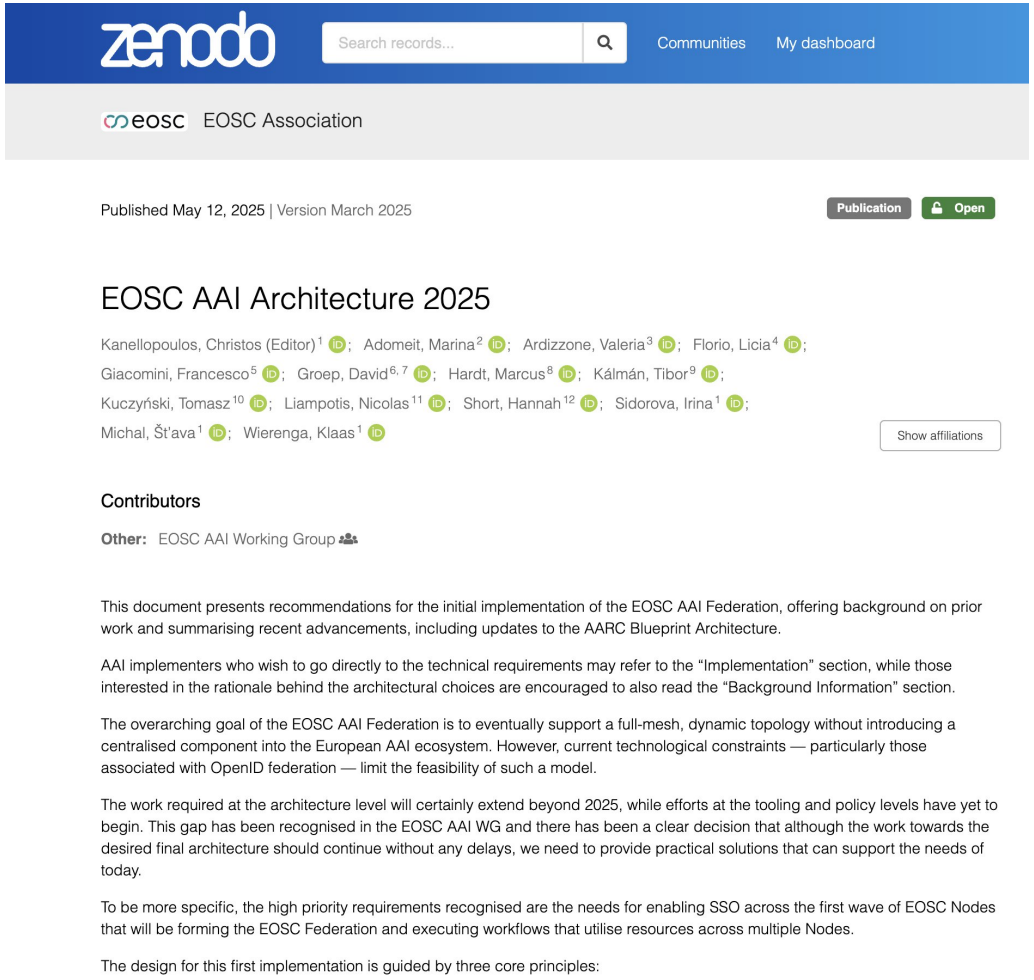
interactive login of users

service to service

Initial EOSC AAI Use Cases

- Single Sign On Across Nodes
- Cross Node Workflows

EOSC AAI Architecture - March 2025 version



zenodo Search records... Communities My dashboard

eosc EOSC Association

Published May 12, 2025 | Version March 2025

Publication Open

EOSC AAI Architecture 2025

Kanellopoulos, Christos (Editor)[1]; Adomeit, Marina[2]; Ardizzone, Valeria[3]; Florio, Licia[4]; Giacomini, Francesco[5]; Groep, David[6, 7]; Hardt, Marcus[8]; Kálmán, Tibor[9]; Kuczyński, Tomasz[10]; Liampotis, Nicolas[11]; Short, Hannah[12]; Sidorova, Irina[1]; Michal, Šťava[1]; Wierenga, Klaas[1]

Show affiliations

Contributors

Other: EOSC AAI Working Group

This document presents recommendations for the initial implementation of the EOSC AAI Federation, offering background on prior work and summarising recent advancements, including updates to the AARC Blueprint Architecture.

AAI implementers who wish to go directly to the technical requirements may refer to the “Implementation” section, while those interested in the rationale behind the architectural choices are encouraged to also read the “Background Information” section.

The overarching goal of the EOSC AAI Federation is to eventually support a full-mesh, dynamic topology without introducing a centralised component into the European AAI ecosystem. However, current technological constraints — particularly those associated with OpenID federation — limit the feasibility of such a model.

The work required at the architecture level will certainly extend beyond 2025, while efforts at the tooling and policy levels have yet to begin. This gap has been recognised in the EOSC AAI WG and there has been a clear decision that although the work towards the desired final architecture should continue without any delays, we need to provide practical solutions that can support the needs of today.

To be more specific, the high priority requirements recognised are the needs for enabling SSO across the first wave of EOSC Nodes that will be forming the EOSC Federation and executing workflows that utilise resources across multiple Nodes.

The design for this first implementation is guided by three core principles:

The EOSC AAI Architecture profiles the AARC Blueprint Architecture for EOSC

MyAccessID - EOSC AAI Federation

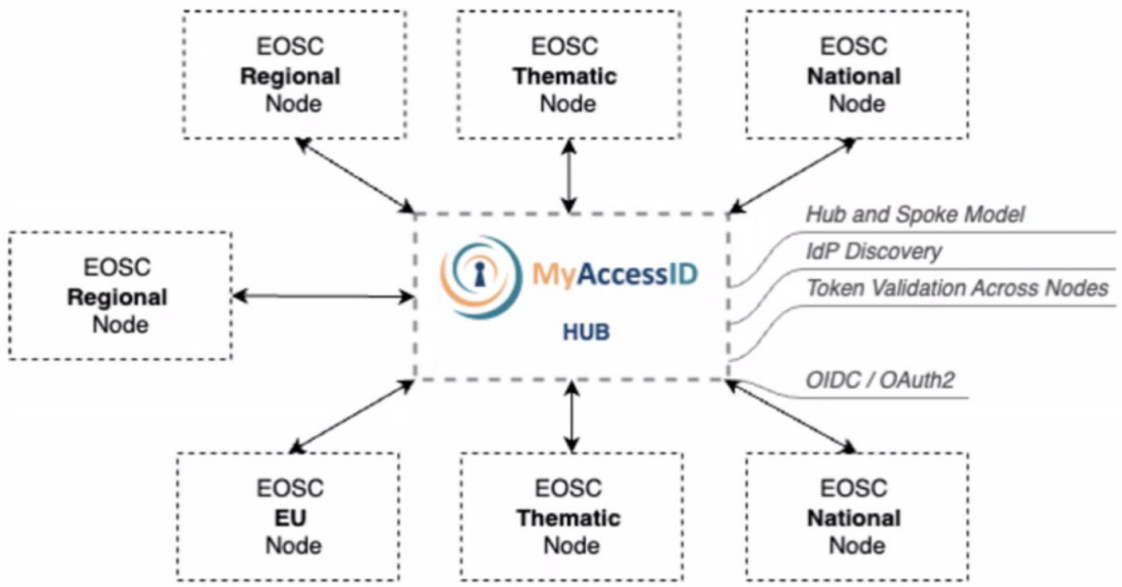
eosc | Technical and Semantic Interoperability Task Force

DOI 10.5281/zenodo.15388270

EOSC AAI Architecture 2025

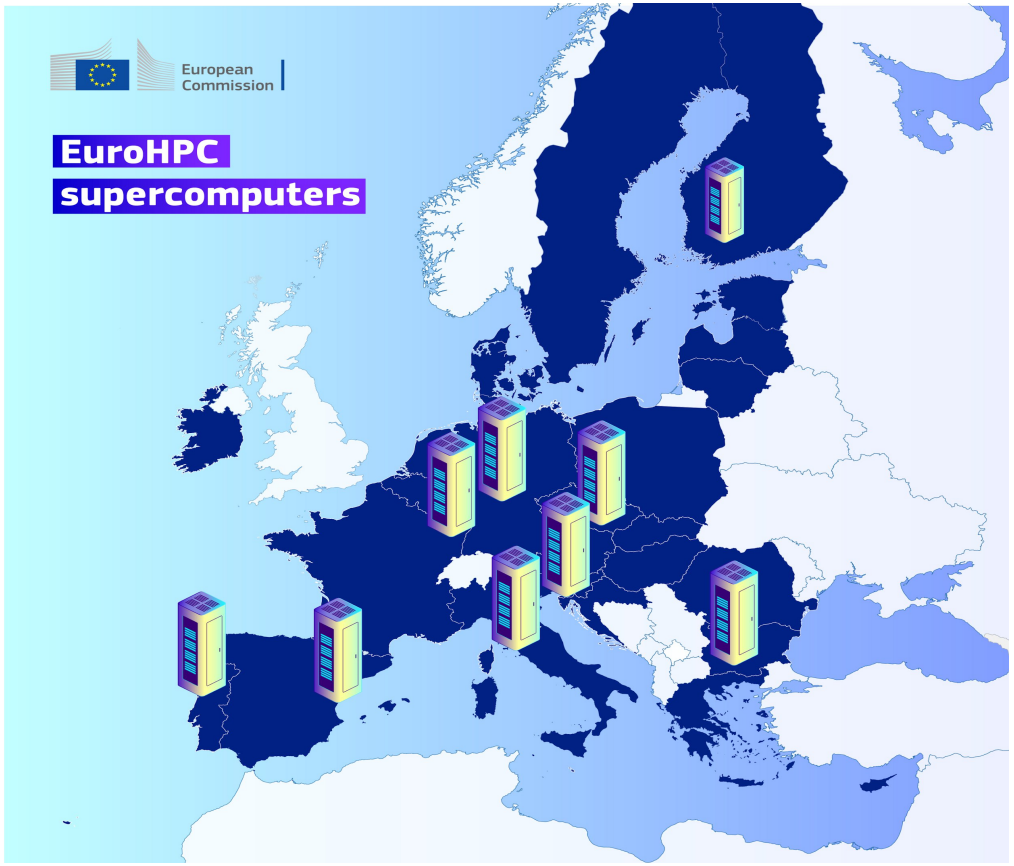
May 12, 2025

- The document presents **recommendations for the initial implementation of the EOSC AAI Federation,** offering background on prior work and summarising recent advancements, including updates to the AARC Blueprint Architecture.
- It is intended as a **practical guide for candidate EOSC Nodes,** outlining the steps necessary to connect with the EOSC AAI Federation. In the EOSC model, Nodes act as the primary integration points for services as it is described in the EOSC Federation Handbook, services are onboarded to individual Nodes rather than directly to the Federation.
- The overarching goal of the EOSC AAI Federation is to eventually support a **full-mesh, dynamic topology** without introducing a centralised component into the European AAI ecosystem.

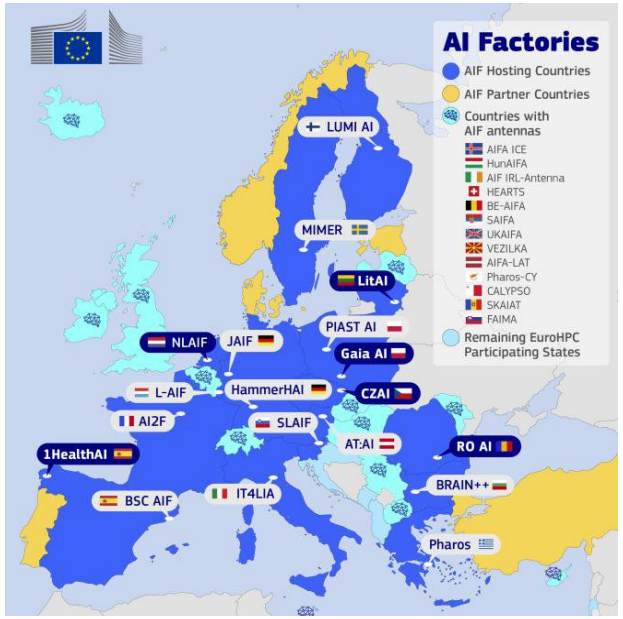


EOSC AAI Federation "hub-and-spoke" model

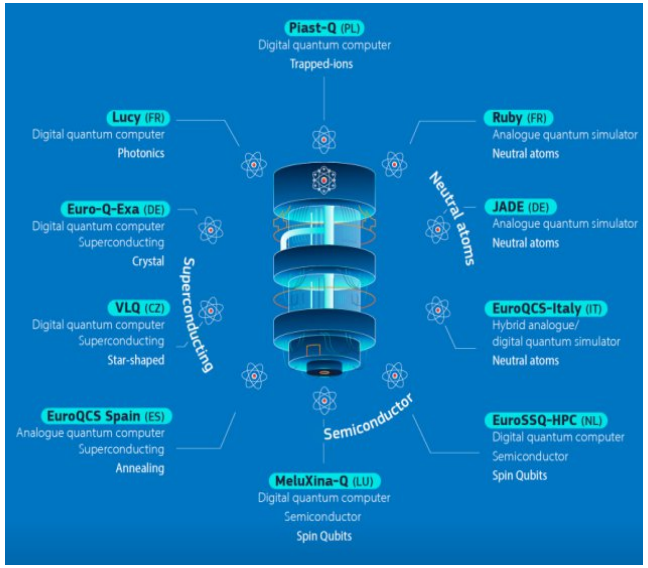
EuroHPC



Alice Recoque, Arrhenius, DAEDALUS, Deucalion, Discoverer, JUPITER, Karolina, Leonardo, LUMI, MareNostrum 5, MeluXina, Vega, …



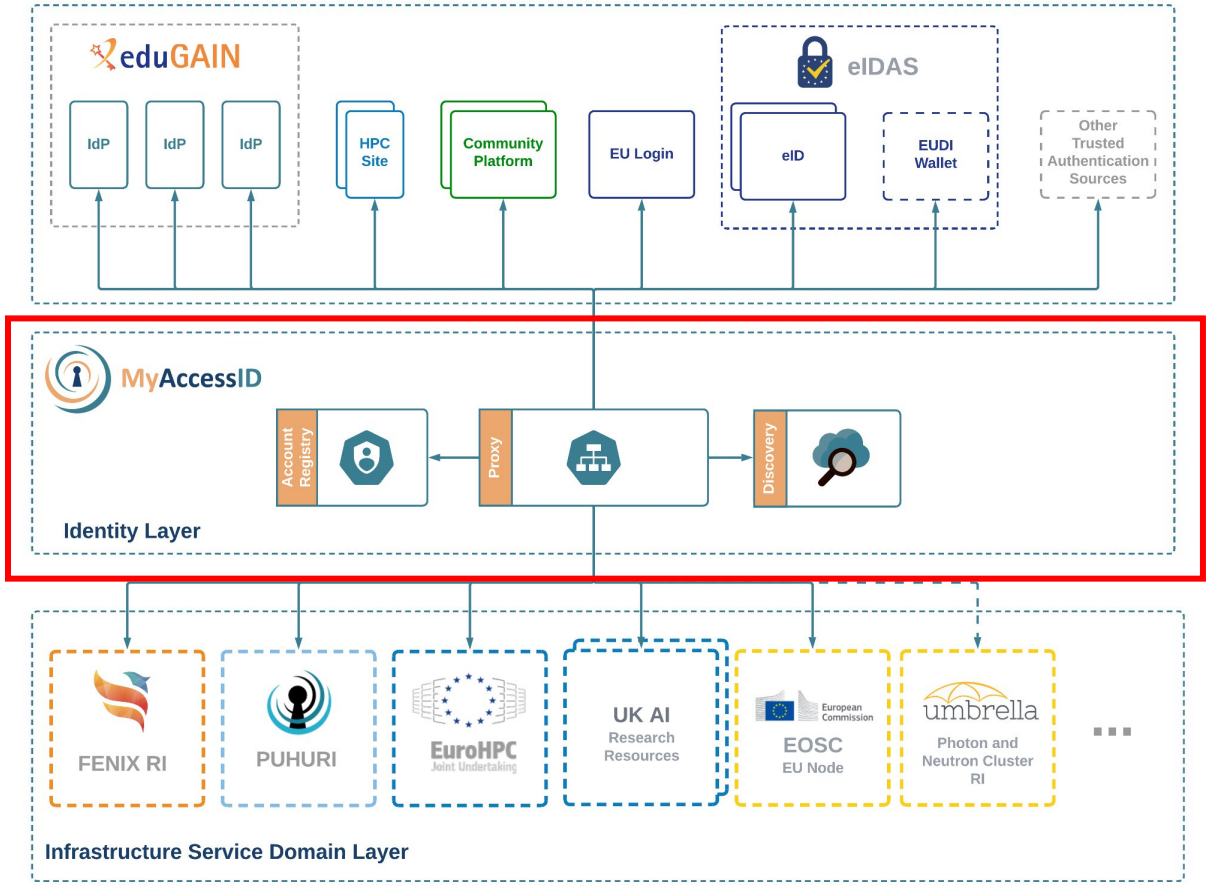
BSC AIF, HammerHAI, IT4LIA, LUMI AIF, Meluxina-AI, MIMER, Pharos
AI2F, AIF Austria, BRAIN++, JAIF, PIAST AIF, SLAIF, …

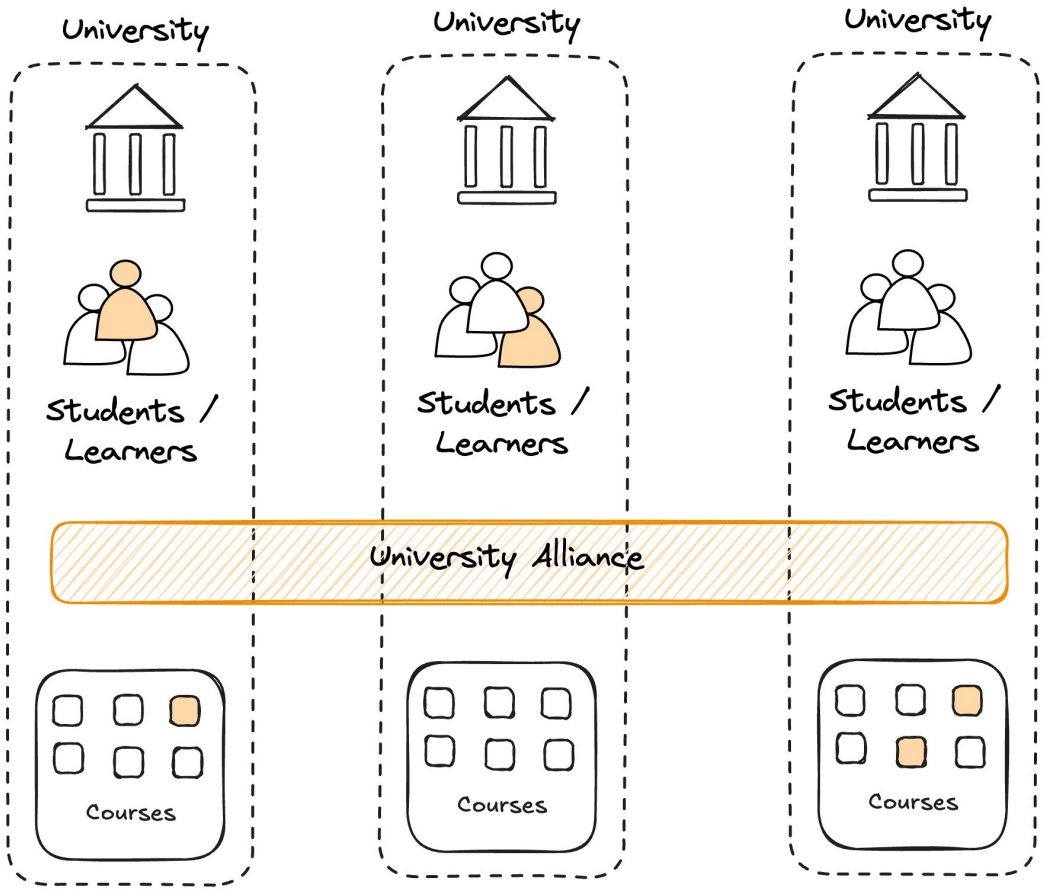


Euro-Q-Exa, EuroQCS-France, EuroQCS-Italy, EuroQCS-Spain, EuroQCS-Poland, VLQ, …

MyAccessID – EuroHPC

- HPC Datacenters are in the process of transforming to **Infrastructure Service Providers** with **a diverse Service Portfolio**
- These services become available in different administrative and policy domains, which we call **Infrastructure Service Domains**
- **A common Authentication and Authorization Infrastructure** enables uniform accessibility to scientists and engineers at European scale

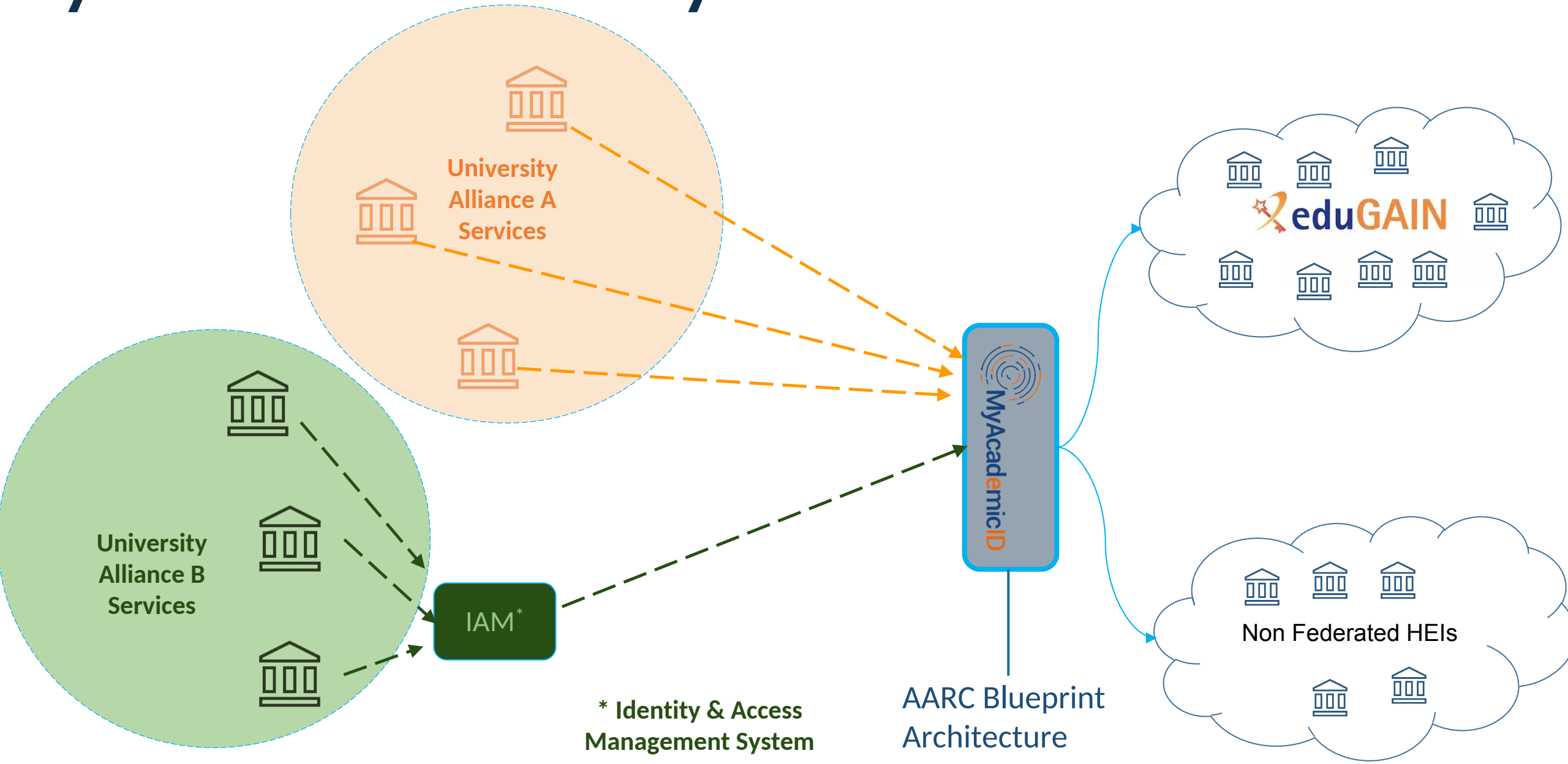


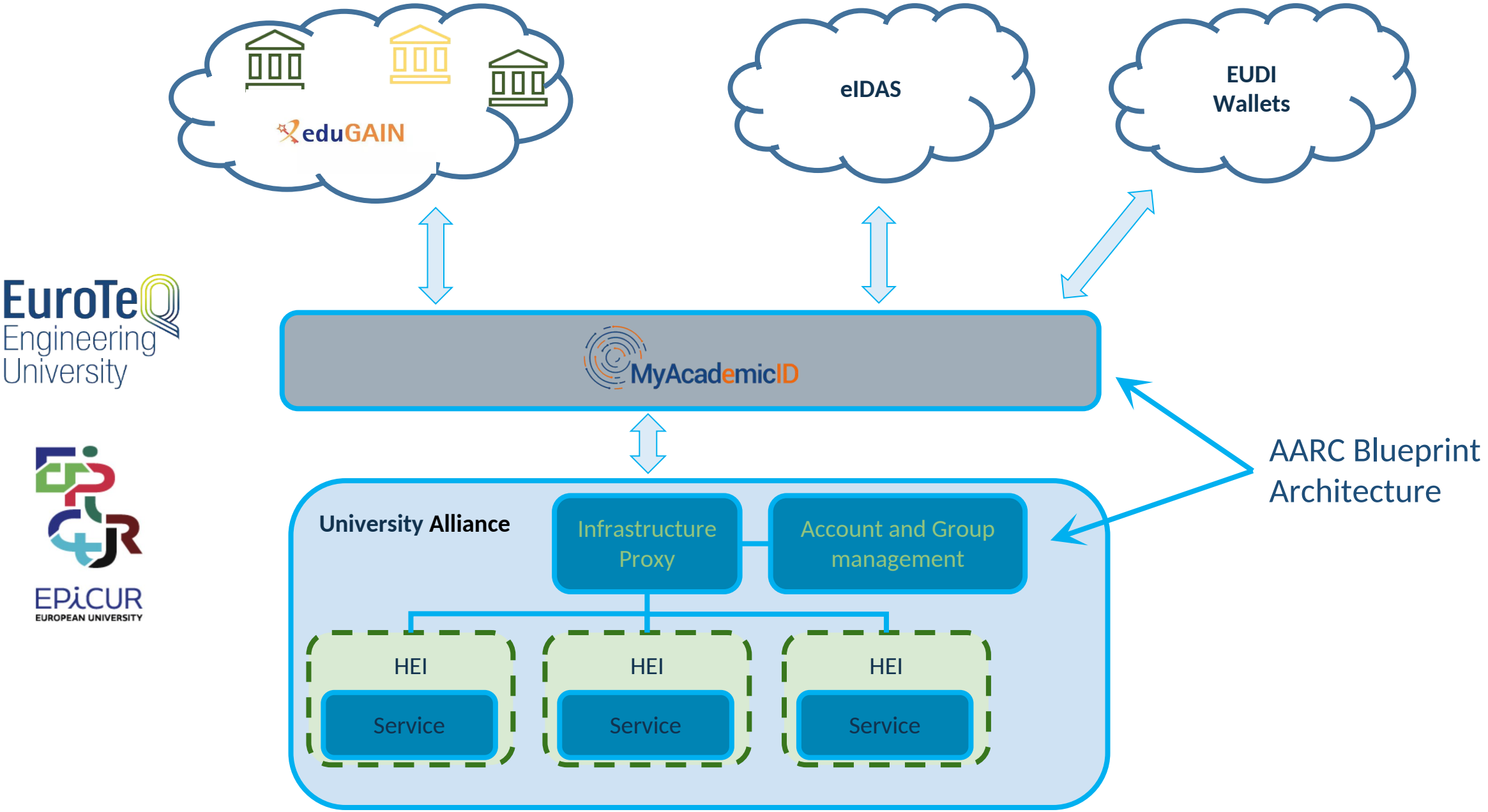


Challenges

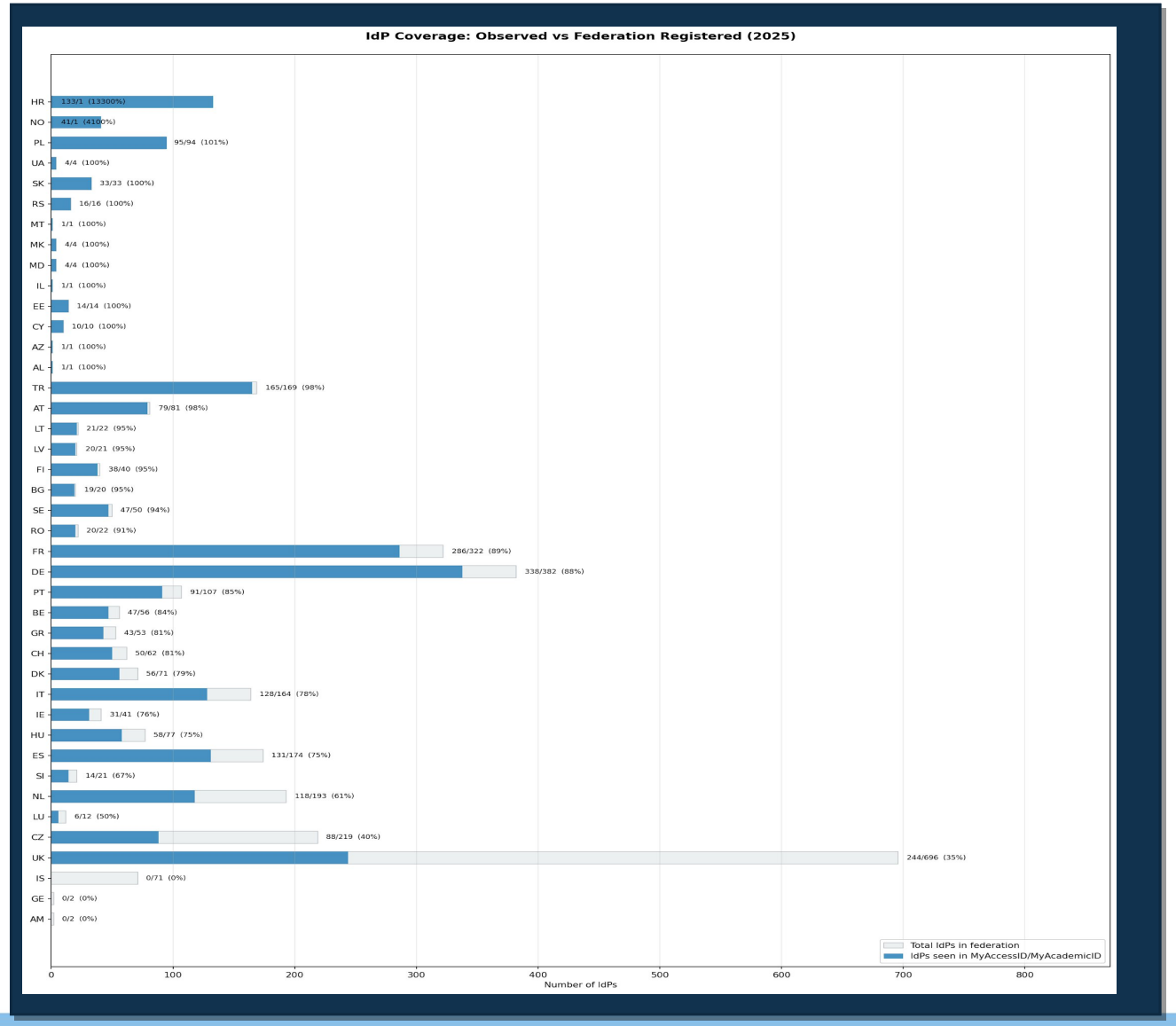
- How can we identify the **students / learners** from their home organisation?
- How do we know in which **university alliance** a **student/learner** is member of?
- How do we know what is the **affiliation/role** of a **student/learner** in the **university alliance**?
- How do we know which **courses** / **services** / **data** can a **student / learner** access?

MyAcademicID – University Alliances and Erasmus




eduGAIN
eIDAS
EUDI
Wallets
MyAcademicID
University Alliance
Infrastructure Proxy
Account and Group management
HEI
Service
HEI
Service
HEI
Service
AARC Blueprint Architecture

Uptake of MyAccessID and MyAcademicID



400K

Authentications per month

750K+

Users

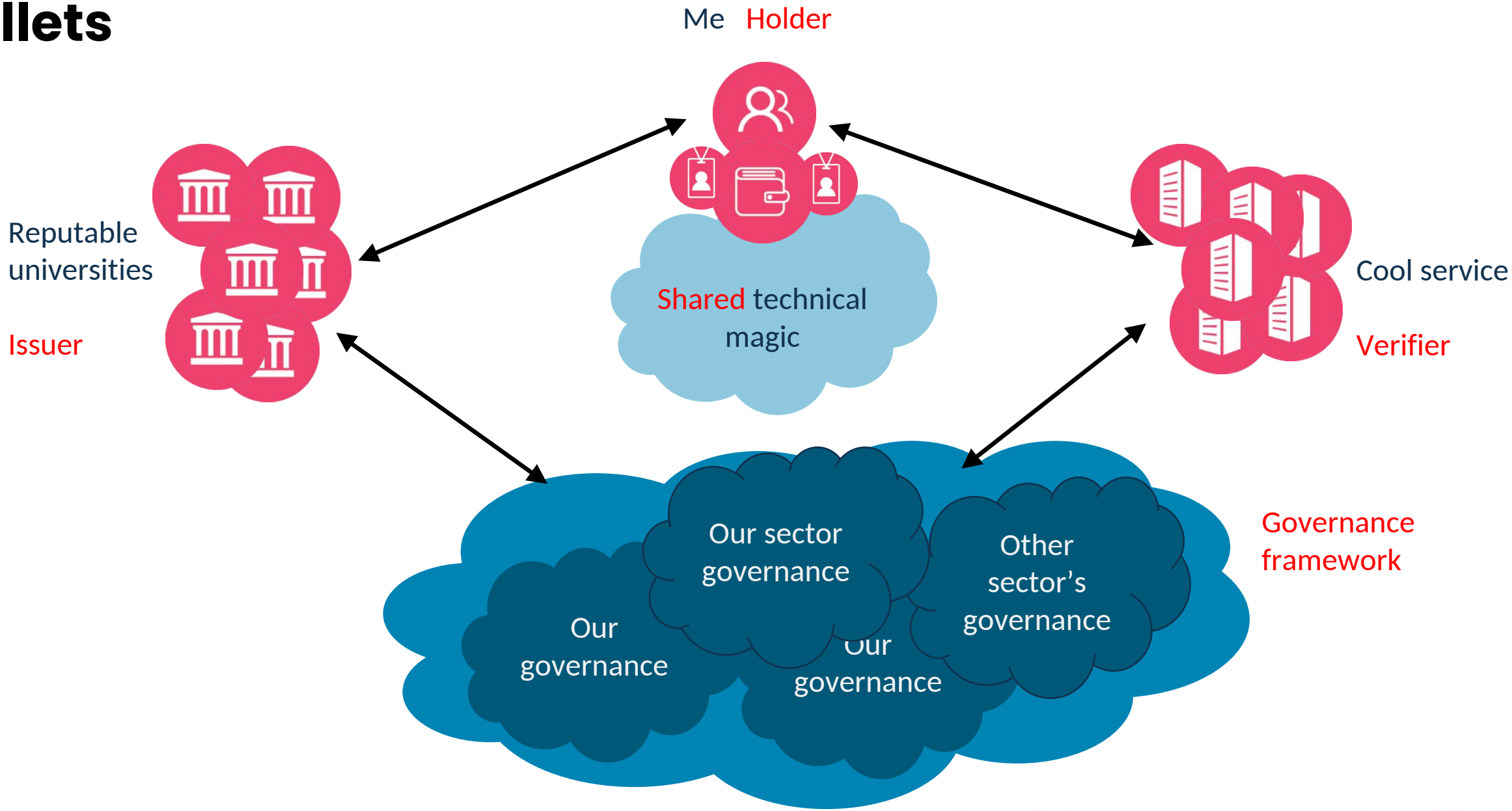
5,300+

Identity Providers

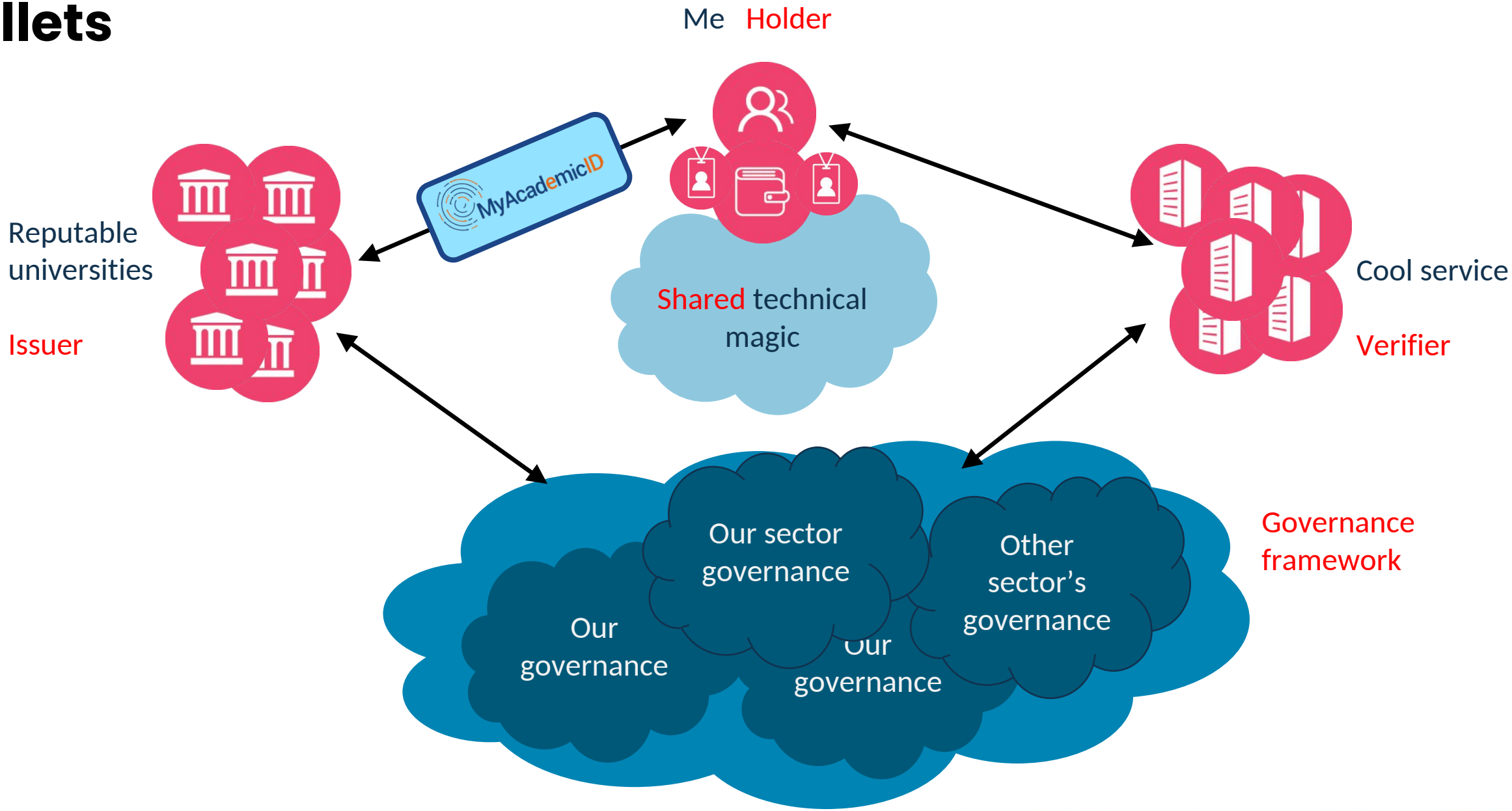
70+

Identity Federations

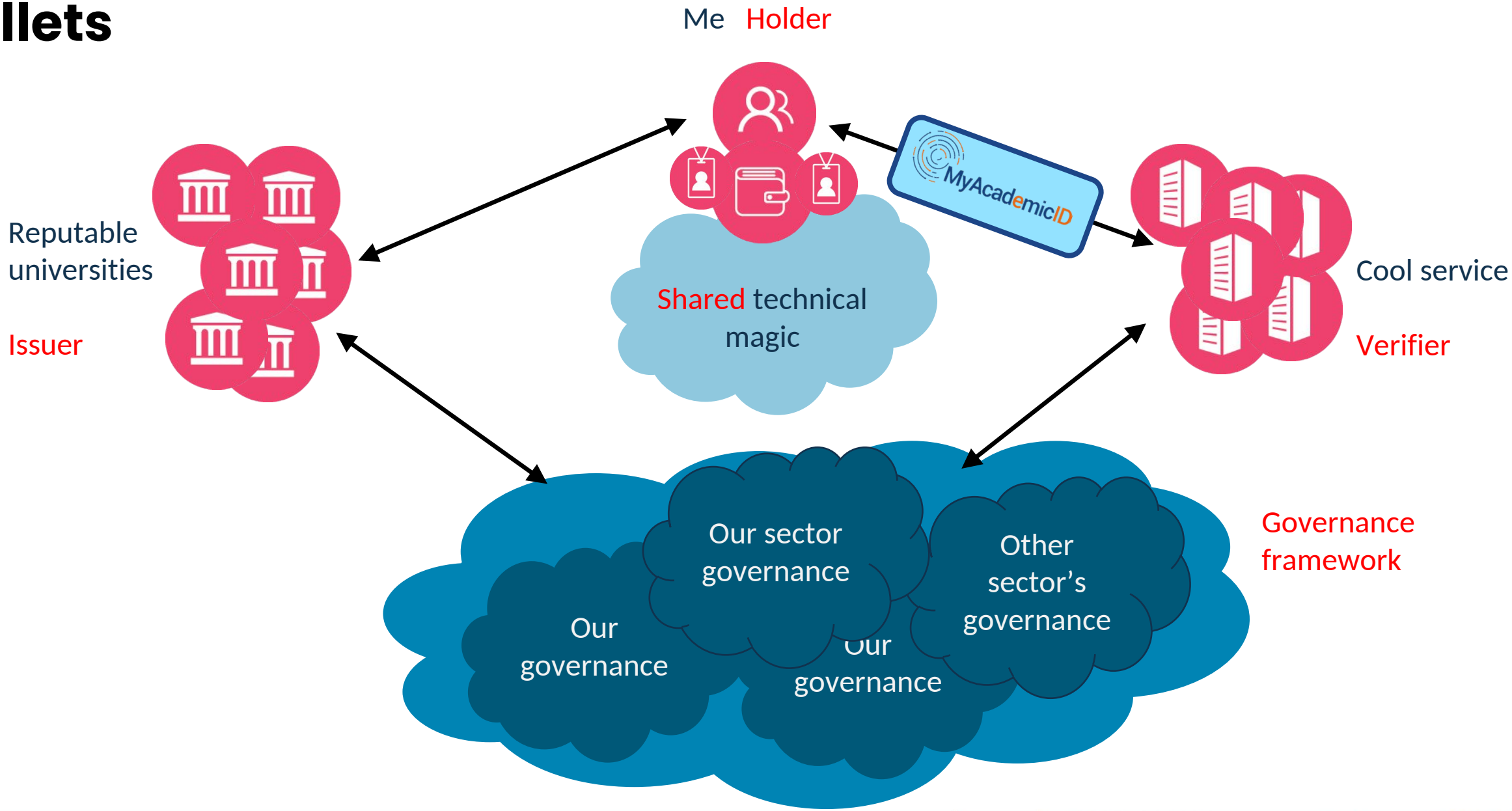
wallets

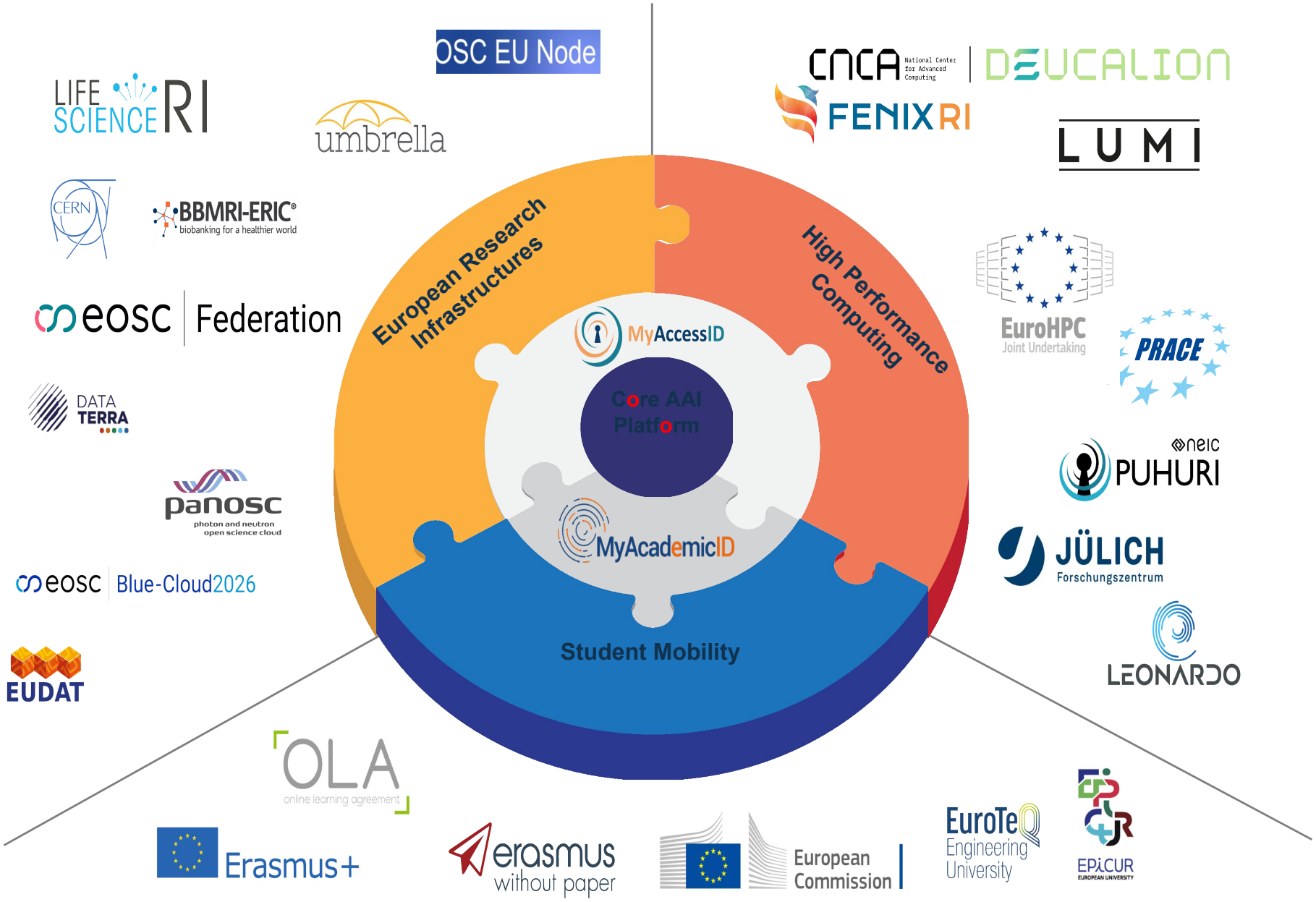

Me Holder
Reputable universities
Issuer
Shared technical magic
Cool service
Verifier
Our sector governance
Other sector's governance
Our governance
Our governance
Governance framework

wallets


Me Holder
MyAcademicID
Reputable universities
Issuer
Shared technical magic
Cool service
Verifier
Our governance
Our sector governance
Our governance
Other sector's governance
Governance framework

wallets


Me Holder
Reputable universities
Issuer
Shared technical magic
MyAcademicID
Cool service
Verifier
Our sector governance
Other sector's governance
Our governance
Our governance
Governance framework


OSC EU Node
LIFE SCIENCE RI
umbrella
CNCA National Center for Advanced Computing
DEUCALION
FENIX RI
LUMI
CERN
BBMRI-ERIC
biobanking for a healthier world
eosc Federation
European Research Infrastructures
High Performance Computing
MyAccessID
Core AAI Platform
MyAcademicID
Student Mobility
EuroHPC
Joint Undertaking
PRACE
DATA TERRA
panosc
photon and neutron open science cloud
neic
PUHURI
JÜLICH
Forschungszentrum
eosc Blue-Cloud2026
EUDAT
LEONARDO
OLA
online learning agreement
Erasmus+
erasmus without paper
European Commission
EuroTeQ Engineering University
EPICUR
EUROPEAN UNIVERSITY

“Without trust we don’t truly collaborate; we merely coordinate or, at best, cooperate. It is trust that transforms a group of people into a team.”

Stephen Covey

Conferenza GARR 2026

La forma del cambiamento

Pitanja?

Domande?

May tanong?

Questions?

Вопросы?

¿Preguntas?

有問題嗎？

سوالات

Grazie!

კითხვები?

प्रश्न

Fragen?

Questões?

Vragen?

Ebibuuzo?

Kysymyksiä

Maswali?

أسئلة

klaas.wierenga@geant.org