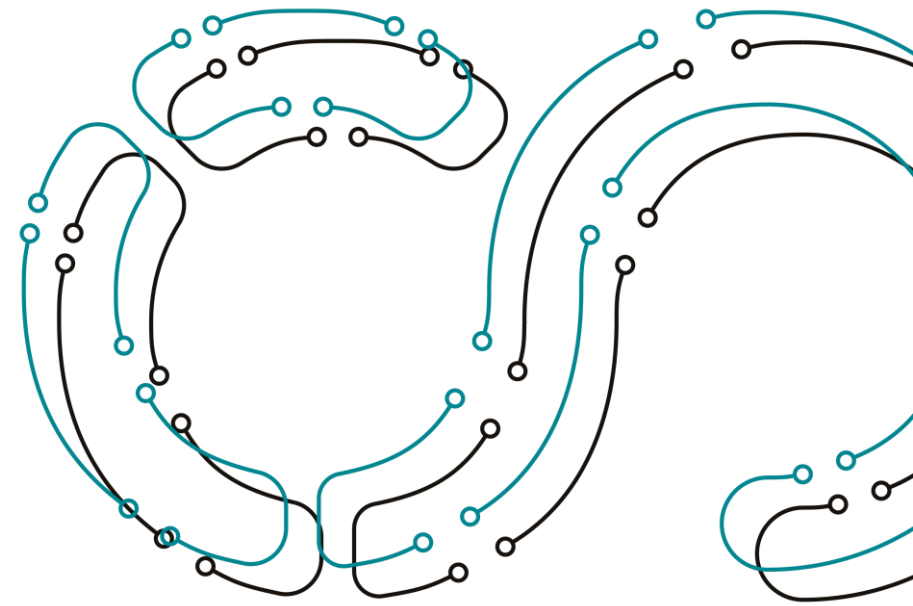


AAI Federating Capability

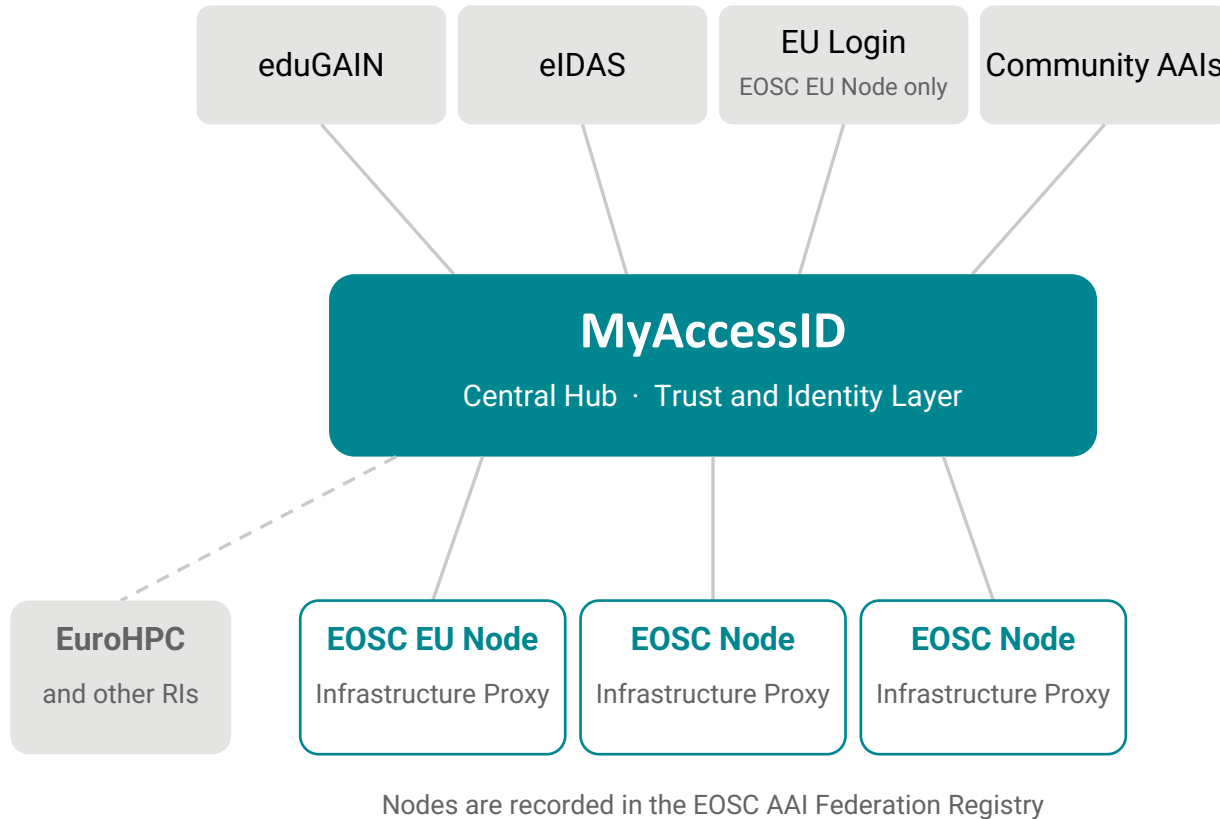
Christos Kanellopoulos

GÉANT | EOSC AAI Working Group



What the AAI Federating Capability is

One identity and trusted access across all EOSC Nodes



Single sign-on

Users sign in once, with the identity they already have.

Cross-Node workflows

Tokens issued in one Node are accepted by services in another.

Trust established once

Each Node connects to the Central Hub, not to every other Node.

Nodes stay in control

Access decisions remain with each Node and its services.

EOSC AAI Architecture 2025

The baseline that every EOSC Node implements

Goals

- Single sign-on across the EOSC Nodes
- Workflows that use resources across multiple Nodes

Design principles

- The minimum set of requirements
- The simplest possible component configuration
- Implementable with today's technology

Key decisions

- MyAccessID as the Central Trust Hub and Identity Layer
- OpenID Connect and OAuth 2.0 as the core protocols
- Complexity should not be kept away from the end services

14 EOSC Nodes at the production launch

Connected to the EOSC AAI production environment

14

EOSC Nodes in
production

11 first wave
3 second wave

FIRST WAVE

EOSC EU Node

BBMRI-ERIC

CERN

Data Terra

EUDAT

European Digital Twin
Ocean

Finland

Italy

PaNOSC

Poland

Slovakia

SECOND WAVE · SEQUENCE 1

Czechia

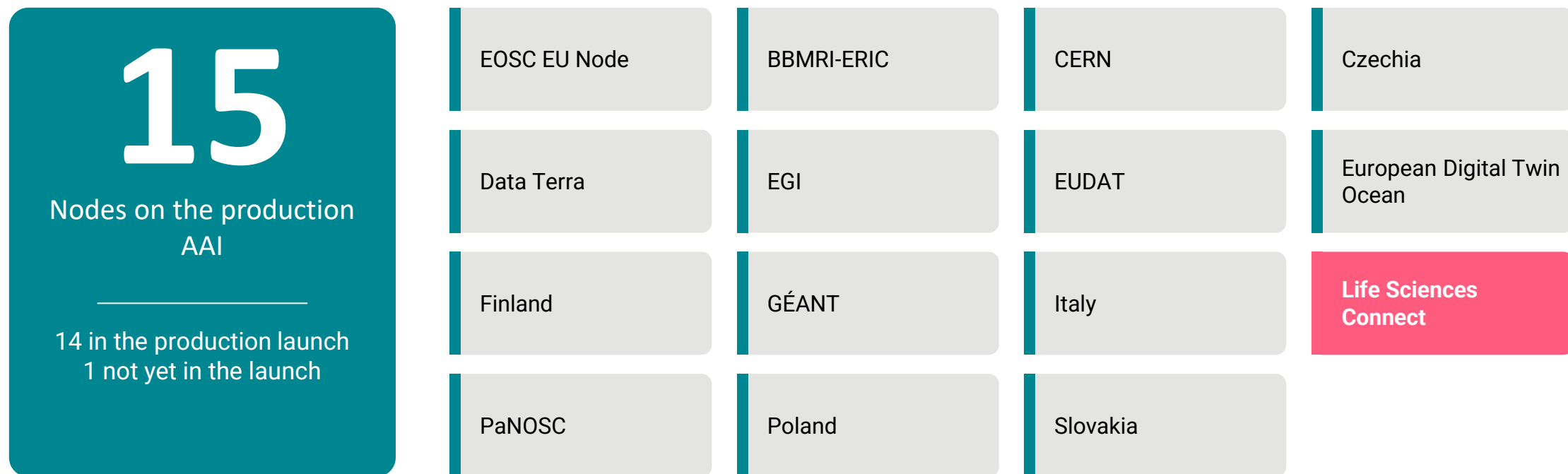
EGI

GÉANT

Onboarding continues: second wave sequence 2 (Sep–Dec 2026) and sequence 3 (Jan–Apr 2027) are connecting through the testing environment.

15 EOSC Nodes connected to the production AAI

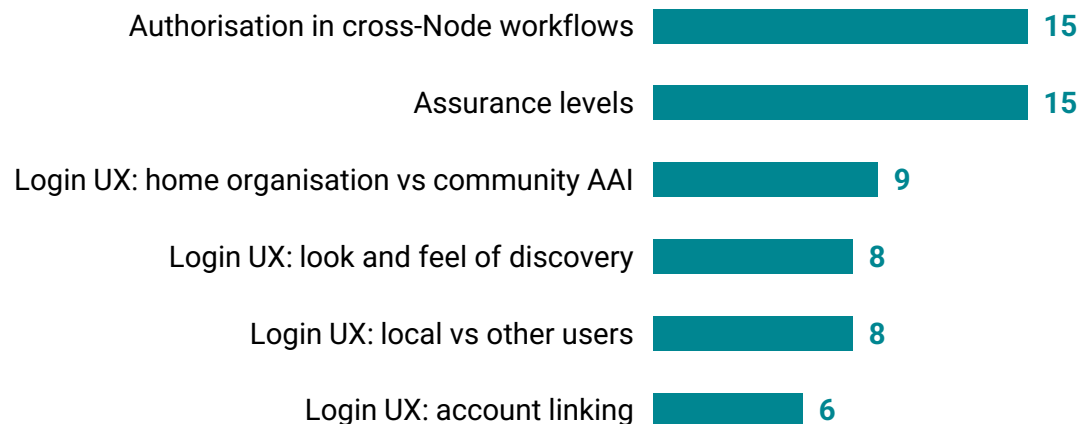
The production launch Nodes, plus Life Sciences Connect



-  Part of the production launch of the EOSC Federation
-  Connected to the production AAI, not yet part of the production EOSC Federation

EOSC AAI Architecture 2026

Where we go next: priorities set by the Nodes



Priority score: 3 × high + 2 × medium + 1 × low votes

1

Authorisation

What the AAI conveys, and who decides

2

Common login experience

One recognisable sign-in journey

3

MFA and identity assurance

Consistent levels across the Federation



Dec 2026

Draft final



Q1 2027

Published

Authorisation in cross-Node workflows

Theme 1 · EOSC AAI Architecture 2026

Authorization across the EOSC Federation is multi-faceted. A team has an allocation of Resources. A home organisation gives information about the affiliation of its personnel. A Resource can also have conditions for access. The EOSC AAI supplies the information that each Node uses to make access decisions that agree with the policies of its Resources.

The EOSC AAI conveys claims about the User

Identity information, affiliations, group memberships and level of assurance.

Nodes and services take the decisions

Each according to its own policies, mandate and obligations.

Allocation and accounting stay outside the EOSC AAI

The EOSC AAI enables project approval, project management and credit management, but does not deliver these capabilities.

A common login experience

Theme 2 · EOSC AAI Architecture 2026

Users should recognise the same sign-in journey at whichever Node they enter the Federation.

1 Home organisation or community AAI

When users sign in through their home organisation, and when through a community AAI.

2 Discovery

A consistent look and feel for choosing an identity provider at every Node.

3 Local and other users

Login flows for the users of the Node itself and for users from the rest of the Federation.

4 Account linking

How users link more than one identity to their account.

Resources need to know how strongly a user was authenticated and identified, in the same way at every Node.

Multi-factor authentication

- Signal MFA in the same way across Nodes (REFEDS MFA Profile)
- Let services require MFA for sensitive resources
- Cover users whose home organisation does not offer MFA

Identity assurance

- Common assurance levels across the Federation (REFEDS Assurance Framework)
- Conveyed as claims; Nodes and services decide what they require
- Paths for users to raise their level of assurance

eosc Looking ahead: OpenID Federation

From the Central Hub towards a dynamic, full-mesh federation

Today

Hub-and-spoke through MyAccessID, on OpenID Connect and OAuth 2.0

Pilot

An OpenID Federation Trust Anchor in the testing environment, with Node proxies as members

Target

A full-mesh, dynamic EOSC AAI Federation on OpenID Federation

Standards ready

OpenID Federation 1.0 final (early 2026); AARC-G100 profile for proxies (draft)

Pilot under way

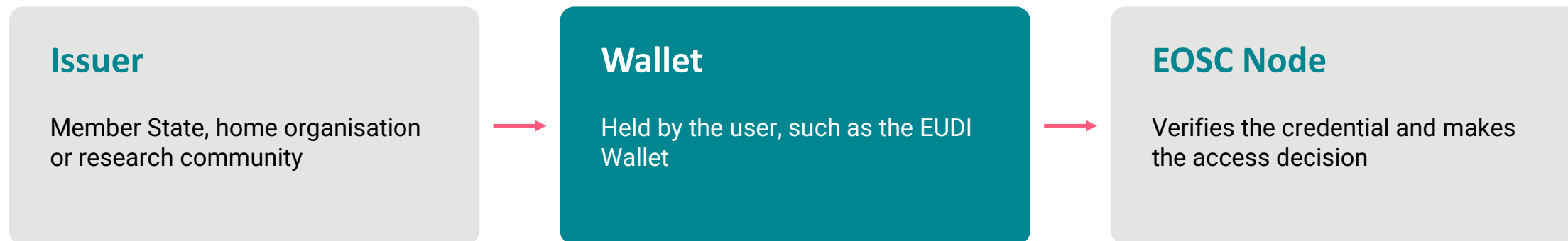
Launched September 2026 with testing instances of EOSC Nodes

Why it matters

Trust without a central component; flexible, scalable topologies

Looking ahead: wallet-based access

Users presenting verifiable credentials to EOSC Nodes



Trust layer: OpenID Federation can establish trust between issuers, wallets and verifiers

- Identity, affiliation and assurance as credentials the user holds
- OpenID for Verifiable Presentations builds on the OAuth 2.0 and OpenID Connect foundations the EOSC AAI already uses
- Next step: explore with AARC how wallets complement eduGAIN and MyAccessID

Q&A

Thank you

