



Enabling access to EOSC and EuroHPC

MyAccessID, the federated identity layer
for research in Europe

Christos Kanellopoulos, GÉANT

NDN2026

Why an identity layer

European researchers work across infrastructures that are operated by different organisations, funded through different instruments and governed under different national policies. Each of them needs to know who the user is, and to trust that answer.



Many services, one person

A single research workflow may touch an EOSC Node, a EuroHPC system, a national data service and a community platform. Without a shared identity layer, each one enrolls the user separately.



Trust is the hard part

Infrastructures need more than a login. They need to know how the identity was verified, whether a second factor was used, and which resources the user is entitled to reach, in the web, from the API and at the terminal.



eduGAIN is the foundation

eduGAIN gives institutional identities global reach and a trust framework every infrastructure can rely on. MyAccessID builds on it, adding the consistent identifiers, standard attributes, assurance and authorisation that research infrastructures need across their services.

One trusted identity



MyAccessID is the GÉANT service that gives the European research community a single, trusted way to authenticate and access the infrastructures they rely on. It is built on the GÉANT Core AAI Platform and follows the AARC Blueprint Architecture.



Use your existing login

Researchers sign in with the credentials they already have, through eduGAIN and other trusted identity providers. No new accounts and passwords for each service.



One identity, everywhere

Each user keeps one consistent identity, with a persistent common identifier across every connected service.



Sign in once

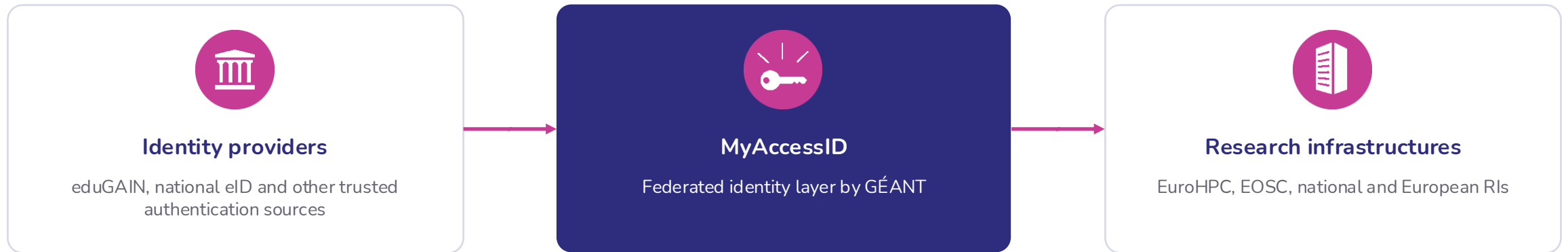
A single sign-on carries researchers seamlessly between services, across organisations and countries.



Serving **EuroHPC**, **EOSC** and national and European research infrastructures, on the same platform and the same identity.

How it works

MyAccessID acts as a proxy between identity federations and the research infrastructures connected to it, handling the complexity of cross-domain authentication on everyone's behalf.



What MyAccessID handles

- Authentication with existing credentials, with no new accounts.
- A persistent, common identifier that stays consistent across every service.
- A standardised set of user attributes, released to connected services.
- Only the data a service actually needs is shared, protecting user privacy.

What it offers

For research infrastructures

- Single sign-on across identity providers from eduGAIN and other trusted sources.
- Multi-protocol support for OpenID Connect, OAuth 2.0 and SAML.
- A standardised attribute set, as defined in the MyAccessID Attribute Specification.
- A persistent, common user identifier across every connected service.
- Higher-assurance options: multi-factor authentication and identity validation, live for EuroHPC today.

For researchers

- Use the login you already have, through the national academic federations and eduGAIN.
- One identity everywhere: the same consistent identity across every connected service.
- Sign in once, then move seamlessly between research infrastructures and their services.
- No one is left behind: options for researchers without an academic federated identity, such as industry users.

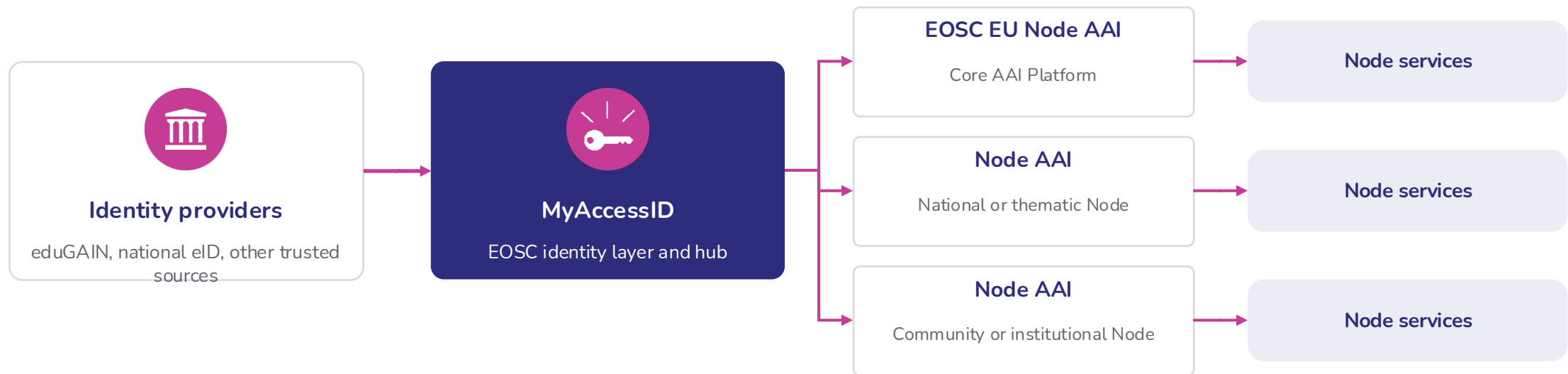
EOSC

One identity layer for a federation of Nodes



EOSC AAI Architecture 2025

EOSC is a federation of Nodes, each with its own services and its own AAI. The architecture connects them through a common identity layer, so that a researcher signs in once and is known consistently across every Node.



Design decisions that make the federation work

- **Hub and spoke.** Nodes connect their AAI to MyAccessID rather than to each other, so trust is established once.
- **OpenID Connect and OAuth 2.0** as the core protocols, with token introspection for services and cross-Node workflows.
- **Node AAI**s are **AARC infrastructure proxies.** The EOSC AAI conveys claims; each Node decides access under its own policy.
- **Logic moves out of the proxies.** Identity, assurance and attributes are consistent because they come from one place.

The EOSC EU Node in practice



The EOSC EU Node is the first Node of the federation and the reference for the others. Its AAI is built on the GÉANT Core AAI Platform and connects to MyAccessID as its identity layer.



One login for every EU Node service

Users authenticate once, through MyAccessID, and move across the EU Node services with a single session and a single, persistent identifier.



Authorisation stays with the Node

The EOSC AAI conveys claims and takes no access decision. The Node links approved Projects to Groups, evaluates its own policy, and its Infrastructure Proxy mints the resulting capabilities.



Ready for cross-Node work

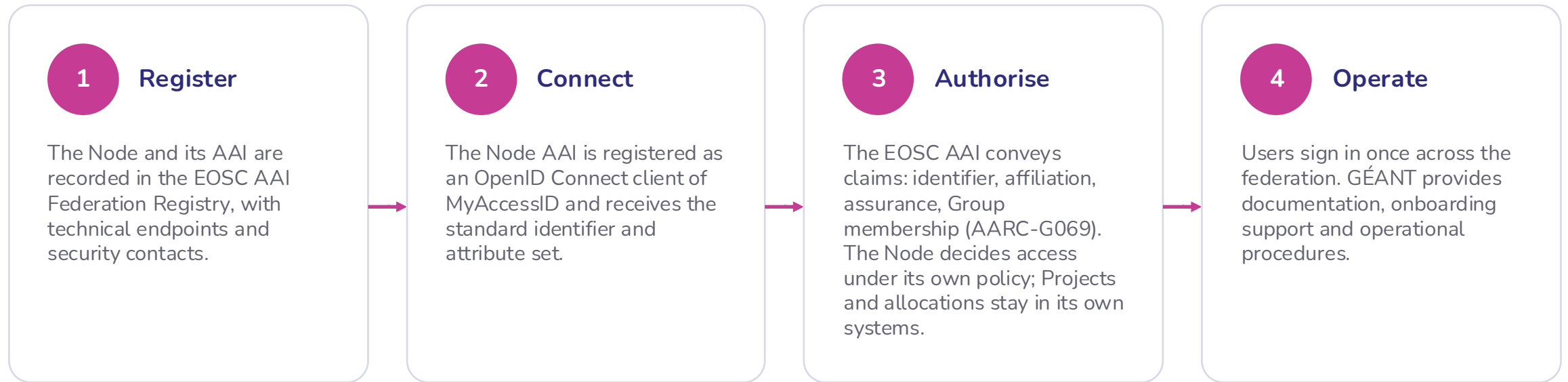
Because every Node sees the same identifier and attribute set, a workflow that spans Nodes can carry the user's identity with it.



The same team and the same platform operate the EU Node AAI and the EuroHPC Federation Platform AAI.

Joining as an EOSC Node

The onboarding path is the same whether a Node is national, thematic or institutional. The Node keeps its AAI; it connects it to the identity layer and registers in the federation.



For NRENs building or hosting a Node, the Core AAI Platform is also available as the Node AAI itself, not only as the hub.

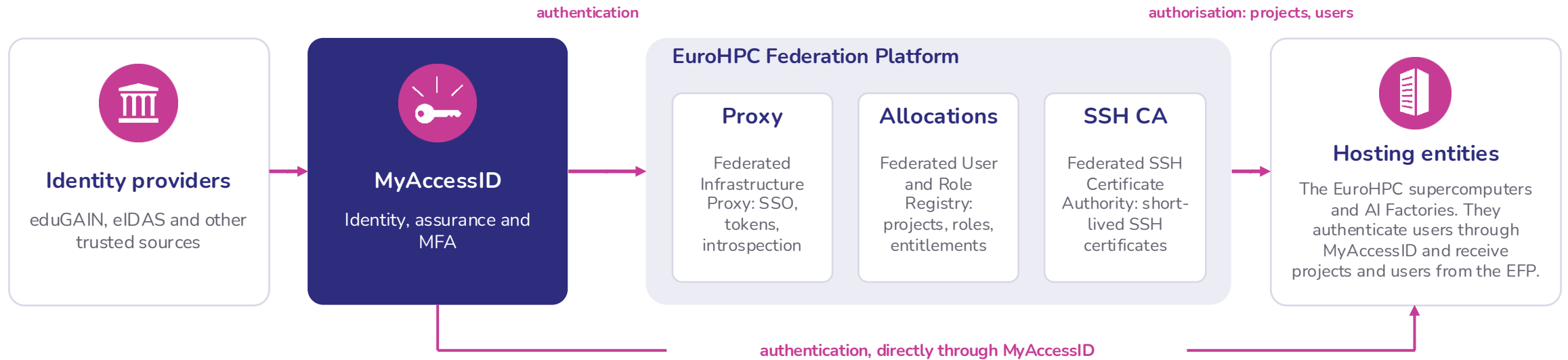
EuroHPC

One identity from the portal to the terminal



EuroHPC Federation Platform

The EuroHPC Federation Platform (EFP) is the single entry point to the EuroHPC systems operated by the hosting entities. Both authenticate users through MyAccessID; the EFP provisions projects and users to the hosting entities.

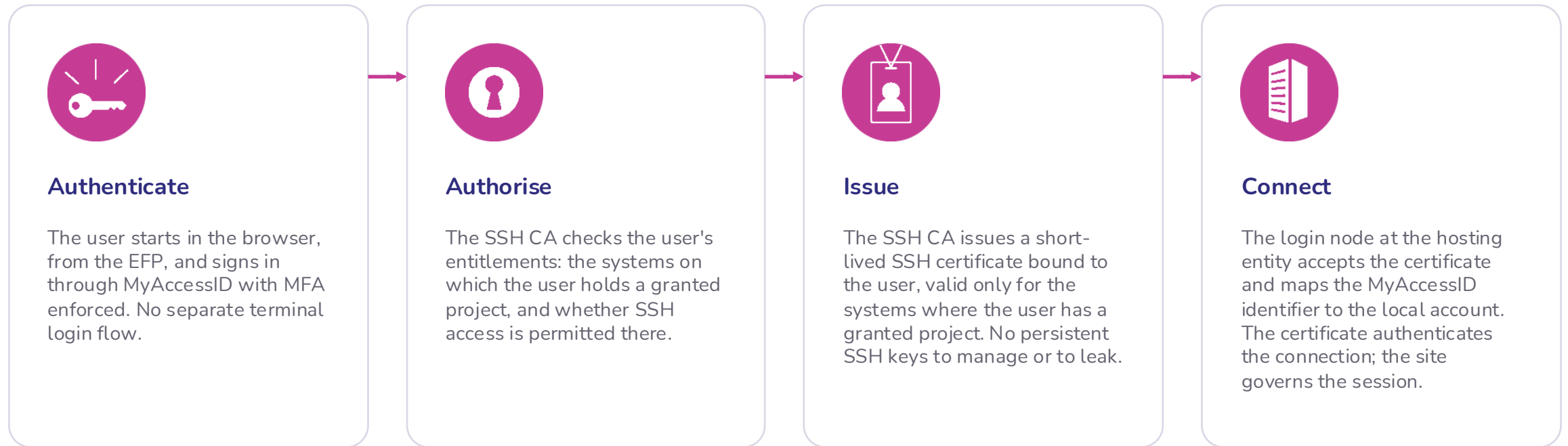


How access is decided

- **Identity from MyAccessID.** The EFP and every hosting entity receive the same persistent identifier, attributes and assurance and MFA signals.
- **Permissions from the EFP.** Projects and users are provisioned to the hosting entities; entitlements encode the resource and the permitted action.
- **Tokens are validated, not parsed.** Services call the FIP introspection endpoint; tokens are audience-bound, short-lived and revocable.
- **Zero trust between components.** Every EFP component holds its own service account and is limited to what its function needs.

From the web to the terminal

HPC users live in a shell. The same federated identity that signs them into the portal has to get them onto the login nodes, with the same policies enforced.



Terminal access now enforces the same identity, assurance and authorisation policies as web and API access.

Assurance for HPC



Live today on the EuroHPC Federation Platform: MyAccessID enforces MFA and passport verification for every user. From 2027, the home identity provider can take over.



Multi-factor authentication

Today MyAccessID enforces its own second factor for every EuroHPC user, whatever the home identity provider does. In 2027 it adds support for REFEDS MFA signalling: when the home identity provider asserts MFA, MyAccessID accepts it and does not prompt again.



Identity validation

Today every EuroHPC user is verified through an online check of a biometric passport. In 2027 MyAccessID adds two further paths: the REFEDS Assurance Framework, so that a home identity provider that asserts a verified identity is trusted, and eIDAS electronic identities.



Anyone can access

Researchers without an academic federated identity, for example from industry, still get a MyAccessID: through other connected identity providers, national digital identity systems or guest provisioning. They pass the same MFA and identity validation as everyone else.

Two Pan-European use cases

One MyAccessID: what EOSC and EuroHPC share

MyAccessID as the identity layer · AARC Blueprint Architecture · OpenID Connect and OAuth 2.0 · persistent identifier and standard attributes · authorisation owned by the platform proxy · token introspection · entitlements in AARC format · the same platform and team

EOSC: allocation is local to each Node

- **Autonomous Nodes.** Each Node runs its own Infrastructure Proxy, its own policies and its own Resource Allocation System.
- **No central allocation.** A team applies to every Node whose Resources it needs; each Node approves Projects under its own process.
- **Groups live in Community AAls.** Membership is managed once, in the team's Community AAl, and conveyed to every Node as claims.
- **The Node decides.** The Infrastructure Proxy local to the Resource links Projects to Groups and mints the capabilities.

EuroHPC: allocation is central, in the EFP

- **Hosting entities look like Nodes.** Each authenticates users through MyAccessID and enforces access on its own systems.
- **One platform allocates across the federation.** The EFP holds the Projects and users and provisions them to the hosting entities.
- **One entry point, one authorisation model.** The FIP and FURR carry the entitlements; no per-site application process for the user.
- **Non-web access is first class.** SSH certificates from a federated CA, bound to the user and to granted projects, with MFA and identity validation mandatory.

What NRENs and IdPs can do

The identity layer is only as good as the identities behind it. Most of what makes access to EOSC and EuroHPC smooth is decided at the home organisation and the national federation.



Release the attributes

Support the attribute set in the MyAccessID Attribute Specification, so that users arrive with a name, an affiliation and a stable identifier rather than an empty profile that has to be completed by hand.



Signal MFA and assurance

Implement the REFEDS MFA profile and the REFEDS Assurance Framework. From 2027, when the home IdP signals them, MyAccessID accepts them instead of adding its own factor or its own identity check, and the user gets one prompt instead of two.



Keep the federation healthy

Sirtfi and up-to-date security contacts, eduGAIN registration for every IdP researchers actually use, and a path for guest and industry users through national eID where it exists.



NRENs are also Node operators and hosting entities. The Core AAI Platform is available to them for both roles.

What comes next



MFA and identity validation

Enforced by MyAccessID for EuroHPC today. In 2027: REFEDS MFA and REFEDS Assurance signalling from the home IdP, eIDAS for identity validation, and availability to all connected services.



OpenID Federation

Evolving the EOSC AAI from hub and spoke towards dynamic, policy-driven trust between Nodes, with MyAccessID as trust anchor.



EUDI Wallet

eIDAS 2.0 wallets as a further source of verified identity, first for identity validation, then as a login option.



More infrastructures

The same identity for national and European research infrastructures that connect to MyAccessID, so that the user's identity travels with them.

Three things to take home

1

One identity layer, two very different infrastructures.

EOSC and EuroHPC do not share a platform, a governance or a risk profile. They share MyAccessID, and that is enough for a researcher to be the same person in both.

2

Identity from MyAccessID, authorisation from the research infrastructures.

MyAccessID says who the user is and how sure we are. The Node AAI or the EFP informs what they may do, the services enforce. Keeping those apart is what lets the model scale.

3

Assurance and non-web access are now part of federation.

MFA, identity validation and SSH certificates are live for EuroHPC and coming to every connected service. From 2027, a home IdP that signals them makes it seamless.



Thank you

Christos Kanellopoulos, GÉANT