EOSC AAI

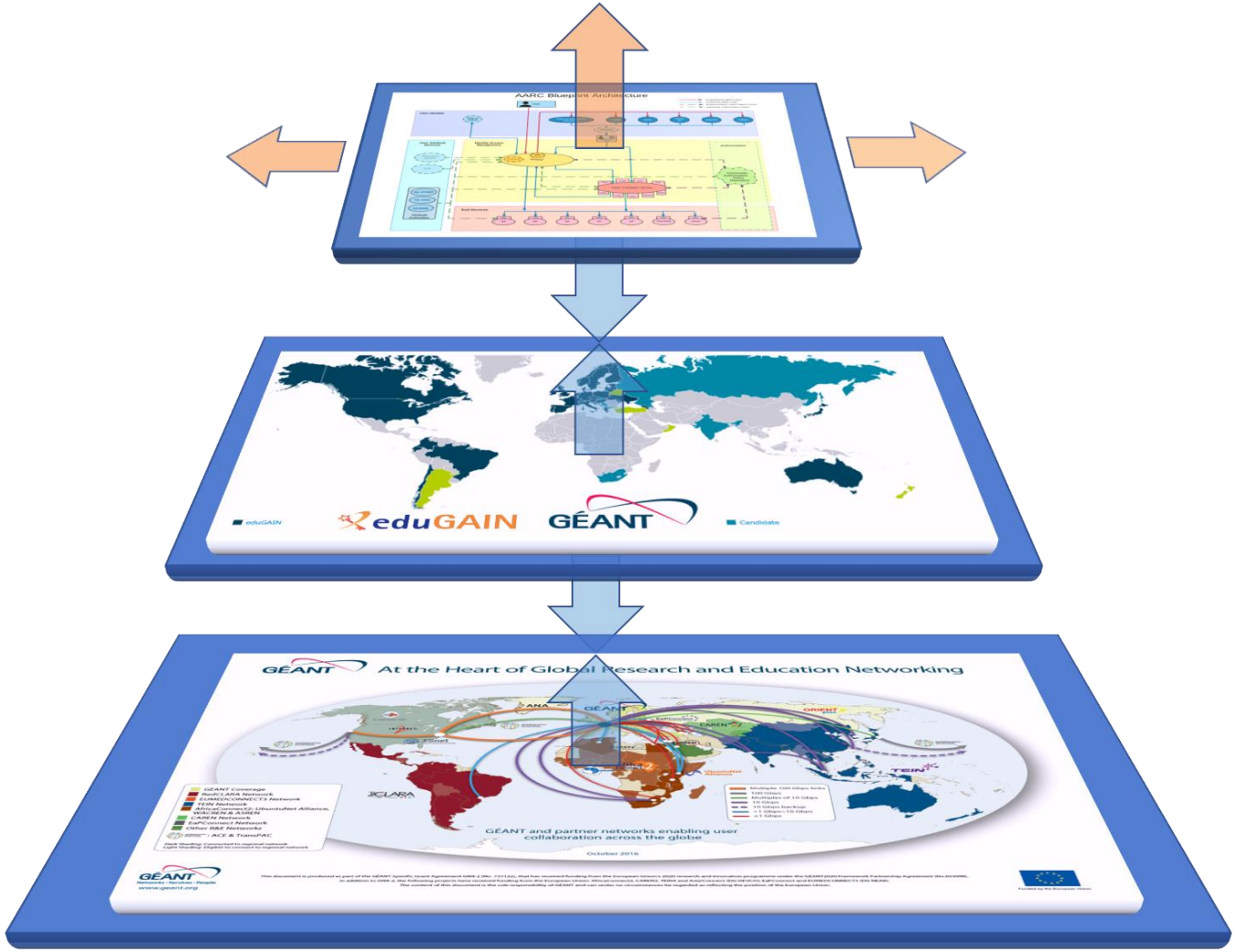
Christos Kanellopoulos, GEANT

The EOSC Future project is co-funded by the
European Union Horizon Programme call
INFRAEOSC-03-2020, Grant Agreement 101017536

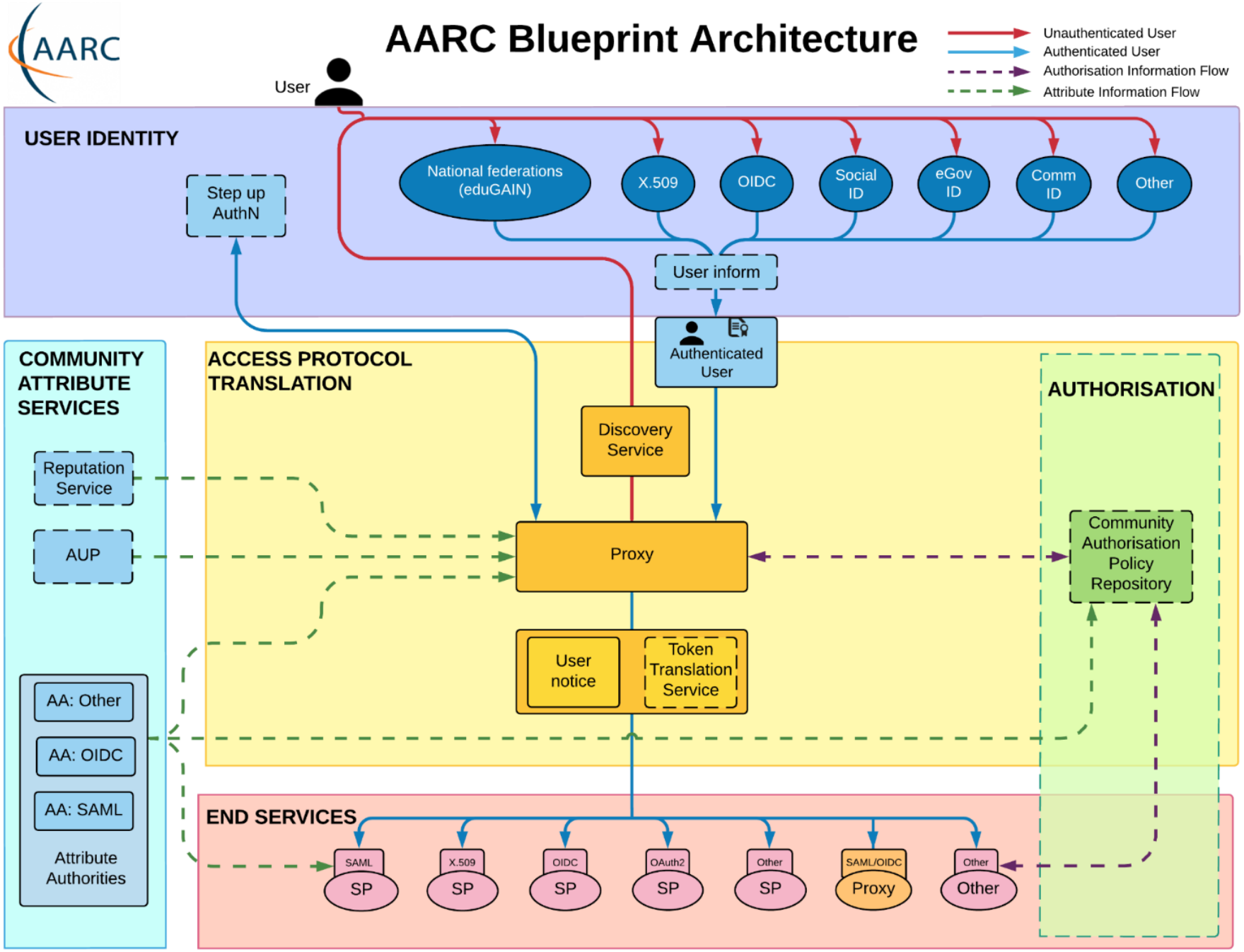
What is AAI?

- 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.

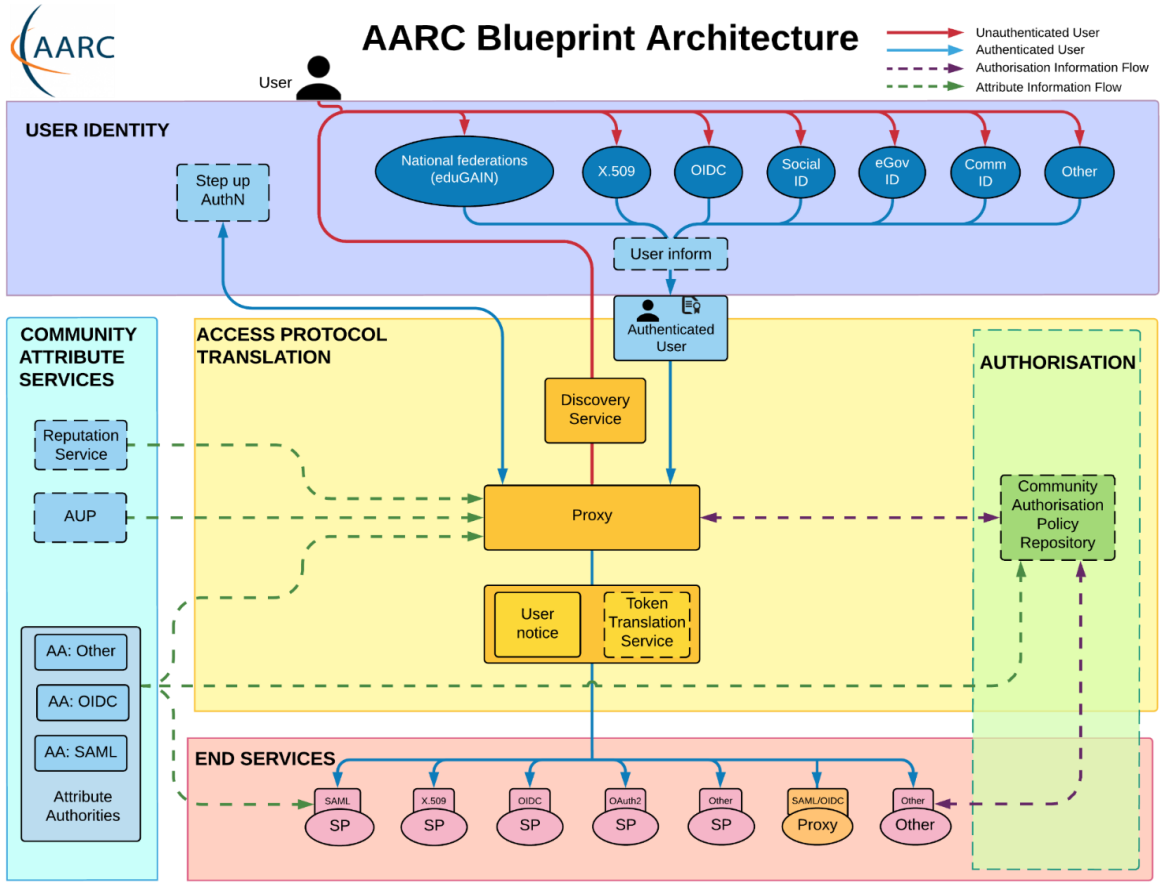
AARC Blueprint Architecture - Enabling an ecosystem of solutions on top of eduGAIN

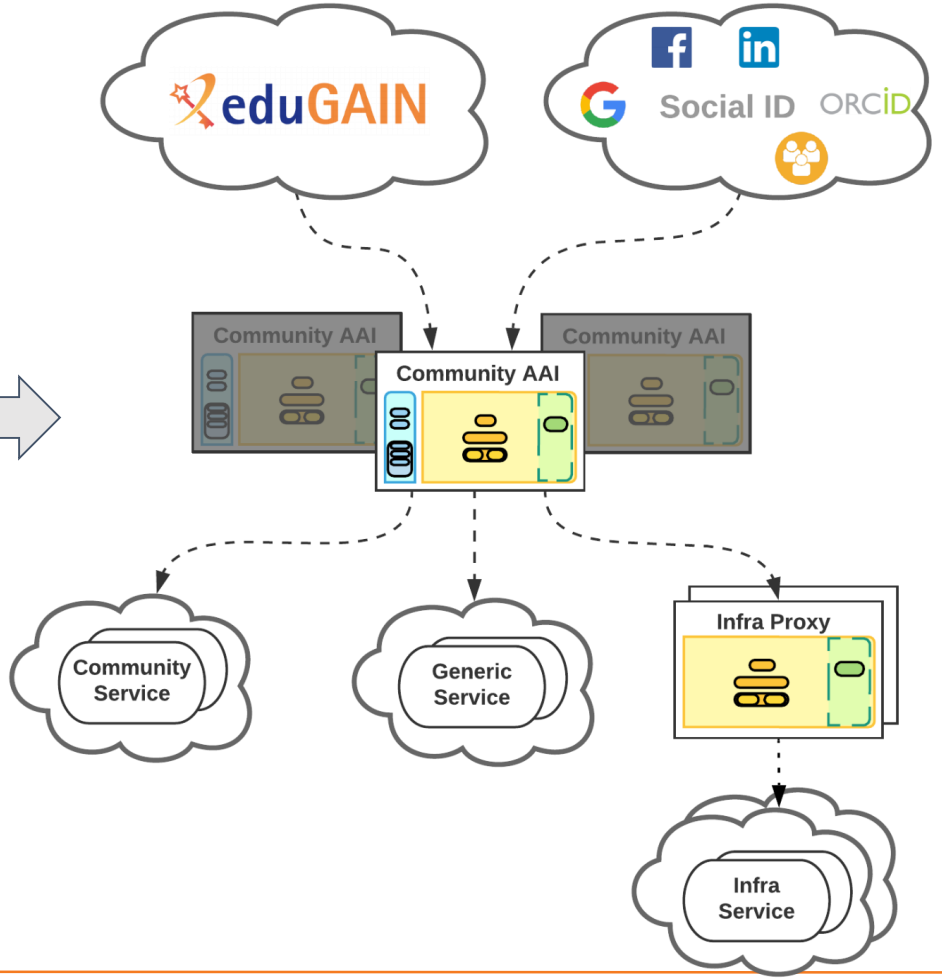


AARC Blueprint Architecture



How the Community-first approach can help research communities to access resources





AARC

A specification for IdP hinting

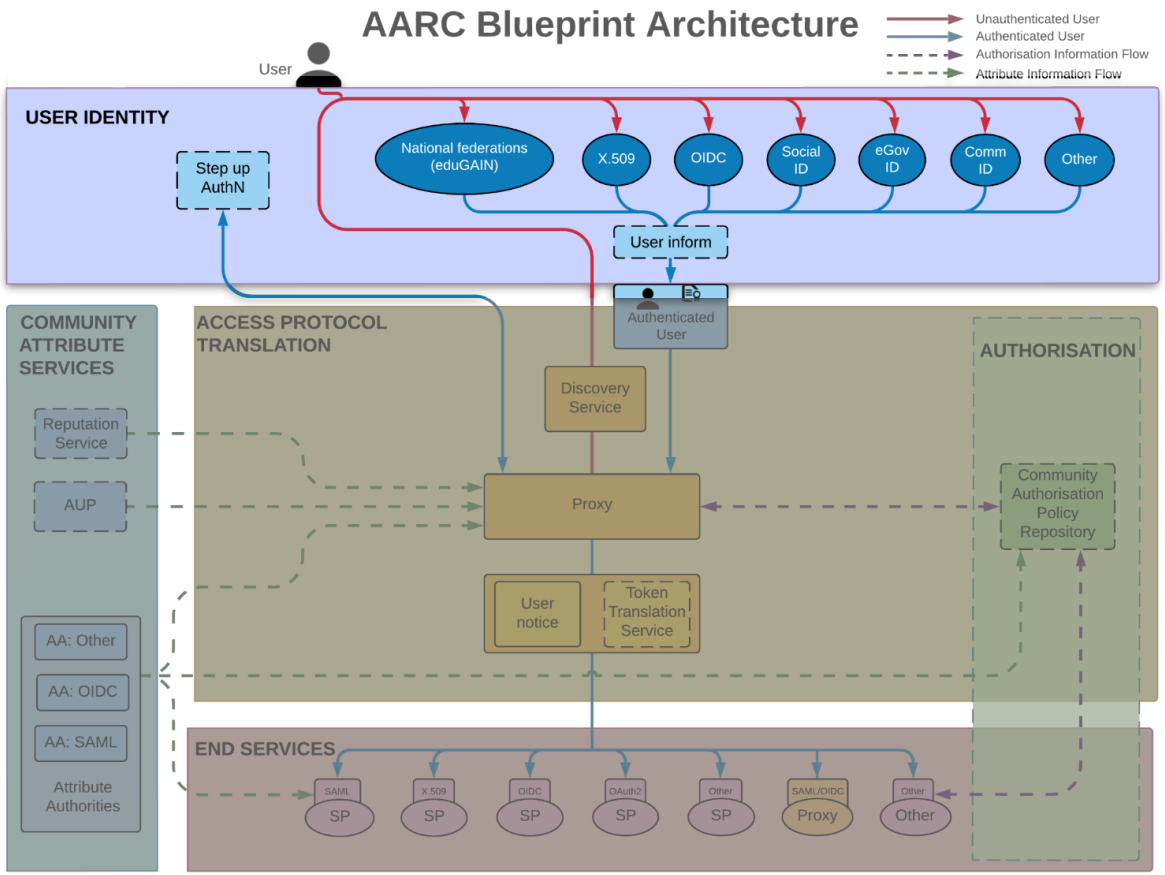
Publication Date: 2021-03-10
Authors: AARC Community members; AppInt members; Marcus Hardt (ed.)
Document Code: AARC-G061
DOI: 10.5281/zenodo.4596667

© members of the AARC community.
The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme and other sources.

Abstract
This document defines a generic browser-based protocol for conveying - to services - hints about the IdPs or SP-IdP-proxies that should be used for authenticating the principal. This protocol, colloquially referred to as Identity Provider (IdP) hinting, can greatly simplify the discovery process for the end-user, by enabling entities to produce and send hints that can be consumed by SP-IdP-proxies for routing the user to the correct upstream SP-IdP-Proxy or authenticating IdP.

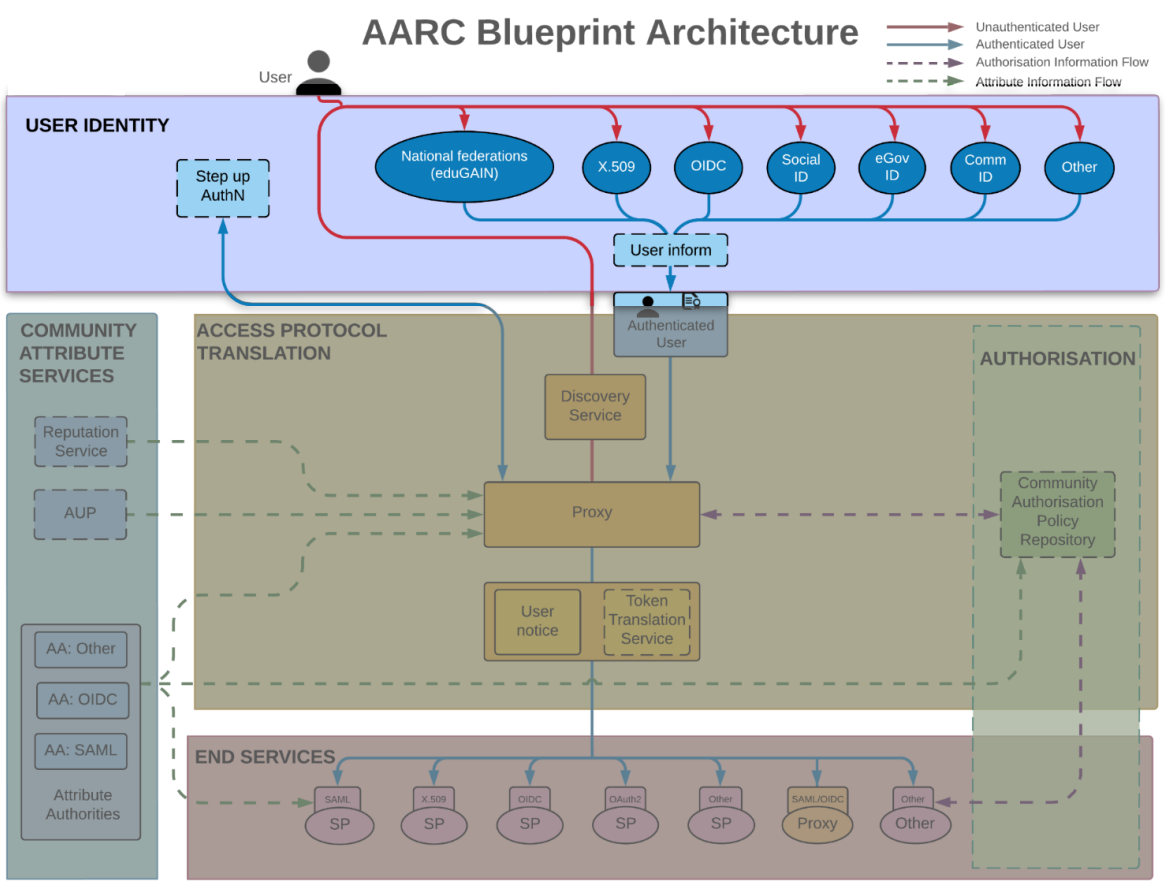
AARC Guidelines

AARC Guidelines: User Identity



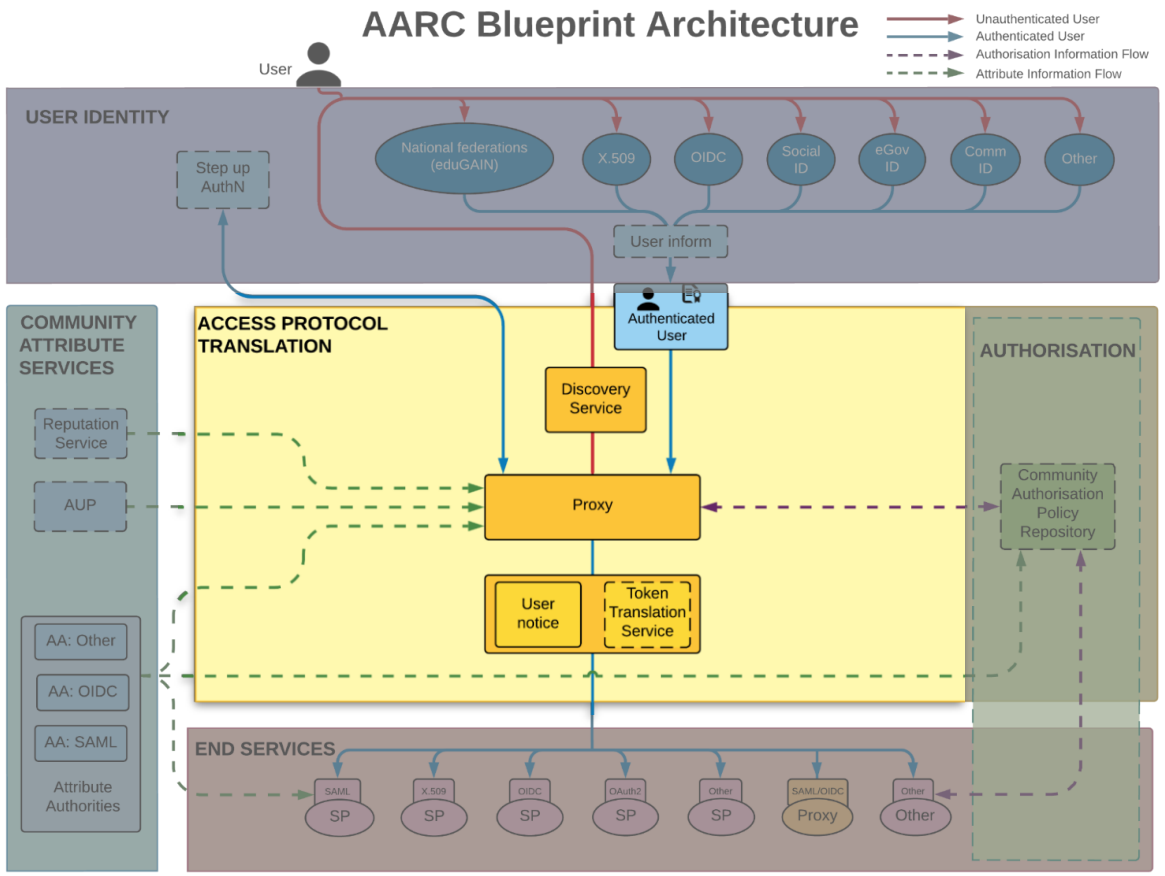
- *"How to integrate Social Media Identity Providers?"* → AARC-G008
- *"How should users link accounts?"* → AARC-G009
- *"How should services indicate that they would like users to authenticate with multifactor authentication?"* → AARC-G029

AARC Guidelines: User Identity



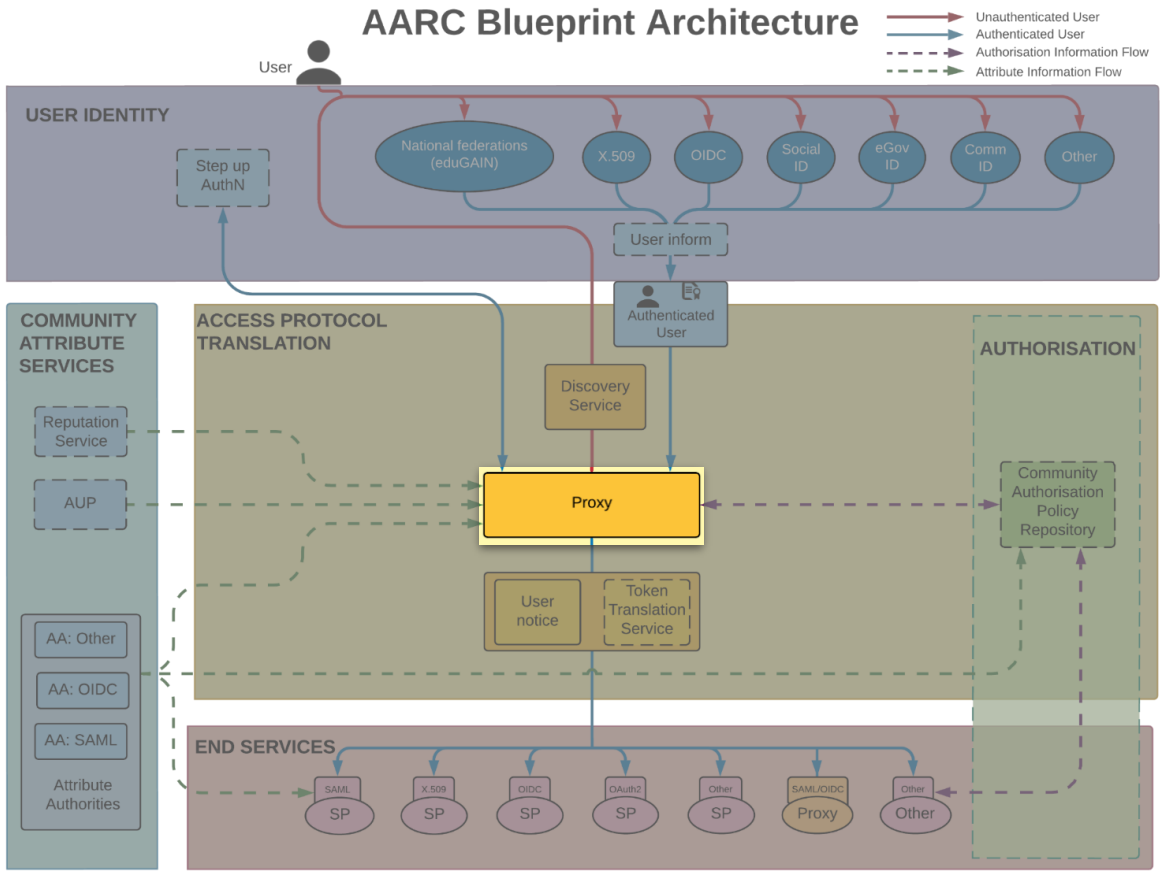
- ***"How to evaluate assurance information when linking identities?" → AARC-G031***
- *"What can I say about assurance of identities from social media accounts?" → AARC-G041*
- ***"How should assurance information be shared between proxies?" → AARC-G021***
- *"Which Assurance Profiles should I use?" → AARC-I050*

AARC Guidelines: Access Protocol Translation



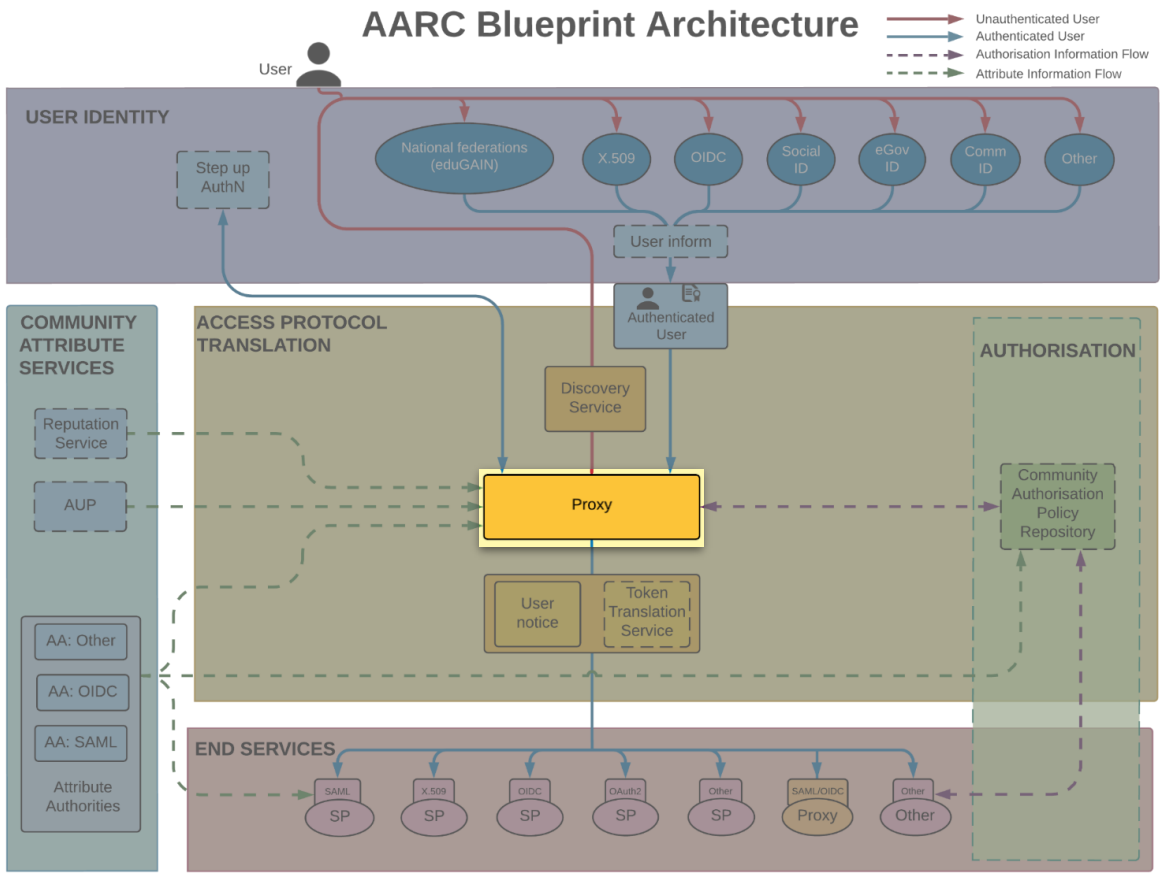
- *"Which best practices to follow for Token Translation Services?"* → AARC-G004
- *"How to translate Federated Identity information to X.509 certificates?"* → AARC-G010

AARC Guidelines: Access Protocol Translation - Proxy



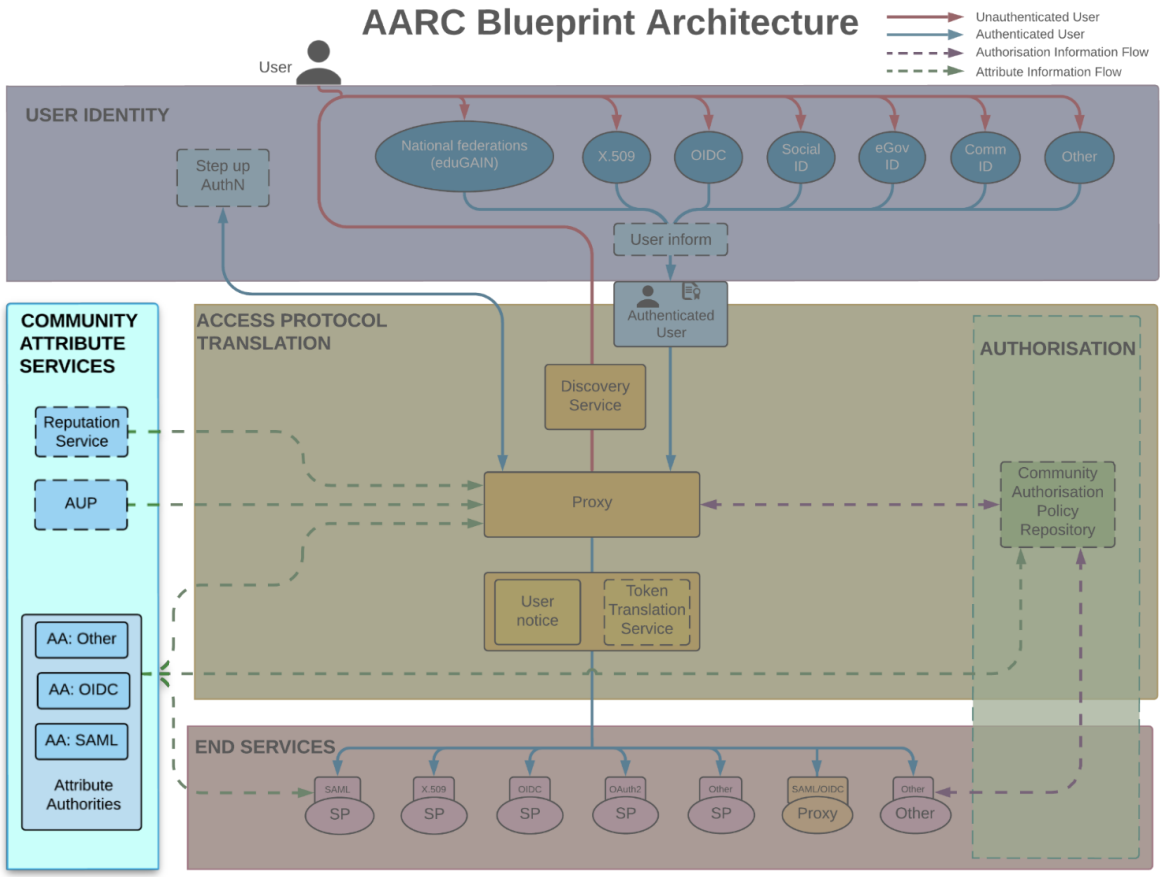
- *"How to ensure that the proxy is able to accurately claim that it supports best practices in Identity Federation?" → AARC-G015*
- ***"How to express the home institute of a user?" → AARC-G025***
- ***"How to express the identifier of a user?" → AARC-G026***

AARC Guidelines: Access Protocol Translation - Proxy



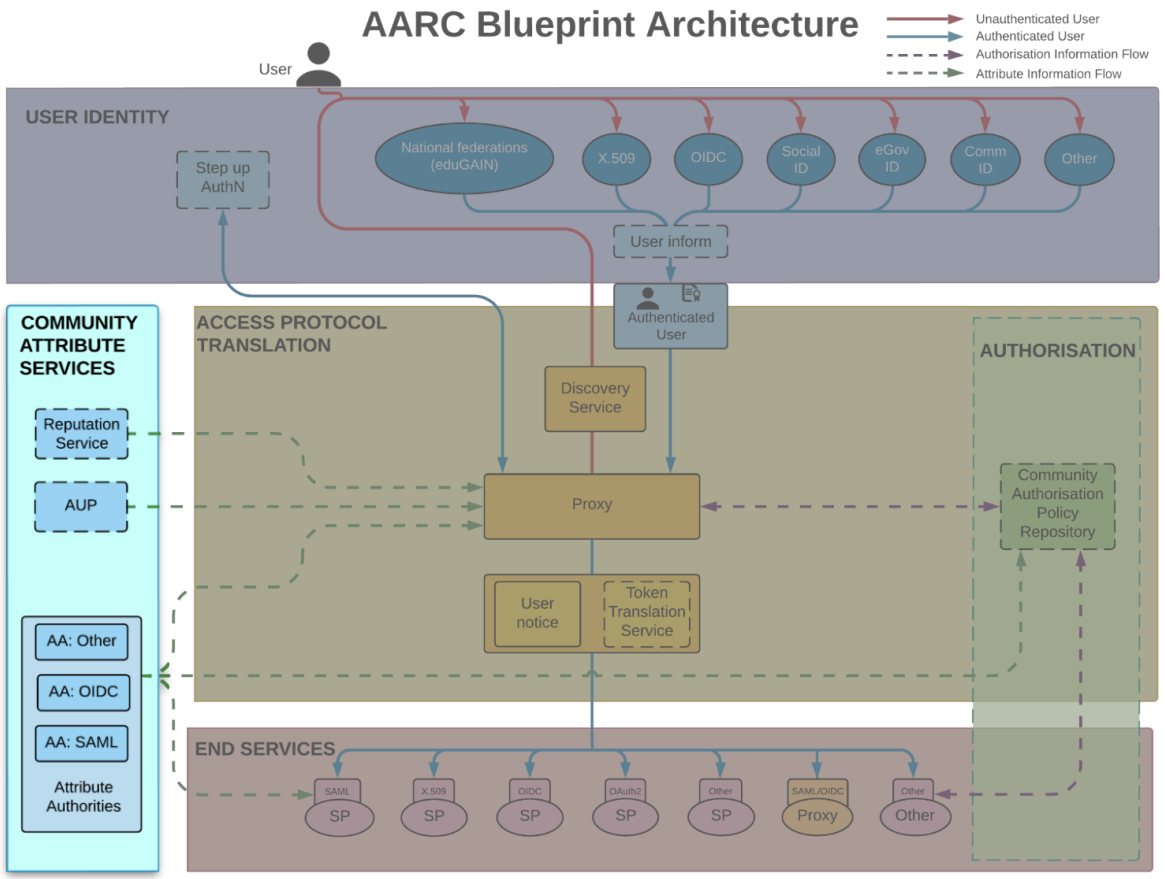
- *"How to express assurance information for users when interacting with another proxy?" →* [AARC-G021]
- *"How can the proxy simplify the discovery process for end-users?" →* [AARC-G061]
- *"How can the proxy route end-users to the correct discovery service?" →* [AARC-G062]

AARC Guidelines: Community Attribute Services



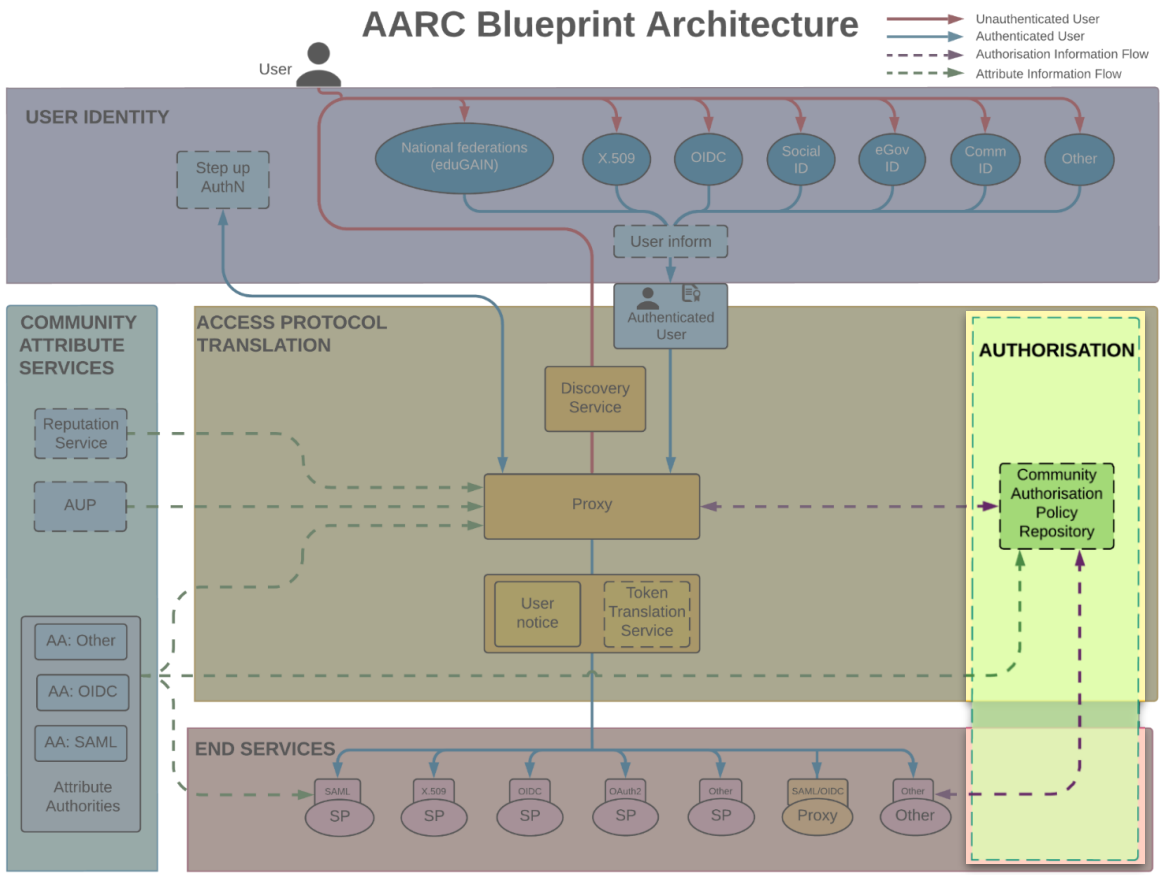
- *"How should attributes from multiple sources be aggregated?"* → [AARC-G003]
- ***"How to express the home institute of a user?"*** → **[AARC-G025]**
- ***"How to express the identifier of a user?"*** → **[AARC-G026]**

AARC Guidelines: Community Attribute Services



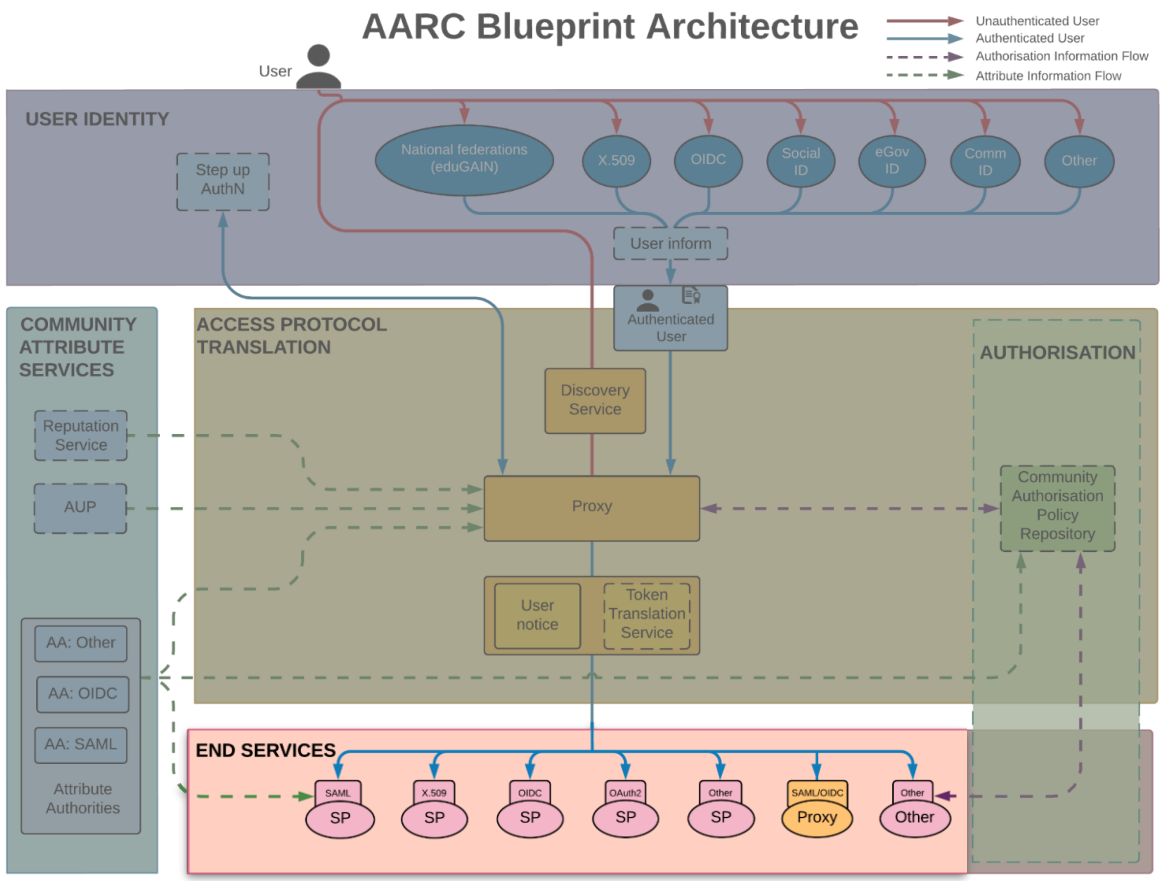
- *"What are the best practices for running my Attribute Authorities securely?"* → AARC-G048
- *"Which Acceptable Use Policy should I use to facilitate interoperability?"* → AARC-I044
- ***"How to infer the affiliation of a user?"* AARC-G057**

AARC Guidelines: Authorisation



- *"How to manage authorisation information from multiple sources?" → AARC-G006*
- ***"How to express group and role information?" → AARC-G002***
- ***"How to express resource capabilities?" → AARC-G027***

AARC Guidelines: End Services



- *"How to handle credential delegation and impersonation to allow my service to act on behalf of the user?"* → AARC-G005
- *"My services are not web based, how can I use identities from the proxy?"* → AARC-G007
- *"How should Services hint which IdP they would like users to use?"* → AARC-G049 & AARC-G061
- *"Which Security practices should I follow?"* → AARC-G014

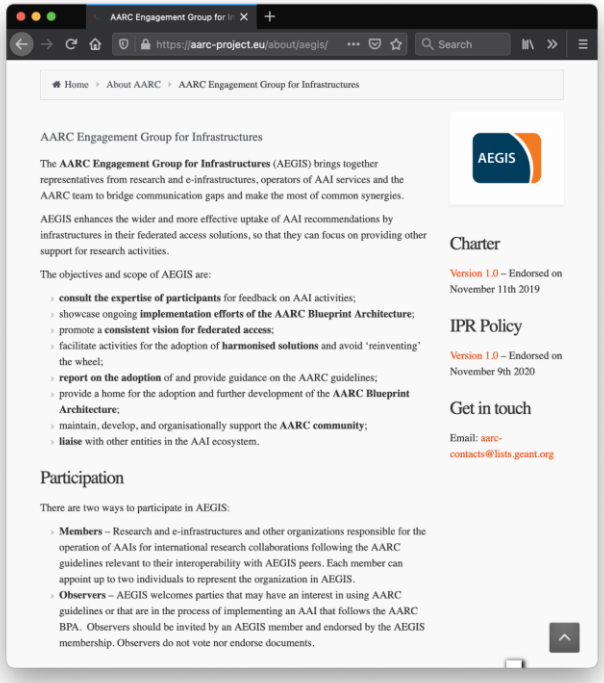
AARC Guidelines: Interoperability

https://wiki.geant.org/display/AARC/AARC+Interoperability+Guidelines+Approved+by+AEGIS

AARC Interoperability Guidelines Approved by AEGIS

Created by Christos Kanellopoulos, last modified by Nicolas Liampotis on Jan 14, 2022

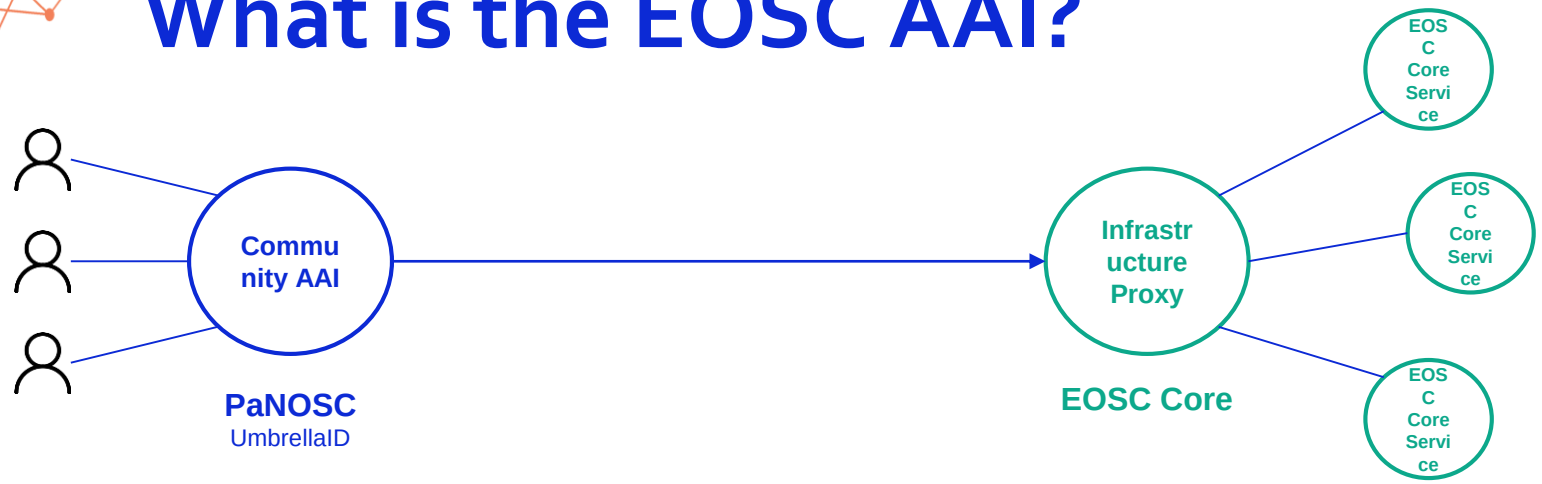
#	Document	AARC Identifier	Date first presented	Date approved	Status
1	Guidelines on expressing group membership and role information	AARC-G002	2017-11-13	2017-11-15	Current
2	Exchange of specific assurance information between Infrastructure	AARC-G021	2018-03-12	2018-03-12	Current
3	Guidelines for evaluating the combined assurance of linked identities	AARC-G031	2018-05-14	2018-07-09	Current
4	Specification for expressing resource capabilities	AARC-G027	2018-12-10	2018-12-10	Current
5	Implementing scalable and consistent authorisation across multi-SP environments	AARC-I047	2019-03-11	2019-03-11	Current
6	A specification for IdP hinting	AARC-G049	2019-03-11	2019-04-08	Superseded by AARC-G061
7	Guidelines for expressing affiliation information	AARC-G025	2019-03-11	2019-10-14	Current
8	AARC Blueprint Architecture 2019	AARC-G045	2019-11-11	2020-02-10	Current
9	Inferring and constructing voPersonExternalAffiliation	AARC-G057	2020-07-13	2021-02-08	Current
10	A specification for IdP hinting	AARC-G061	2020-05-11	2021-02-08	Current
11	Guidelines for expressing community user identifiers	AARC-G026	2019-09-09	2021-06-14	Current
12	Specification for hinting an IdP which discovery service to use	AARC-G062	2021-09-13	2021-10-11	Current



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

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

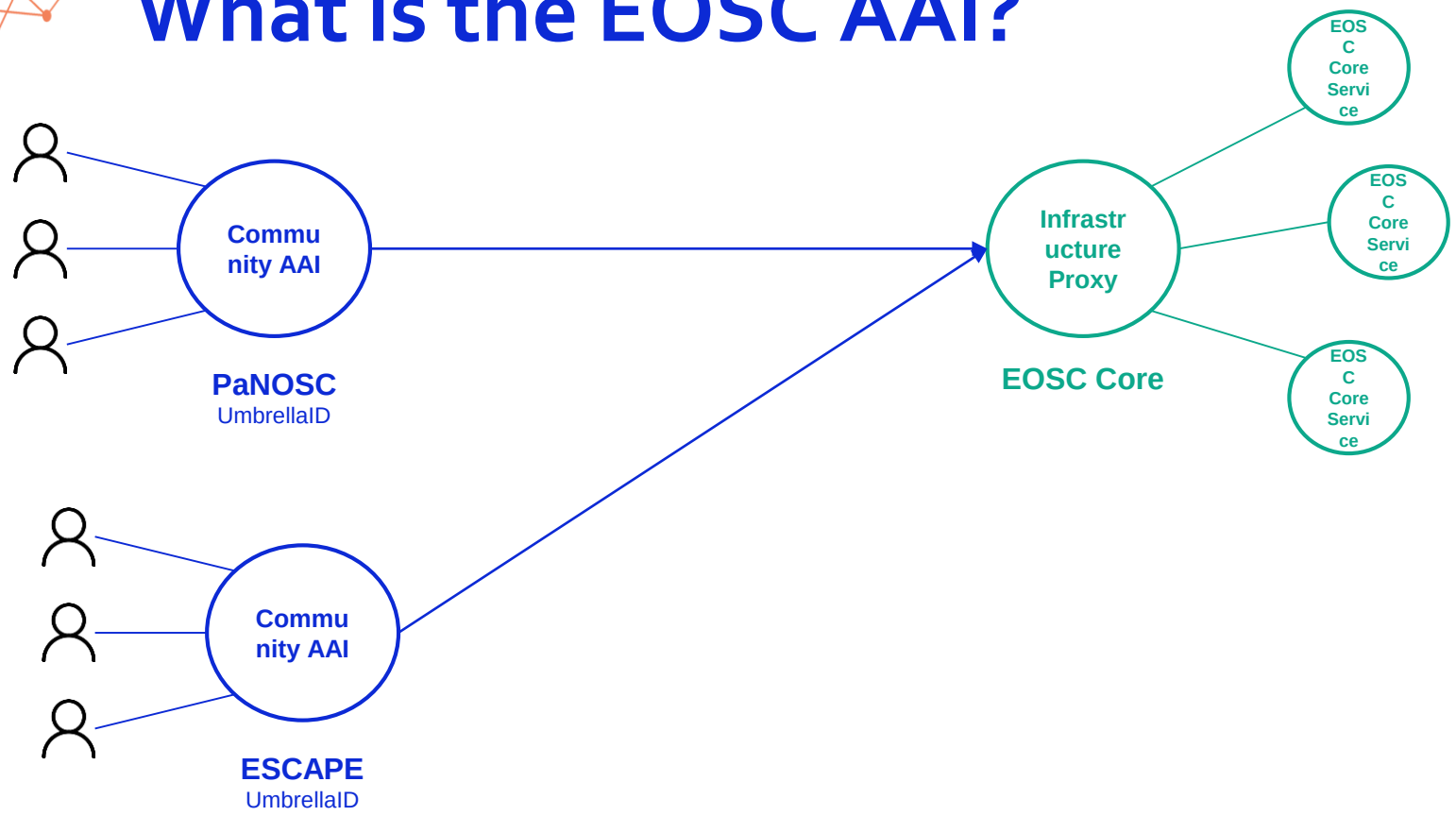
The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single integration point, where the Infrastructure can maintain centrally all the relevant policies and business logic for making available these resources to multiple communities

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 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.

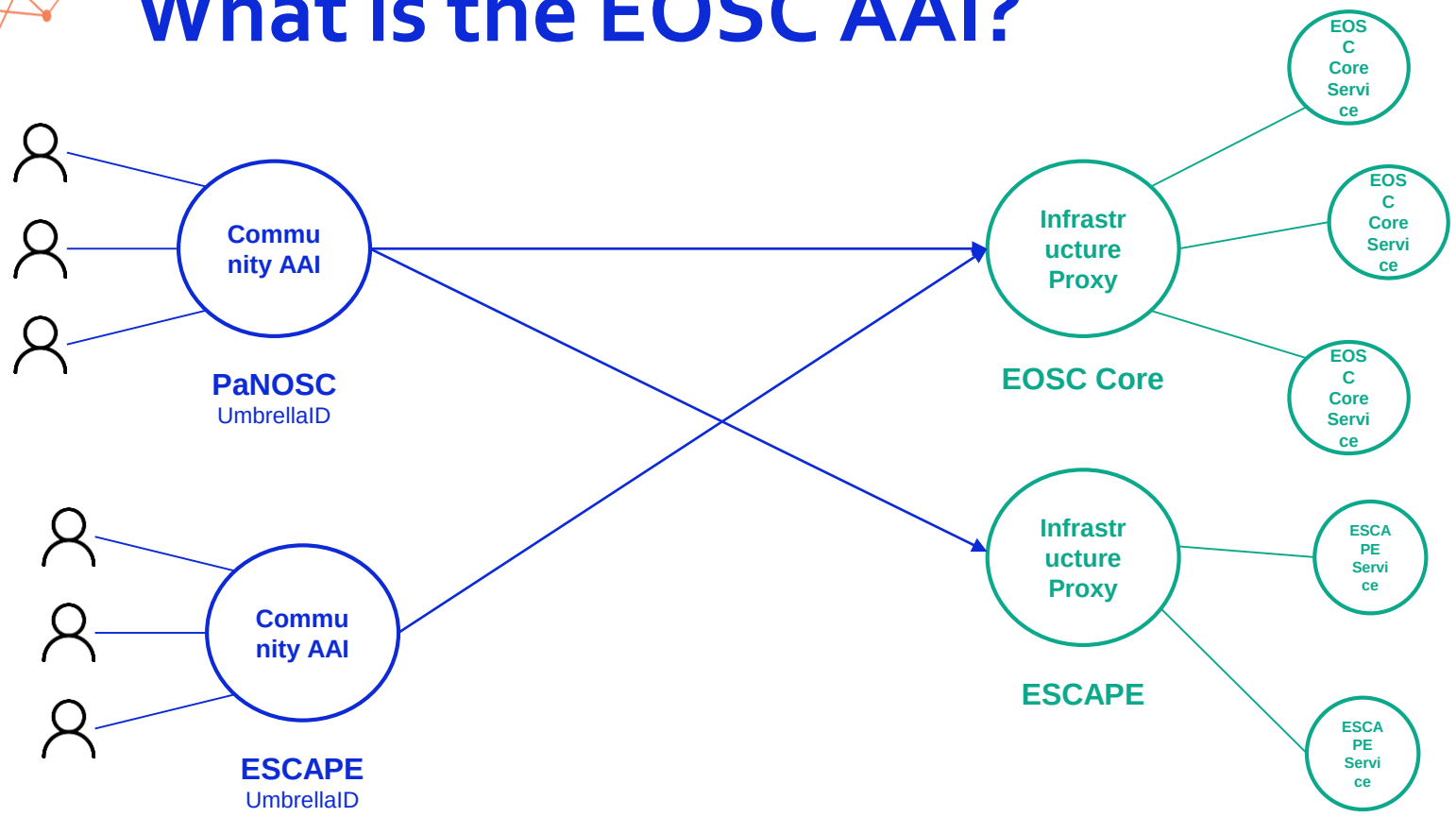
Infrastructure Proxy

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 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.

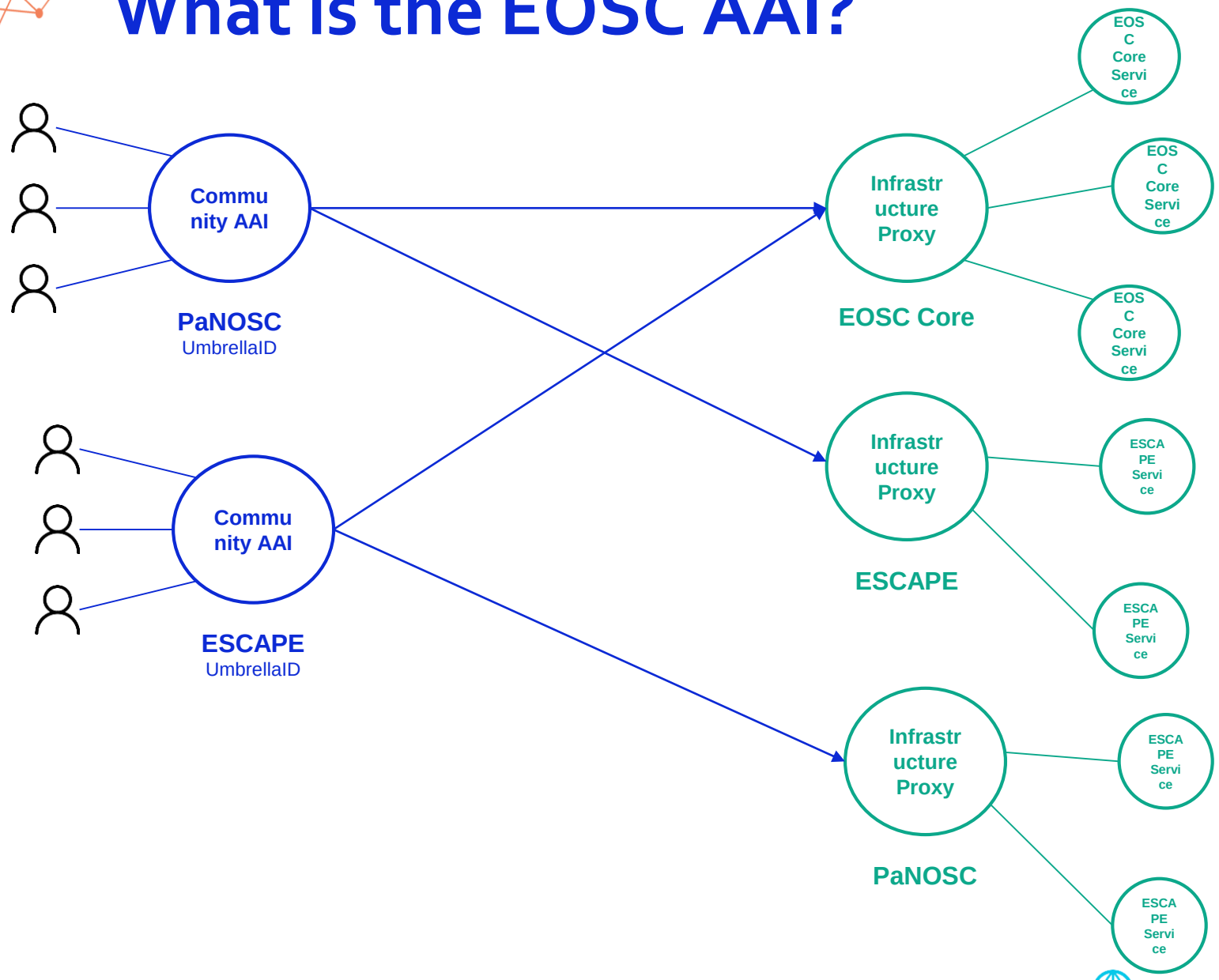
Infrastructure Proxy

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 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.

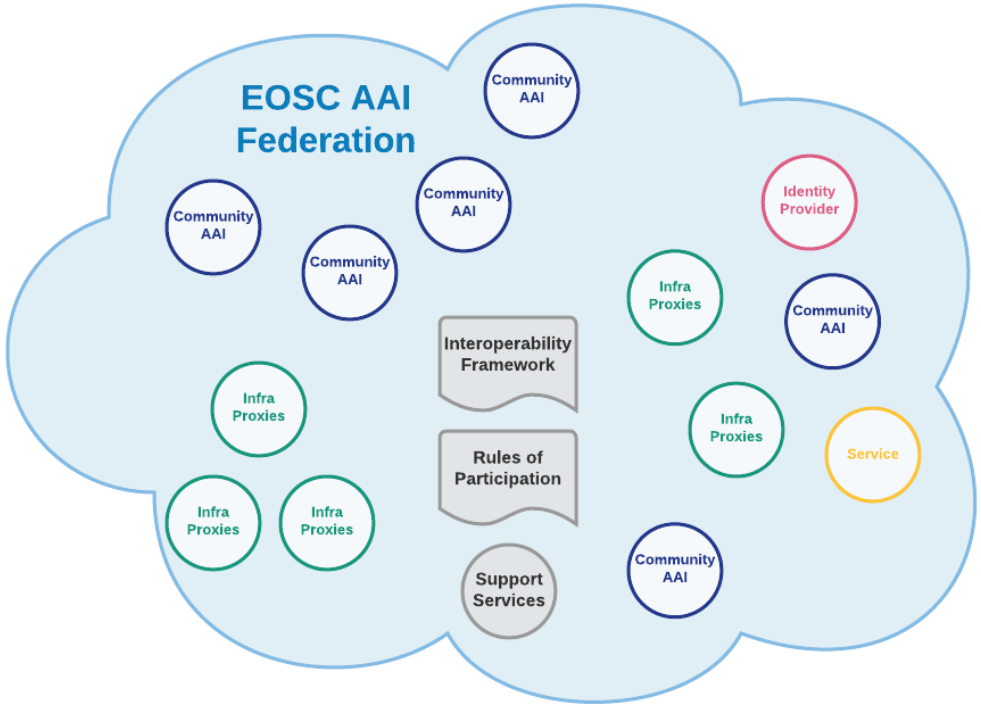
Infrastructure Proxy

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

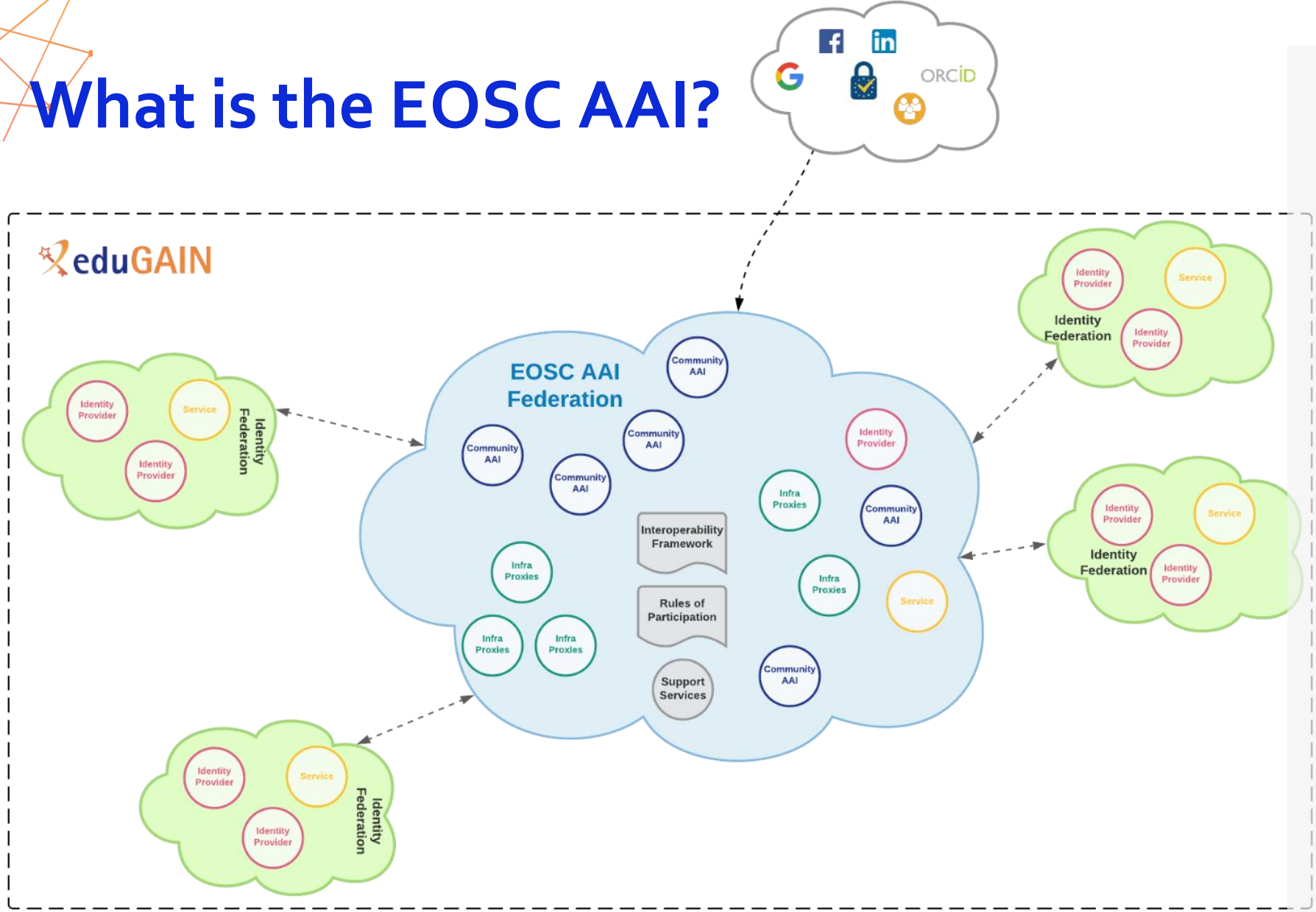
AARC Blueprint Architecture 2019
https://doi.org/10.5281/zenodo.3672784

What is the EOSC AAI?



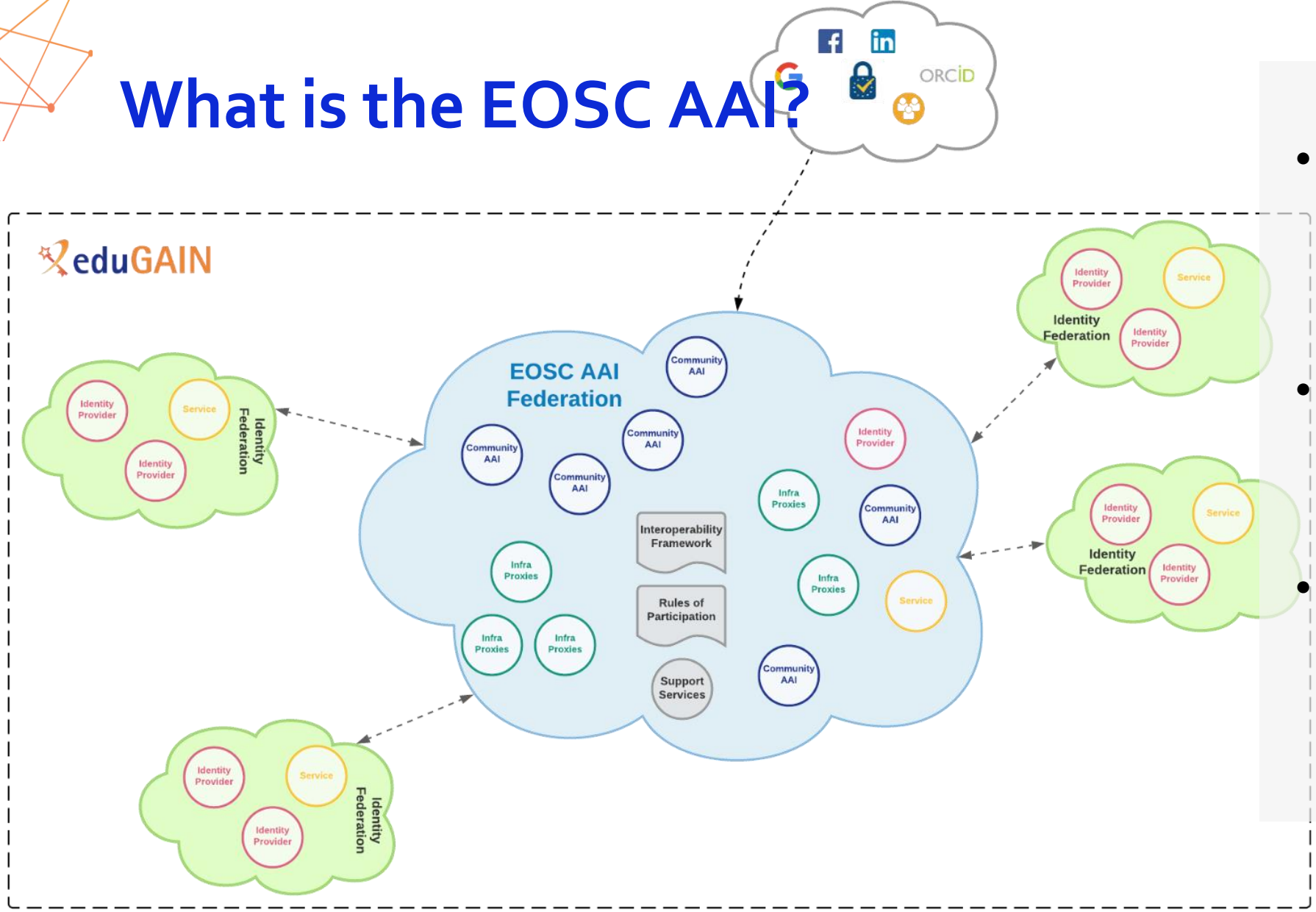
- Community AAIs and Infrastructure Proxies connect once with the EOSC AAI Federation (register metadata, URN namespaces, policies etc)
- Technical interoperability conformance tested and monitored by the EOSC AAI FEderation.
- GDPR and Security Policy conformance (Policy Notices, Acceptable Use Policy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



- 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
- 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

Implementation Roadmap

- Q6 (M18) Goal - October 2022
  - The EOSC AAI Federation is fully operational. EOSC AAI e-Infrastructure SP-proxies and cluster community AAIs fully integrated to EOSC AAI Federation. Community AAIs can integrate.
  - Initial technical guidelines to connect IdP and AAI proxies from public and private sector service providers to the EOSC Federated AAI
  - Use case: A researcher from PaNOSC can access an ESCAPE resource with the PaNOSC (UmbrellaID) identity. Cross Research Infrastructure Access.

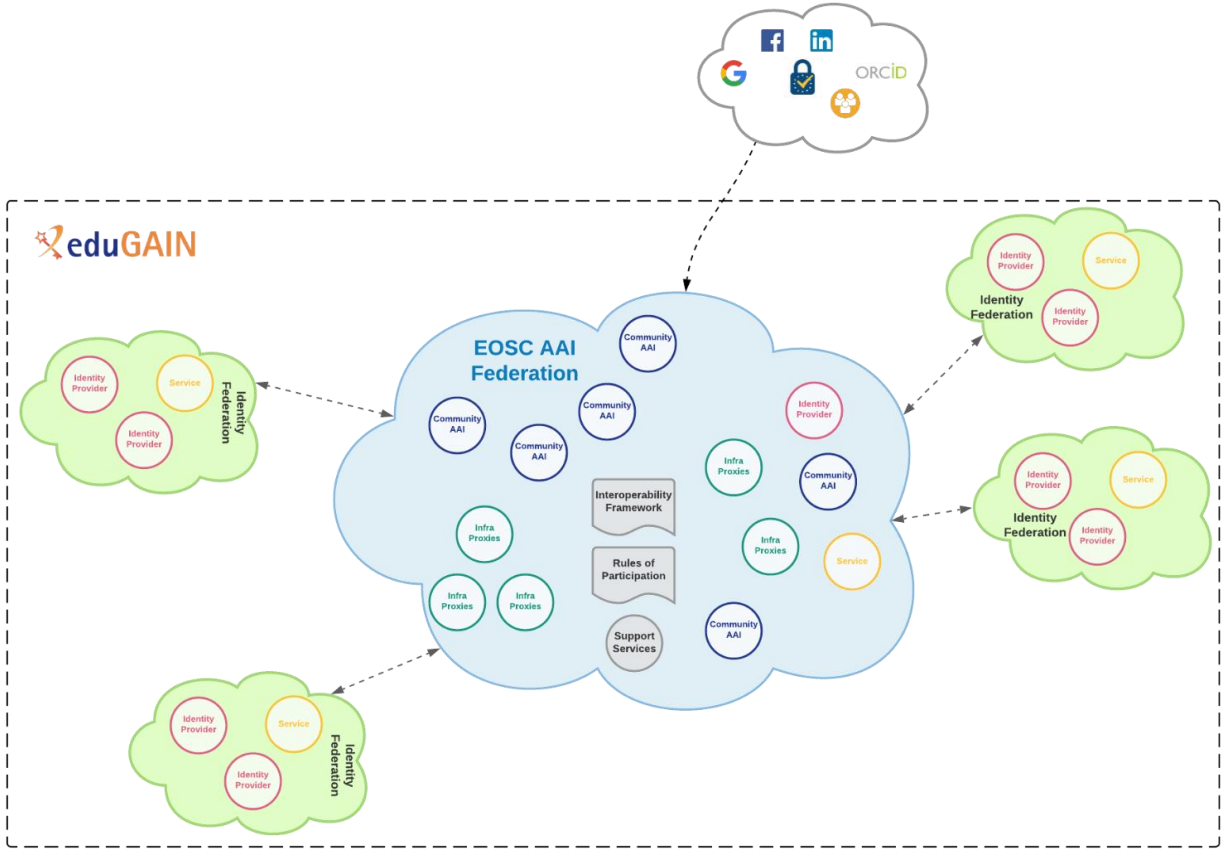
Implementation Roadmap

- Q10 (M30) Goal - October 2023
  - A researcher can do the full lifecycle of data processing, storage, analysis, and publishing supported by resources available and transparently integrated through EOSC.
  - Community AAIs seamless integration with EOSC AAI federation through self-service onboarding.
  - Technical interoperability guidelines for supporting cross-sector access to the EOSC Federated AAI.

EOSC AAI Architecture 2022

- **Scalability**
- Multi-infrastructure workflows
- Consistent user experience and interfaces for service providers
- Growth of EOSC beyond the research and education community
- Community attributes and authorisation

EOSC AAI Architecture 2022 Working Areas: Scalability



Solution: EOSC AAI Federation

- **Policies** – Interoperability Framework, Rules of Participation
- **Support Services**
- **Members** - Can register entities
  - Services to the EOSC
  - Proxies that aggregate other service providers or enrich identities
  - Providers of authentication whose identities are used by EOSC services or by EOSC proxies

Open issue: How to cater for OpenID Connect entities?

- Short-term: OIDC-to-SAML Proxies
- Long-term: OIDC Federation

EOSC AAI Architecture 2022

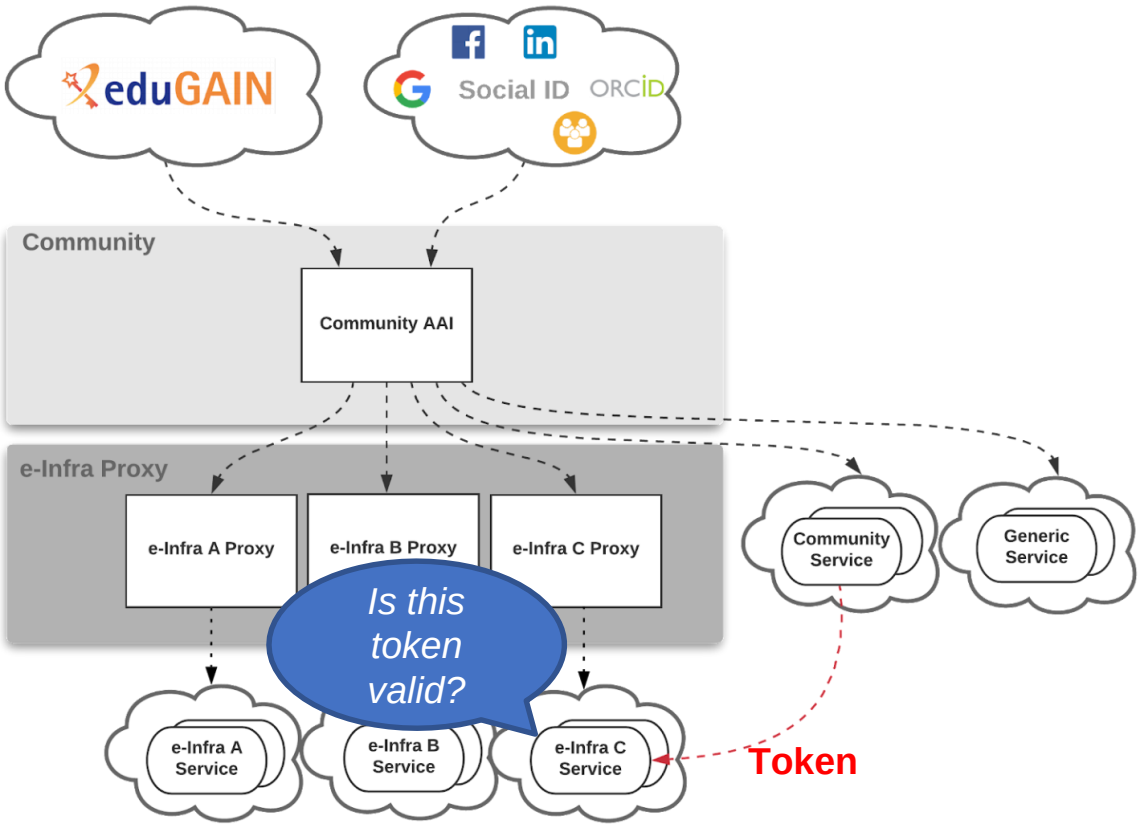
- Scalability
- **Multi-infrastructure workflows**
- Consistent user experience and interfaces for service providers
- Growth of EOSC beyond the research and education community
- Community attributes and authorisation

EOSC AAI Architecture 2022 Working Areas: Multi-infrastructure workflows

- Current EOSC AAI architecture works when the user is consuming services directly
- However some use cases require a service agent to be able to act autonomously –on behalf of the user– to consume services and resources
- If the services consumed by the agent are behind the same proxy the current architecture works
- But what happens if an agent running on Service A needs to access resources on Service B connected by a different proxy?

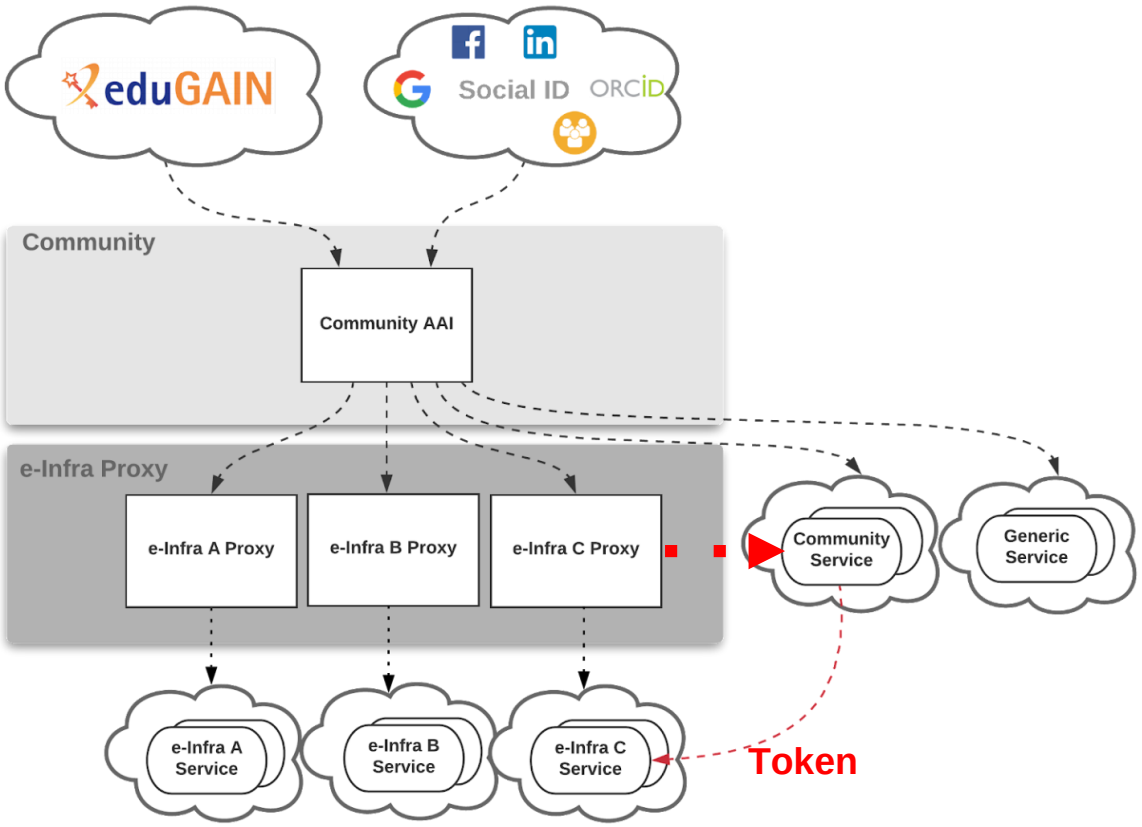
EOSC AAI Architecture 2022 Working Areas: Multi-infrastructure workflows (Contd.)

- OAuth2 token validation: Existing implementations of OAuth2-based Authorisation Servers do not support the validation of tokens issued by a different Authorisation server
- Example: Community service accessing e-Infra service on behalf of user



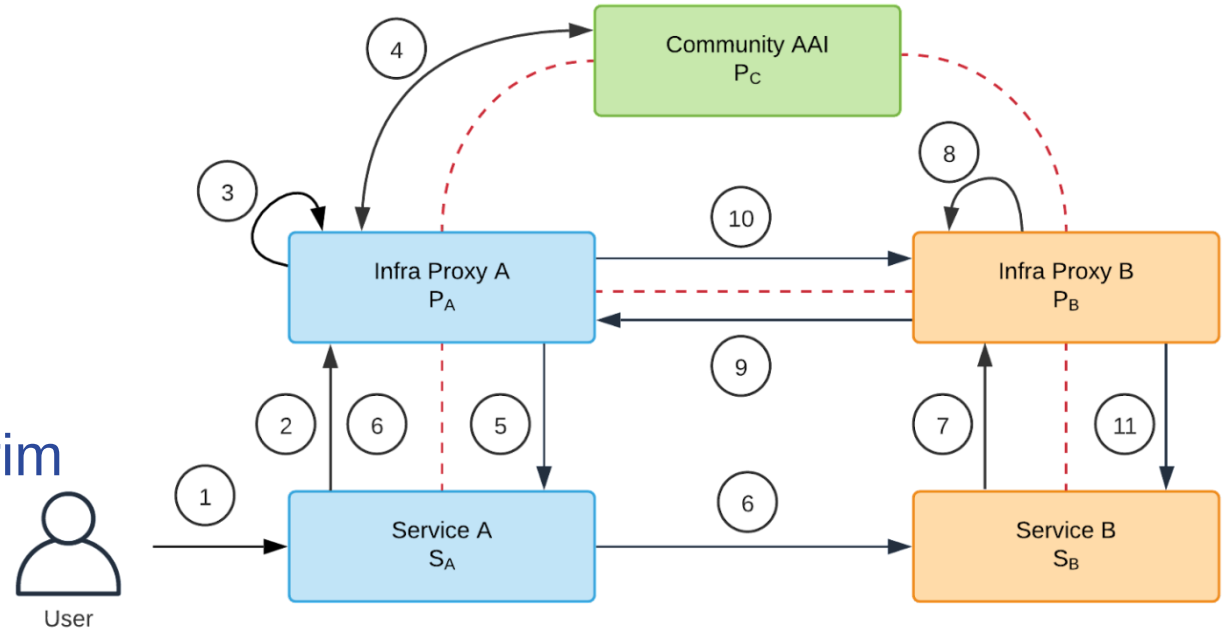
EOSC AAI Architecture 2022 Working Areas: Multi-infrastructure workflows (Contd.)

- Workaround: Services need to connect to different Authorisation Servers instead of relying on a single Proxy
- *BUT*
  - Requires additional integration effort from services
  - Cannot scale



EOSC AAI Architecture 2022 Working Areas: Multi-infrastructure workflows (Contd.)

- Solution for dynamically establishing trust in a distributed environment will be provided by the [OpenID Connect Federation specification v1.0 (draft)]
- AARC community is investigating an extension of the OAuth2 Token Introspection specification as an interim solution until the OIDC Federation Specification is widely available.

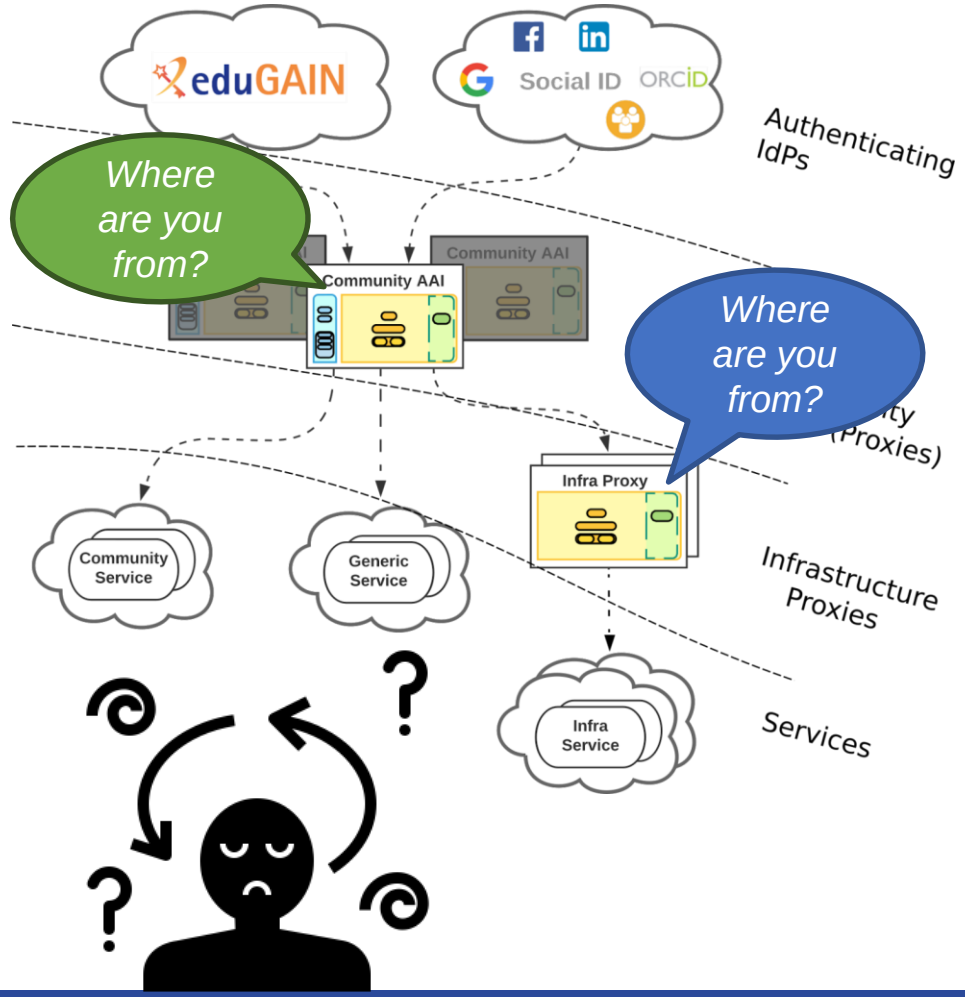


EOSC AAI Architecture 2022

- Scalability
- Multi-infrastructure workflows
- **Consistent user experience and interfaces for service providers**
- Growth of EOSC beyond the research and education community
- Community attributes and authorisation

EOSC AAI Architecture 2022 Working Areas: Consistent user experience and interfaces

- Users need to go through multiple Identity Provider discovery steps
  - Example: Select Community AAI and then select the Identity Provider of their Home Organisation
- Users don't need to re-enter their login credentials ***but*** the IdP selection can be frustrating
- Adoption of AARC "hinting" documents
  - IdP selection hints AARC-G061
  - Discovery Service selection hints AARC-G062
  - Service hints AARC-G063 [WIP]

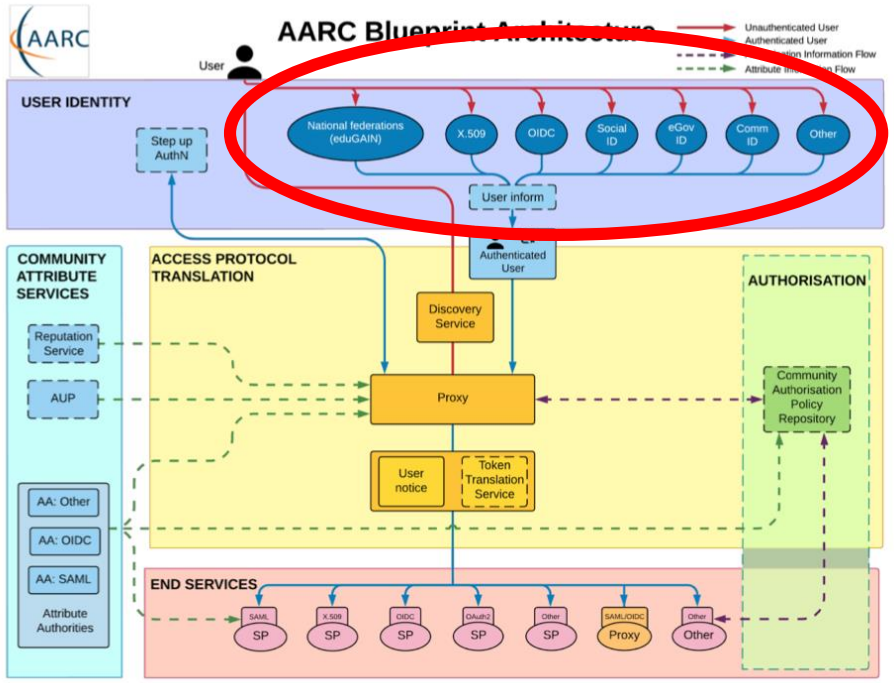


EOSC AAI Architecture 2022

- Scalability
- Multi-infrastructure workflows
- Consistent user experience and interfaces for service providers
- **Growth of EOSC beyond the research and education community**
- Community attributes and authorisation

EOSC AAI Architecture 2022 Working Areas: Beyond the research and education community

- Need to support citizen scientists, public sector organisations, and industry users
- Support authentication via national electronic identification schemes (eIDAS)
- Other?

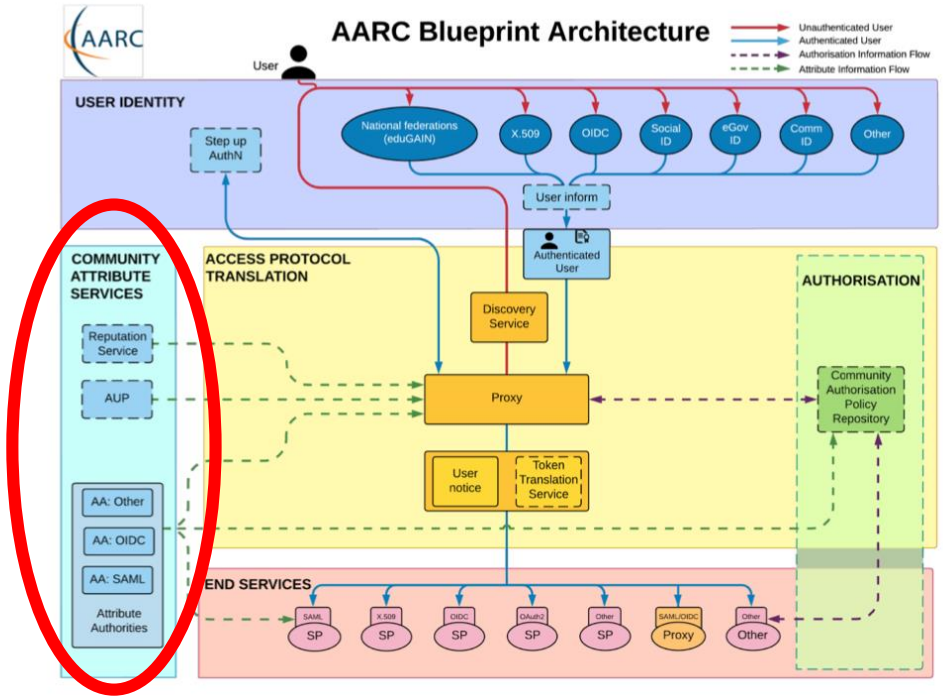


EOSC AAI Architecture 2022

- Scalability
- Multi-infrastructure workflows
- Consistent user experience and interfaces for service providers
- Growth of EOSC beyond the research and education community
- **Community attributes and authorisation**

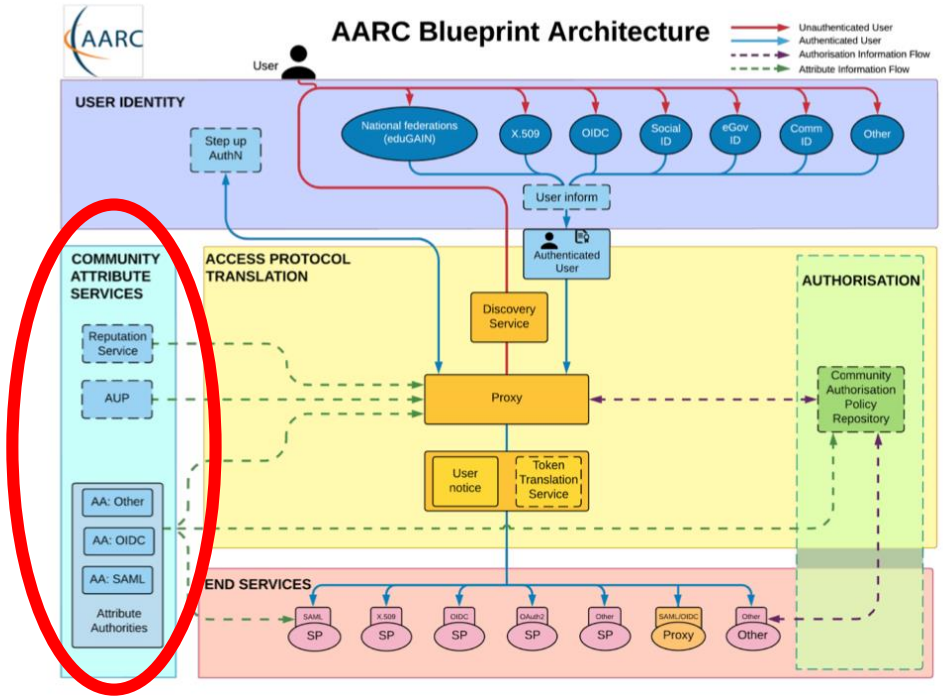
EOSC AAI Architecture 2022 Working Areas: Community attributes & authZ

- Attribute Providers (AtP) can be independent from IdPs
- "Community" is not well-enough defined as an authoritative entity
- Need to consider different –not only community-controlled– attribute/access management services



EOSC AAI Architecture 2022 Working Areas: Community attributes & authZ (Contd.)

- Need to revisit “Community” definition?
  - From EOSC AAI Baseline Architecture report / AARC BPA 2019: *“Community: A group of users, organised with a common purpose, and jointly granted access to resources (see also [WISE-SCI])”*
  - From EOSC AAI First Principles – All trust flows from communities: *“Communities may act as the interface between individual users and the resources. Trust in this sense means a community’s ability to know and determine its users and their permissions”*



Thank you for your attention

The EOSC Future project is co-funded by the European Union Horizon Programme call INFRAEOSC-03-2020, Grant Agreement 101017536