Secure Access Management with EGI Check-in: Latest Advancements and Future Direction

June, 2023

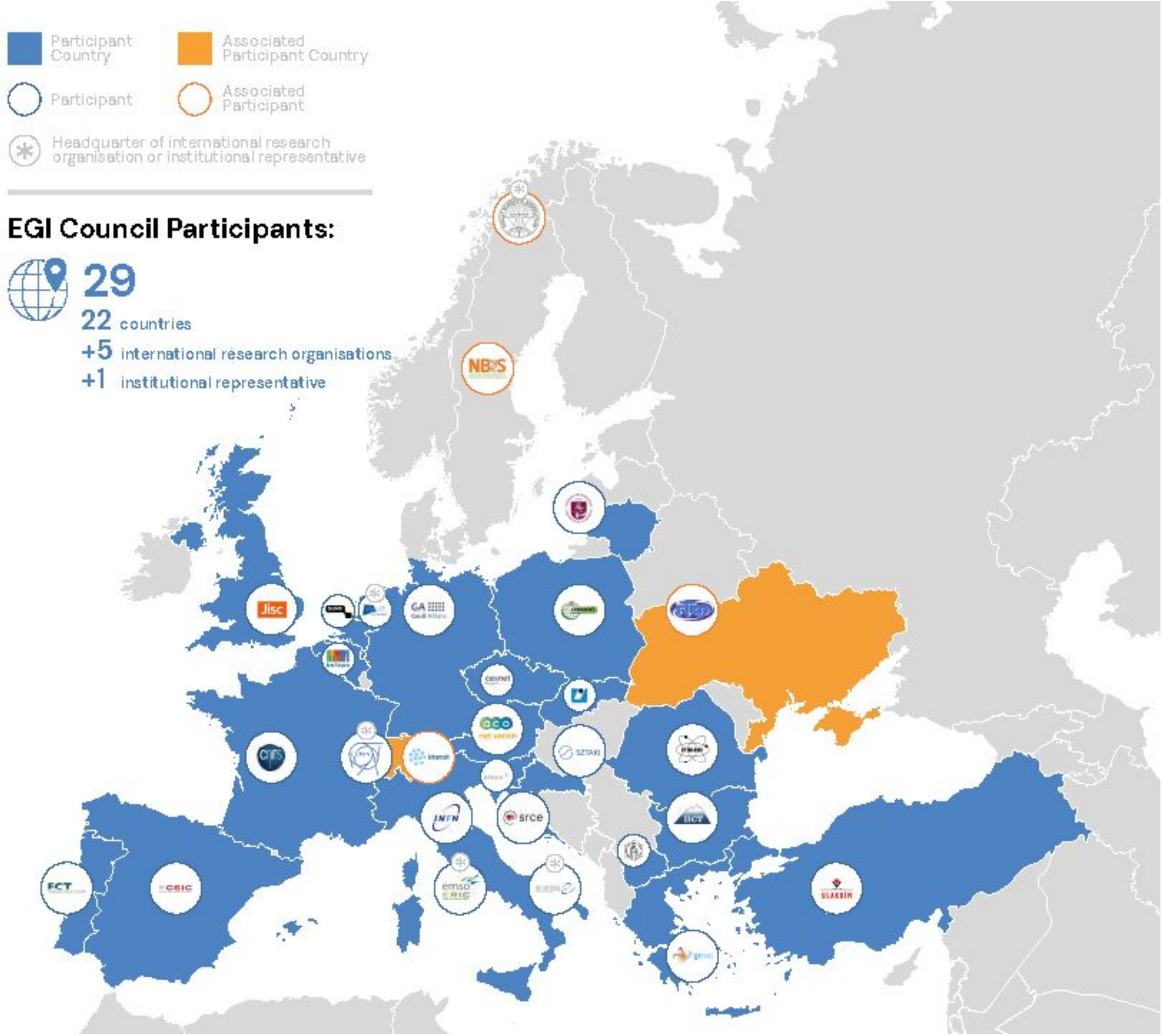
Nicolas Liampotis & Konstantinos Georgilakis (GRNET)
Valeria Ardizzone (EGI Foundation)

EGI in a Nutshell

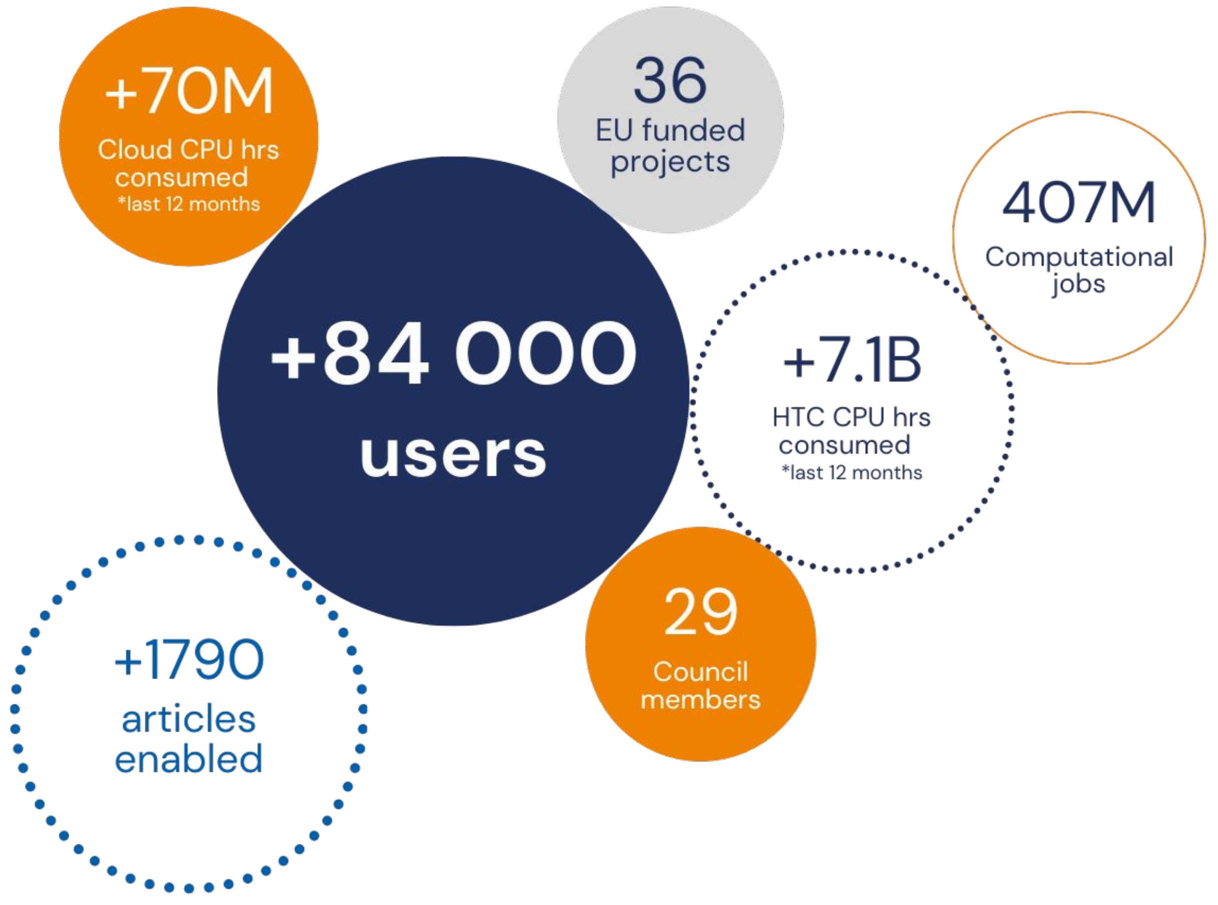
www.egi.eu

EGI Federation

A European flagship digital infrastructure for data-intensive scientific computing


Participant Country
Associated Participant Country
Participant
Associated Participant
Headquarter of international research organisation or institutional representative
EGI Council Participants:
29
22 countries
+5 international research organisations
+1 institutional representative
NBIS

EGI in numbers[1]



+70M Cloud CPU hrs consumed *last 12 months

36 EU funded projects

407M Computational jobs

+84 000 users

+7.1B HTC CPU hrs consumed *last 12 months

+1790 articles enabled

29 Council members

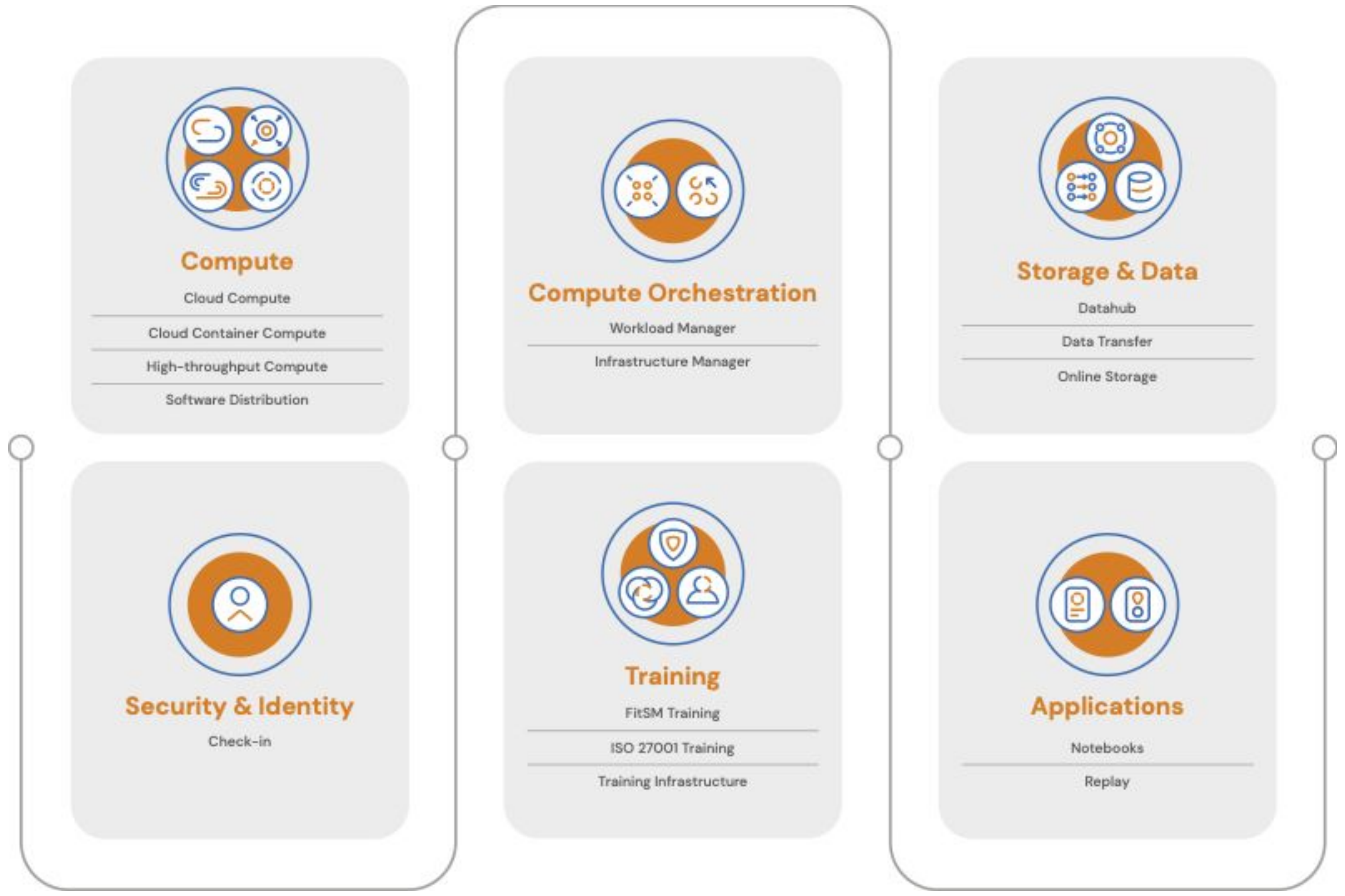
Why a federation?

- Support science at international scale
- Build an hyperscale facility for research
- Invest nationally, access globally
- Bring computing to the data

EGI Services

EGI delivers advanced computing services to support scientists, international projects, research infrastructures and businesses.

EGI services for research



Compute
- Cloud Compute
- Cloud Container Compute
- High-throughput Compute
- Software Distribution

Compute Orchestration
- Workload Manager
- Infrastructure Manager

Storage & Data
- Datahub
- Data Transfer
- Online Storage

Security & Identity
- Check-in

Training
- FitSM Training
- ISO 27001 Training
- Training Infrastructure

Applications
- Notebooks
- Replay

[1] the key numbers are correct as of June 2023. The are the key numbers based on 2022 Annual report

Check-in

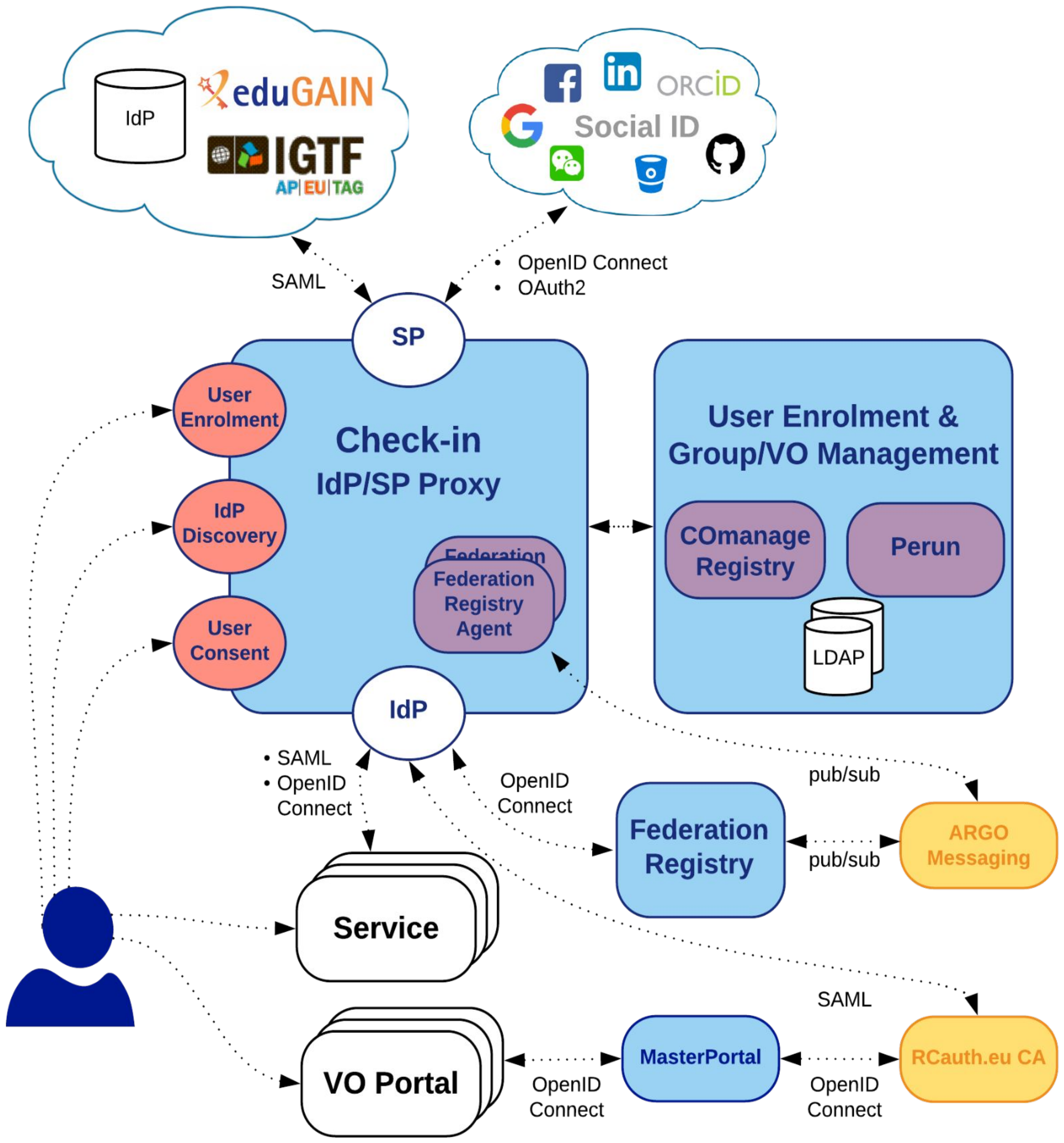
In a nutshell

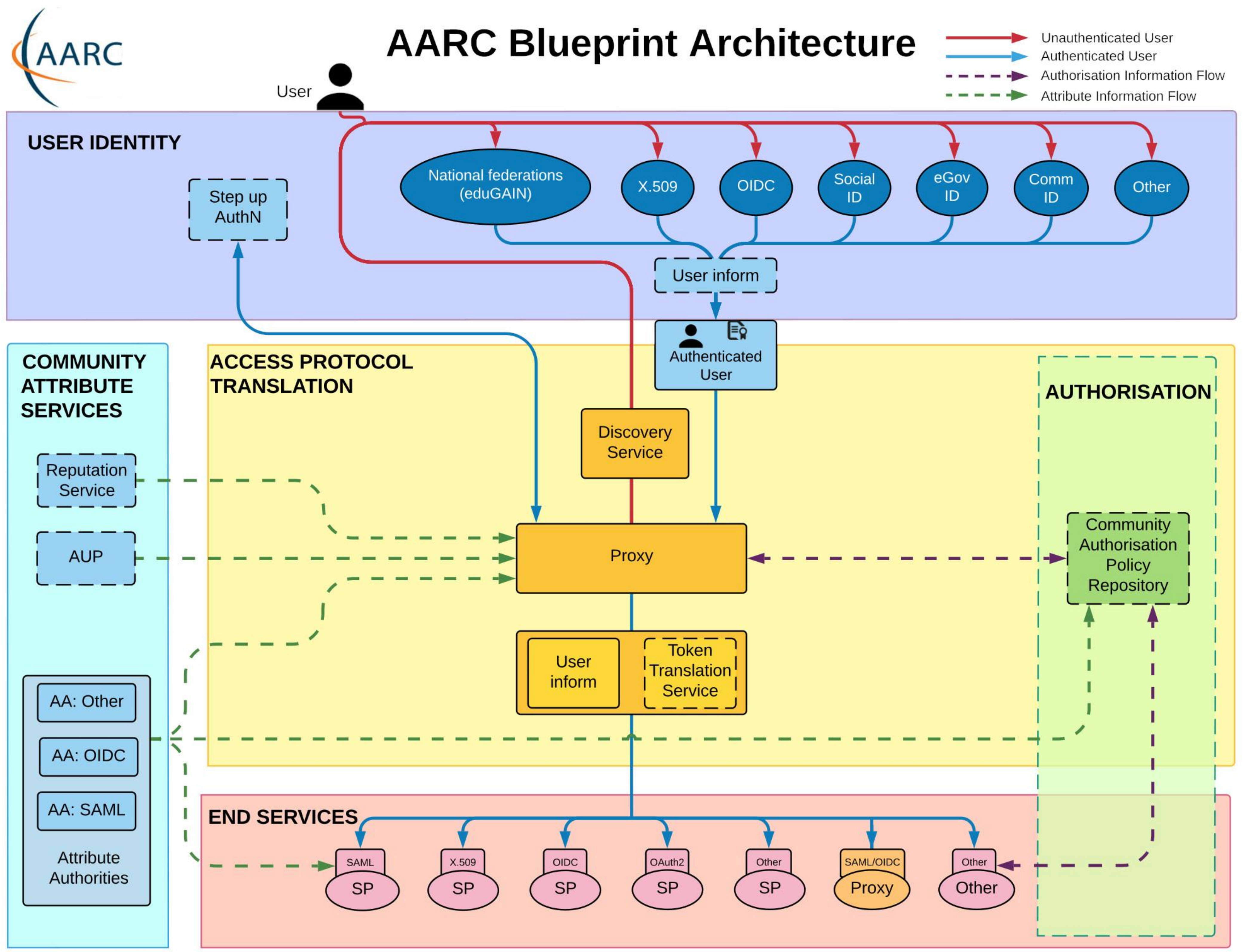
- Identity and Access Management solution that makes it easy to secure access to services and resources
- Single sign-on to services using existing credentials:
  - Academic (e.g. eduGAIN, ORCID)
  - Social media (e.g. Google, Facebook, LinkedIn)
  - Community-managed identities (e.g. Research Infrastructures)
- Federated access to multiple heterogeneous (web and non-web) services using different technologies (SAML, OpenID Connect/OAuth 2.0, X.509)
- Aggregation and harmonisation of authorisation information (groups, roles, assurance) from multiple sources
- Identity linking for accessing resources using different login credentials (institutional/social)
- Expressing the level of trust in the identity assertions (assurance)

Check-in

Architecture

Implementation of the AARC Blueprint Architecture





EOSC vision in a nutshell

What

EOSC is the European web of FAIR data and related services for research

Research data that is easy to find, access, interoperate and reuse (FAIR)

Trusted and sustainable research outputs are available within and across scientific disciplines

Why

Unlock the full potential of research data to accelerate discoveries and innovation

How

- **Ensure that Open Science practices and skills are rewarded and taught, becoming the ‘new normal’**
- **Enable the definition of standards, and the development of tools and services, to allow researchers to find, access, reuse and combine results**
- **Establish a sustainable and federated infrastructure enabling open sharing of scientific results**

Strategic Research and Innovation agenda (SRIA)
eosc.eu/sria-mar

eosc | Focus

Funded by
the European Union

From vision to implementation: “the EOSC federation”

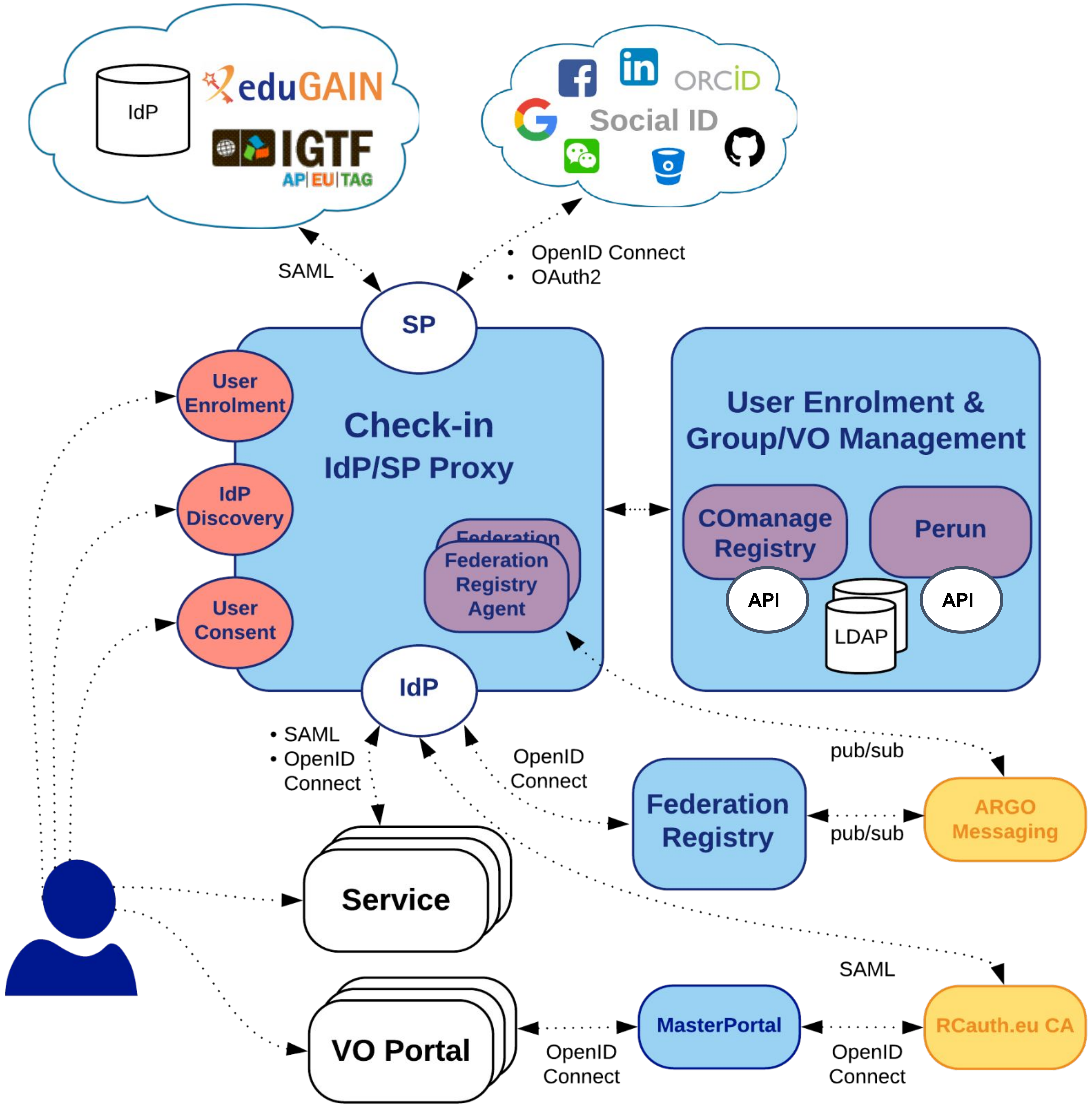
The EOSC vision is to set up a ‘Web of FAIR Data and Services’ for science in Europe. Central to this ambition is the deployment of a trusted, virtual, federation of existing infrastructures in Europe to store, share and reuse FAIR research outputs across borders and scientific disciplines also called the “**EOSC Federation**”.

- EOSC is **NOT** a new digital infrastructure
- The EOSC ambition is to **federate existing data, research and e- infrastructures** nodes to make them all **available to European researchers across borders and across disciplines** (distributed EOSC ´system of systems´)
- In doing so, **the federation will be augmented with new additional services and tools** that will enable the EU web of FAIR data and related services (EOSC can be seen as a thin federation layer based on FAIR principles)
- The federation will provide **coordinated entry points primarily for researchers in Europe (the so called “nodes”)** to find and access FAIR data and interoperable services that address elements of the whole research cycle (from discovery and mining to storage, management, analysis, publication, and re-use)
- **The entry points for EU researchers will be via their traditional channels** (e.g. via the national, regional, pan-European or thematic infrastructure nodes they are currently using) **or via the EU EOSC node central instance** (for the researchers that do not have existing access channels in place)
- **EOSC rules of participation and access policies** will be developed for the users and providers of the federation

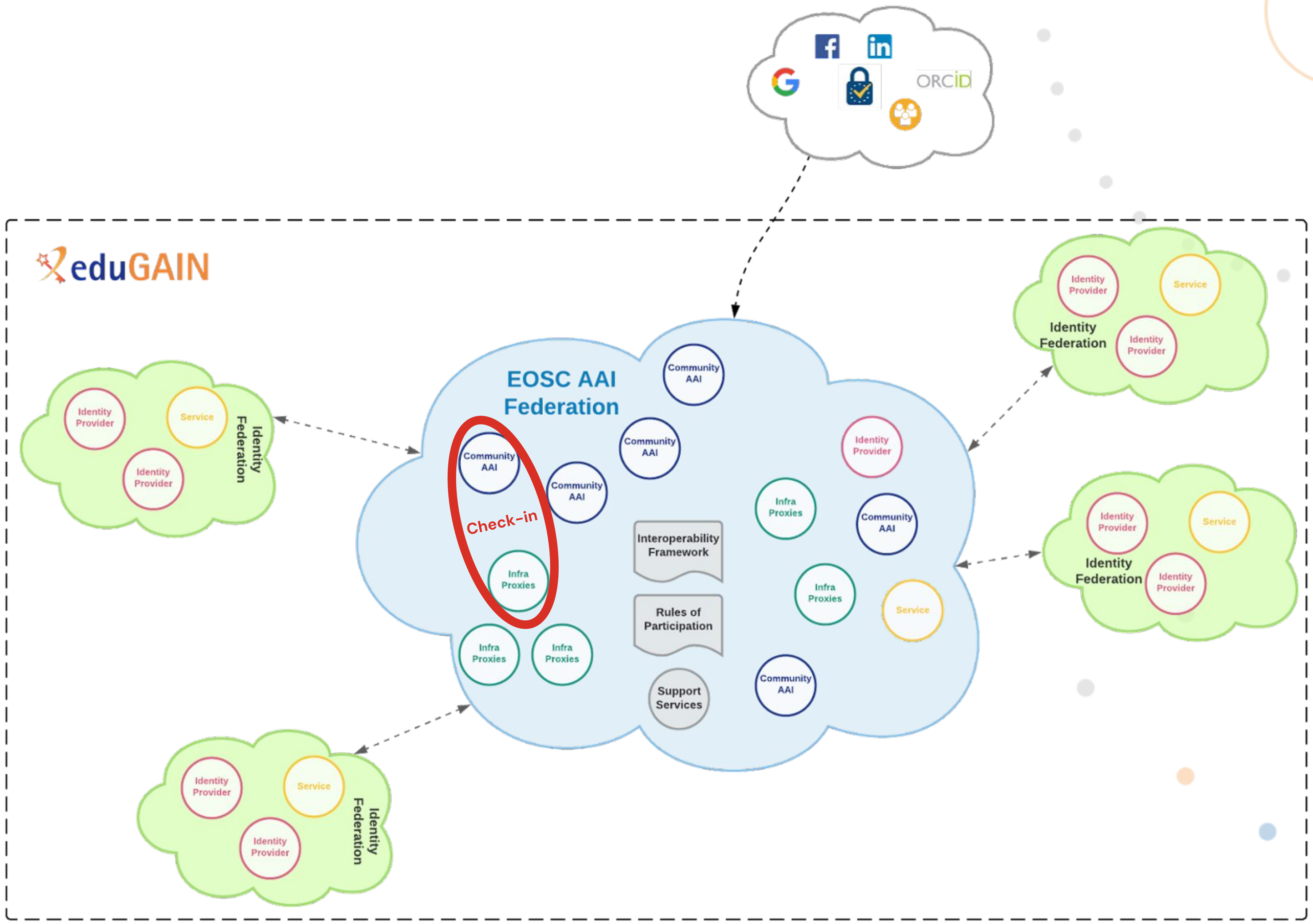
eosc Focus
Funded by the European Union

Check-in

Architecture



Interoperability with EOSC AAI Federation



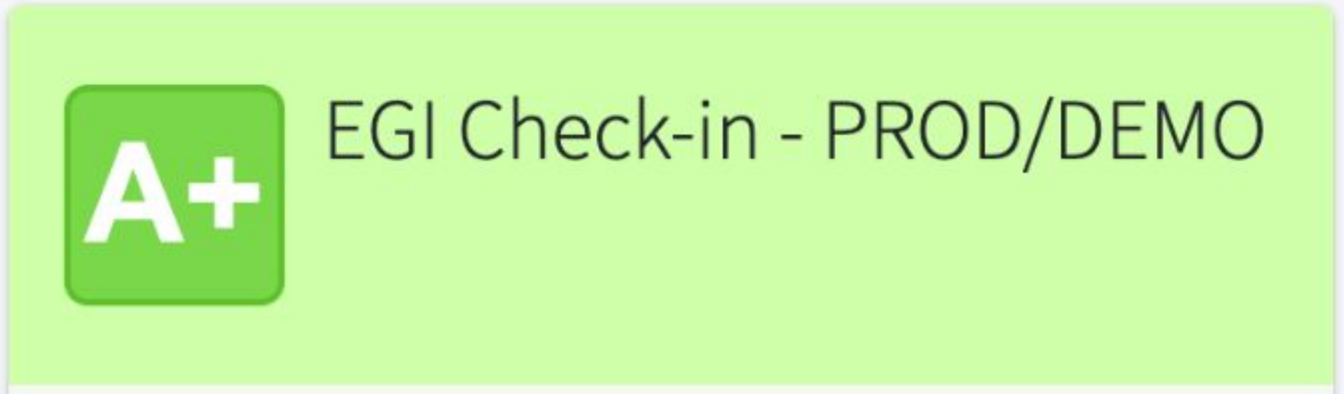
Latest advancements

Federated AuthN/AuthZ with Keycloak

Keycloak

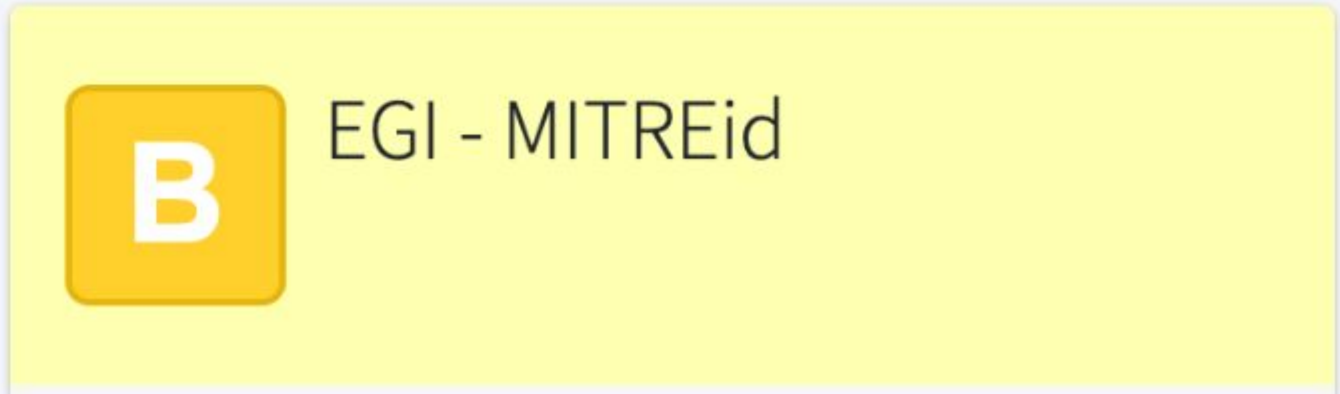
Improved compliance with OpenID Connect / OAuth 2.0 standards

- **Completed Phase I of Keycloak migration**
  → Keycloak as OpenID Provider for OIDC relying parties and OAuth 2.0 clients/protected resources
  - Improved compliance with OIDC, SecBCP, RFC6749, RFC6750, RFC8628, RFC7636, RFC6819, RFC7523


A+ EGI Check-in - PROD/DEMO

4,2%

Fail rate


B EGI - MITREid

20,2%

Fail rate

Keycloak Enhancements

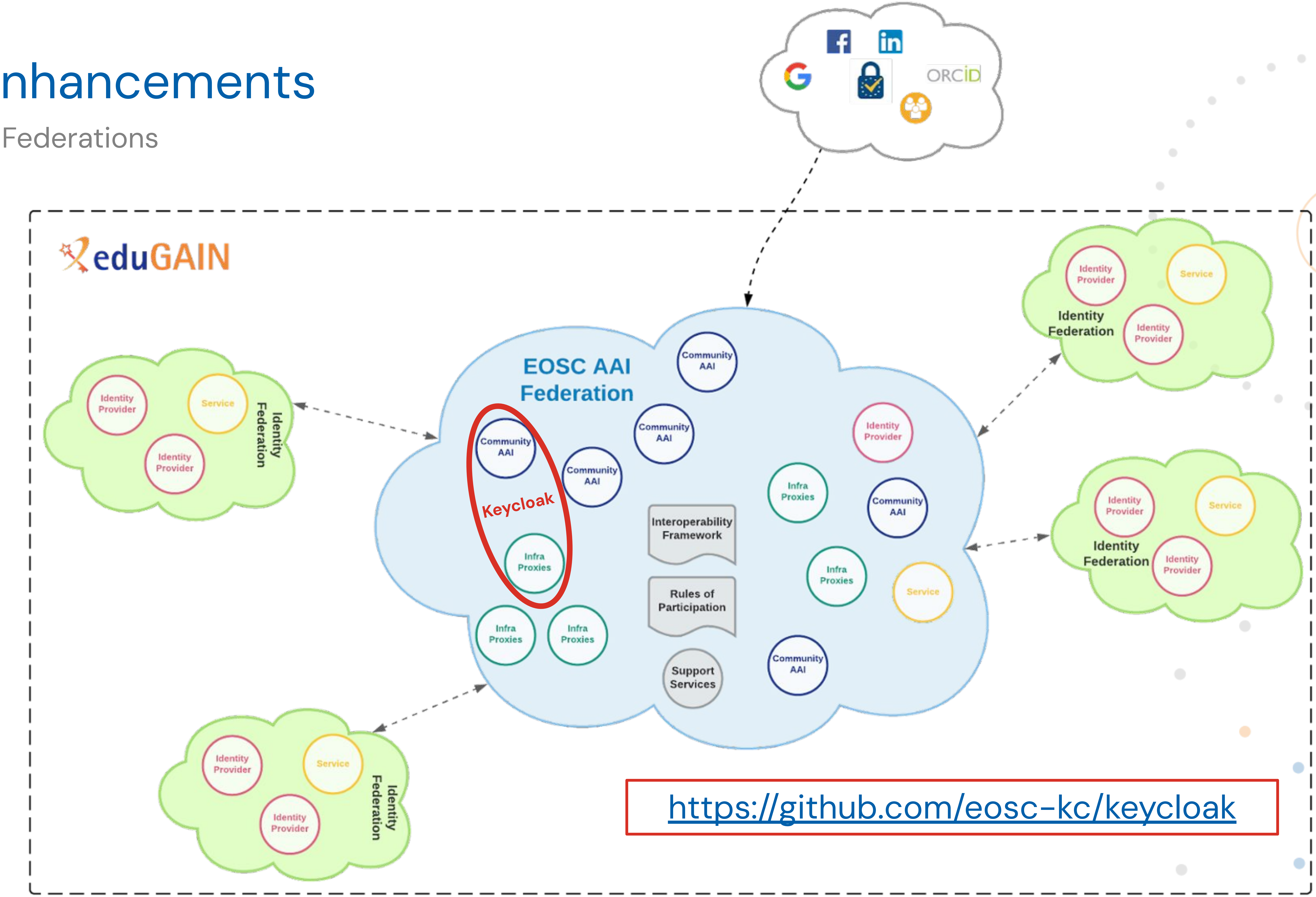
- Support for SAML Federations
- Advanced Group Management
- New OpenID Connect / OAuth 2.0 flows

Keycloak Enhancements

Support for SAML Federations

- Support for **SAML IdP Federations** (e.g. 5400+ IdPs from eduGAIN)

- Support for **SAML SP Federations** (e.g. EOSC AAI Federation)



https://github.com/eosc-kc/keycloak

Keycloak Enhancements

Support for SAML Federations

- Challenge
  - Upstream Keycloak reluctant to accept current implementation:
    - Enterprise use cases assume low number of IdPs
    - Requires lots of changes (including account/admin console) for handling large number of IdPs

Keycloak Enhancements

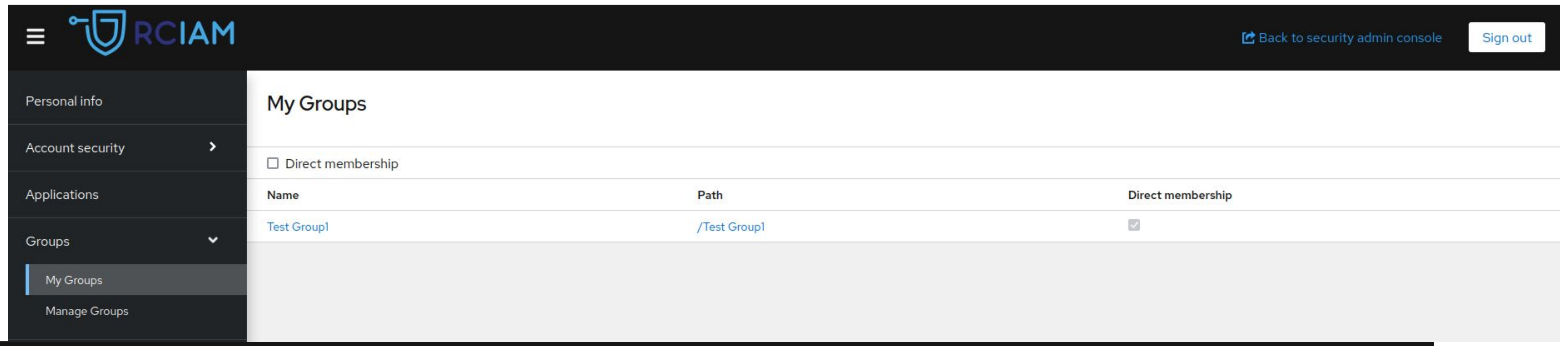
Advanced Group Management

https://github.com/rciam/keycloak-group-management

- User-driven group enrollment flows:
  - Users can request membership in groups
    - Accept group Terms & Conditions
    - Provide comment/justification
  - Membership requests are reviewed by group managers
  - Multi-group enrollment flows

- Time-based group membership:
  - Automatic expiration of group membership beyond a configurable time period after joining the group
  - Membership renewal process

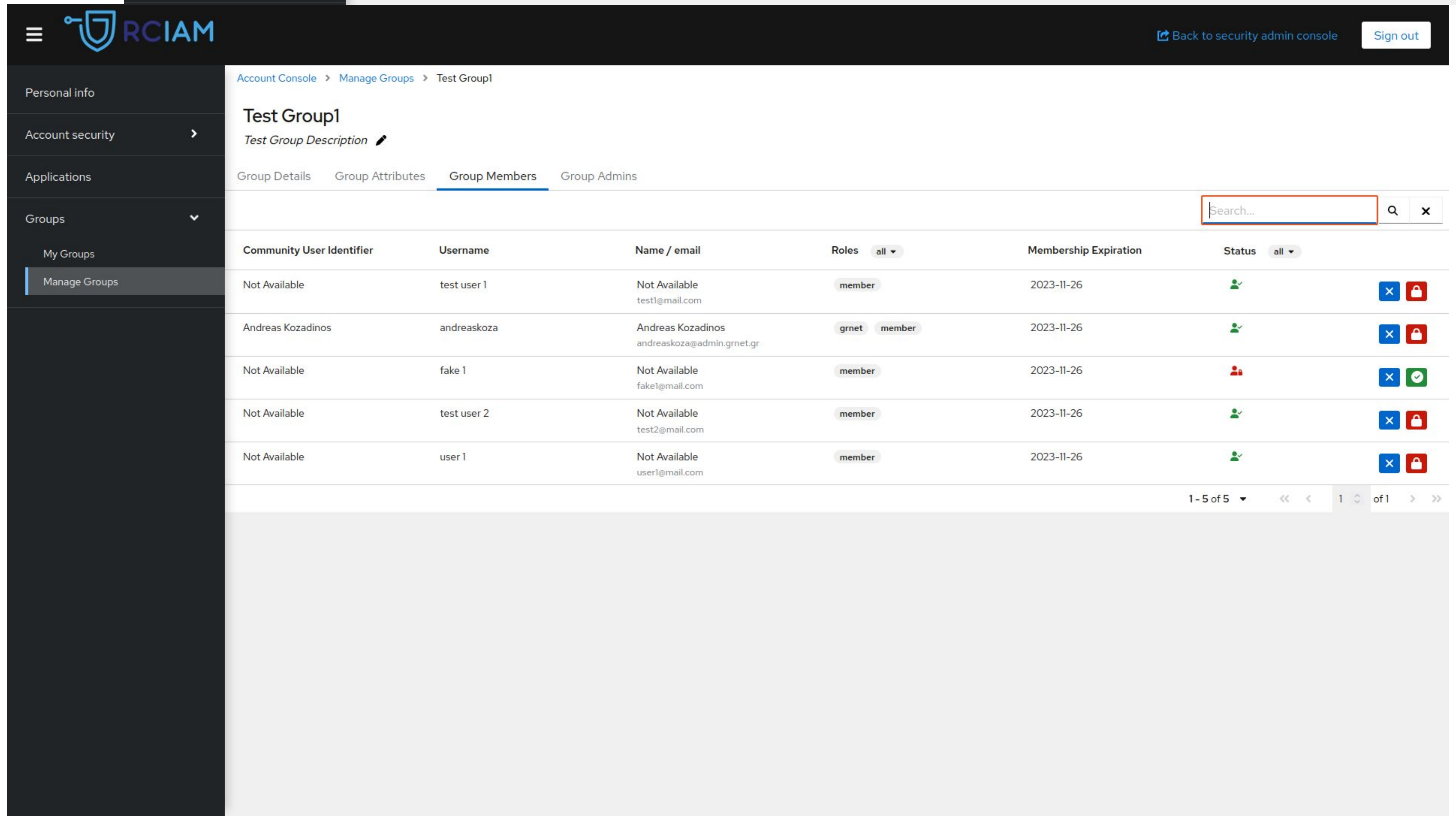
- Roles within groups



My Groups

□ Direct membership

Name	Path	Direct membership
Test Group1	/Test Group1	☑



Account Console > Manage Groups > Test Group1

Test Group1

Test Group Description

Community User Identifier	Username	Name / email	Roles all	Membership Expiration	Status all
Not Available	test user 1	Not Available test1@mail.com	member	2023-11-26	
Andreas Kozadinos	andreaskoza	Andreas Kozadinos andreaskoza@admin.grnet.gr	grnet member	2023-11-26	
Not Available	fake 1	Not Available fake1@mail.com	member	2023-11-26	
Not Available	test user 2	Not Available test2@mail.com	member	2023-11-26	
Not Available	user 1	Not Available user1@mail.com	member	2023-11-26	

1 - 5 of 5 1 of 1

Keycloak

New OpenID Connect / OAuth 2.0 flows

- **Resource Indicators for OAuth 2.0** (RFC8707) for allowing clients to signal to the authorization server where they intend to use the access token using the **“`resource`”** parameter
- **Remote OAuth 2.0 Proxied Token Introspection** from trusted external Authorization Servers (AARC-G052)
- Scope-based mechanism for allowing clients to **request specific Claim values** (e.g. to filter groups/roles)
- **Scope policies** for enabling control over whether the scope (e.g. **`compute.*`**) should be included in the access token requested by the client
- **OpenID Connect Federation** (OIDCFed) (PoC implementation)

Thank you

EGI Check-in

✉ check-in@egi.eu

www.egi.eu

This work is partially funded by the EU research and innovation programme