GEANT Core AAI Platform

MyAccessID - EuroFP - EOSC

2027 Vision

- eduGAIN is the Global Trust Fabric for Research & Education
- The GEANT AAI is omnipresent in the European Research & Education space
- A Data Sharing infrastructure for education is delivered by the NRENs

2027 Vision

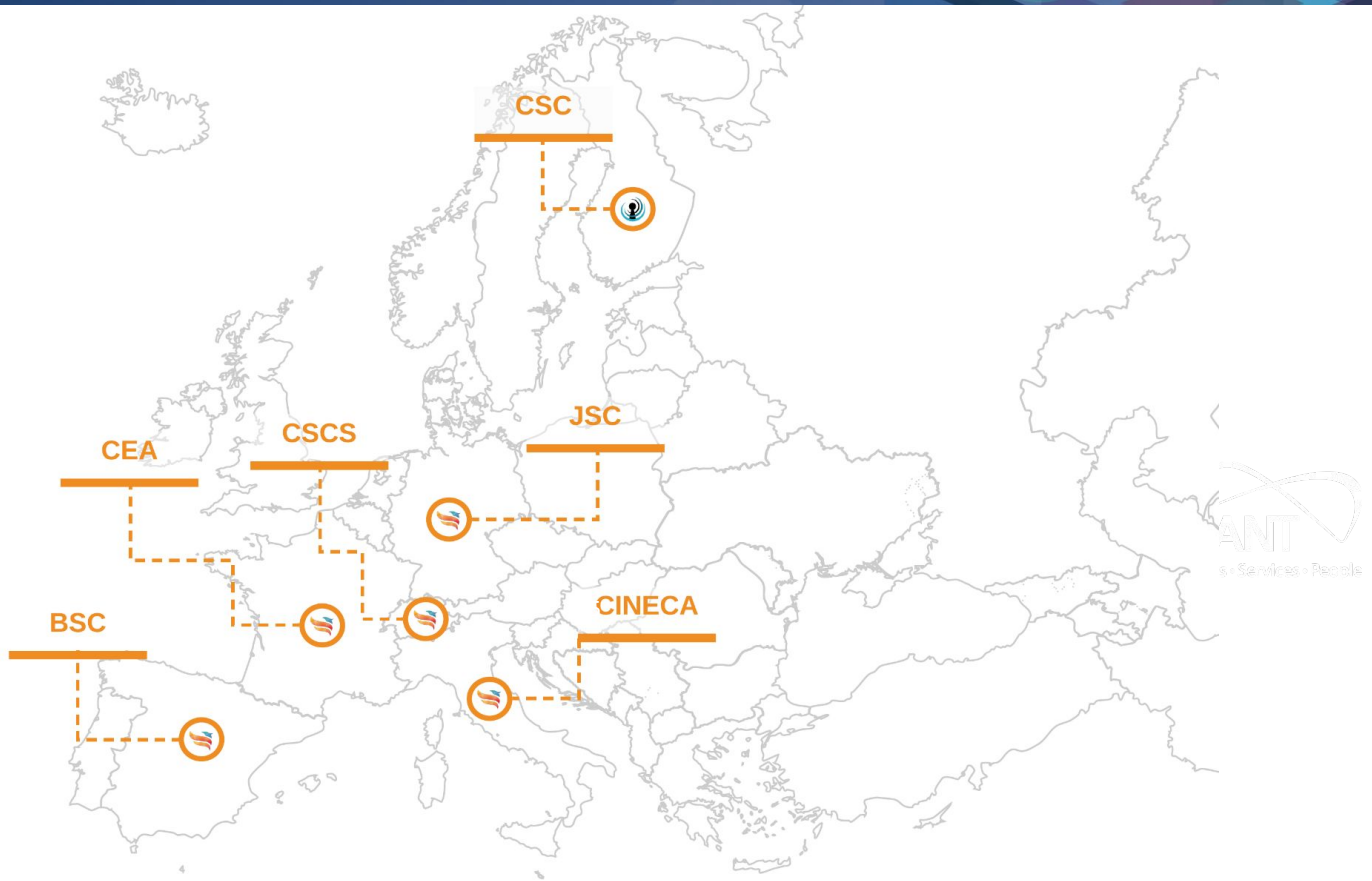
From the EOSC Multi-Annual Roadmap (MAR) 2025–2027

EOSC should continue to utilise existing AAI, as provided by the National Research and Education Networks and GÉANT. ***Akin to network provision, this is supported under other programmes and should continue as such, rather than funding duplicate work in EOSC****.*

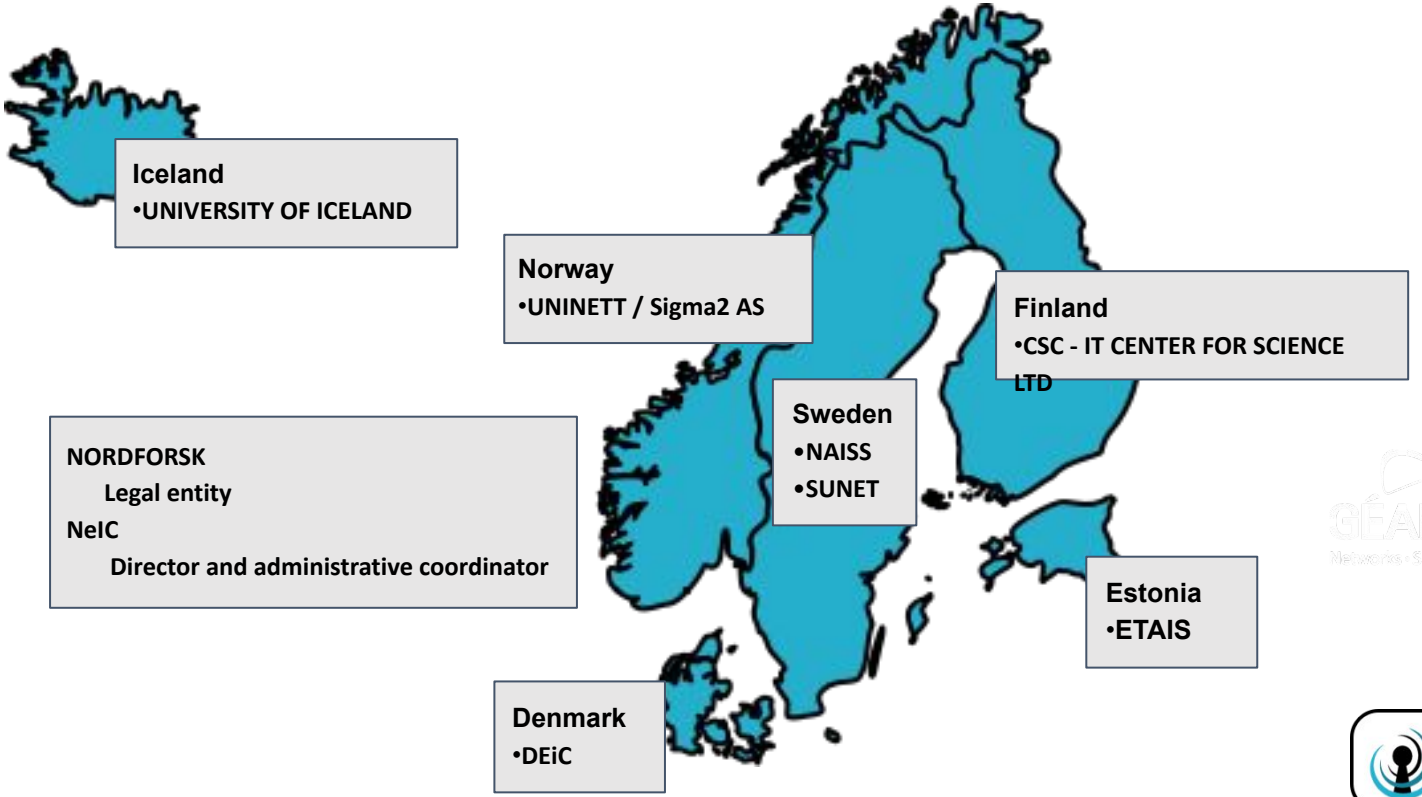
From 2027 onwards, EOSC will remain a major stakeholder in the pan-European AAI for research and education and will actively contribute with requirements, use cases and participation in standardisation activities.


MyAccessID

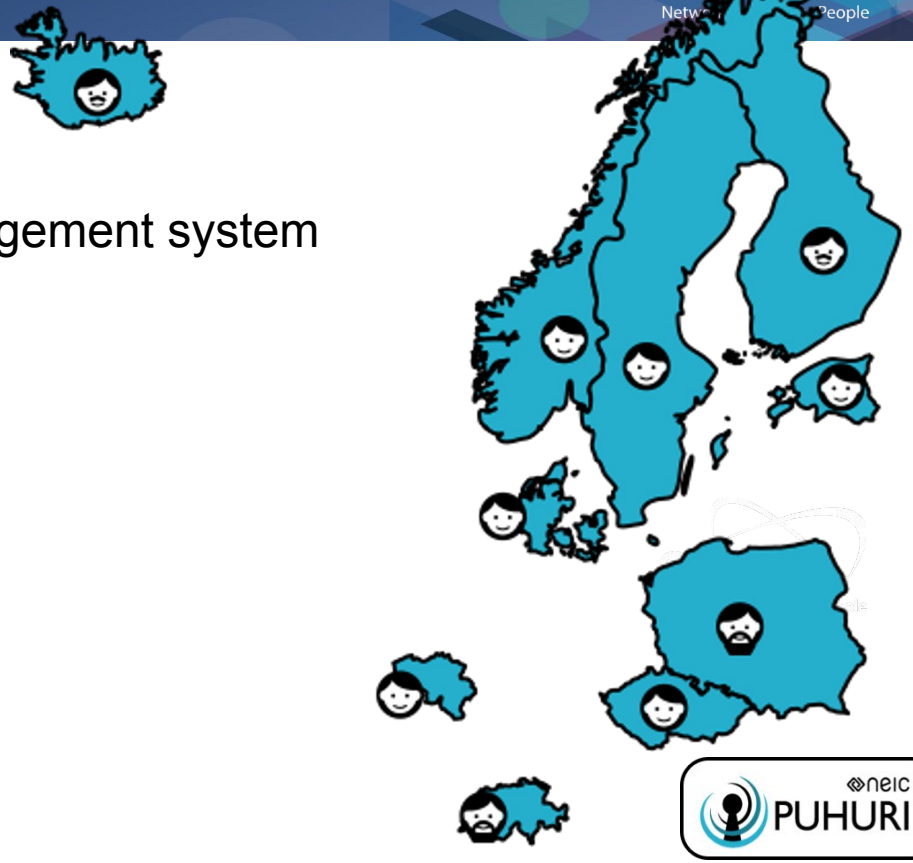
FENIX
RESEARCH INFRASTRUCTURE



Who are behind Puhuri?



Scope of Puhuri

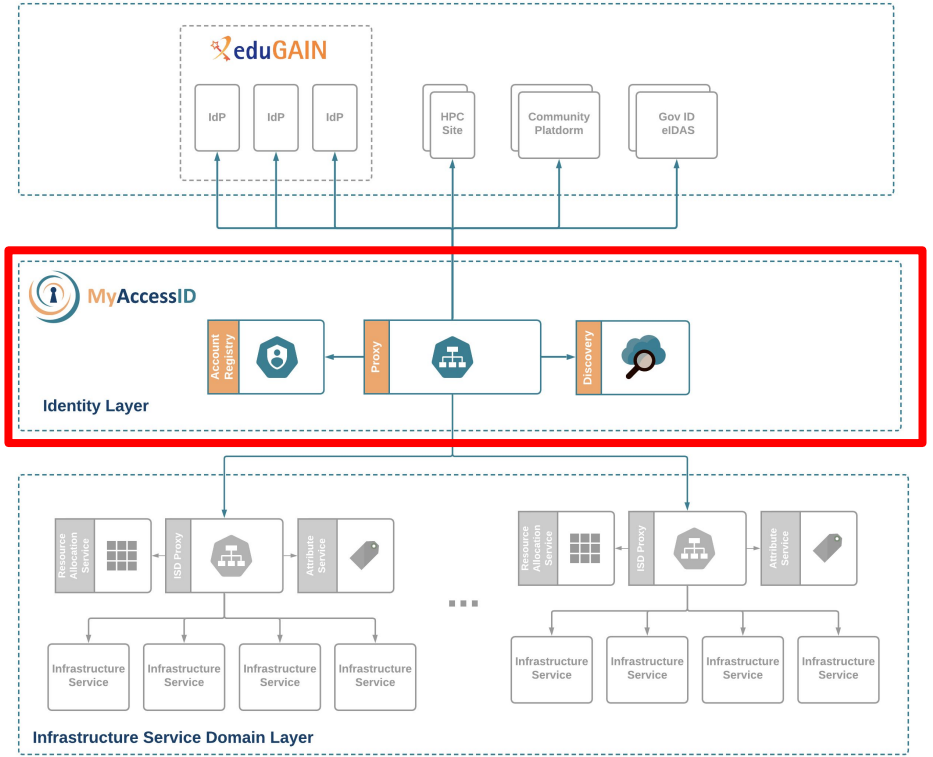


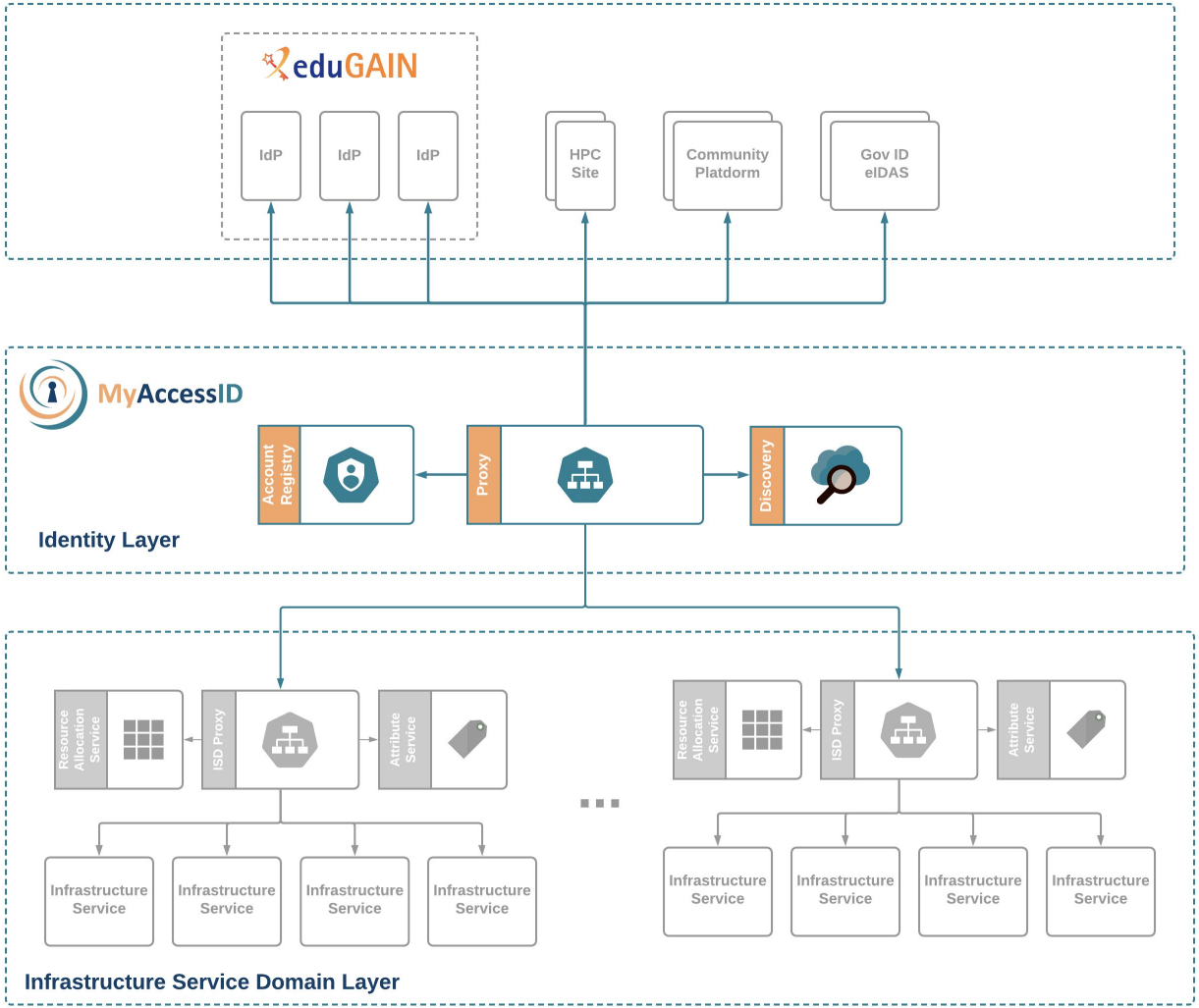
Single system multiple service owners
Unified allocation, project, and user management system

- Authentication
- Authorisation
- Identification
- Resource allocation
- Project management
- Etc.

Towards a common AAI

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

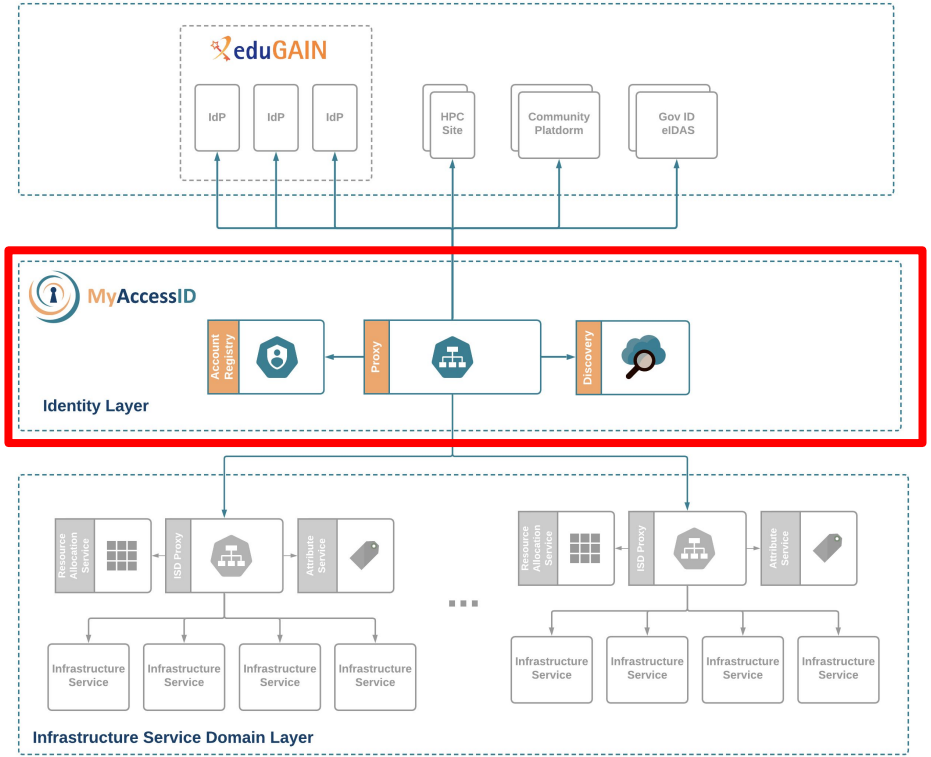



eduGAIN
IdP
IdP
IdP
HPC Site
Community Platdorm
Gov ID eIDAS
MyAccessID
Account Registry
Proxy
Discovery
Identity Layer
Resource Allocation Service
ISD Proxy
Attribute Service
Infrastructure Service
Infrastructure Service
Infrastructure Service
Infrastructure Service
Resource Allocation Service
ISD Proxy
Attribute Service
Infrastructure Service
Infrastructure Service
Infrastructure Service
Infrastructure Service
Infrastructure Service Domain Layer

Towards a common AAI

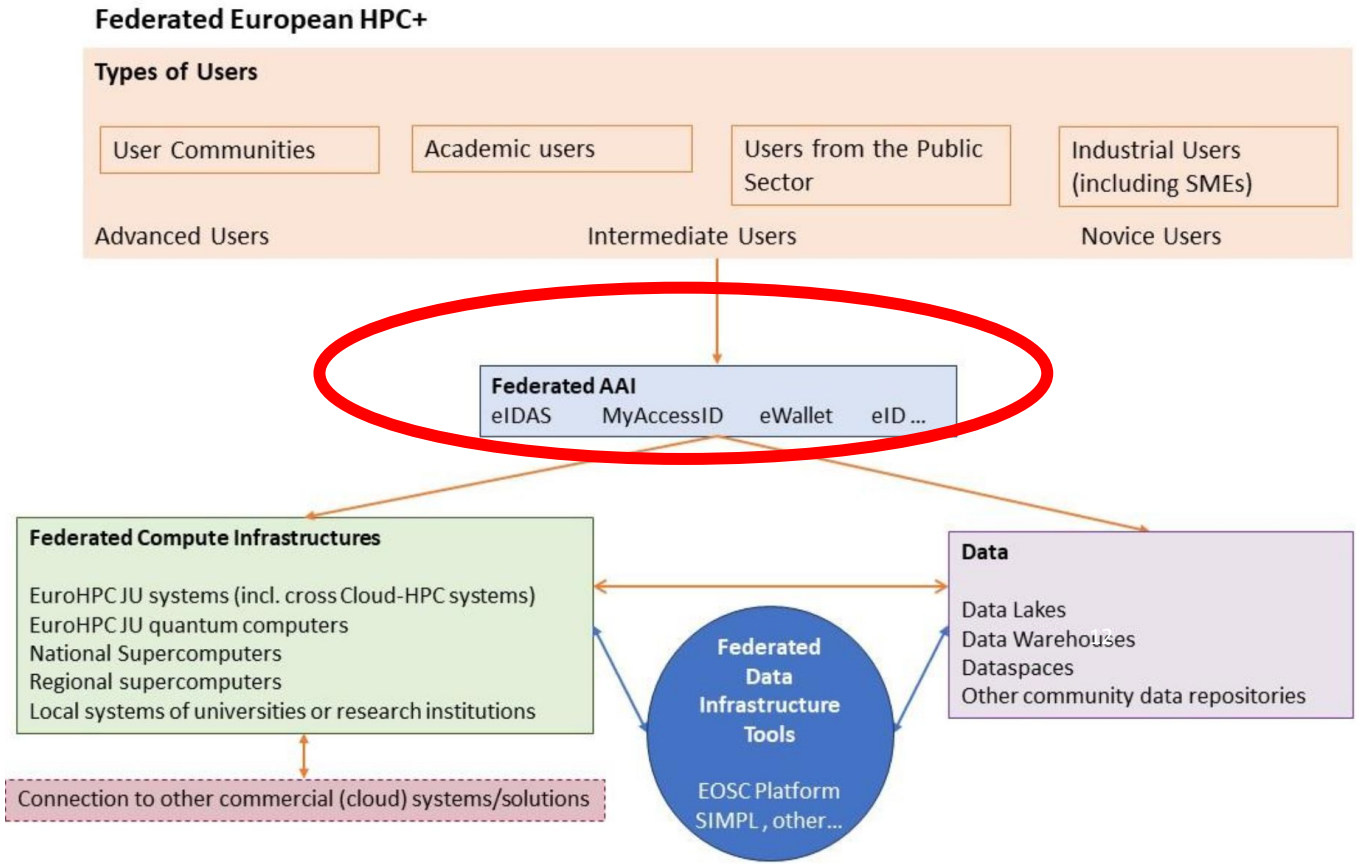
- **For users**
  - One identity to access resources across HPC sites and other infrastructures
  - Ability to link multiple external identities (e.g. institutional accounts, national eIDs etc)
  - Easy for novice users, unlocks new capabilities for advanced users.

- **For Infrastructures:**
  - A common way of authenticating users
  - Strong identity assurance
  - Multi-factor authentication
  - Multi-protocol support (OIDC, SAML)
  - Improved access management including terminal access

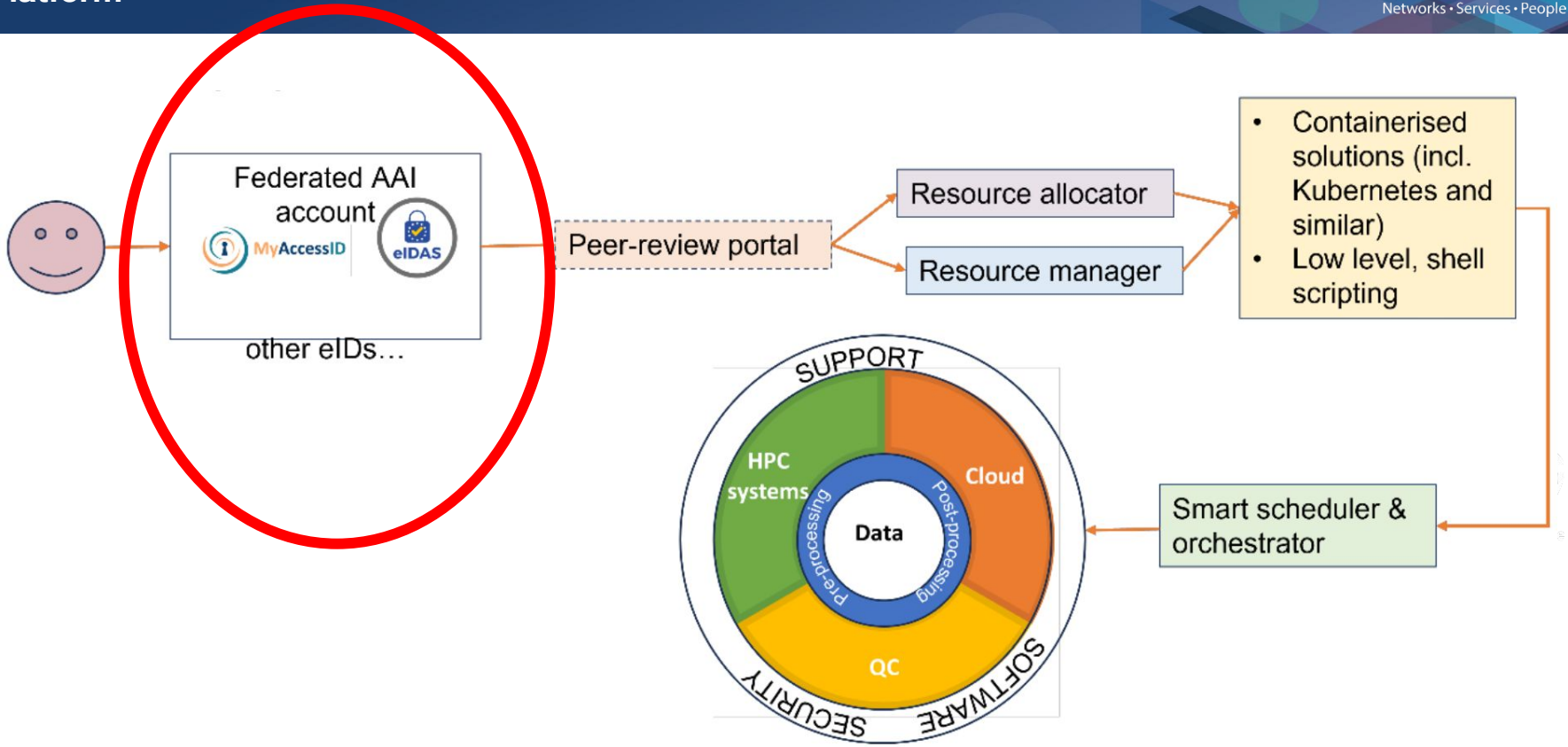


“Invitation to Tender: Acquisition, delivery, installation and services of the EuroHPC federation platform for the EuroHPC JU”

Overall vision of a world-leading federated and secure HPC, Quantum and Cloud service infrastructure ecosystem in the Union



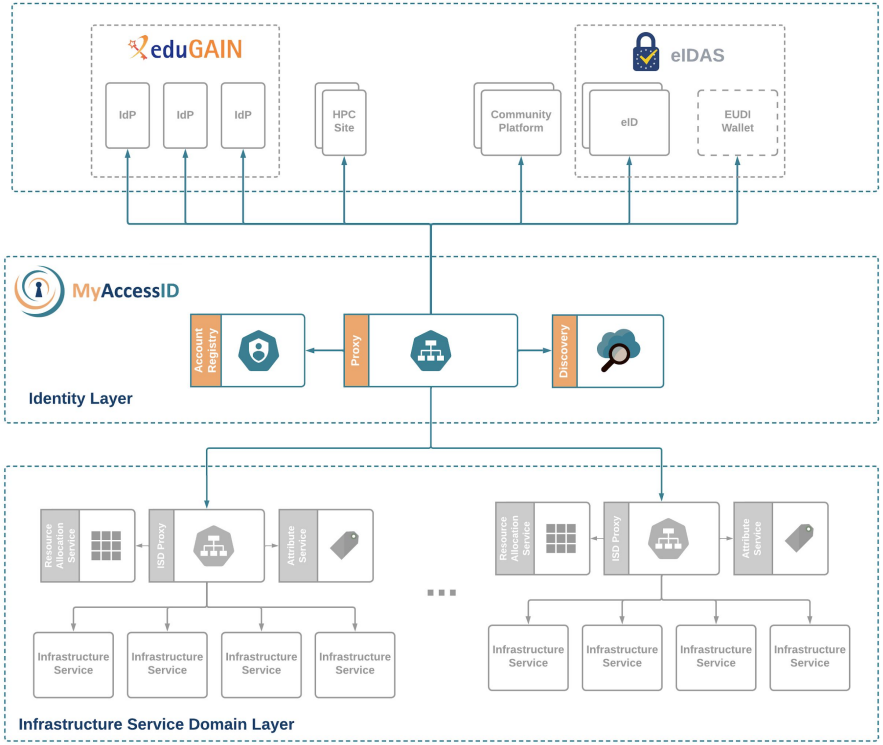
Overall architecture concept of the EuroHPC Federation Platform



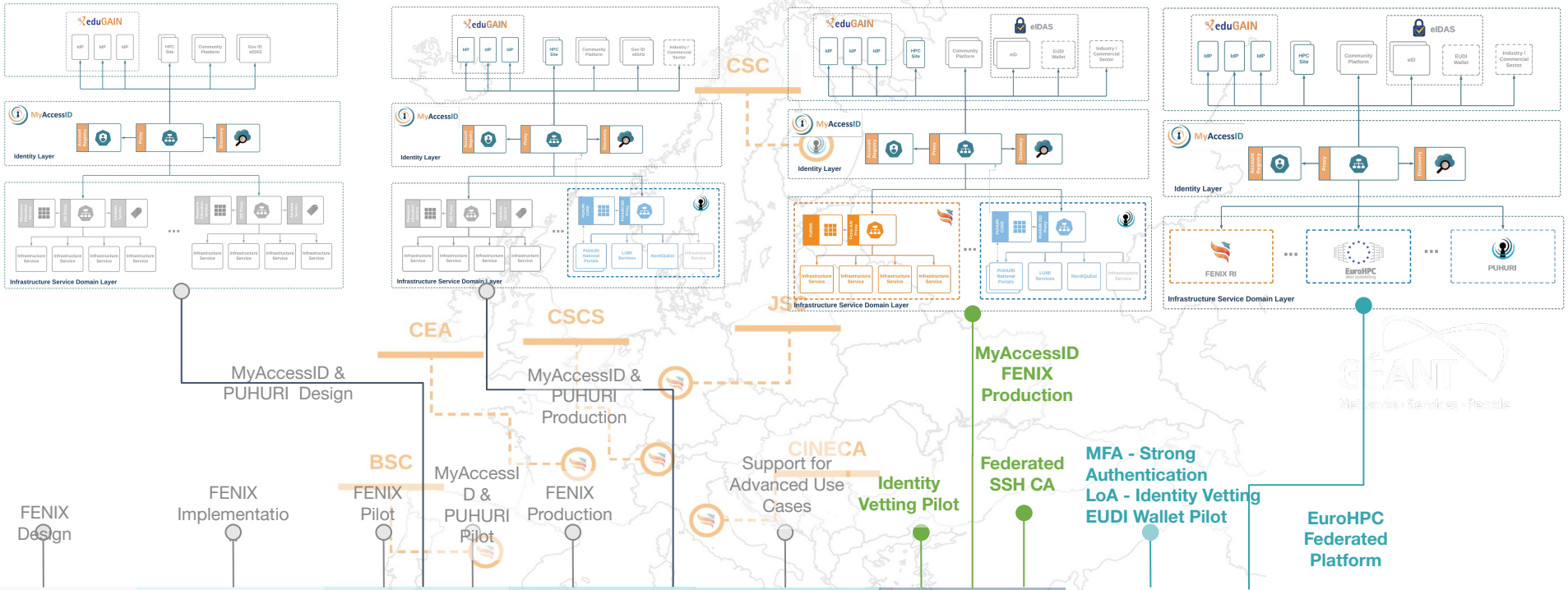
EuroHPC Federation Platform Call

*"Accommodates **MyAccessID and eIDs based on eIDAS regulation such as EUDI wallet** should be the bases of the EuroFP solution across all EuroHPC HPCQ+ current and upcoming hosting entities."*

*"The creation of **a trusted AAI user ID through EuroFP should already start from the moment the user would like to access the peer-review platform for application submission** and later have the possibility to be coupled to the resource allocation and resource management components across EuroHPC systems"*



Roadmap


eduGAIN
MyAccessID
Identity Layer
Infrastructure Service Domain Layer
eIDAS
FENIX RI
EuroHPC
PUHURI
CSC
CEA
CSCS
JSC
CINECA
BSC
MyAccessID & PUHURI Design
MyAccessID & PUHURI Production
MyAccessID FENIX Production
FENIX Design
FENIX Implementatio
FENIX Pilot
MyAccessI D & PUHURI Pilot
FENIX Production
Support for Advanced Use Cases
Identity Vetting Pilot
Federated SSH CA
MFA - Strong Authentication
LoA - Identity Vetting
EUDI Wallet Pilot
EuroHPC Federated Platform
2018
2019
2020
2021
2022
2023
2024
2025
2026


eosc

What is AAI?

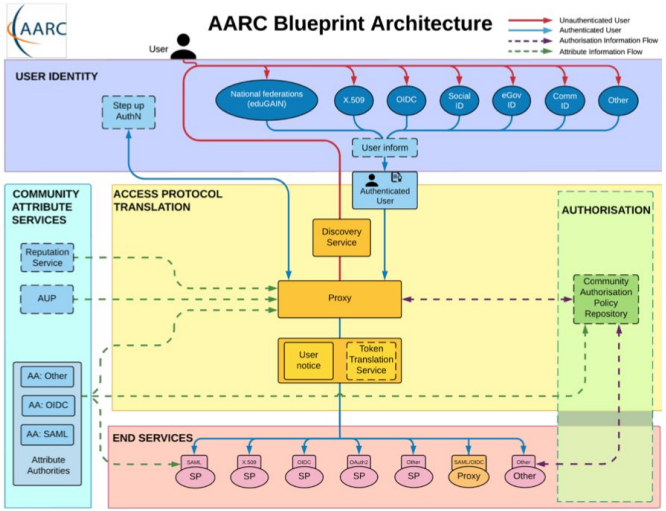
- AAI stands for Authentication and Authorization Infrastructure
- Science Clusters, Research Infrastructures and e-Infrastructure Providers have been been implementing their AAIs using the AARC Blueprint Architecture in order to manage their users and the access rights to resources
    - The AARC Blueprint Architecture (BPA) provides a set of building blocks for software architects and technical decision makers who are designing and implementing access management solutions for international research collaborations.

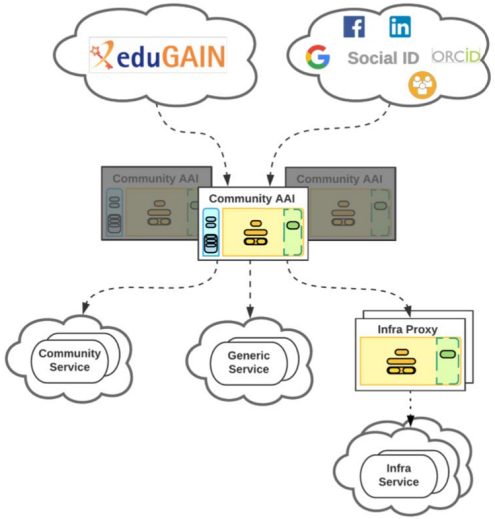
What is the EOSC AAI?

- The goal for the EOSC AAI is to provide the trust mortar with which we join the many bricks of the current set of scientific communities, collaborations and infrastructures together.
    - *The term "EOSC AAI" has sometimes been interpreted as a singular instance of the EOSC AAI Architecture. Nothing could be further from the truth. The EOSC AAI is a set of principles and governance structures for how the architecture evolves and grows over time.*
- The EOSC AAI is comprised of the AAIs of the Science Clusters, Research Infrastructures and e-Infrastructure Providers, which are being brought together through the EOSC AAI Federation

EOSC AAI Baseline Architecture

Based on the AARC Blueprint Architecture





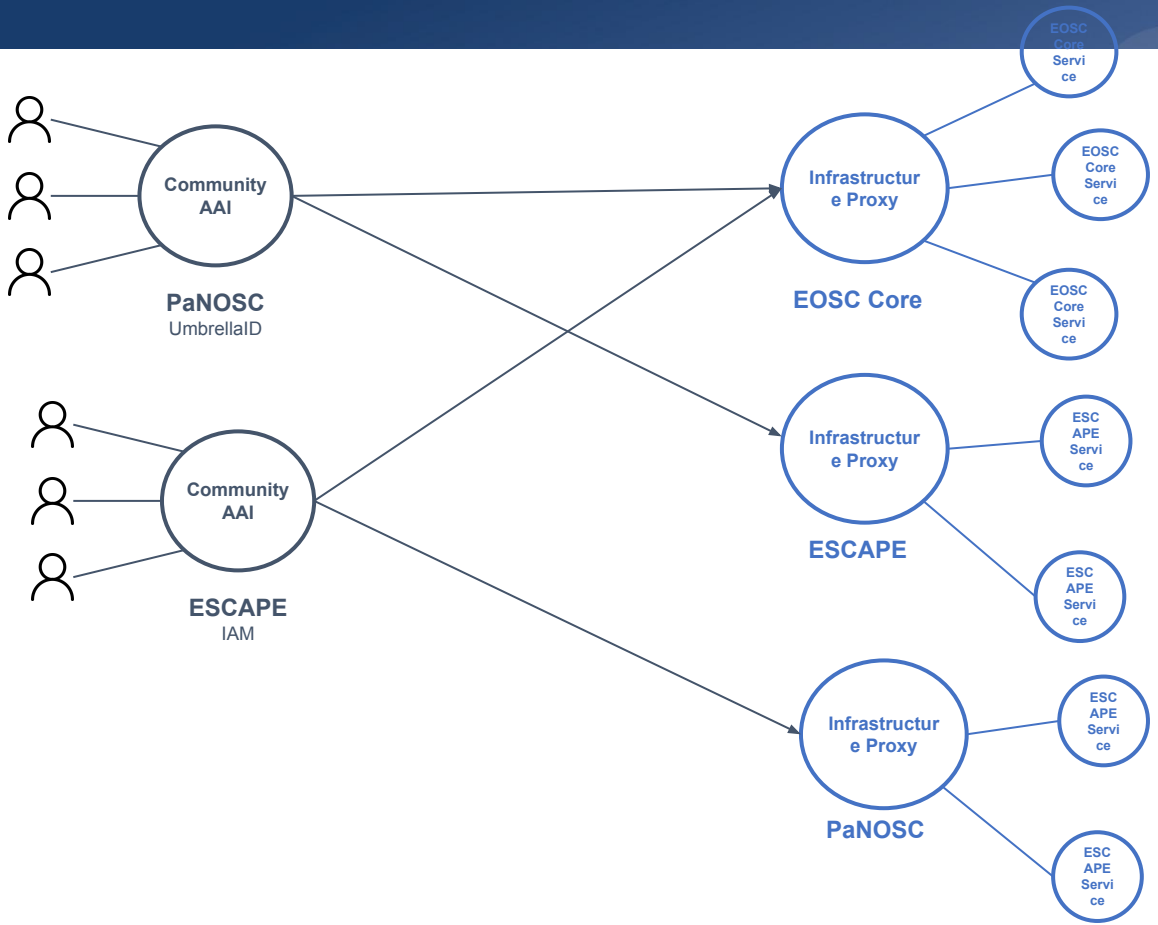
Community AAI

The purpose of the Community AAI is to streamline researchers' access to services, both those provided by their own infrastructure as well as the services provided by infrastructures that are shared with other communities.

Infrastructure Proxy

The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single
integration point, where the Infrastructure can maintain centrally all the relevant policies
and business logic for making available these resources to multiple communities

What is the EOSC AAI?



Community AAI

The purpose of the Community AAI is to streamline researchers' access to services, both those provided by their own infrastructure as well as the services provided by infrastructures that are shared with other communities.

Infrastructure Proxy

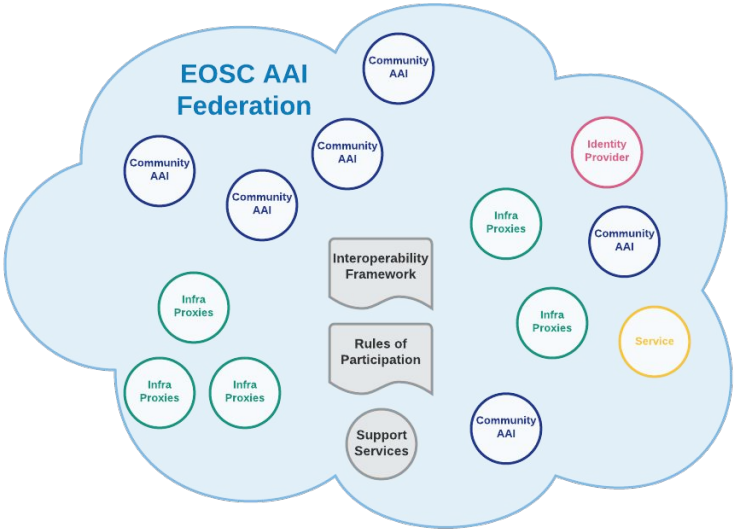
The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single
integration point, where the Infrastructure can maintain centrally all the relevant policies
and business logic for making available these resources to multiple communities

EOSC Authentication and Authorization Infrastructure (AAI) : report from the EOSC Executive Board Working Group (WG) Architecture AAI Task Force (TF)

https://data.europa.eu/doi/10.2777/8702

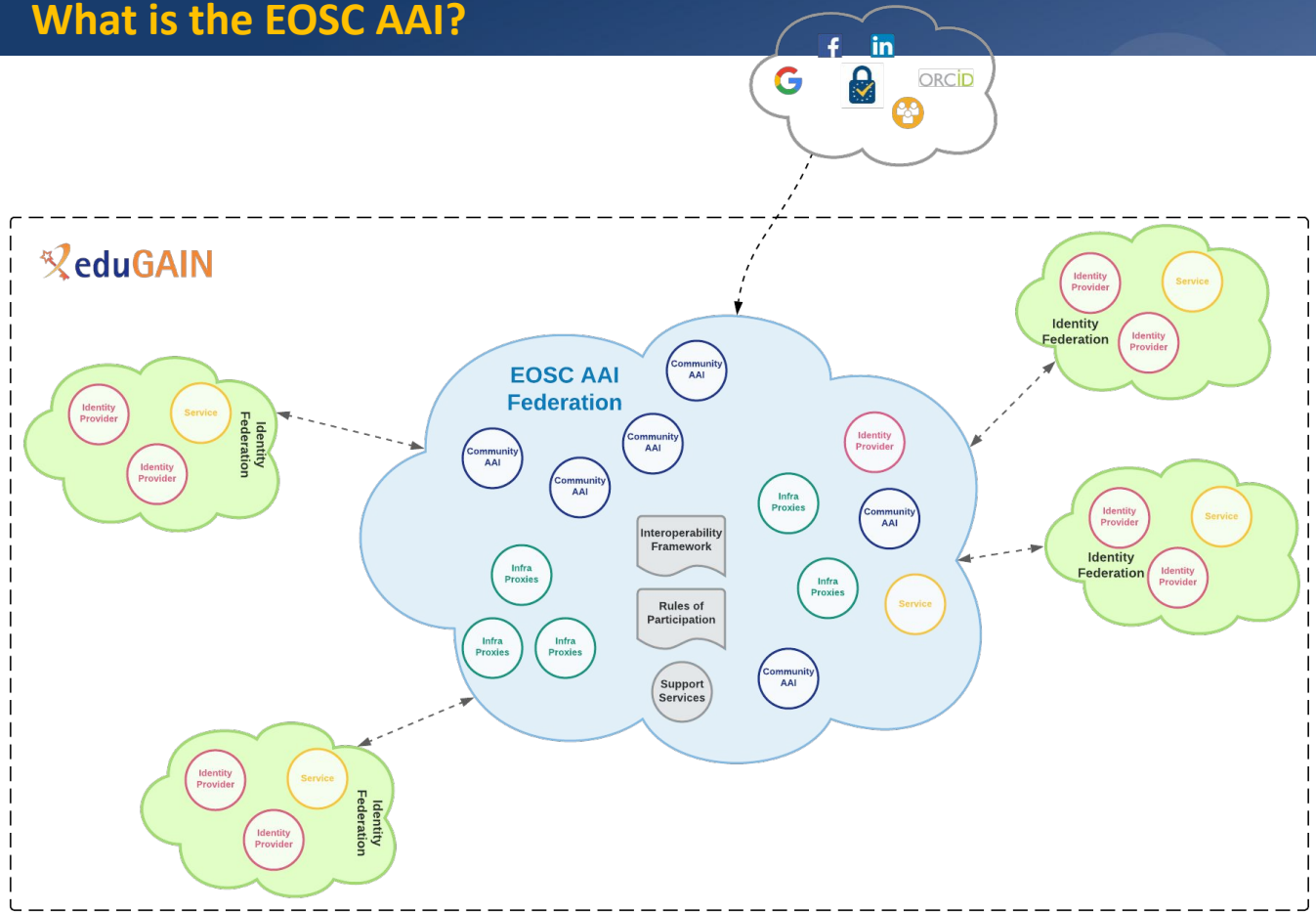
AARC Blueprint Architecture 2019
https://doi.org/10.5281/zenodo.3672784

What is the EOSC AAI?



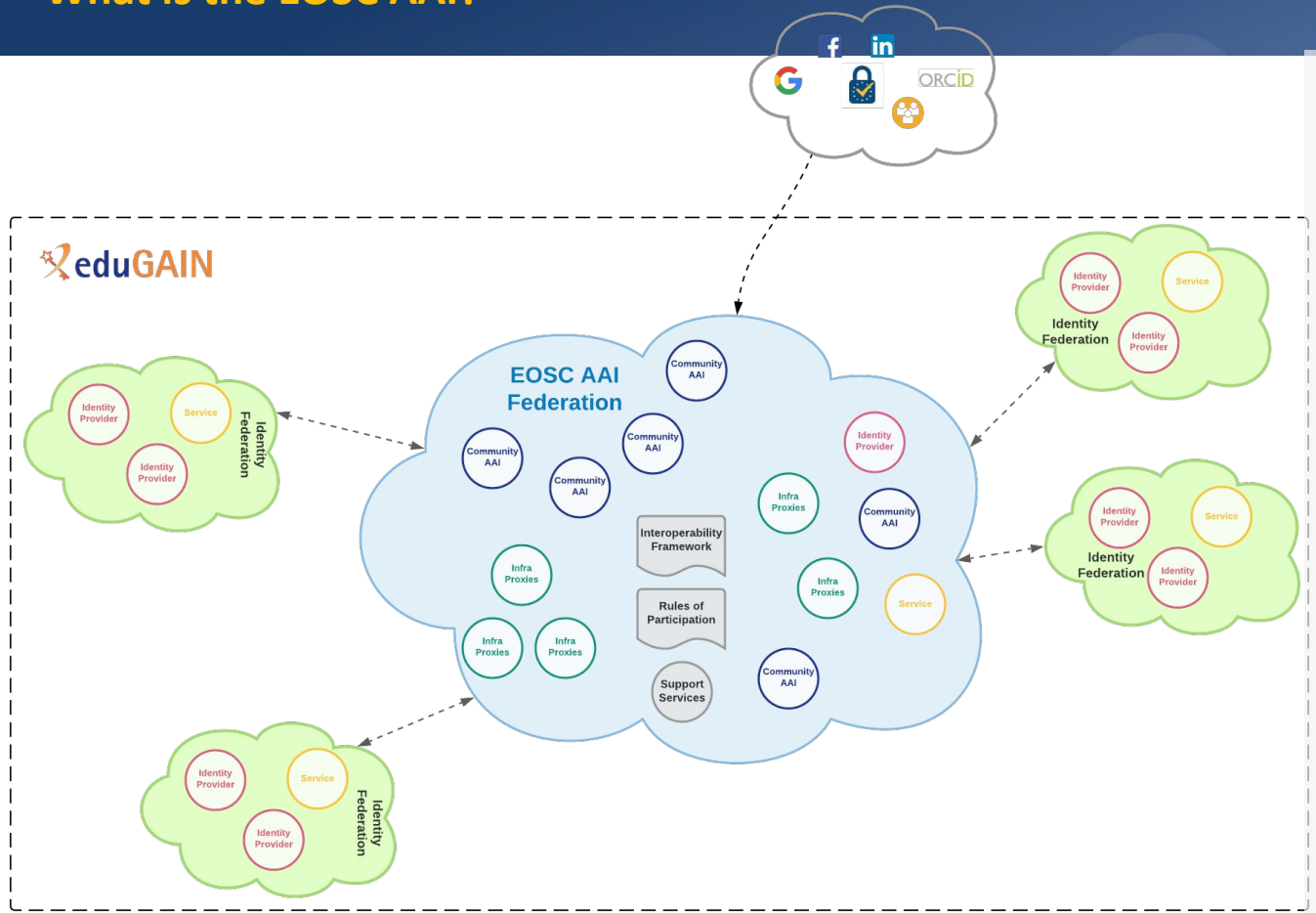
- Community AAIs and Infrastructure Proxies connect once with the EOSC AAI Federation (register metadata, URN namespaces, policies etc)
- Technical interoperability conformance tested and monitored by the EOSC AAI FEderation.
- GDPR and Security Policy conformance (Policy Notices, Acceptable Use Policy etc) assessed by the EOSC AAI Federation.
- Community AAIs and Infrastructure Proxies discovery and establish trust with the rest of the Community AAIs and Infrastructure Proxies through the EOSC AAI Federation

What is the EOSC AAI?



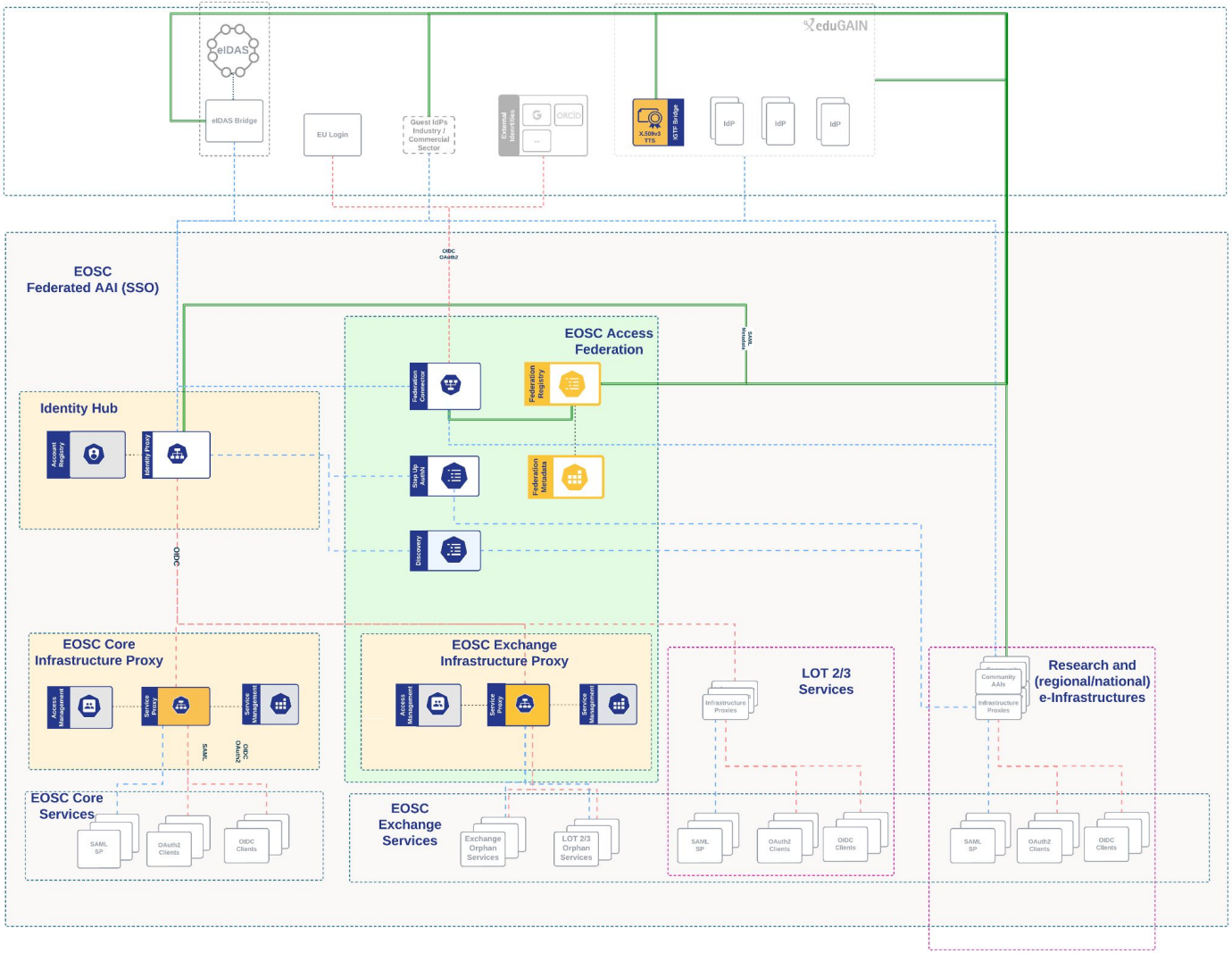
The EOSC AAI Federation participates in the eduGAIN Inter-Federation to discovery and establish trust with Identity Providers and Services Providers that the EOSC AAI Federation requirements

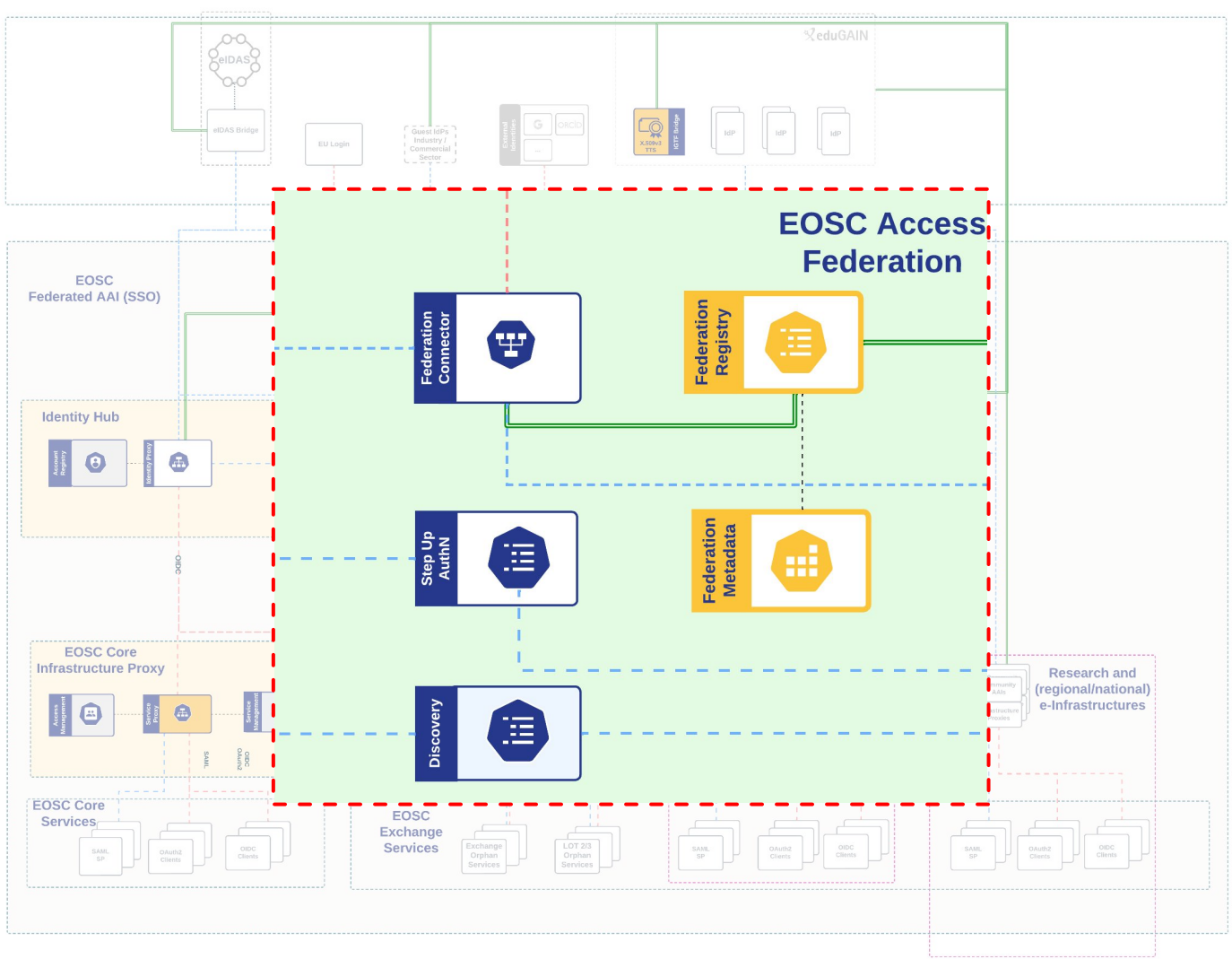
What is the EOSC AAI?



What the EOSC AAI Federation is NOT

- **It is not a resource allocation mechanism**. Being part of the federation does not mean that users automatically have access to resources. Services will be able to authenticate and identify users and communities.
- **It is not the EOSC Core Infrastructure Proxy used.** The EOSC Core Infrastructure Proxy is one of the Infrastructure Proxies that will be members of the EOSC AAI Federation.
- **It does not remove the need for community and sciences clusters to have their Community AAI and/or Infrastructure Proxies.** Participants are expected to use an AARC BPA Compliant Community AAI / Infrastructure Proxy


eIDAS
eIDAS Bridge
EU Login
Guest IdPs Industry / Commercial Sector
External Identities
ORCID
...
eduGAIN
X.509v3 TTS
IGTF Bridge
IdP
IdP
IdP
EOSC Federated AAI (SSO)
OIDC OAuth2
SAML Metadata
EOSC Access Federation
Federation Connector
Federation Registry
Identity Hub
Account Registry
Identity Proxy
Sirtfi Up AssVAs
Federation Metadata
Discovery
OIDC
EOSC Core Infrastructure Proxy
Access Management
Service Proxy
Service Management
SAML
OIDC OAuth2
EOSC Exchange Infrastructure Proxy
Access Management
Service Proxy
Service Management
LOT 2/3 Services
Infrastructure Proxies
Research and (regional/national) e-Infrastructures
Community AAIs
Infrastructure Proxies
EOSC Core Services
SAML SP
OAuth2 Clients
OIDC Clients
EOSC Exchange Services
Exchange Orphan Services
LOT 2/3 Orphan Services
SAML SP
OAuth2 Clients
OIDC Clients
SAML SP
OAuth2 Clients
OIDC Clients



EOSC Access Federation

Provided by GEANT

Registers, maintains, and publishes the trust anchors and the associated metadata for all the entities in the **EOSC Federated AAI.** Provides common horizontal functionalities.

Federation Registry
Fetches, validates, and stores information about all connected services and identity providers. Exposes metadata feeds and APIs (MDQ).

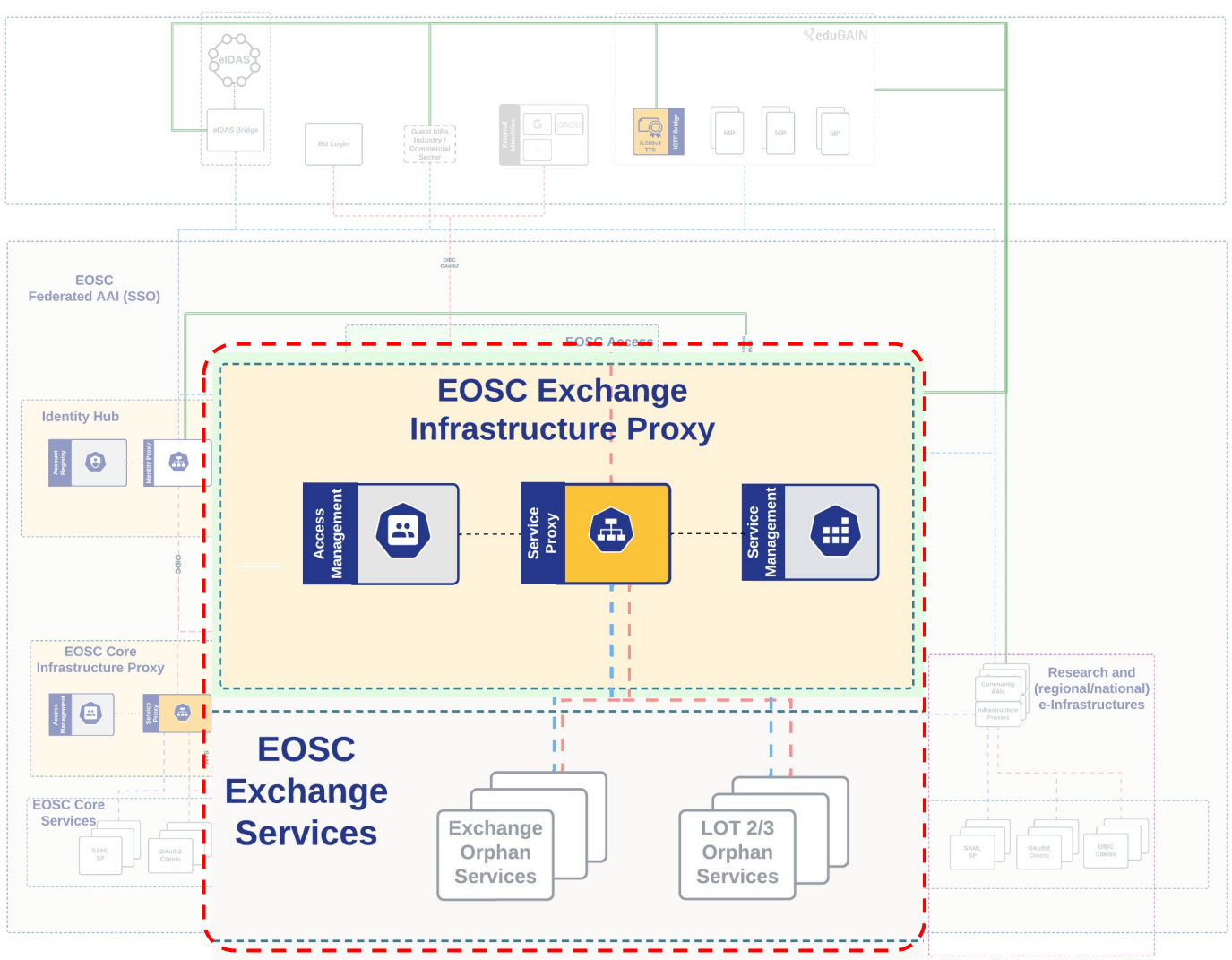
Discovery Service
Allows the user to find and select their Identity Provider.

Federation Connector
It supports OAuth2 and OpenID Connect for authenticating users.

Federation Registry
Registry for al; the entities in the EOSC Access Federation.

Federation Metadata
Stores and delivers the EOSC Access Federation metadata.

Step-Up Authentication
Enhances the authentication strength when users request access to security-sensitive resources.



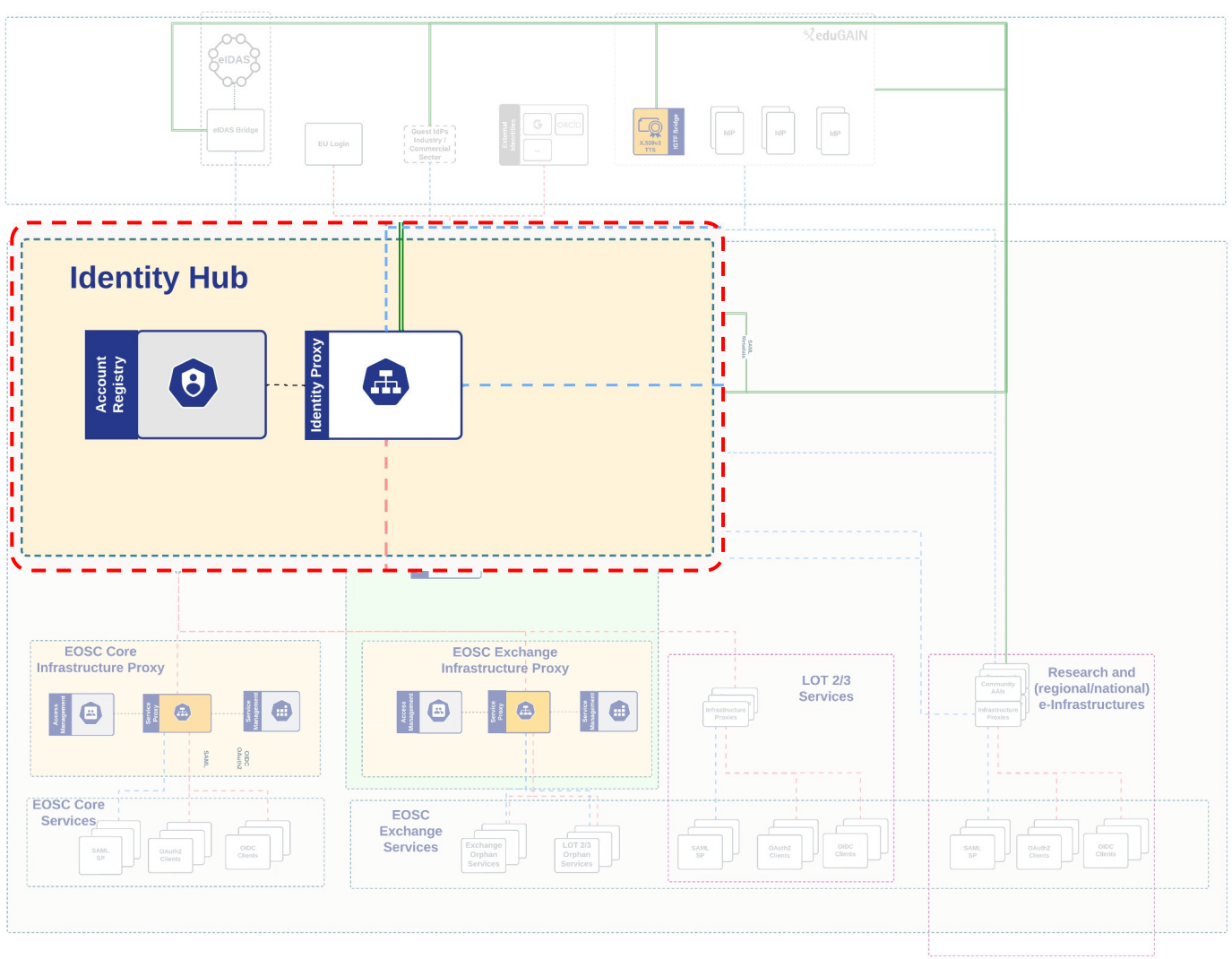
EOSC Exchange Infrastructure Proxy
Provided by GEANT

Connects EOSC Exchange Services that do not have their own Infrastructure Proxy.

Service Proxy
A multi-protocol service provider proxy, supporting OAuth2, OpenID Connect and SAML2 for connecting to services. It is connected to the Identity Proxy in the Identity Hub via OpenID Connect to authenticate users in a consistent way.

Access Management
Manages entitlements and resource capabilities pertaining to EOSC Exchange Services. This information typically includes group membership and roles for controlling access to the EOSC Exchange Services.

Service Management
Service Owners of the connected EOSC Exchange Services can manage the lifecycle of their services. This simplifies the registration and reconfiguration of EOSC Exchange services, minimising operational and management efforts



Identity Hub

Provided by GEANT

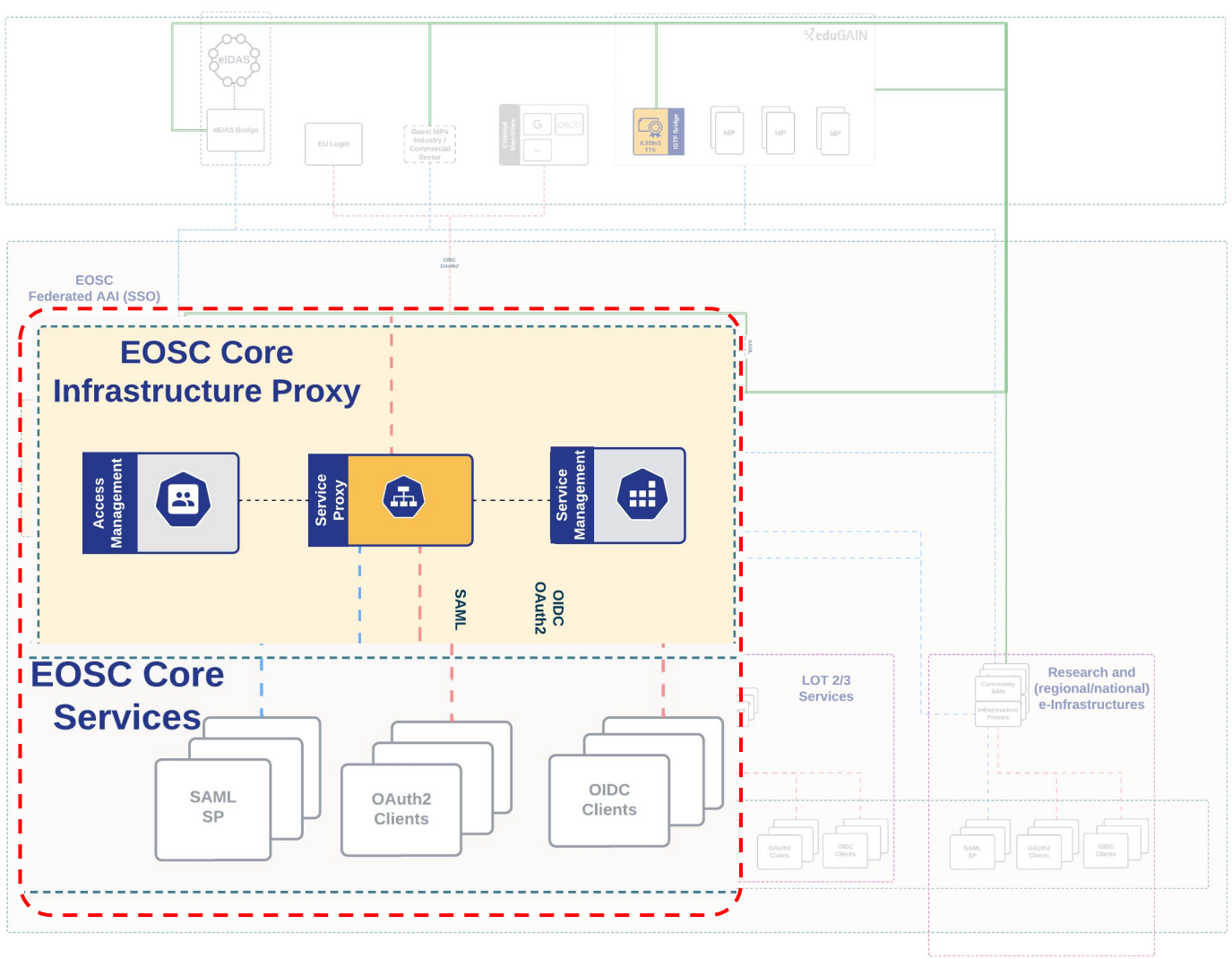
Provides user authentication and consistent user information to services in the EOSC Federated AAI.

Identity Proxy

A multi-protocol authentication proxy supporting OAuth2, OpenID Connect and SAML2 for authenticating users to identity providers. It provides a consistent way for the EOSC Core Infrastructure Proxy, the EOSC Exchange Infrastructure Proxy and LOT 2/3 services to authenticate users. T

Account Registry

Maintains the user accounts, their attributes and the user personal groups ensuring that all users have the required attributes in the account profiles. It is used by EOSC Portal Services to retrieve profile information about the users and to create, manage and retrieve personal groups for the users.



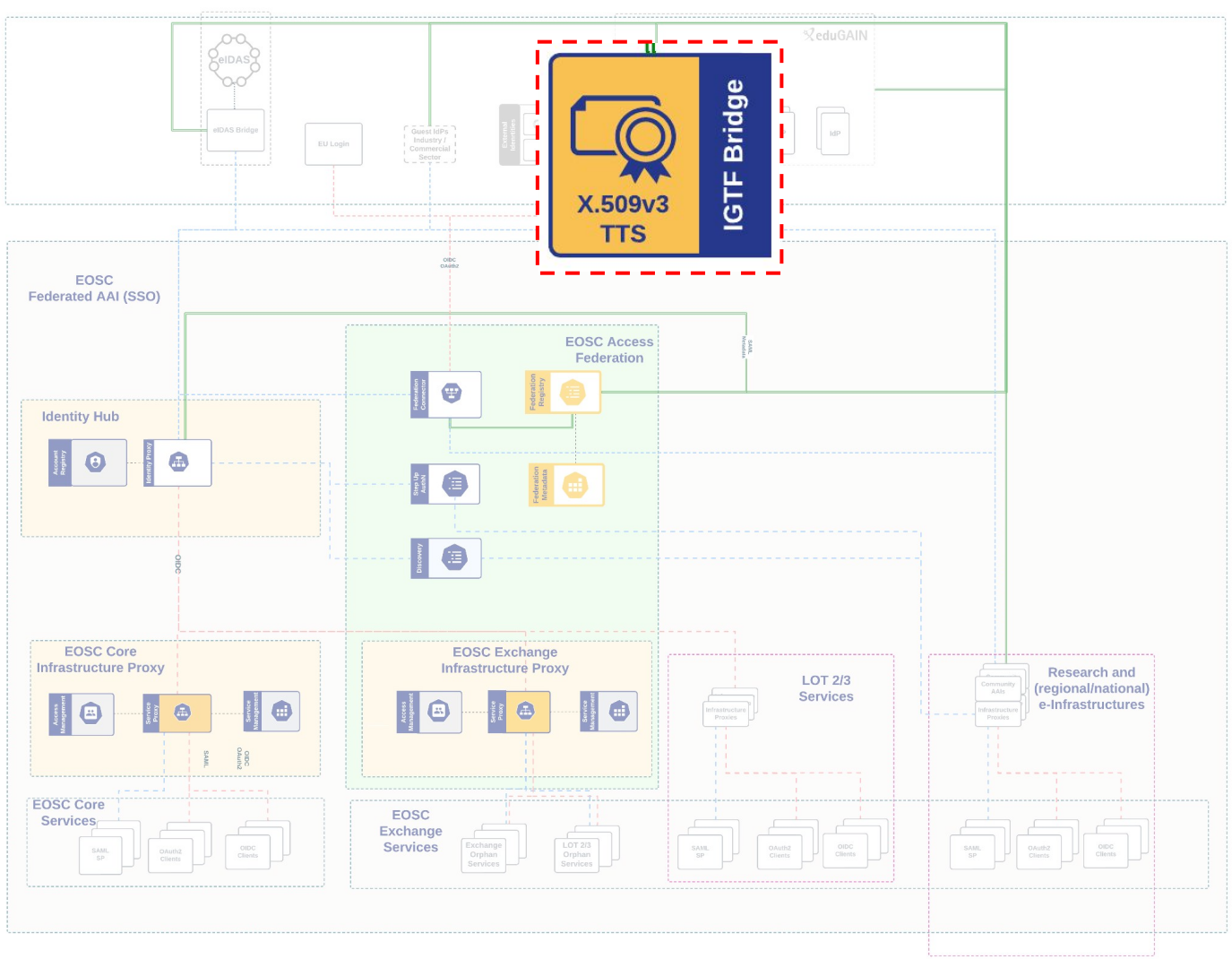
EOSC Core Infrastructure Proxy
Provided by EGI/GRNET

Connects the EOSC Core Services.

Service Proxy
A multi-protocol service provider proxy, supporting OAuth2, OpenID Connect and SAML2 for connecting to services. It is connected to the Identity Proxy in the Identity Hub via OpenID Connect to authenticate users in a consistent way.

Access Management
Manages entitlements and resource capabilities pertaining to EOSC Core Services. This information typically includes group membership and roles for controlling access to the EOSC Core Services.

Service Management
Service Owners of the EOSC Core Services can manage the lifecycle of their services.

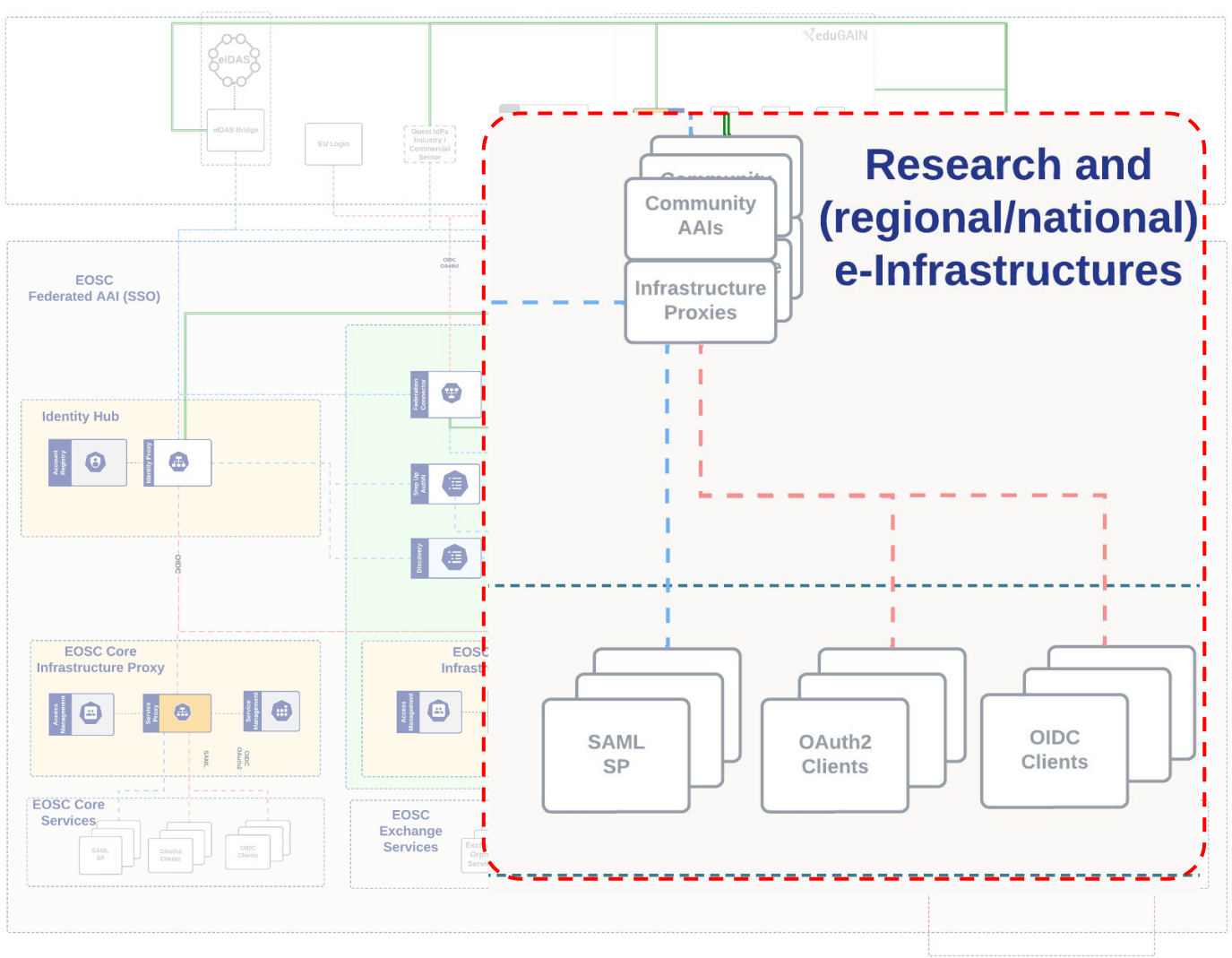


X509v3 Token Translation Service (TTS)
Provided by EGI/GRNET

Provides support for X.509v3 credentials.

IGTF Bridge
Authenticates users with their X.509v3 credentials.

X509v3 TTS
Issue x509 certificates to end-entities based on a successful authentication to Identity Providers that meet specific policy requirements.



National - Regional - European Research Infrastructures

Can connect with their own AARC compliant AAIs both as providers of services and as community AAIs.

The GEANT Core AAI will be available as a Service for all NRENs to create and manage their own national AAIs (if they do not have their own implementation).

Bringing everything together