The EOSC AAI Task Force

Charter - Background

The AAI for EOSC is built on top of a large body of existing work in the :

- Federated Identity Management for Research (FIM4R) (2012 – Today)

- AARC Community and AEGIS (2015 – Today)

- EOSC AAI Task Force of EOSC Architecture WG (2019 – 2020)

Charter - Main goals

- Evolution of the EOSC AAI Architecture and the EOSC AAI Federation, following the AARC Blueprint Architecture and AARC Interoperability Guidelines.

- Identification and assessment of requirements and gaps through liaison efforts and collaboration with other bodies inside and outside EOSC, such as EOSC Task Forces, EOSC projects, community bodies like AEGIS.

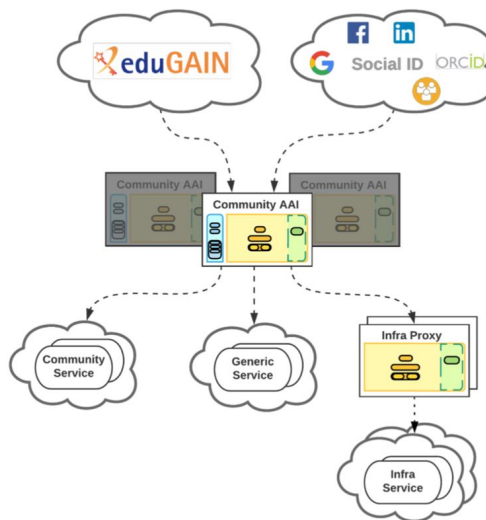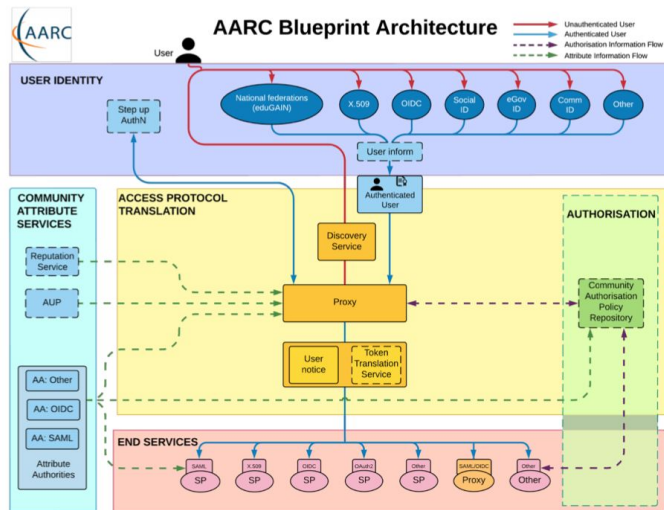- Identification and assessment of governance models for the EOSC AAI architecture.

The evolution of the EOSC AAI architecture

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

EUROPEAN OPEN
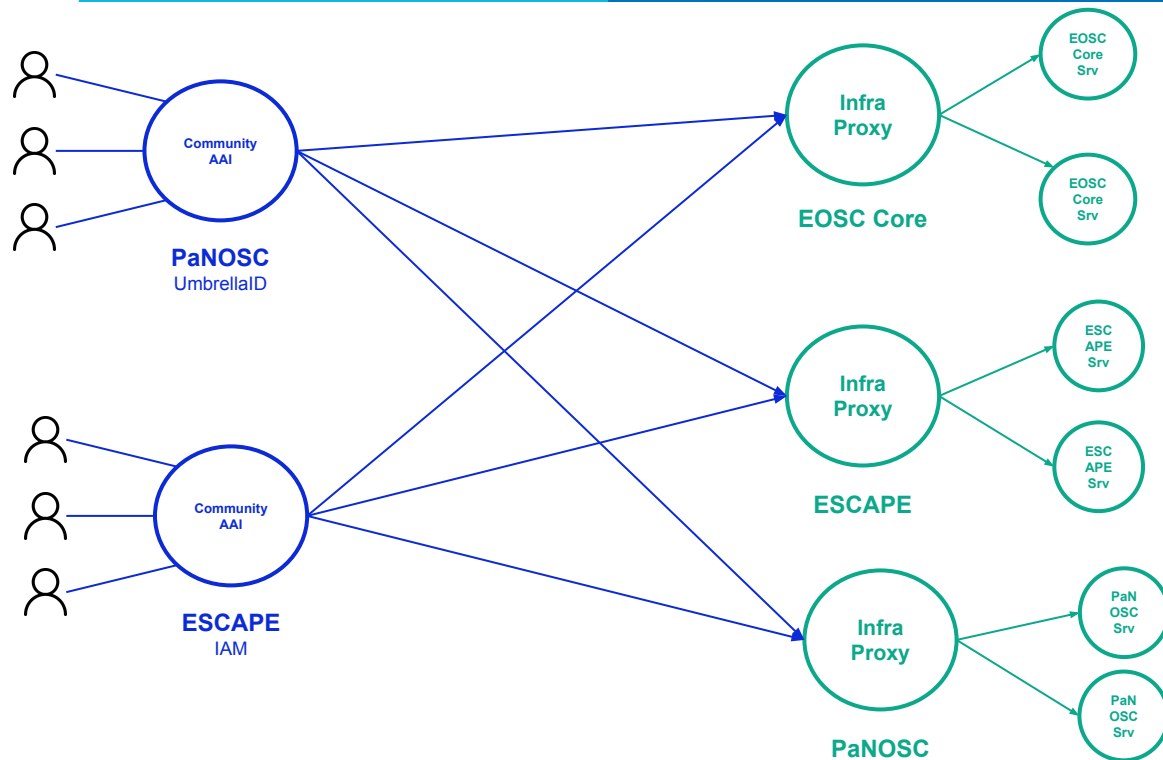SCIENCE CLOUD

EOSC AAI Baseline 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

EOSC AAI Baseline Architecture (Contd.)

Based on the [AARC Interoperability Guidelines](#)

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
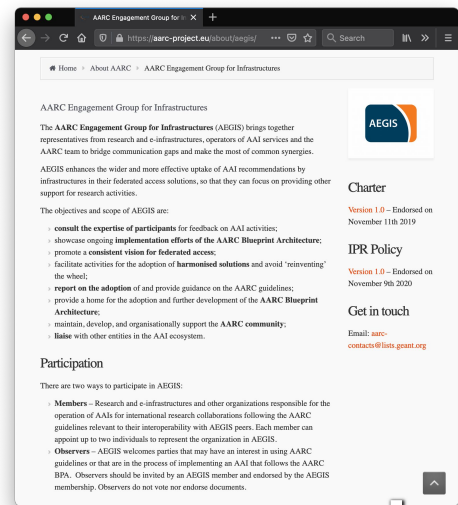
EUROPEAN OPEN SCIENCE CLOUD

EOSC AAI Architecture 2022

- Consistent user experience and interfaces for service providers

- Multi-infrastructure workflows

- Scaling trust

- Growth of EOSC beyond the research and education community

- Community attributes and authorisation

EUROPEAN OPEN
SCIENCE CLOUD

EOSC AAI Architecture 2022

- **Consistent user experience and interfaces for service providers**

- Multi-infrastructure workflows

- Scaling trust

- Growth of EOSC beyond the research and education community

- Community attributes and authorisation

EUROPEAN OPEN
SCIENCE CLOUD

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

- Users need to go through multiple Identity Provider discovery steps
  - Example: First select Community AAI 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
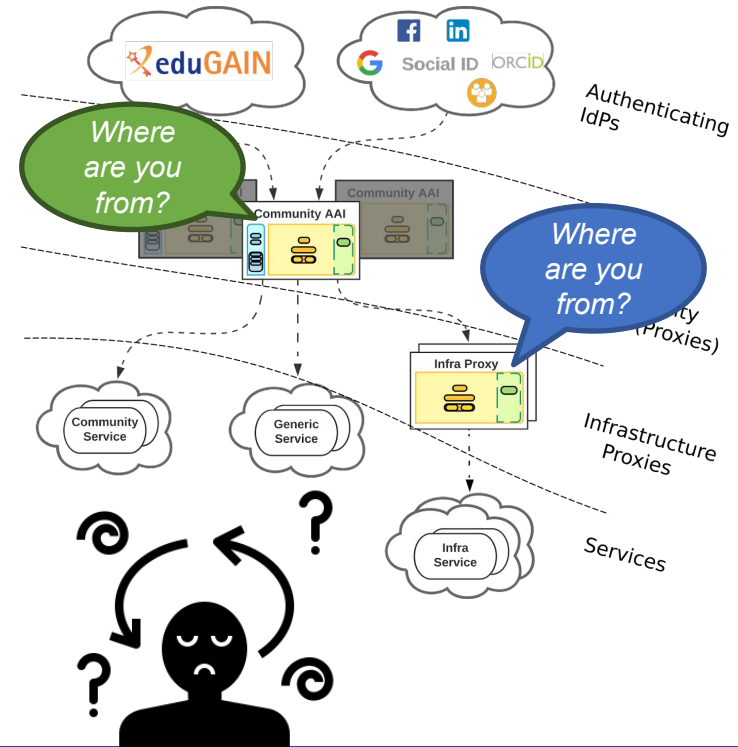
EOSC AAI Architecture 2022 Working Areas: Consistent user experience and interfaces (Contd.)

- Adoption of [AARC Community-based Access Entity Category (AARC-G079)](#) can be used to:

  - Distinguish Community AAIs from authenticating IdPs during discovery

  - Services that control access based on community identity attributes (e.g. community-managed groups and roles) ⇒ Filter out IdPs that don't assert the Community Entity Category Support attribute

  - Services that don't rely on community identity attributes ⇒ Include only authenticating IdPs during discovery

  - Facilitate IdP decisions to release a defined set of attributes to services.

The AARC Community-based Access Entity Category is a category of Service Providers that have a proven need to receive a set of community-managed information about their users in order to effectively provide their service to the user. These Service Providers include:

- Infrastructure Proxy services (Service Provider interface) [AARC-G045]
- Generic services [AARC-G045]

Identity Providers may indicate support for Service Providers in this Entity Category to facilitate discovery and improve the user experience at Service Providers. Self-assertion is the typical approach used but this is not the only acceptable method.

The following sections detail the requirements for both SAML 2.0 Service Providers and Identity Providers, in category membership and support respectively. For OpenID Connect based Service Providers, the technical requirements will be defined in a specification following the finalisation of the OpenID Connect Federation specification [OIDC-Fed].

2 Syntax

The following URI is used as the attribute value for the AARC Community-based Access Entity Category and the Entity Category Support attribute:

```
https://aarc-community.org/entity-category/community
```

3 Semantics

By asserting a Service Provider to be a member of this Entity Category, a registrar claims that:

- 3.1 The Service Provider has applied for membership in the Category and complies with this entity category's registration criteria as defined in Section 4.
- 3.2 The Service Provider's application for using the Community-based Access Entity Category has been reviewed against the guidelines provided in this specification and approved by the registrar.

By asserting this Entity Category Attribute, a Service Provider claims that it will not use attributes for purposes that fall outside of the service definition as presented at the time of registration and will support this statement within their published Privacy Statement.

By asserting this Entity Category Support Attribute, an Identity Provider claims that it will release attributes to approved Service Providers as outlined in Section 7.

EOSC AAI Architecture 2022

- Consistent user experience and interfaces for service providers

- **Multi-infrastructure workflows**

- Scaling trust

- Growth of EOSC beyond the research and education community

- Community attributes and authorisation

EUROPEAN OPEN SCIENCE CLOUD

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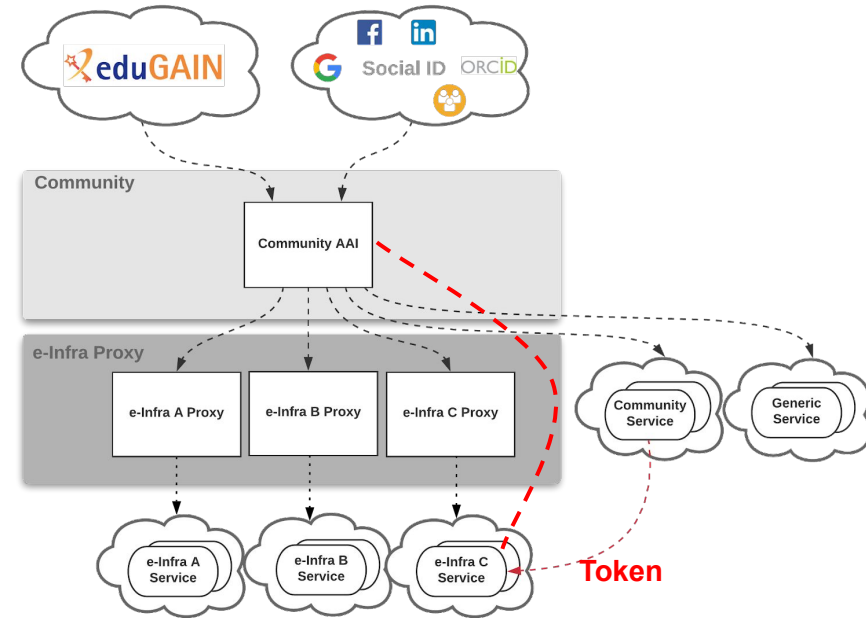
EOSC AAI Architecture 2022 Working Areas: Multi-infrastructure workflows (Contd.)

- OAuth 2.0 token validation: Existing standards rely on direct trust relationship between the protected resources and the Authorisation servers issuing OAuth 2.0 tokens

- Example: Community service (infrastructure A) accessing e-Infra service (infrastructure B) on behalf of user
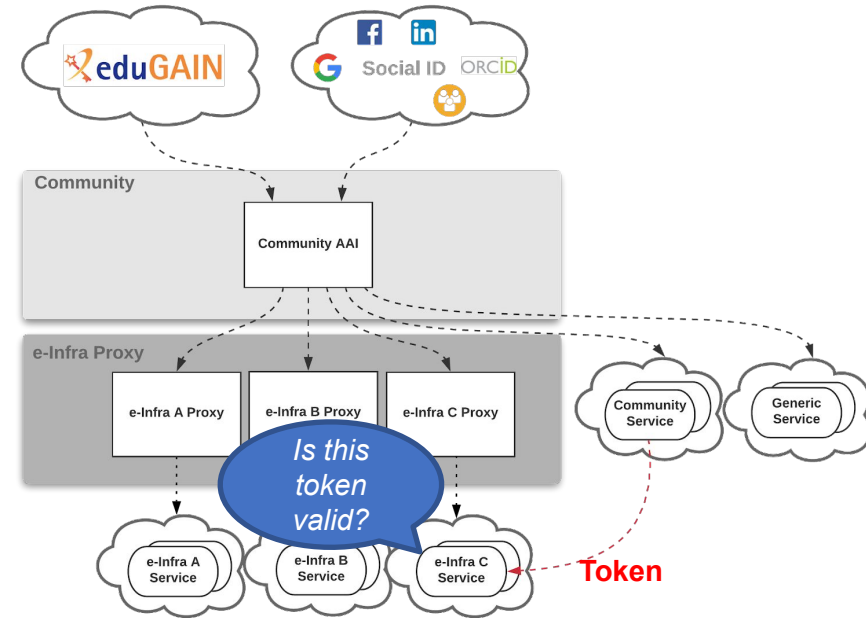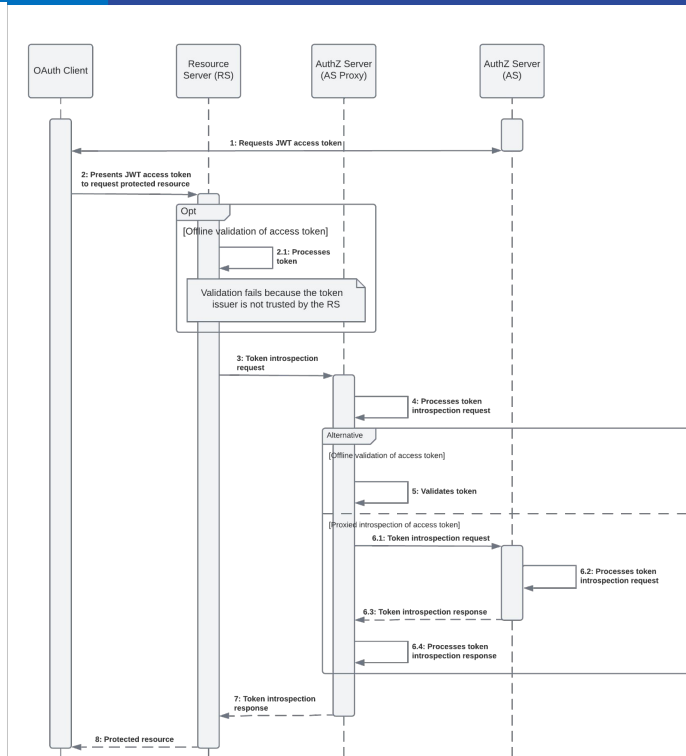
EOSC AAI Architecture 2022 Working Areas: Multi-infrastructure workflows (Contd.)

- Resource servers need to directly trust multiple Authorisation Servers across infrastructures 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.)

- [OpenID Connect Federation specification v1.0 (draft)](#) ⇒ Long-term solution for dynamically establishing trust in a distributed environment

- [OAuth 2.0 Token Proxied Introspection specification (AARC-G052)](#) ⇒ Interim solution until the OIDC Federation Specification is finalised & becomes widely available.
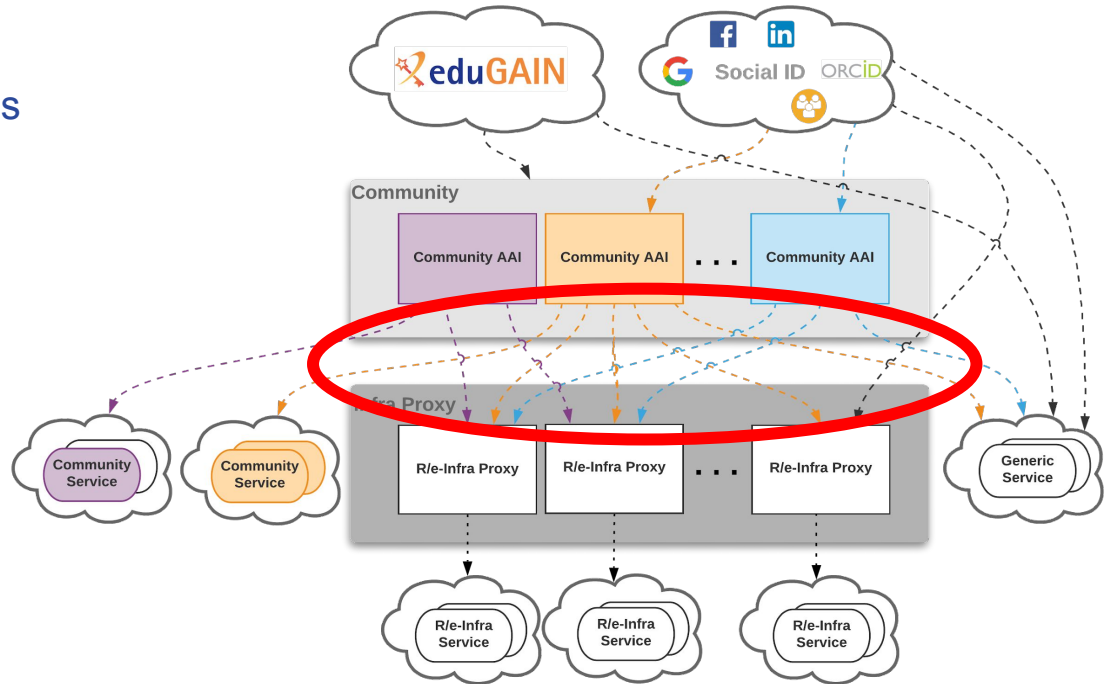
EOSC AAI Architecture 2022

- Consistent user experience and interfaces for service providers

- Multi-infrastructure workflows

- **Scaling trust**

- Growth of EOSC beyond the research and education community

- Community attributes and authorisation

EUROPEAN OPEN
SCIENCE CLOUD

EOSC AAI Architecture 2022 Working Areas: Scaling trust for OIDC

- Trust between Community AAI and Infrastructure Proxy services needs to be established via exchange of metadata

- Growing number of Community AAI and Infrastructure Proxy services that need to be interconnected for enabling access to resources across infrastructures within the wider EOSC environment

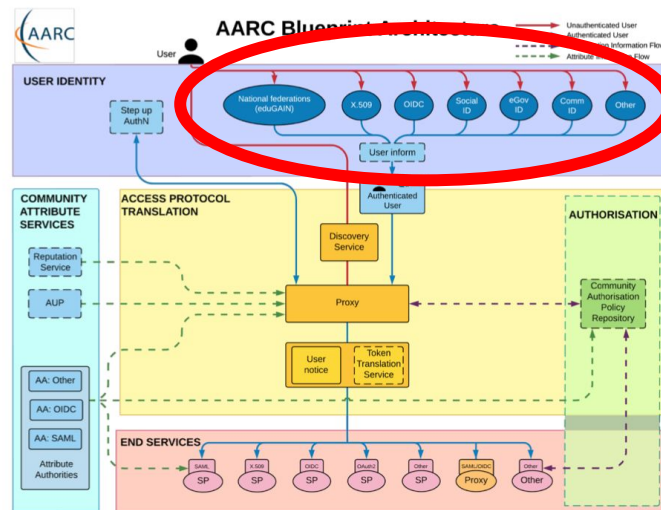- Establishment of M:N relationships → *scalability* issues

EOSC AAI Architecture 2022

- Consistent user experience and interfaces for service providers

- Multi-infrastructure workflows

- Scaling trust

- **Growth of EOSC beyond the research and education community**

- Community attributes and authorisation

EUROPEAN OPEN SCIENCE CLOUD

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

- Enables access to users from 5100+ identity providers from R&E community but needs to support citizen scientists, public sector organisations, and industry users

- Extending access:

  - Social media identities

  - eIDAS (national identification scheme) identities

  - Organisations beyond R&E:
    - Organisation can join National Federation to register the authenticating entity; or
    - EOSC AAI Federation Operator can import the authenticating entity of that organisation into the federation
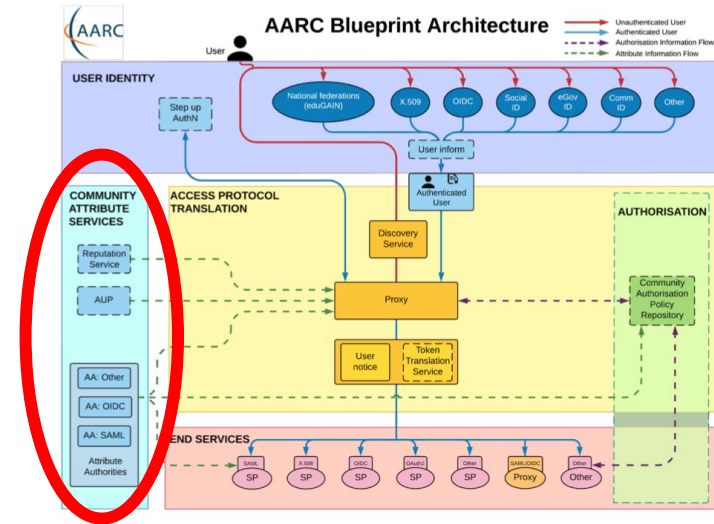
EOSC AAI Architecture 2022

- 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**

EUROPEAN OPEN SCIENCE CLOUD

EOSC AAI Architecture 2022 Working Areas: Community attributes & authZ

- Attribute Providers (AtP) can be independent from authenticating/Community IdPs

- Need to consider different –not only community-controlled– attribute/access management services

EOSC AAI Architecture 2022

Next steps:

- Specify scalable mechanism for establishing trust between OAuth 2.0 Authorization Servers within the EOSC AAI Federation

- More streamlined discovery process (e.g. "EOSC Login" button)?

- Introduce minimum assurance requirements?

Working Document

EOSC AAI Architecture 2022

EOSC-A AAI TF - Report (DRAFT)

Introduction

This document is a DRAFT version of the EOSC AAI Architecture 2022 which follows the EOSC Authentication and Authorization Infrastructure (AAI) report from the EOSC Executive Board Working Group Architecture AAI Task Force.

The current EOSC AAI architecture is based on the AARC Blueprint Architecture 2019 (AARC-BPA-2019). The goal of the EOSC-A AAI TF is not to define a new AAI architecture, but rather to define an AAI architecture that follows the AARC BPA and the AARC Interoperability Guidelines. Specifically, the EOSC-A AAI Task Force will work in collaboration with AEGIS, the AARC Community and other stakeholders to evolve the AARC Blueprint Architecture & Guidelines and use them as the basis for delivering the EOSC AAI Architecture 2022 version by the end of 2022.

EUROPEAN OPEN SCIENCE CLOUD

THANK YOU

EUROPEAN OPEN
SCIENCE CLOUD