EOSC AAI Architecture 2025

Implementation of the EOSC AAI Federation

March 2025 Version

This document is an output of the EOSC Authentication and Authorisation Infrastructure (AAI) Working Group. The EOSC AAI WG is one of three WGs under the "Technical and Semantic Interoperability Task Force" [EOSC-TSI-TF] of the EOSC Association [EOSC-Association]. The focus of the AAI WG is to deliver the next versions of the EOSC AAI architecture. It operates under the AARC Engagement Group for Infrastructures [AEGIS] of the Authentication and Authorisation for Research and Collaboration Community [AARC], with direct support from the AARC-TREE project [AARC-TREE] and it works closely with the AARC Architecture [AARC-Architecture] and Policy WGs [Policy-WGs], as well as the other WGs within the Technical and Semantic Interoperability Task Force [EOSC-TSI-TF]. The group brings together ***more than 40 experts on Authentication and Authorisation Infrastructures from 31 organisations across 16 countries, representing national, regional, European, and international initiatives.*** *More information about the group's membership can be found on the group's web pages [EOSC-AAI].*

EOSC Association AISBL

Rue du Luxembourg 3, BE-1000 Brussels, Belgium
+32 2 537 73 18 | info@eosc.eu | www.eosc.eu
Reg. number: 0755 723 931 | VAT number: BE0755 723 931

Editor(s):

Kanellopoulos, C.,

Author(s):

Adomeit, M.[1], Ardizzone, V.[2] Florio, M.[3], Giacomini, F.[4], Groep, D.[5], Hardt, M.[6], Kalman, T[7]. Kanellopoulos, C.[8], Kuczyński, T.[9], Liampotis, N.[10], Short, H.[11], Sidorova, I., Šťava, M.[8], Wierenga, K.[8]

SUNET[1], EGI[2], NORDUNet[3], INFN[4], Nikhef[5], KIT[6], GWDG[7], GEANT[8], PSN[9]C, GRNET[10], CERN[11]

Contributors:

EOSC AAI Working Group

Abstract

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:

- Defining the minimum set of requirements;
- Prioritising the simplest possible component configuration; and
- Ensuring the solution is implementable with today's technology.

To establish a solid foundation and deliver the essential functionality of the EOSC AAI Federation, several architectural and technical decisions have been made. These are detailed in the Implementation section and include, among others, the delegation of logic away from proxies, the adoption of OpenID Connect and OAuth2 as core protocols, and the integration of MyAccessID.

This document 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 [EOSC-Handbook]; services are onboarded to individual Nodes rather than directly to the Federation.

Connecting a Node and its services to the Federation requires specific capabilities - such as an Infrastructure Proxy, Community AAI, or the use of a unified Identity Layer. These are detailed in the section "*EOSC Node Federated AAI Requirements*".

Where possible, we offer alternative solutions to accommodate legal, technical, or organisational constraints that may prevent Nodes from fully adopting the recommended setup.

Content

Background information

EOSC Association

The EOSC Association is the legal entity responsible to strategically guide and support the development of the **European Open Science Cloud (EOSC)**. It represents the research community that contributes to building EOSC, including research performing organisations, service providers, policy institutions and funders among others. The Association facilitates collaboration between stakeholders, defines strategic priorities, and aligns efforts towards the **EOSC Federation**.

Relation to other concepts:

- Steers the establishment of the EOSC Federation.
- Oversees working groups and task forces, including the EOSC AAI Working Group.
- Provides the Strategic Research and Innovation Agenda (SRIA) as well as the Multi Annual Roadmap (MAR), that define a set of priorities for future investment in EOSC.

EOSC AAI Working Group

The EOSC AAI Working Group is one of the three Working Groups of the EOSC Association's Technical and Semantic Interoperability Task Force. The EOSC AAI WG focuses on defining and promoting Authentication and Authorization Infrastructure (AAI) policies, standards and best practices for EOSC. It works to ensure interoperability and trust among identity and access management systems across EOSC services.

Relation to other concepts:

- Operates under the **EOSC Association and AEGIS** with the support of the AARC-TREE project.
- Delivers and maintains the **EOSC AAI Architecture**.
- Supports the **EOSC AAI Federation** in establishing trust and interoperability policies.

EOSC AAI (Authentication and Authorisation Infrastructure)

The **EOSC AAI** is the **federated identity and access management framework** that enables researchers and service providers within EOSC to authenticate and authorize users to access resources in a secure and interoperable way. It integrates with national and institutional identity providers, allowing seamless Single Sign-On (SSO) across EOSC services.

Relation to other concepts:

- Provides the **technical foundation** for the **EOSC AAI Federation**
- Connects with **EOSC Nodes** to enable secure access to resources.
- Implements policies set by the **EOSC AAI Working Group**.

EOSC AAI Federation

The **EOSC AAI Federation** is the **operational framework** that ensures the AAI interoperability across the EOSC Nodes. It builds upon the EOSC AAI and integrates multiple identity federations (e.g., eduGAIN, national research identity federations) to create a **trusted, federated ecosystem** for identity management.

Relation to other concepts:

- Implements the **EOSC AAI** framework at a broader level.
- Provides identity federation services to **EOSC Nodes**.
- Supports the **EOSC Federation** in enabling seamless access to services.

EOSC Federation

The **EOSC Federation** is the overall **federated structure** of interconnected EOSC services, resources, and infrastructure across Europe. It enables research institutions, national research infrastructures, and service providers to contribute to and access EOSC resources under a common governance model.

Relation to other concepts:

- Composed of multiple **EOSC Nodes** that provide federated services.
- Relies on the **EOSC AAI Federation** for secure access to services.
- Coordinated by the EOSC Association.

EOSC Nodes

EOSC Nodes are **regional, national or thematic infrastructures** that participate in the **EOSC Federation** by providing resources, services, and data. Each node represents a specific group of service providers and follows EOSC Policies for interoperability.

Relation to other concepts:

- Act as the **building blocks** of the **EOSC Federation**
- They are integrated with the **EOSC AAI Federation**.

EOSC EU Node AAI

The **EOSC EU Node AAI** is a **central AAI service** that supports **core EOSC services** at the European level. It provides authentication and authorization for users accessing EOSC resources.

Relation to other concepts:

- A critical component of the **EOSC AAI Federation**.
- Facilitates interoperability between **EOSC Nodes** and the broader **EOSC AAI** ecosystem.
- Ensures that EOSC **Core** services comply with AAI policy.

Work of previous EOSC Task Forces

The seminal work on the EOSC AAI is the initial "EOSC Authentication and Authorisation Infrastructure Report" [EOSC-AAI-Report]. It was finalised in 2020 by the EOSC Executive Board Working Group (WG) Architecture PID Task Force (TF) and was published at the beginning of 2021.

This report built on the AARC Blueprint Architecture (AARC-BPA) [AARC-BPA-2019] and established it as the reference architecture for the implementation of the EOSC AAI. The EOSC Authentication and Authorisation Infrastructure Report defined an initial concept for the "EOSC AAI Federation" based on the best practices known for running and operating eduGAIN and the national Federations across the globe. The report also provided an initial set of requirements about registration to the AAI federation, technical and policy interoperability and basic principles of operations.

At the time, the technical profile was based on SAML as the only pragmatic standard for federated access, treating Identity and Service Providers as first-class citizens of the “EOSC AAI Federation”.

The EOSC AAI Architecture version 2022 [EOSC-Architecture-2022] finalised in 2022 and published in 2023 by the EOSC AAI Task Force [EOSC-AAI-TF] provided a number of important updates to the initial report discussing the following areas:

- Consistent user experience and interfaces for service providers’ workflows spanning multiple infrastructures,

- Growth of EOSC beyond the research and education community, and
- User and community attributes and authorisation.

In addition, v2022 of the EOSC AAI Architecture elaborated on the work ahead and identified the following areas that needed to be addressed:

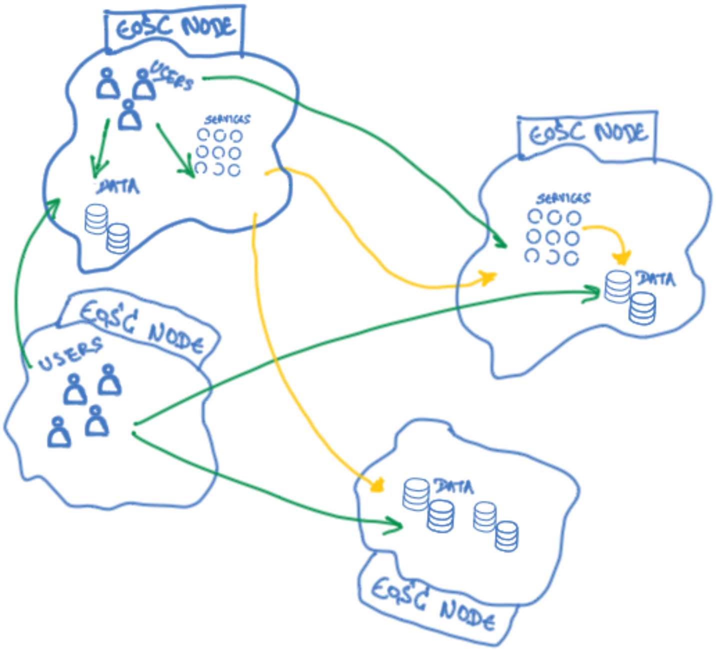
- Evaluation of OpenID Federation [OID-Fed] as a replacement of the SAML federation protocol,
- Transition from SAML to OpenID Connect and OAuth2 as the "de facto" federation protocols across the EOSC AAI Federation, given the fact that SAML is a standard that is not being maintained anymore. Besides that, it can only support a limited set of the intended use cases and is lacking adoption on the service provider side,
- Consistent Identity Discovery process across the EOSC AAI Federation,
- Integration of best current practices for personal data protection in federated authentication and authorisation, including the REFEDS Data Protection Code of Conduct v2 [DPCoCo], and
- Harmonisation and streamlining of effective best practices for secure usage and operation of resources, and security enforcement.

The EOSC EU Node & the EOSC Federation

The EOSC EU Node [EOSC-EU-NODE] is the first operational node of what will become the EOSC Federation — a federated ecosystem of research infrastructures across Europe and beyond. The EOSC Federation serves as a cornerstone in realising the vision of a coordinated, interoperable

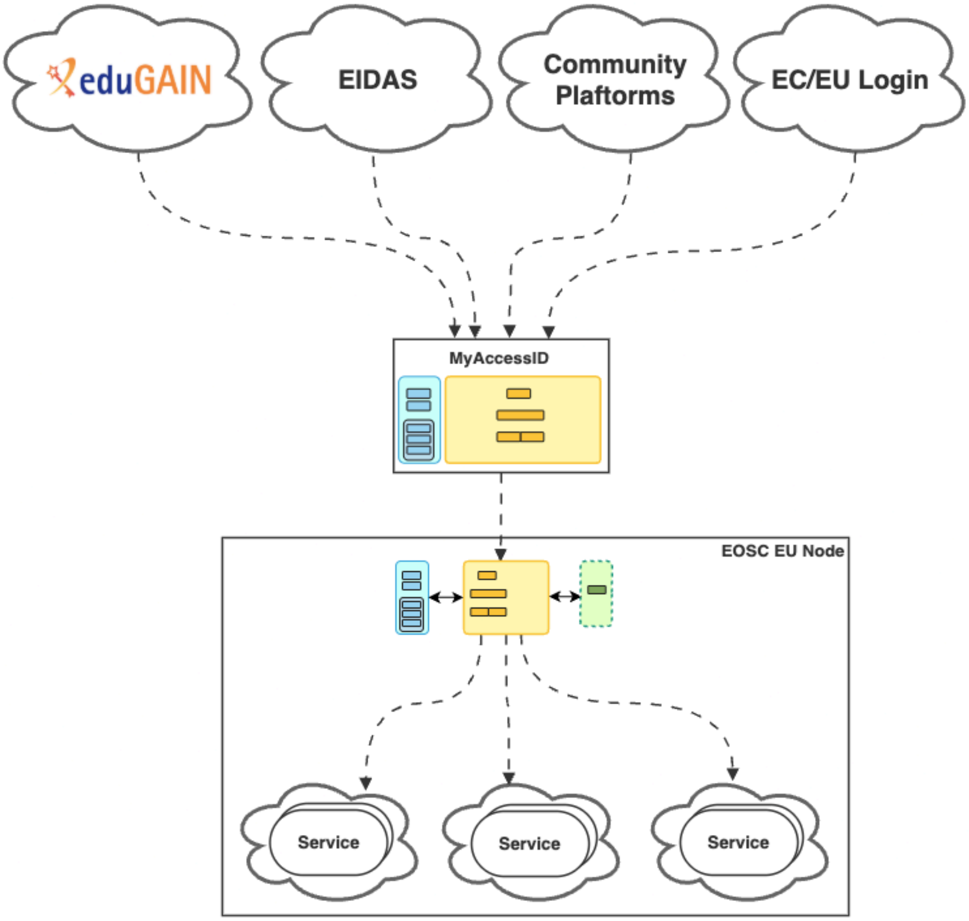
European Open Science Cloud. More information about the EOSC Federation can be found in the EOSC Federation Handbook [EOSC-Handbook].

The EOSC EU Node, designed to support multi-disciplinary and cross-border research, promotes the use of FAIR (Findable, Accessible, Interoperable, Reusable) data and services. It offers researchers user-friendly tools and essential support to plan, execute, disseminate, and evaluate their research workflows across the EOSC ecosystem. Beyond its immediate capabilities, the EOSC EU Node plays a foundational role in enabling the broader EOSC Federation. Following a "system of systems" architectural approach, it provides both a technical and administrative blueprint for future national and thematic nodes.



The Federation of EOSC Nodes: The organisational view illustrates the inter-node communication and the exchange of data across nodes. The green lines represent user to service flows. The yellow lines represent service to service flows.

The EOSC EU Node AAI provides the Federated Identity and Single-Sign-On (SSO) and Centralised User Management capabilities for the EOSC EU Node, enabling seamless and secure access across the platform.



The EOSC Federation and the EOSC EU Node: The hierarchical view shows how user identity information is aggregated on its route from the authenticating Identity Provider, via several proxies, to the end services.

Single Sign-On (SSO), enables users to access the node by logging in once via MyAccessID [MyAccessID] and then be recognised across all the services provided through the EOSC EU Node without having to log in again. Through MyAccessID, users can log in using credentials from their home organisations, national eIDs (eIDAS), EU Login, and other trusted authentication sources. Because of the adoption of MyAccessID by National and European Research Infrastructures, HPC centers, and the EuroHPC Federation, users of the EOSC EU Node have a single, consistent, and secure login experience for their scientific work, eliminating the need to manage multiple sets of credentials and thus reducing the risk surface related to credential compromise and the cognitive load for the users.

The User Management capability of the EOSC EU Node streamlines administrative processes and reinforces a cohesive policy across the platform. Tokens issued by the EOSC EU Node AAI carry the appropriate authorisation information, enabling users to orchestrate complex workflows that will be executed across the EOSC EU Node services.

The EOSC EU Node AAI supports industry-standard protocols:

- OAuth2 [RFC6749]: enables the EOSC EU Node service components to obtain limited access to a resource, either on behalf of a user by orchestrating an approval interaction between the user and the protected resource, or by allowing an EOSC EU Node service component to obtain access on its own behalf. The EOSC EU Node AAI implements the latest Best Current Practice for OAuth 2.0 Security [RFC9700].

- OpenID Connect [OIDC-Core]: A simple identity layer on top of the OAuth 2.0 protocol, which allows clients to verify the identity of the end-user and to obtain user information. The EOSC EU Node AAI implements the OpenID Connect Core specification along with the OpenID Connect Discovery [OIDC-Discovery] and the OpenID Connect Dynamic Client Registration [OIDC-Dynamic-Reg] specifications.

- SAML2 (Security Assertion Markup Language 2.0) [SAML2]: This protocol is used for exchanging authentication and authorisation data between parties, specifically, between an identity provider and a service provider. SAML2 is also supported in the EOSC EU

Node as a protocol for connecting services that cannot support OpenID Connect or OAuth2. Implementers of services that are onboarded on the EOSC EU Node are strongly advised to use the OpenID Connect and OAuth2 protocol families.

The EOSC EU Node AAI supports several OAuth 2.0 authentication grants, catering to a range of devices and interaction modes:

- Authorisation Code Grant [RFC6749-1.3.1] with PKCE [RFC7636]
  For interactive user authentication, the EOSC EU Node AAI employs the Authorisation Code flow, enhanced with Proof Key for Code Exchange (PKCE). This method is particularly useful in web-based scenarios, offering an additional layer of security.

- OAuth 2.0 Device Authorisation Grant [RFC8628]
  Recognizing the need for versatility, the EOSC EU Node AAI supports the OAuth2 Device Authorisation Grant, which is optimized for devices like workstations, user terminals, and mobile phones, facilitating authentication in scenarios where they either lack a browser to perform a user-agent-based authorisation or are input constrained to the extent that requiring the user to input text in order to authenticate during the authorisation flow is impractical.

- OAuth 2.0 Refresh Token Grant [RFC6749-6]
  Used by clients to exchange a refresh token for an access token when the access token has expired. This allows the EOSC EU Node components to continue having a valid access token without further interaction with the user.

- OAuth 2.0 Client Credentials Grant [RFC6749-4.4]
  Used by the EOSC EU Node AAI components to obtain an access token outside of the context of a user. This is typically used by clients to access resources accessible to themselves rather than to access a user's resources.

All components of the EOSC EU Node that require user authentication are configured as clients to the EOSC EU Node AAI. This integration ensures that any access request to EOSC EU Node resources undergoes a streamlined authentication process managed by the EOSC EU Node AAI.

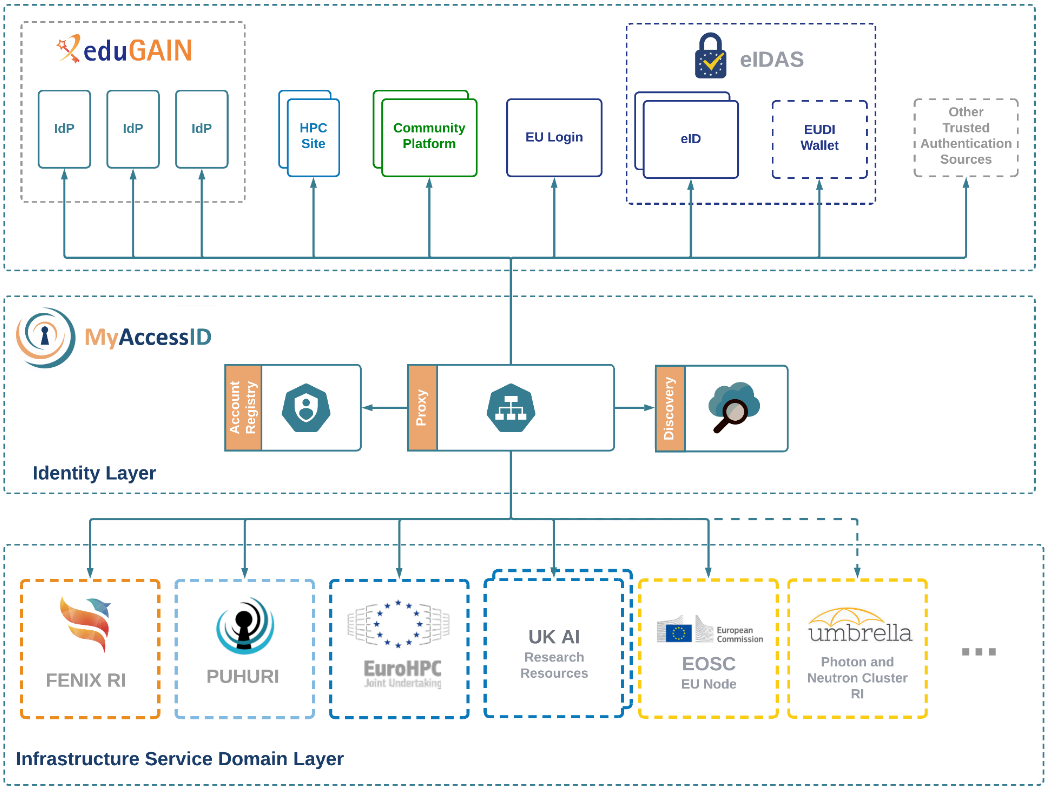
The EOSC EU Node AAI supports both Confidential clients and Public clients [RFC6749-2.1]. Confidential clients are applications that are able to securely authenticate via the AAI, for example being able to store their registered client secret safely. Public clients are unable to use registered client secrets, such as applications running in a browser, on a mobile device, on a multi-user server, or on limited-input devices (e.g., CLI tools using the Device Authorisation Grant).

For token validation, the EOSC EU Node AAI supports OAuth2 Token Introspection [RFC7662] and acts as a central point for the EOSC EU Node services to query the state of OAuth2 tokens and retrieve their metadata, thus providing real-time verification of token validity.

MyAccessID

MyAccessID is a relatively new service launched by GÉANT in 2020, building on top of the success and capabilities of eduroam, eduGAIN, and the AARC Blueprint Architecture and taking advantage of the experience and knowledge gained of building and operating a truly global federated environment for Research and Education for more than 20 years.

MyAccessID builds on top of and augments eduGAIN, providing an “Identity Layer” for Science in Europe, and is already being used by the EOSC EU Node, the EuroHPC Federation Platform and EuroHPC Hosting Sites, and by European and national Research Infrastructures.



Schematic view of the "hub-and-spoke" approach for the EOSC AAI

Through MyAccessID, users can securely login with their organisational accounts via eduGAIN, national eIDs via eIDAS, EU Login, Community AAIs and other trusted authentication sources. For users utilising their national eIDs, the system adheres to the eIDAS regulation. This compliance ensures that the electronic identification is interoperable across all EU Member States, offering a robust framework that respects both security standards and legal requirements.

Furthermore, GÉANT is working closely with the EUDI Wallet ecosystem and is a member of the DC4EU (Digital Credential For Europe) Large Scale Pilot. As part of this, GÉANT is committed to making MyAccessID one of the first services to support the EUDI Wallet [EUDI-Wallet], ensuring that, as soon as EUDI Wallets become available, users can immediately use them without any further action required from the services that rely on MyAccessID.

As described in the previous chapter of this document, the EOSC EU Node connects to MyAccessID as an "Infrastructure Service Domain" (ISD) via its "Infrastructure Proxy" in accordance with the "AARC Blueprint Architecture".

The term ISD refers to a group of services that are part of one infrastructure and/or administrative domain. ISDs can use MyAccessID to authenticate users and receive user identities that meet the required levels of assurance. ISDs may operate their own Resource Allocation Systems and/or integrate with external Resource Allocation Systems. ISDs connect to MyAccessID via their own "Infrastructure Proxies".

The "Infrastructure Proxy" in the ISD is responsible for connecting the "End Services" that are part of the ISD. The concept of the ISD is compatible with the AARC Blueprint Architecture model. The Authorisation component in the AARC BPA is already taking into account the fact that authorisation can and does happen at several different layers.

OpenID Federation specification

As the work on the EOSC AAI Architecture and the guidelines around it is ongoing, the direction is already clear, pointing towards the eventual adoption of OpenID Federation as the next generation federation protocol, which will provide a standard mechanism to establish trust in the context of OpenID Connect, OAuth 2.0, and possibly the EUDI Wallet.. The OpenID Federation specification has significantly matured during the past 2 years, already being in draft version 42 [OID-Fed], but there is still no final specification. The Research and Education community is currently (spring 2025) engaged in a number of implementation pilots such as the eduGAIN PoC [eduGAIN-PoC], the upcoming OpenID Federation interop testing event[1] hosted by SUNET in collaboration with the OpenID Forum, and the upcoming meeting of REFEDS PORE Working Group which is profiling OpenID Federation for Research and Education at TIIME 2025 conference[2]. The AARC Architecture Working Group, with contributions from the EOSC AAI WG, is expected to provide an initial version of the deployment Profile for OpenID Federation for consultation at the end of 2025. Additionally, the R&E community is contributing actively to a new specification for supporting the digital wallet ecosystem with the OpenID Federation [OID-Fed-Wallet] trust model.

Although a lot of activity is taking place around OpenID Federation, there is still much work required in the areas of the specification, the profiling requirements for AARC and EOSC, and the support of the tooling. The OpenID Federation standard will provide a foundational new building block that will enable the implementation of flexible and scalable trust topologies, but further work on federation components (e.g. libraries, metadata resolvers) is needed for creating functional systems.

AARC Blueprint Architecture

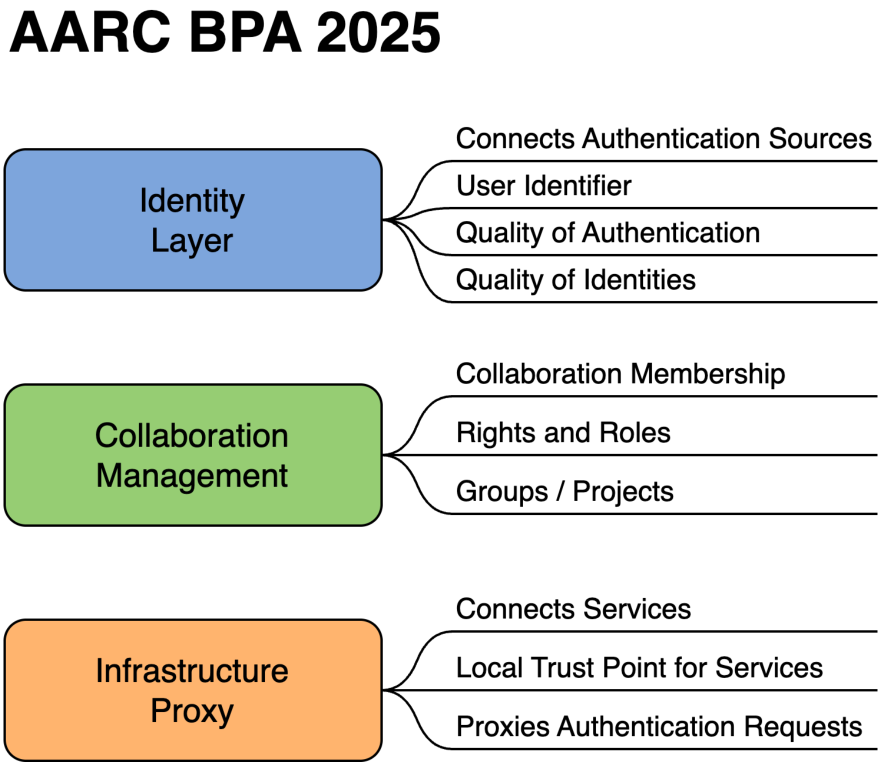
Some of the building blocks needed for OpenID Federation have already been identified, and the EOSC AAI WG is working jointly with the AARC Architecture WG on the following foundational guidelines for the AARC Blueprint Architecture 2025 [AARC-BPA-2025] that are expected to be ready later in 2025:

- OAuth 2.0 Proxied Token Introspection [AARC-G052]
- Establishing Trust between OAuth 2.0 Proxies [AARC-I058]

[1] https://openid.net/openid-federation-interop-apr-28-30-2025/
[2] https://tiime-unconference.eu/

- AARC Profile for expressing identity attributes [AARC-G056]

The AARC Blueprint Architecture 2025 [AARC-BPA-2025] is expected to be available for consultation at the end of Q2 2025. One of the important things that the AARC BPA 2025 is introducing is the "Identity Layer" as a new logical component, in addition to the existing "Community AAI" and "Infrastructure Proxy".



The reason for introducing this new logical component is because the Identity and the Community Management are two separate functions, as further explained in the AARC BPA 2025[3] [AARC-BPA-2025] version.

In early implementations of the AARC BPA, each community was handling its own "Identity Layer", having to manage connections to authentication sources, attribute release, levels of assurance, linking of identities in addition to typical community management aspects. With the introduction of MyAccessID by GEANT, as a gateway to identities from eduGAIN and other trusted authentication sources, a number of Infrastructures have started to rely on MyAccessID for their identities, while still retaining full control of the community management aspects on the Community AAI side. The same goes for the growing number of edu-ID systems operated by some European NRENs at the national level.

The introduction of the "Identity Layer", allows the implementers of AARC BPA compliant solutions, to handle this layer separately in the architectural model, allowing for more flexibility and a clearer separation of concerns.

By the end of 2025, the AARC Working Group is going to work further on key areas, such as authorisation for accessing federated resources, an initial AARC deployment Profile for OpenID Federation, use of decentralised identities and reassessing the suitability of the eID assurance model.

The work required at the specification 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

[3] At the time of writing, the AARC BPA 2025 is still under development. This link will be updated in future versions of this document.

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 EOSC AAI Federation

The term “EOSC AAI Federation” was first introduced in the "EOSC Authentication and Authorisation Infrastructure Report" [EOSC-AAI-Report] published in 2021 and has been used since in the published works of the EOSC Task Forces and Working Groups. In 2023, the European Commission introduced the term “EOSC Access Federation” as part of the EOSC EU Node procurement. In parallel, the term “EOSC Federation” has been introduced to denote the wider federation of EOSC Nodes that goes beyond just the AAI.

In this document, the terms “EOSC AAI Federation” and “EOSC Access Federation” can be used interchangeably and refer to the AAI Federation capability that provides the trust fabric across the entire “EOSC Federation” by:

- Enabling **federated authentication** among EOSC nodes,
- Offering **Single Sign-On (SSO)** across all EOSC nodes and services,
- Providing **token-based access** for APIs and resources, and
- Establishing a **single, unified identity** for end-users across all EOSC nodes and services.

Please note: The “EOSC AAI Federation” is not “EOSC Federation” even though the word “Federation” is used in both terms.

While not all resources in EOSC may require authenticated access, every node participating in EOSC MUST support federated authentication via the EOSC AAI Federation.

The focus of the EOSC Federation and in extension of the "EOSC AAI Federation" is to enable users of EOSC to seamlessly and securely access resources across EOSC Nodes. Even though

an EOSC Node MAY have its own users and resources, the scope of the EOSC Federation is not the localised access to resources of a Node by the users of that same Node.

AAI Federation Models

There are three basic topology models for establishing AAI Federations. The first model is the **bilateral federation model,** where entities in the federation have bilateral trust. This model is commonly found in the commercial space where the federated trust follows the contractual relationship between the parties. The second model is the **"hub-and-spoke" federation model**, where all participants in the federation trust one central hub, that is then responsible to proxy the trust among all the federation participants. The AARC Blueprint Architecture allows modelling such a scenario, in which a proxy plays the role of the central hub in the local federation. A small number of national academic federations in eduGAIN are also implementing this model. The third model is the **"full-mesh" federation model**, where multilateral trust must be established across all the participants of the federation. This is the model that is implemented today in eduGAIN, where there is multilateral trust across all the participating federations, while at the same time within each federation either the "full-mesh" or the "hub-and-spoke" model is implemented.

Supporting "full-mesh" topologies in the "EOSC AAI Federation" is not possible today, without significant compromises. The only mature federation protocol for a "full-mesh" AAI federation is SAML 2.0. The use of this protocol for the "EOSC AAI Federation" would immediately impose limitations to the use cases that "EOSC AAI Federation" can support, as the only capability that can be supported would be web-based Single Sign On (SSO) across the EOSC Nodes. User workflows across EOSC Nodes with authorization delegation cannot be supported and would require a completely different federation protocol. The OpenID Federation standard, as was already discussed, is a perfect match for the use cases of the EOSC AAI Federation, but significant work is still required towards this direction.

Using this model in the initial phase of the EOSC AAI Federation, EOSC Nodes are connected to the EOSC AAI Federation via MyAccessID, which acts as a central hub, providing the Trust & Identity Layers across the EOSC AAI Federation.

Implementation

Requirements Notation and Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this section are to be interpreted as described in [RFC2119].

Scope

The implementation discussed herein focuses on the interoperability and user experience requirements across EOSC Nodes.

EOSC AAI Federation

Adopting the "hub-and-spoke" model in the initial phase of the EOSC AAI Federation is a practical step forward, and it is implementable today, while the design and development work for the OpenID Federation and "full-mesh" topologies continues in the background in the AARC Architecture WG and the EOSC AAI WG.

In the EOSC Federation, a service **MUST** always be onboarded to a Node. A Node is considered an EOSC Node if it has formally enrolled in the EOSC Federation.

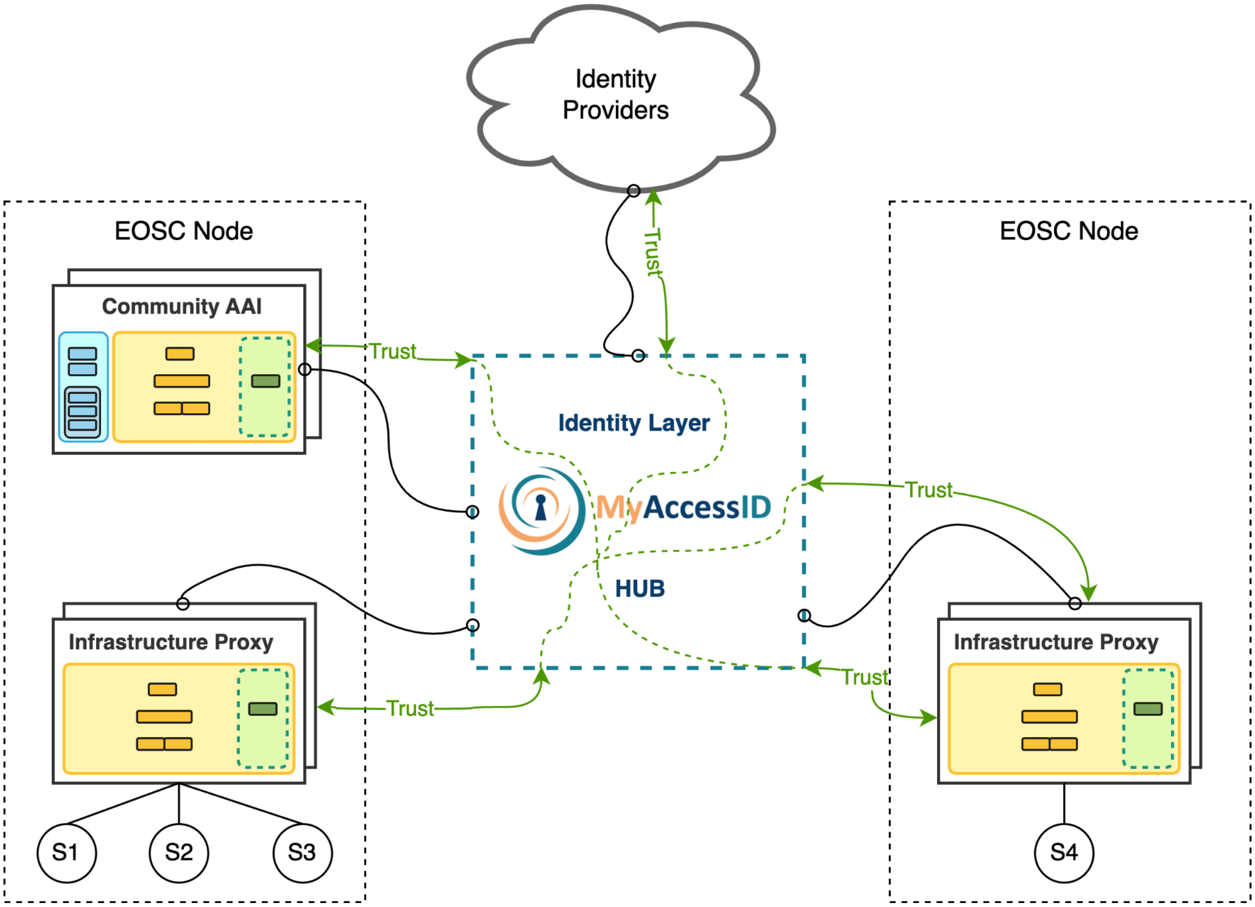
From the EOSC AAI Federation perspective, each Node **MUST** have at least one Infrastructure Proxy, that implements the AARC Blueprint Architecture and conforms to the EOSC AAI Architecture requirements defined in this document. An EOSC Node **MAY** have one or more Community AAIs. The same Infrastructure Proxy or Community AAI endpoints **MUST NOT** be registered by multiple EOSC Nodes[4].

[4] Although each Node typically deploys its own "Infrastructure Proxy" or Collaboration Platform instance, this does not preclude multiple Nodes from using the same physical deployment. The crucial factor is

The Central Hub provides the Trust and Identity Layer across the EOSC AAI Federation. It collects the trust anchors and related metadata of all the Infrastructure Proxies and Community AAIs available in the EOSC AAI Federation. Because of the "hub-and-spoke" structure, each EOSC Node establishes trust once with the Central Hub. This trust relationship is then transitively extended to all other EOSC Nodes that have similarly registered and met the EOSC AAI Federation's criteria.

that each Node is represented as a distinct logical instance, exposing Node-specific technical endpoints (e.g., unique URLs or APIs) and enforcing its own policies and configurations. In other words, while the underlying hardware or software installation may be shared, each Node's traffic and user flows are partitioned logically, preserving the autonomy and policy control that each EOSC Node requires.

From an architectural standpoint, this means that shared components can route and authenticate User requests separately for each Node, effectively simulating multiple installations even though they run on a single platform. Each Node thereby retains its own rules around token issuance, introspection, and account management, all while leveraging the efficiencies gained from sharing a single, centralized infrastructure.



The transitive trust model via the Central Hub

The Central Hub of the EOSC AAI Federation also provides the Identity Layer. The Identity Layer provides a consistent and unified user identity across the EOSC AAI Federation. Its key principles include:

- One User Identity across the EOSC Federation

- Common Login Experience
- Common Baseline of Identity Providers in Research and Education
- EOSC AAI Federation wide support for National eIDs (eIDAS)
- EOSC AAI Federation wide support for emerging technologies (e.g. EUDI Wallet [EUDI-Wallet])
- Common Assurance Levels based on the REFEDS Assurance Framework and EOSC AAI Federation assurance step-up mechanisms.

In order for an EOSC Node to be connected to the EOSC AAI Federation, it will have to register in the "EOSC AAI Federation Registry”. The registry stores information such as:

- Node Details

  Basic information about the Node or service, including name, description, and contact information.

- Infrastructure Proxy / Collaboration Platform (Community AAI) Details

  Technical Metadata

  Redirect URIs, supported protocols (e.g., OIDC, OAuth2), and security endpoints for token introspection.

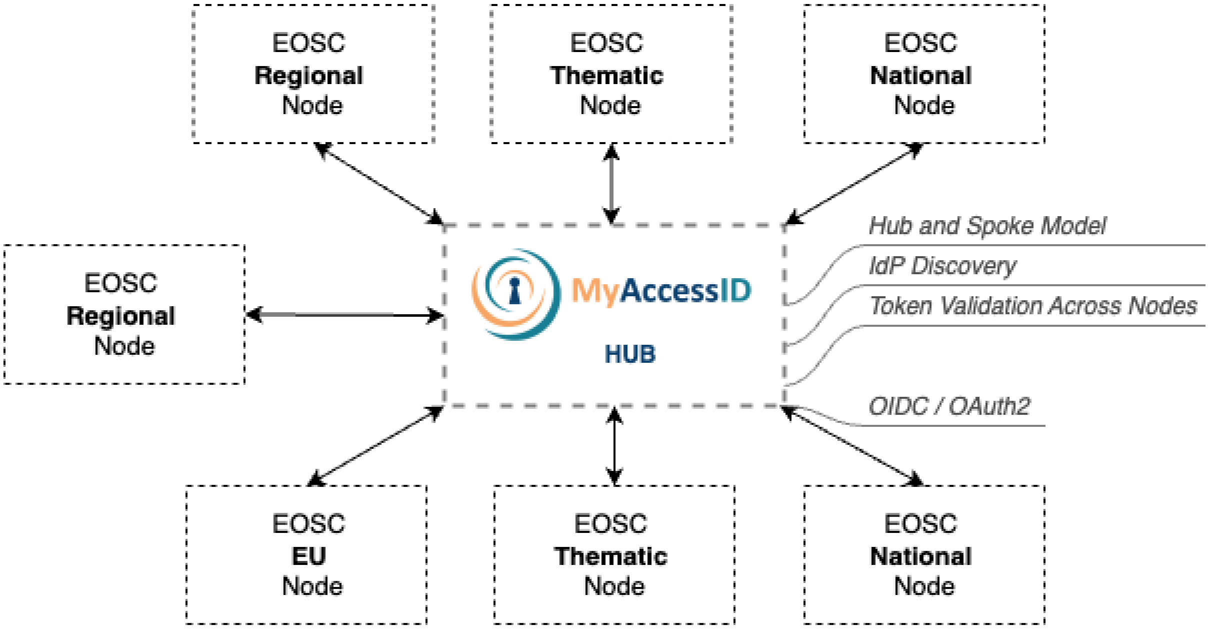
  Policies and Compliance

  Links to acceptable use policies, privacy policies, and confirmations that the Node complies with the federation’s security and data protection requirements.

By registering, an EOSC Node establishes trust with the Central Hub, allowing for SSO and secure exchange and validation of tokens. The section “EOSC Node Federated AAI requirements” describes the requirements that must be met by an EOSC Node in order to participate in the EOSC AAI Federation. The section "Registration to the EOSC AAI Federation" describes what information each EOSC Node has to provide, in order to establish trust with the hub of the EOSC AAI Federation and to be able to support Single Sign On and user workflows across two or more EOSC Nodes.

MyAccessID, provides the "Central Hub" and the "Identity Layer" in the EOSC AAI Federation. The reasoning behind this choice is that MyAccessID is already used as the trusted Identity Layer by the EOSC EU Node, by Research Infrastructures (national and European), by the EuroHPC sites, and by the EuroHPC Federation. The alternative would be to implement a central hub for the EOSC AAI Federation as a new component, in which case the only realistic option would be one that is provided by the EOSC EU Node.

Given the clear direction of the "EOSC AAI Federation" to use the "hub-and-spoke" model only in this initial phase the EOSC AAI WG at this point advises to avoid the investment of time and resources to implement a new hub, and focus such efforts on actively supporting the EOSC Nodes for the build-up of the EOSC Federation. Moreover, adding the hub in one of the EOSC Nodes could further distort the balance and equality between all the participating Nodes in the EOSC Federation or lead to alliteration. GÉANT is already committing significant resources for the adoption of and transition of the federation protocol to OpenID Federation and the EUDI Wallet ecosystem for Research and Education, which is fully aligned with the direction of the "EOSC AAI Federation". Lastly, in the case where it is deemed that an EOSC Federation specific Hub is required, transitioning the hub functionality out of MyAccessID would be a relatively simple exercise as the hub, by design, is focused on "simplicity". It implements the minimum required functionality, and it is based fully on open standards (AARC Blueprint Architecture, OAuth 2.0, and OpenID Connect).



EOSC AAI Federation "hub-and-spoke" model

EOSC Node Federated AAI requirements

The AARC Blueprint Architecture [AARC-BPA] is the foundation for the EOSC AAI Federation and the AAI within the EOSC Nodes. An EOSC Node **MUST** support the AARC Blueprint Architecture as outlined in this section. Additional federated AAI requirements (e.g. support of the AARC guidelines, relevant standards etc.) are also specified.

At a minimum, an EOSC Node **MUST** have at least one **Infrastructure Proxy** dedicated to the Node, that will broker authentication and requests for its services. An EOSC Node **MAY** have zero or more **Community AAIs.** An EOSC Node **SHOULD** use the "Identity Layer" provided by the

"EOSC AAI Federation" and **MUST** connect to the Hub for the purposes of token validation across Nodes. Each Infrastructure Proxy and Collaboration Platform (Community AAI) is registered as a single relying party from a specific EOSC Node.

Infrastructure Proxy

1. **MUST** be connected as a Relying Party to the hub of the EOSC AAI Federation.
   - An Infrastructure Proxy of an EOSC Node registered in the "EOSC AAI Federation Registry" receives client credentials with which they connect to the hub as OpenID Connect Relying Parties. With this integration, EOSC Nodes can (a) use the "Proxied Token Introspection" specification [AARC-G052] to validate OAuth 2.0 tokens issued by Authorisation Servers in other EOSC Nodes and (b) use the "Identity Layer" of the "EOSC AAI Federation".

2. **MUST** support the **OpenID Connect Discovery** [OIDC-Discovery] specification to be able to determine the location of the OpenID Provider of the hub.

   - *In future versions of this document, support for **OAuth 2.0 Protected Resource Metadata** [RFC9728], a metadata format enabling OAuth 2.0 clients and authorization servers to obtain information needed to interact with an OAuth 2.0 protected resource, will be also considered.*

3. **MUST** support the **Authorisation Code Grant** [OIDC-Core-3.1] **with PKCE** [RFC7636]

   - OIDC Relying Parties utilizing the Authorisation Code [OIDC-Core-3.1] grant **SHOULD** use Proof Key for Code Exchange (PKCE) [RFC7636]. PKCE helps detect and prevent injection or replay of authorisation codes into the authorisation response.

- Challenges **MUST** be transaction-specific and securely bound to the user agent where the transaction started.

4. **MUST make use of the nonce Parameter**

- OIDC Relying Parties **MAY** use the nonce parameter (as specified in OpenID Connect Core [OIDC-Core]) alongside the corresponding nonce claim in the ID Token.
- This further mitigates replay attacks and ensures the integrity of the authentication process.

5. **MUST support Token Introspection**

- **Compliance with OAuth 2.0 Token Introspection** [RFC7662]
  Authorisation Servers in the "EOSC AAI Federation" **MUST** implement the OAuth 2.0 Token Introspection endpoint to verify the validity and active state of tokens they have issued.

- **Scope and Policy Enforcement**
  By performing token introspection, the EOSC Node's services can retrieve authorised scopes and user claims from the token response. This information **SHOULD** be used to enforce fine-grained access control policies and ensure the requestor's permissions match the resource's requirements.

- **Reduced Exposure of Access Tokens**
  EOSC Nodes **SHOULD** minimize exposing raw access tokens to various service components. Instead, they **SHOULD** rely on a dedicated component (e.g., the Infrastructure Proxy) to handle introspection, thus limiting security risks.

- **Token Revocation and Freshness**
  Regular introspection checks help detect revoked or expired tokens before granting access to protected resources. The EOSC Node **SHOULD** define a suitable caching or re-validation strategy (e.g., time-based) to balance performance with security needs.

- **Confidential Client Authentication**
  The Infrastructure Proxy (acting as an OAuth 2.0 client) **MUST** use a confidential client credential (e.g., client secret or mutual TLS) when communicating with the token introspection endpoint to ensure a secure and trusted channel.

- **Proxied Token Introspection** [AARC-G052]
  Infrastructure Proxies **MUST** support the Proxied Token Introspection extension to the OAuth2 Protocol, as described in the Proxied Token Introspection [AARC-G052]. AARC-G052 is an extension to the OAuth 2.0 Token Introspection specification [RFC7662] developed by AARC. The AARC Architecture WG is preparing to submit [AARC-G052] to the IETF for consideration as an internationally recognised standard beyond the research and education space. There is already support for commonly used software solutions by Research Infrastructures across Europe.

6. **MUST prohibit insecure flows**

- The **Implicit Grant** and any response type causing the Authorisation Server to issue an Access Token directly in the authorisation response are **PROHIBITED**.

7. **MUST support the Claims and Scopes available in the EOSC AAI Federation**

- Infrastructure Proxies as OIDC Relying Parties **MUST** support requesting claims about the End-User and the authentication event using specific scope values as described in OpenID Connect Core [OIDC-Core] and the section Claims available in the EOSC AAI Federation.

8. **MUST support processing and expressing group and role information according to "AARC-G069 Guidelines for expressing group membership and role information"** [AARC-G069]

   ○ This document provides guidelines for expressing group membership and role information across AARC BPA compliant AAI Services. Specifically, it defines a URN namespace for expressing this information using common identity federation protocols. In the EOSC AAI Federation is used for exchanging group and role information across EOSC Nodes.

9. **SHOULD support "AARC-G061 A specification for IdP Hinting"** [AARC-G061]

10. **SHOULD implement the "AARC-G083 Guidance for notice management by proxies"** [AARC-G083]

   o This guideline is part of AARC Blueprint Architecture 2025 and streamlines the presentation of user information notices (such as acceptable use policies or GDPR privacy notices) and how to support their presentation in infrastructures built on the AARC Blueprint Architecture (BPA) model.

The use in the initial phase of a common Identity Layer across the EOSC AAI Federation, simplifies and streamlines the end user experience.

EOSC Nodes having both users and services **MAY** have their own "Identity Layer" for their own users accessing their services locally within the Node. In such a case, EOSC Nodes **MUST** differentiate between the local, internal access authentication flows and the authentication flows for inter-Node access. This document does not provide information about how such a differentiation should be implemented by an EOSC Node.

EOSC Node Implementers may consider using different landing pages or Identity Provider hinting for services they provide to the EOSC Federation in order to trigger different authentication flows based on whether the access to the service is local to the EOSC Node or is happening across via the EOSC Federation. For example, a service might have one landing page in the local catalogue of the EOSC Node where it is registered and a different one in the catalogues of other EOSC Nodes. The landing page published to the service catalogues of the other nodes **MUST** trigger a login flow via the Identity Layer of the EOSC AAI Federation. Future versions of this document may include further guidance on this topic.

If an EOSC Node is unable to adopt the “Identity Layer” provided by the EOSC AAI Federation due to technical or policy constraints, the user experience for individuals coming from other EOSC Nodes will be negatively affected. In such cases, the authentication and registration processes will be specific to that Node, potentially differing in look and feel and available authentication methods, resulting in a fragmented and inconsistent user experience across the federation.

In order to limit the negative impact on the user experiences, EOSC Nodes that cannot use the Identity Layer of the EOSC AAI Federation:

- **MUST** implement on their Identity Layer any branding guidelines required by the EOSC Federation so that the user experience is consistent for all the services across the Federation.
- **MUST support at least the following Identity Providers**:
    - Identity Providers from the research and education federations in eduGAIN either directly or via the “Identity Layer” of the EOSC AAI Federation using “AARC-G061” for hinting the IdP selection from their own Discovery Service

        - Community AAIs registered via other Nodes in the EOSC AAI Federation via the “Identity Layer” of the EOSC AAI Federation using “AARC-G061” for hinting the IdP selection from their own Discovery Service.
    - **SHOULD** support login via eIDAS either directly or via the “Identity Layer” of the EOSC AAI Federation using “AARC-G061” for hinting the IdP selection from their own Discovery Service.
    - **MAY** support other login methods (e.g. ORCID), for users that cannot login using their home organisation accounts via eduGAIN or their national eIDs via eIDAS. These alternative methods can be offered either directly or via the “Identity Layer” of the EOSC AAI Federation using “AARC-G061” for hinting the IdP selection from their own Discovery Service.

11. **MUST support common security procedures**
    Security procedures define procedures and duties to allow an organised incident response. Distributed systems, in particular when spanning multiple organisational domains and countries, need a common approach for security related matters.
    The following are well established in distributed infrastructures, and therefore mandatory for being supported:

    - Security Incident Response Trust Framework for Federated Identity Sirtfi [REFEDS-SIRTIFI]
    - Security Operational Baseline [AARC-G084] to enable secure infrastructure operation
    - **Data Protection** for *access* to personal data: Compliance with the REFEDS Code of Conduct version 2 [REFEDS-DPCoCo] or other GDPR-aligned code of conduct.Collaboration Platform (Community AAI)

Community AAI

EOSC Nodes **MAY** have one or more Community AAIs whose users should be able to access services provided by other EOSC Nodes. In such cases the Community AAIs:

1. **MUST** connect their OpenID Connect Providers / OAuth 2.0 Authorisation Servers to the Hub of the EOSC AAI Federation.

   The Collaboration Platform (Community AAI) registered in the "EOSC AAI Federation Registry" may provide or receive client credentials with which the central hub of the EOSC AAI Federation is connected as an OpenID Connect Relying Party / OAuth 2.0 client. With this integration:

   1. OAuth 2.0 tokens issued by these Community AAIs can be used to access services provided by other EOSC Nodes, enabling cross-Node workflows.
   2. The central hub of the "EOSC AAI Federation" will be able to authenticate users at and/or link the collaboration identities of the users of these Community AAIs

2. **MUST** support the **OpenID Connect Discovery** [OIDC-Discovery] specification so that the central hub of the EOSC AAI Federation can dynamically determine the location and related trust metadata of the OpenID Provider of the Collaboration Platform (Community AAI).

   *In future versions of this document, support for **OAuth 2.0 Protected Resource Metadata** [RFC9728], a metadata format enabling OAuth 2.0 clients and authorization servers to obtain information needed to interact with an OAuth 2.0 protected resource, will be also considered.*

3. **MUST** support the **Authorisation Code Grant** [OIDC-Core-3.1] **with PKCE** [RFC7636]

- OIDC Providers utilizing the Authorisation Code [OIDC-Core-3.1] grant **MUST** support Proof Key for Code Exchange (PKCE) [RFC7636]. PKCE helps detect and prevent injection or replay of authorisation codes into the authorisation response.
- Challenges **MUST** be transaction-specific and securely bound to the user agent where the transaction started.

4. **MUST use the nonce Parameter**

- OIDC Providers **MUST** support the use of the nonce parameter (as specified in OpenID Connect Core [OIDC-Core]) alongside the corresponding nonce claim in the ID Token.
- This further mitigates replay attacks and ensures the integrity of the authentication process.

5. **MUST support Token Introspection**

- **Compliance with OAuth 2.0 Token Introspection** [RFC7662]
  The Community AAIs as OpenID Connect Provider / OAuth 2.0 Authorisation Servers issuing OAuth 2.0 access tokens that are used across services in the "EOSC AAI Federation" **MUST** implement the OAuth 2.0 Token Introspection endpoint for central hub of the EOSC AAI Federation to verify the validity and active state of tokens they have issued.

- **Scope and Policy Enforcement**
  By supporting token introspection, the Infrastructure Proxies of other EOSC Nodes, via the central hub of the EOSC Federation, can retrieve authorised scopes and user claims from the introspection responses. This information **SHOULD** be used to enforce fine-grained access control policies and ensure the requestor’s permissions match the resource’s requirements.

- **Token Revocation and Freshness**
  Regular introspection checks help detect revoked or expired tokens before granting access to protected resources. The EOSC Node **SHOULD** define a suitable caching or re-validation strategy (e.g., time-based) to balance performance with security needs.

6. **MUST prohibit insecure flows**

   - The **Implicit Grant** and any response type causing the Authorisation Server to issue an Access Token directly in the authorisation response are **PROHIBITED**.

7. **MUST support the Claims and Scopes available in the EOSC AAI Federation**

   - OIDC Providers **MUST** support requests for claims about the End-User and the authentication event using specific scope values as described in OpenID Connect Core [OIDC-Core] and the section Claims available in the EOSC AAI Federation.

8. **MUST support "AARC-G069 Expressing of Group and Roles"** [AARC-G069]

   - The Collaboration Platform (Community AAI) **MUST** express the information about group membership and roles, managed in the Collaboration Platform (Community AAI) itself, according to the AARC-G069 guideline.

9. **SHOULD support "AARC-G061 A specification for IdP Hinting"** [AARC-G061]

10. **SHOULD implement the "AARC-G083 Guidance for notice management by proxies"** [AARC-G083]

    This guideline is part of AARC Blueprint Architecture 2025 and streamlines the presentation of user information notices (such as acceptable use policies or GDPR privacy notices) and how to support their presentation in infrastructures built on the AARC Blueprint Architecture (BPA) model.

11. **MUST provide a web page that lists all Collaborations / Projects they support and which need to be recognised across the EOSC AAI Federation.**
    Such a page should include the name of the collaboration / project, the URN namespace per AARG-G069, status (active, decommissioned), date started, date decommissioned, jurisdiction.

12. **SHOULD** provide the same information in machine readable form.

Registration to the EOSC AAI Federation

- EOSC Nodes **MUST** be registered in the "EOSC AAI Federation Registry".
- EOSC Nodes **MUST** register at least one Infrastructure Proxy dedicated to the Node. EOSC Nodes **MAY** register one or more Community AAIs
- The EOSC AAI Federation maintains a single point of entry. Infrastructure Proxies and Community AAIs **CANNOT** be registered by multiple EOSC Nodes.
- The "EOSC AAI Federation Registry" maintains metadata about the participating nodes, including security contacts, logos, privacy policies, and more.

Supported Protocols in the EOSC AAI Federation

- **OAuth 2.0** and **OpenID Connect** (OIDC) are the **primary protocols** used in the EOSC AAI Federation.
- **SAML 2.0** is NOT supported across the EOSC AAI Federation as relying solely on SAML 2.0 for inter-Node interoperability would lead to limited functionality and extra complexity for protocol translation.

Enrolling a Node with the EOSC AAI Federation

When enrolling a Node in the EOSC AAI Federation, the **Federation Operator SHALL** require at least the following information about the Node and the AAI entities (Infrastructure Proxy / Collaboration Platform (Community AAI)):

1. **Node Information**
   - **Name** (in English; additional languages are optional). The name must be unambiguous and unique across the EOSC Federation.
   - **Description**: In English; A brief summary of the Node's function or purpose.
   - **Website URL**: A link providing more detailed information about the entity.
2. **Legal Entity Details**
   - **Organisation Name**: Official name of the legal entity representing the Node.
   - **Display Name**: Name used for user-facing interfaces (if different from the official name).
   - **Organisation Website URL**: For more in-depth information.
3. **Contact Information**
   - **Technical / Helpdesk / Support**: For user redirection or technical inquiries.
   - **Security / Incident Response**: Complying with Sirtfi [REFEDS-Sirtfi].
   - **Administrative**: (Optional, for administrative communications).
4. **Entity-Specific Contacts**
   - **Technical / Helpdesk / Support**
   - **Security / Incident Response**
   - **Administrative** (optional)

5. **Infrastructure Proxy Technical Information**
    - Redirect URL(s)
6. **Collaboration Platform (Community AAI) Technical Information**
    - Issuer supporting OpenID Connect Discovery
    - URN Namespace(s) (per [AARC-G069])
7. **Logo URL** (optional)
    - If provided, it **SHOULD**:
        - Use a transparent background (if appropriate).
        - Use PNG or GIF format.
        - Be accessible via HTTPS to avoid mixed-content issues.
        - Be under 50,000 bytes when Base64-encoded.
        - Have a maximum height of 32px and a maximum length of 320px.
8. **Policy Links**
    - **Privacy Policy**: URL to the service/organisation's privacy policy.
    - **Acceptable Use Policy / Terms of Use**: URL to AUP/ToU.
9. **Compliance Assertions**
    - **Data Protection** for *access* to personal data: Compliance with the REFEDS Code of Conduct version 2 [REFEDS-DPCoCo] or other GDPR-aligned code of conduct.
    - **Sirtfi**: Compliance with [REFEDS-Sirtfi] for incident response.
    - EOSC I/F **Security Operational Baseline** to enable secure infrastructure operation [EOSC-Security-Baseline-2022]

Claims available in the EOSC AAI Federation

This section specifies and further profiles the OpenID Connect (OIDC) claims available within the EOSC AAI Federation, which provide standardised attributes for expressing user authentication and authorisation information.

Subject Identifiers

Public Subject Identifier

Description	A string representation of the subject's identifier that is globally unique; In the context of the EOSC AAI Federation, the identifier released across EOSC Nodes meets the following requirements: ● It MUST be assigned so that no two values created by distinct identity systems could collide when identifying different subjects. ● Once assigned, MUST NOT be reassigned to another subject ● It SHOULD be permanent ● It MUST be persistent ● It MUST contain only ASCII characters ● It MUST be shared; if there are privacy and regulatory requirements that need to be met, the issuing system may not release this identifier to specific relying parties; for instance to prevent them from using the identifier as a basis for correlation (see Pairwise Subject Identifier)
OIDC claim(s)	sub [RFC7519, OIDC-Core, RFC9068] voperson_id (either a single string or an array containing a single value) [AARC-G026]

OIDC claim location	The claim is available in: ☑ ID token ☑ Userinfo endpoint ☑ Introspection endpoint ☑ Access Token Note that ☑ denotes that the attribute is REQUIRED to be available.
OIDC scope(s)	openid
Changes	No
Uniqueness	Globally unique
Multiplicity	Single-valued
Case sensitivity	Yes (see [RFC7519-4.1.2])
Availability	Always available
Example	ba660371-3278-4c8c-824c-1c56ed9ec6bf@myaccessid.org
Notes	Global uniqueness of the Public Subject Identifier can be achieved by combining an identifier locally unique to the issuing system with a unique property of the issuing system, such as a domain.
Status	Stable
Standards	[RFC7519], [RFC9068], [OIDC-Core], [voPerson-v2]

Name

Display Name

Description	Subject’s full name in displayable form.
OIDC claim(s)	name [OIDC-Core]
OIDC claim location	The claim is available in ☐ ID token ☑ Userinfo endpoint ☑ Introspection endpoint ☐ Access Token Note that ☑ denotes that the attribute is REQUIRED to be available.
OIDC scope(s)	profile [OIDC-Core] or aarc
Changes	Yes
Uniqueness	Not unique
Multiplicity	Single-valued
Case sensitivity	No
Availability	Always available when requested
Example	Jane Doe
Notes	-

Status	Stable
Standards	[RFC2798], [RFC7643], [OIDC-Core]

Given Name

Description	Name strings that are the part of a subject's name that is not their surname.
OIDC claim(s)	given_name [OIDC-Core]
OIDC claim location	The claim is available in (select one or more) □ ID token ☑ Userinfo endpoint ☑ Introspection endpoint □ Access Token Note that ☑ denotes that the attribute is REQUIRED to be available.
OIDC scope(s)	profile or aarc
Changes	Yes
Uniqueness	Not unique
Multiplicity	Multi-valued: The given_name claim can contain multiple given names with the names being separated by space characters
Case sensitivity	No

Availability	May be available when requested
Example	Jane
Notes	-
Status	Stable
Standards	[eduPerson], [REFEDS-Personalized-EC], [RFC4519], [RFC7643], [OIDC-Core]

Family Name

Description	Family name
OIDC claim(s)	family_name
OIDC claim location	The claim is available in (select one or more) ☐ ID token ☑ Userinfo endpoint ☑ Introspection endpoint ☐ Access Token Note that ☑ denotes that the attribute is REQUIRED to be available.
OIDC scope(s)	profile or aarc

Origin	May be registered directly during the subject's enrollment. Alternatively, the proxy can extract this information from the registered Display Name attribute.
Changes	Yes
Uniqueness	Not unique
Multiplicity	Multi-valued: The family_name claim can contain multiple family names (or no family name) with the names being separated by space characters [OIDC-Core]
Case sensitivity	No
Availability	May be available when requested
Example	Doe
Notes	
Status	Stable
Standards	[eduPerson], [REFEDS-Personalized-EC], [RFC2798], [RFC7643], [OIDC-Core]

Email

Email Address

Description	The subject’s primary (preferred) email address for contact purposes. This email

	address must be formatted in Mailbox form as specified in [RFC2821].
OIDC claim(s)	email [OIDC-Core]
OIDC claim location	The claim is available in: ☐ ID token ☑ Userinfo endpoint ☑ Introspection endpoint ☐ Access Token
OIDC scope(s)	email [OIDC-Core] or aarc
Changes	Yes
Uniqueness	Not unique
Multiplicity	Single-valued
Case sensitivity	No
Availability	Always available when requested
Example	jane.doe@example.org
Notes	A single email address MUST be used for contact purposes. If there is a need to associate multiple email addresses with a subject (e.g., for different purposes such as primary and backup emails), these should be represented with separate claims or attributes that clearly convey the intended purpose of each email address. However, an AARC BPA-compliant proxy MUST be capable of handling scenarios where multiple email addresses are received in the mail attribute (SAML) without failure. In such cases, the proxy MUST implement a process to select one email

	address to serve as the contact email for the subject. The proxy MUST release a single value in the email claim.
Status	Stable
Standards	[RFC281], [OIDC-Core]

Organisation

Organisation Domain

Description	Specifies a subject's home organisation using the domain name of the organisation according to [RFC1035], [REFEDS-SCHAC].
OIDC claim(s)	schac_home_organization
OIDC claim location	The claim is available in: □ ID token ☑ Userinfo ☑ Introspection endpoint □ Access Token Note that ☑ denotes that the attribute is REQUIRED to be available.
OIDC scope(s)	schac_home_organization or aarc
Changes	Yes (e.g., as a result of affiliation change)
Uniqueness	Globally unique

Multiplicity	Single-valued
Case sensitivity	No (see [RFC1035])
Availability	May be available when requested
Example	tut.fi
Notes	An AARC-compliant AAI SHOULD only release this attribute if the subject's identity provider, authoritative for the home organisation domain, released the schacHomeOrganization value within the same authentication session, ensuring the information is accurate and properly validated, for example by checking attribute values against the Issuer's published shibmd:Scope elements in SAML metadata.
Status	Experimental
Standards	[RFC1035], [REFEDS-SCHAC]

Affiliation

Affiliation within Home Organisation

<table>
<tr><td><b>Description</b></td><td>One or more home organisations (such as, universities, research institutions or private companies) that this subject is affiliated with. The syntax and semantics follows the eduPersonScopedAffiliation attribute [eduPerson].

The following values are recommended for use to the left of the "@" sign:<table><tr><td>faculty</td><td>The subject is a researcher or educator within an</td></tr></table></td></tr>
</table>

	academic institution. The exact definition may vary by organisation, but it typically refers to a subject whose primary focus involves research and/or education within their academic organisation. **Note**. This attribute value is specifically intended for subjects affiliated with the *academic* sector.
member	member is intended to include faculty, industry-researcher, staff, student and other subjects with a full set of basic privileges that go with membership in the home organisation, as defined in eduPerson. In contrast to faculty, among other things, this covers positions with managerial and service focus, such as service management or IT support.
affiliate	The affiliate value indicates that the holder has some definable affiliation to the home organisation NOT captured by any of faculty, industry-researcher, staff, student and/or member.
unknown	If the origin does not provide any affiliation information, but the scope of the origin provider can be reliably determined, the affiliation is constructed by concatenating the string literal unknown@ and the determined scope of the origin provider [AARC-G057]

If a subject has faculty or industry-researcher affiliation with a certain organisation, they also have the member affiliation. However, that does not apply in a reverse order. Furthermore, those persons who do not qualify to be a member have an affiliation of affiliate.

	Apart from the values listed above, the presence of other affiliation values defined in the eduPerson schema (e.g., staff, student, etc.) is not precluded. Each organisation determines its own criteria, so differences in interpretation are expected. For further details, see the eduPersonAffiliation attribute definition [eduPerson].
OIDC claim(s)	voperson_external_affiliation
OIDC claim location	The claim is available in: ☐ ID token ☑ Userinfo ☑ Introspection endpoint ☐ Access Token Note that ☑ denotes that the attribute is REQUIRED to be available.
OIDC scope(s)	voperson_external_affiliation or aarc
Changes	Yes
Uniqueness	Not unique
Multiplicity	Multi-valued
Case sensitivity	unclear
Availability	Always available when requested

Example	faculty@helsinki.fi industry-researcher@zeiss.com member@ebi.ac.uk unknown@accounts.google.com
Notes	The Relying parties are not expected to check the scope of this attribute. See also [AARC-G025].
Status	Stable
Standards	[AARC-G025], [AARC-G057], [eduPerson], [voPerson-v2]

Assurance

Description	The assurance of the subject's identity, following the components defined in the REFEDS Assurance Framework (RAF) [REFEDS-Assurance], including Identifier Uniqueness, Identity Assurance, and Attribute Assurance. AARC-compliant AAIs MAY also support additional assurance frameworks where relevant.
OIDC claim(s)	eduperson_assurance [REFEDS-Assurance]
OIDC claim location	The claim is available in: ☐ ID token ☐ Userinfo ☑ Introspection endpoint ☑Access Token Note that ☑ denotes that the attribute is REQUIRED to be available.

OIDC scope(s)	eduperson_assurance or aarc
Changes	Yes
Uniqueness	Not unique
Multiplicity	Yes
Case sensitivity	Yes
Availability	Always
Example	https://refeds.org/assurance https://refeds.org/assurance/ID/unique https://refeds.org/assurance/IAP/low https://refeds.org/assurance/ATP/ePA-1m https://refeds.org/assurance/ATP/ePA-1d https://refeds.org/assurance/IAP/medium https://refeds.org/assurance/profile/cappuccino https://aarc-community.org/assurance/ATP/ePA-1m https://aarc-community.org/assurance/ATP/ePA-1d https://aarc-community.org/assurance/ATP/vPEA-1m https://aarc-community.org/assurance/ATP/vPEA-1d https://igtf.net/ap/authn-assurance/birch https://aarc-project.eu/policy/authn-assurance/assam
Notes	This attribute defines just the identity assurance. Authentication assurance is described using authentication contexts (OIDC acr claim).
Status	Stable
Standards	[AARC-G021], [AARC-G025], [AARC-G031], [REFEDS-Assurance],

	[REFEDS-Personalized-EC], [eduPerson]

Group and Role information

Description	This attribute describes the groups and roles this user is a member of.
OIDC claim(s)	entitlements [AARC-G069], [RFC9068]
OIDC claim location	The claim is available in: ☐ ID token ☑ Userinfo endpoint ☑ Introspection endpoint ☐ Access token
OIDC scope(s)	entitlements [AARC-G069]
Changes	Yes
Uniqueness	Not unique
Multiplicity	Multi-valued
Case sensitivity	Refer to Section 2.3, [AARC-G069]
Availability	May be available when requested
Example	urn:example:foo:group:parentgroup:role=member#authority urn:example:foo:group:parentgroup:childgroup:role=member urn:example:foo:group:parentgroup:childgroup:grandchildgroup:role=manager

Notes	-
Status	Stable
Standards	[AARC-G069], [RFC9068], [eduPerson]

Authorisation in the EOSC AAI Federation

The EOSC AAI Federation does not perform authorization directly. It builds on top of the AARC Blueprint Architecture and offers foundational components that EOSC Nodes and their services can use to implement their own authorization policies. Ultimately, resource owners determine how and when access is granted to their resources. Often, resource owners centralize authorization across multiple services and resources to minimize cost and complexity while maintaining a consistent mechanism to review and enforce access.

How authorization is implemented within the EOSC Nodes is beyond the scope of this document. Instead, the EOSC AAI Federation focuses on providing the capabilities needed for each Node and its services to define, implement, and enforce their own access and authorization policies in the wider federated environment. Below are several access models, along with an overview of what the EOSC AAI Federation provides to support them:

Open Access Model

This is the simplest possible scenario, in which a service grants access to any user in the EOSC Federation who can successfully authenticate. Here, the EOSC AAI Federation ensures a minimal, consistent set of user information (claims) and identity providers that all EOSC Nodes accept. Simply proving one's identity through any recognized method is sufficient for service access.

Affiliation-Based Model

A second common approach, employed by the EOSC EU Node to assign credits, uses a user's affiliation (e.g., student, faculty, or staff at their home institution) to determine which resources they can access. This model leverages the "Affiliation" claim provided by the EOSC AAI Federation so that service owners can define policies that grant different levels of access based on a user's organizational role.

Collaboration-Based Model

In this setup, users gain access through membership in a collaboration, project, or other assigned allocation. The [AARC-G069] specification defines how to express a user's membership in such collaborations across administrative domains. Building on the AARC Blueprint Architecture, the EOSC AAI Federation requires using AARC-G069 to support this type of access policy, ensuring services can accurately determine whether a user is part of the collaboration entitled to the resource.

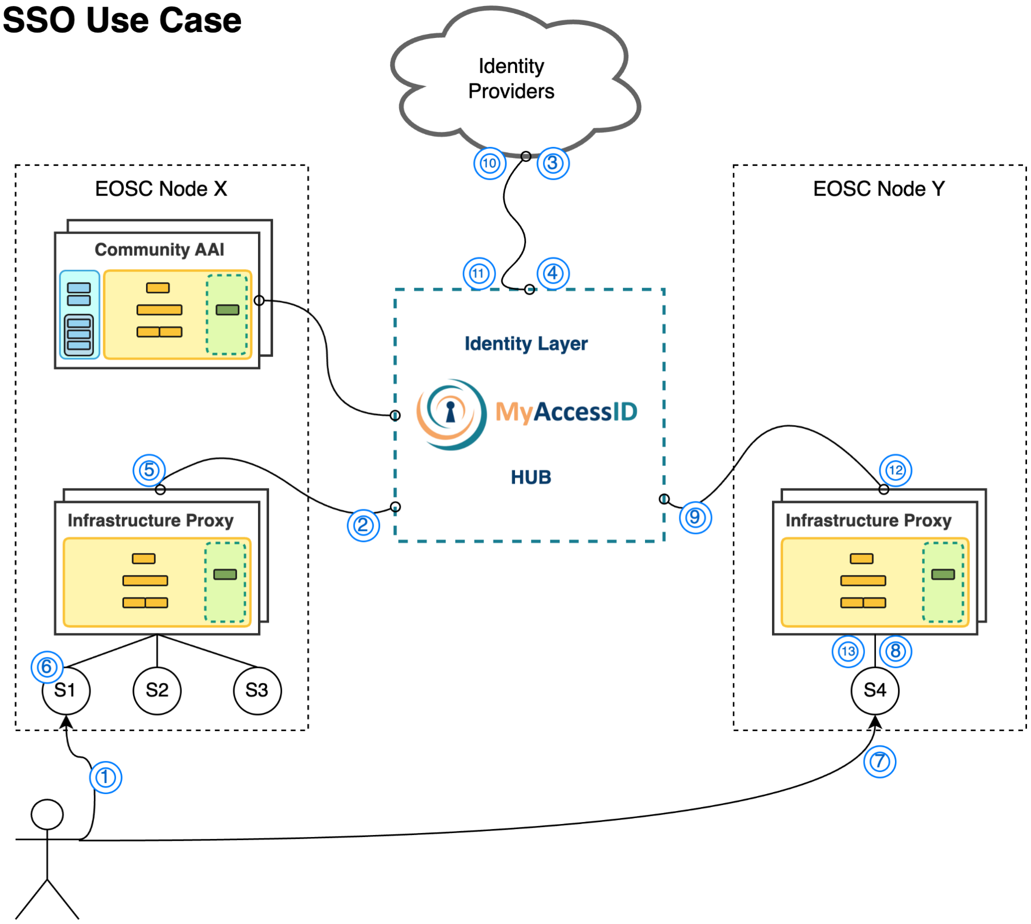
The Community AAIs in the EOSC Nodes provide the space for users to manage their collaborations, projects, and memberships. As outlined in the EOSC Node Federated AAI Requirements section, these platforms are connected to the central hub of the EOSC AAI Federation as OpenID Connect Providers / OAuth2 Authorization Servers.

When users log in to services provided by EOSC Nodes through these Community AAIs, information about their collaborations, groups, and projects is shared with the Infrastructure Proxy for the relevant service using the protocol described in AARC-G069. This approach ensures that membership and collaboration details are available as needed to control access and provide a consistent user experience across different services in the EOSC Federation.

Flows

Single Sign On

The sequence begins when the User tries to reach Service 1 (S1), which is integrated with the EOSC Node X Infrastructure Proxy. When the User arrives, Service 1 detects that the User is not yet authenticated and redirects them to the EOSC Node X Infrastructure Proxy (1). This Infrastructure Proxy then sends the User to MyAccessID (2), a central identity and access management system, to handle the authentication.



The SSO Use Case (see Annex - I for the UML diagram)

Once at MyAccessID, the User sees a discovery interface listing available Identity Providers (IdPs). The User picks their preferred IdP, and MyAccessID forwards them there (3). The chosen IdP presents its familiar login page, where the User enters credentials and consents to share any required personal attributes. Upon successful authentication, the IdP relays the User's identity information and attributes back to MyAccessID (4).

MyAccessID now checks whether the User's account is recognized. If it is not, MyAccessID triggers a quick registration procedure. The User is redirected to a registration page to fill in mandatory information and confirm any additional consents. With that done, MyAccessID creates a new account for the User. If MyAccessID already has the User on file, it simply retrieves their account details.

Having confirmed the User's identity, MyAccessID provides the User's information to the EOSC Node X Infrastructure Proxy (5), which in turn may enrich these attributes before sending the User back to Service 1. With all identity checks complete, Service 1 authorizes the User to proceed (6).

Later, the User decides to access Service 4 (S4), which runs under EOSC Node Y. Upon arriving at Service 4 (7), the User is redirected to the EOSC Node Y Infrastructure Proxy for authentication (8). This Infrastructure Proxy recognizes that the User must be authenticated through MyAccessID, so it sends them there (9).

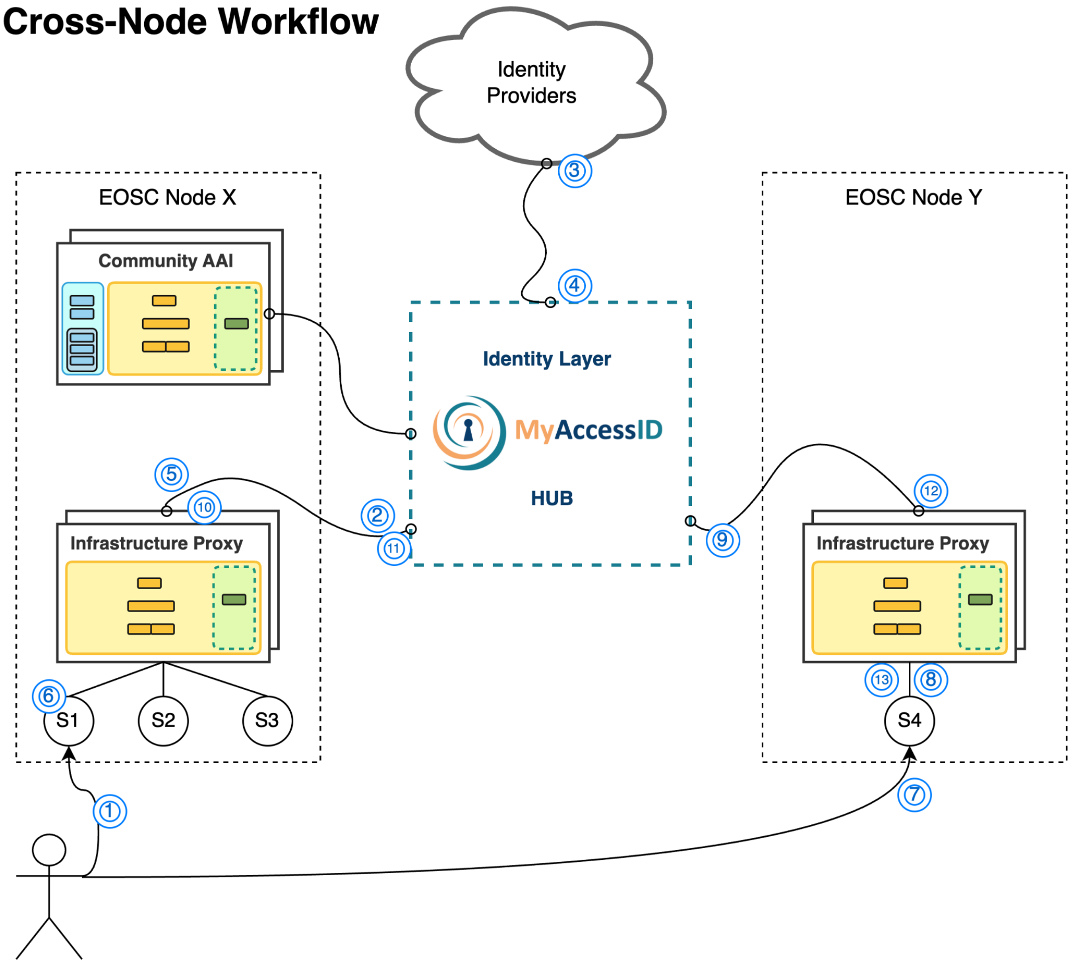
Since the User has a valid Single Sign-On (SSO) session, MyAccessID quickly redirects to the same Identity Provider (10). The IdP confirms that the User is already logged in via SSO and reaffirms the User's identity and attributes without requiring fresh credentials. This information is passed back to MyAccessID, which recognizes the User internally once again (11).

MyAccessID then returns the User's identity information to the EOSC Node Y Infrastructure Proxy (12). As before, the Infrastructure Proxy can enhance these attributes as needed before forwarding the User back to Service 4. Now fully aware of who the User is, Service 4 authorizes them (13) to consume its services without requiring another full login flow.

This flow highlights how once the User is registered in the overall ecosystem, they can traverse multiple services and Nodes using a streamlined Single Sign-On experience, facilitated by MyAccessID and the respective Infrastructure Proxies. A sequence diagram is provided in Appendix I.

Cross-node Workflow

The process begins when the User attempts to access Service 1 (S1) hosted in EOSC Node X (1). Since the User is not yet authenticated, Service 1 immediately redirects them to the EOSC Node X Infrastructure Proxy, which is responsible for handling authentication within that environment. The EOSC Node X Infrastructure Proxy, in turn, sends the User to MyAccessID (2), a centralized identity management service.



The Cross-node workflow use case (see Annex - I for the UML diagram)

Upon arriving at MyAccessID, the User is presented with a discovery interface listing all available Identity Providers. The User chooses an Identity Provider from this list, and MyAccessID then forwards them to the corresponding IdP's login page (3). The User enters their credentials, consents to share the mandatory attributes required for accessing EOSC services and completes the login process. The chosen Identity Provider sends the authenticated User's details and attributes back to MyAccessID (4), which confirms the User's identity and relays this information to the EOSC Node X Infrastructure Proxy (5).

With the User's identity verified, the EOSC Node X Infrastructure Proxy issues an Access Token (AT-X) to Service 1 (6), which in turn presents this token to the User (often made available for command-line use).

The User takes the access token (AT-X from EOSC Node X) and attempts to invoke an API exposed by Service 4 in EOSC Node Y (7). Service 4 is configured to perform token introspection and it calls the introspection endpoint of its local EOSC Node Y Infrastructure Proxy (8). The Node Y Infrastructure Proxy determines it did not issue AT-X, so it uses proxied token introspection and calls the introspection endpoint of MyAccessID (9). While MyAccessID also did not issue the token, it does identify that the token was issued by the EOSC Node X Infrastructure Proxy, with which it already has a trust relationship. MyAccessID calls the introspection endpoint of the Node X Infrastructure Proxy (10), which introspects AT-X and confirms its validity, along with the User's identity attributes. This verification result flows back through MyAccessID (11) to the EOSC Node Y Infrastructure Proxy (12). With the confirmation that AT-X is valid and tied to an authenticated User, the Node Y Infrastructure Proxy informs Service 4 (13), which then authorizes the User's request. With the token successfully validated, the User can proceed to consume the Service 4 API within EOSC Node Y. A sequence diagram is provided in Appendix I.

Evolution of the EOSC AAI Federation

The goal of the initial implementation of the "EOSC AAI Federation" is to provide the minimum viable functionality required to enable seamless access across the EOSC Nodes taking into account the limitation of the technology today.

The EOSC AAI Working Group acknowledges that a centralised *hub-and-spoke* model will be adopted in the initial phase of the EOSC AAI Federation. This approach serves as a practical starting point while the AARC Blueprint Architecture continues to evolve, incorporating emerging standards such as OpenID Federation and the EUDI Wallet. These advancements will enable the EOSC AAI Federation to support more complex configurations, ultimately expanding beyond the initial model to allow for dynamic *full-mesh* topologies.

References

- **[AARC-BPA-2019]:** AARC Blueprint Architecture 2019 https://aarc-community.org/guidelines/aarc-g045/
- **[AARC-G052]:** AARC Guideline on Proxied Token Introspection https://aarc-community.org/guidelines/aarc-g052/
- **[DPCoCo]:** REFEDS Code of Conduct version 2 https://zenodo.org/records/6518055
- **[RFC3986]:** Uniform Resource Identifiers https://datatracker.ietf.org/doc/html/rfc3986
- **[RFC7636]:** Proof Key for Code Exchange by OAuth Public Clients https://datatracker.ietf.org/doc/html/7636
- **[RFC2119]**: Key words for use in RFCs to Indicate Requirement Levels https://datatracker.ietf.org/doc/html/rfc2119
- **[OIDC-Core]:** OpenID Connect Core 1.0 incorporating errata set 2 https://openid.net/specs/openid-connect-core-1_0.html
- **[OIDC-Discovery]:** OpenID Connect Discovery 1.0 https://openid.net/specs/openid-connect-discovery-1_0.html
- **[OAuth2-BCP]:** OAuth 2.0 for Browser-Based Apps (Best Current Practice) (or the latest relevant BCP) https://datatracker.ietf.org/doc/html/rfc9700
- **[RFC3986]:** Uniform Resource Identifier (URI): Generic Syntax https://datatracker.ietf.org/doc/html/rfc3986
- **[REFEDS-Sirtfi]:** Security Incident Response Trust Framework for Federated Identity (Sirtfi) https://refeds.org/sirtfi
- **[REFEDS-R&S]:** REFEDS Research and Scholarship Entity Category https://refeds.org/category/research-and-scholarship

- **[REFEDS-DPCoCo]:** REFEDS Data Protection Code of Conduct https://refeds.org/category/code-of-conduct/v2
- **[eduGAIN]:** https://edugain.org/
- **[EuroHPC]:** https://eurohpc-ju.europa.eu/
- **[eIDAS]:** eIDAS Regulation https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
- **[EOSC-TSI-TF]:** EOSC Technical and Semantic Interoperability Task Force https://eosc.eu/advisory-groups/technical-and-semantic-interoperability-task-force/
- **[EOSC-Association]:** https://eosc.eu/
- **[EOSC-EU-NODE]:** https://open-science-cloud.ec.europa.eu/about/eosc-eu-node
- **[AEGIS]:** AARC Engagement Group for Infrastructures https://aarc-community.org/about/aegis/
- **[AARC]:** Authentication and Authorisation for Research and Collaboration (AARC) https://aarc-community.org/
- **[AARC-TREE]:** AARC Technical Revision to Enhance Effectiveness https://aarc-community.org/aarc-tree-project/
- **[AARC-Architecture]:** https://wiki.geant.org/display/AARC/AARC+Architecture
- **[Policy-WGs]:** AARC Policy Harmonisation https://wiki.geant.org/display/AARC/AARC+Policy+Harmonisation
- **[EOSC -AAI]:** https://wiki.geant.org/display/AARC/EOSC+AAI
- **[EOSC-Handbook]:** EOSC Federation Handbook https://zenodo.org/records/14999577
- **[EOSC-AAI-Report]:** Report from the EOSC Executive Board Working Group (WG) Architecture AAI Task Force (TF) https://op.europa.eu/en/publication-detail/-/publication/d1bc3702-61e5-11eb-aeb5-01aa75ed71a1/language-en

- **[EOSC-Architecture-2022]:** EOSC AAI Architecture 2022 https://zenodo.org/records/10379293
- **[EOSC-AAI-TF]:** Authentication and Authorization Infrastructure Architecture (AAI) Task Force https://eosc.eu/advisory-groups/aai-architecture
- **[OID-Fed]:** OpenID Federation 1.0 - draft 42 https://openid.net/specs/openid-federation-1_0.html
- **[MyAccessID]:** https://wiki.geant.org/display/MyAccessID
- **[RFC6749]:** The OAuth 2.0 Authorization Framework https://datatracker.ietf.org/doc/html/rfc6749
- **[RFC9700]:** Best Current Practice for OAuth 2.0 Security https://datatracker.ietf.org/doc/html/rfc9700
- **[OIDC-Dynamic-Reg]:** OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 2 https://openid.net/specs/openid-connect-registration-1_0.html
- **[SAML2]:** Security Assertion Markup Language (SAML) V2.0 Technical Overview https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
- **[RFC6749-1.3.1]:** Authorization Code https://datatracker.ietf.org/doc/html/rfc6749#section-1.3.1
- **[RFC8628]:** OAuth 2.0 Device Authorization Grant https://datatracker.ietf.org/doc/html/rfc8628
- **[RFC6749-6]:** Refreshing an Access Token https://datatracker.ietf.org/doc/html/rfc6749#section-6
- **[RFC6749-4.4]:** Client Credentials Grant https://datatracker.ietf.org/doc/html/rfc6749#section-4.4
- **[RFC6749-2.1]:** Client Types https://datatracker.ietf.org/doc/html/rfc6749#section-2.1
- **[RFC7662]:** OAuth 2.0 Token Introspection https://datatracker.ietf.org/doc/html/rfc7662

- **[EUDI-Wallet]:** EU Digital Identity Wallets https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home
- **[eduGAIN-PoC]:** eduGAIN PoC https://wiki.geant.org/display/GWP5/eduGAIN+PoC
- **[OID-Fed-Wallet]:** OpenID Federation Wallet Architectures 1.0 - draft 03 https://openid.net/specs/openid-federation-wallet-1_0.html
- **[AARC-BPA]:** AARC Blueprint Architecture https://aarc-community.org/architecture/
- **[AARC-BPA-2025]:** AARC Blueprint Architecture 2025 (Under development) https://aarc-community.org/guidelines/aarc-g080/
- **[AARC-I058]:** Methods for Establishing Trust between proxies in different trust domains (Under development) https://aarc-community.org/guidelines/aarc-i058/
- **[AARC-G056]:** AARC Profile for expressing identity attributes (Under development) https://docs.google.com/document/d/1jO1X7GSXWf_R604j5LXinr37ZUf96YVdIXSvjpS_Vyk/edit?tab=t.0
- **[OIDC-Core-3.1]:** Authentication using the Authorization Code Flow https://openid.net/specs/openid-connect-core-1_0.html#CodeFlowAuth
- **[EOSC-Security-Baseline-2022]:** EOSC Security Operational Baseline 2022 https://zenodo.org/records/7396725
- **[RFC7519]:** JSON Web Token (JWT) https://www.rfc-editor.org/rfc/rfc7519
- **[RFC7519-4.1.2]:** "sub" (Subject) Claim https://datatracker.ietf.org/doc/html/rfc7519#section-4.1.2
- **[RFC9068]:** JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens https://www.rfc-editor.org/rfc/rfc9068
- **[AARC-G026]:** AARC-G026 Guidelines for expressing community user identifiers https://aarc-community.org/guidelines/aarc-g026/
- **[voPerson-v2]:** voPerson v2.0.0 https://github.com/voperson/voperson/blob/2.0.0/voPerson.md

- **[RFC2798]:** Definition of the inetOrgPerson LDAP Object Class https://www.rfc-editor.org/rfc/rfc2798
- **[RFC7643]:** System for Cross-domain Identity Management: Core Schema https://www.rfc-editor.org/rfc/rfc7643
- **[eduPerson]:** https://wiki.refeds.org/display/STAN/eduPerson
- **[REFEDS-Personalized-EC]:** Personalized Access Entity Category https://refeds.org/category/personalized
- **[RFC4519]:** Lightweight Directory Access Protocol (LDAP) https://www.rfc-editor.org/info/rfc4519
- **[RFC2821]:** Simple Mail Transfer Protocol https://datatracker.ietf.org/doc/html/rfc2821
- **[RFC1035]:** Domain names - implementation and specification https://www.rfc-editor.org/info/rfc1035
- **[REFEDS-SCHAC]:** SCHAC Releases https://wiki.refeds.org/display/STAN/SCHAC+Releases
- **[AARC-G057]:** Inferring and constructing origin-affiliation information across infrastructures https://aarc-community.org/guidelines/aarc-g057/
- **[AARC-G025]:** Guidelines for expressing affiliation information https://aarc-community.org/guidelines/aarc-g025/
- **[REFEDS-Assurance]:** REFEDS Assurance Framework https://refeds.org/assurance
- **[AARC-G021]:** Exchange of specific assurance information between Infrastructures https://aarc-community.org/guidelines/aarc-g021/
- **[AARC-G069]:** Guidelines for expressing group membership and role information https://aarc-community.org/guidelines/aarc-g069/
- **[AARC-G031]:** Guidelines for the evaluation and combination of the assurance of external identities https://aarc-community.org/guidelines/aarc-g031/
- **[AARC-G083]:** Guidance for Notice Management by Proxies https://aarc-community.org/guidelines/aarc-g083/

- **[AARC-G061]:** A specification for IdP hinting https://aarc-community.org/guidelines/aarc-g061/
- **[RFC9728]:** OAuth 2.0 Protected Resource Metadata https://datatracker.ietf.org/doc/rfc9728/
- **[AARC-G084]:** Security Operational Baseline https://aarc-community.org/guidelines/aarc-g084/

Annex I - Sequence Diagrams

The following sequence diagrams are written using **MermaidJS**, a text-based diagramming syntax. To visualise them, you can use any MermaidJS-compatible viewer, such as:

- Mermaid Live Editor
- VS Code with the Mermaid extension
- Markdown preview tools that support MermaidJS (e.g. Obsidian, Typora, or GitHub with Mermaid enabled)

Simply copy and paste the Mermaid code into one of these tools to render the diagram.

Rendered versions of the diagrams can be found at:
https://wiki.geant.org/display/AARC/EOSC+AAI+Architecture+March+2025

SSO Use Case

```
sequenceDiagram
participant User
participant Service 1
participant EOSCNodeXInfra as Infrastructure Proxy (EOSC Node X)
participant Service 4
participant EOSCNodeYInfra as Infrastructure Proxy (EOSC Node Y)
participant MyAccessID
participant Identity Provider

Note right of User: Accessing Service 1 connected to the Infrastructure Proxy of EOSC Node X

User->>Service 1: Accesses Service 1 provided by EOSC Node X

Service 1->>EOSCNodeXInfra: Redirects User to the Infrastructure Proxy of EOSC Node X
```

```
EOSCNodeXInfra->>MyAccessID: Redirects User to MyAccessID for authentication
MyAccessID->>User: Presents a list of available Identity Providers (Discovery Service)
User->>MyAccessID: Selects preferred available Identity Provider
MyAccessID->>Identity Provider: Redirects User to the selected Identity Provider
Identity Provider->>User: Displays login page
User->>Identity Provider: Authenticates and consents to share required attributes
Identity Provider->>MyAccessID: Returns User’s identity and attributes
MyAccessID->>MyAccessID: Attempts to identify the User internally
Note left of MyAccessID: If User is not recognised, initiate registration flow
MyAccessID->>User: Redirects User to the registration page
User->>MyAccessID: Completes and confirms required information and consents
MyAccessID->>MyAccessID: Creates a new account and recognises the User
Note left of MyAccessID: If User is recognised, collect identifier and attributes
MyAccessID->>EOSCNodeXInfra: Sends User information to EOSC Node X Infrastructure Proxy
EOSCNodeXInfra->>Service 1: Enriches User information and redirects back to Service 1
Service 1->>User: Grants access to Service 1
Note right of User: Accessing Service 4 via the Infrastructure Proxy of EOSC Node Y with an active SSO session
User->>Service 4: Accesses Service 4 provided by EOSC Node Y
Service 4->>EOSCNodeYInfra: Redirects User to the Infrastructure Proxy of EOSC Node Y
EOSCNodeYInfra->>MyAccessID: Redirects User to MyAccessID for authentication
MyAccessID->>Identity Provider: Redirects User to Identity Provider (SSO session active)
```

```
Identity Provider->>MyAccessID: Authenticates via SSO and returns identity and attributes

MyAccessID->>MyAccessID: Recognises the User

MyAccessID->>EOSCNodeYInfra: Sends User information to the Infrastructure Proxy of EOSC Node Y

EOSCNodeYInfra->>Service 4: Enriches User information and redirects back to Service 4

Service 4->>User: Grants access to Service 4
```

Cross-node workflow

```
sequenceDiagram
    participant User
    participant Service 1
    participant EOSCNodeXInfra as Infrastructure Proxy (EOSC Node X)
    participant Service 4
    participant EOSCNodeYInfra as Infrastructure Proxy (EOSC Node Y)
    participant MyAccessID
    participant Identity Provider

    Note right of User: Obtaining an Access Token (AT) issued for Service 1 by EOSC Node X

    User->>Service 1: Accesses Service 1 provided by EOSC Node X

    Service 1->>EOSCNodeXInfra: Redirects User to the Infrastructure Proxy of EOSC Node X

    EOSCNodeXInfra->>MyAccessID: Redirects User to MyAccessID for authentication

    MyAccessID->>User: Presents list of available Identity Providers (Discovery Service)

    User->>MyAccessID: Selects preferred Identity Provider

    MyAccessID->>Identity Provider: Redirects User to selected Identity Provider

    Identity Provider->>User: Displays login page

    User->>Identity Provider: Authenticates and consents to share required attributes
```

```
Identity Provider->>MyAccessID: Returns User’s identity and attributes

MyAccessID->>MyAccessID: Identifies User internally

MyAccessID->>EOSCNodeXInfra: Sends User information to EOSC Node X Infrastructure Proxy

EOSCNodeXInfra->>Service 1: Issues Access Token (AT-X) to Service 1

Service 1->>User: Provides Access Token (AT-X) to User (e.g., for CLI use)

Note right of User: Using Access Token (AT-X) issued by EOSC Node X at EOSC Node Y

User->>Service 4: Accesses API of Service 4 in EOSC Node Y using AT-X

Service 4->>EOSCNodeYInfra: Sends AT-X for introspection to EOSC Node Y Infrastructure Proxy

EOSCNodeYInfra->>EOSCNodeYInfra: Cannot validate AT-X (was not issued here)

EOSCNodeYInfra->>MyAccessID: Sends AT-X for introspection to MyAccessID

MyAccessID->>MyAccessID: Recognises issuing proxy for AT-X

MyAccessID->>EOSCNodeXInfra: Performs introspection request to EOSC Node X Infrastructure Proxy

EOSCNodeXInfra->>EOSCNodeXInfra: Validates AT-X (issuer of token)

EOSCNodeXInfra->>MyAccessID: Returns introspection results to MyAccessID

MyAccessID->>EOSCNodeYInfra: Returns introspection results to EOSC Node Y Infrastructure Proxy

EOSCNodeYInfra->>Service 4: Returns introspection results to Service 4

Service 4->>User: Authorises User request to access Service 4 API
```