# EOSC-hub / PSNC Workshop

## *EOSC-hub Authentication & Authorisation Infrastructure*

eosc-hub.eu

@EOSC_eu

**Dissemination level**: Public

EOSC-hub receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 777536.

# Agenda

- EOSC-hub Authentication & Authorisation Infrastructure
  - Overview
  - High-level Service Architecture
  - Standards & interoperability guidelines
  - Technical solutions
  - Future plans

# EOSC-hub Authentication & Authorisation Infrastructure

## Overview

# In a nutshell

The EOSC-hub AAI:

- Contributes to the EOSC infrastructure implementation roadmap by enabling seamless access to a system of research data and services provided across nations and disciplines
- Builds on existing interoperable AAI solutions from EGI Federation, EUDAT CDI, GÉANT, and INDIGO-DataCloud that have successfully delivered a portfolio of operational services in this field over the last years
- Leverages eduGAIN identity providers and other institutional or social media credentials to expand the access to researchers, high-education, and business organisations

# EOSC-hub Authentication & Authorisation Infrastructure

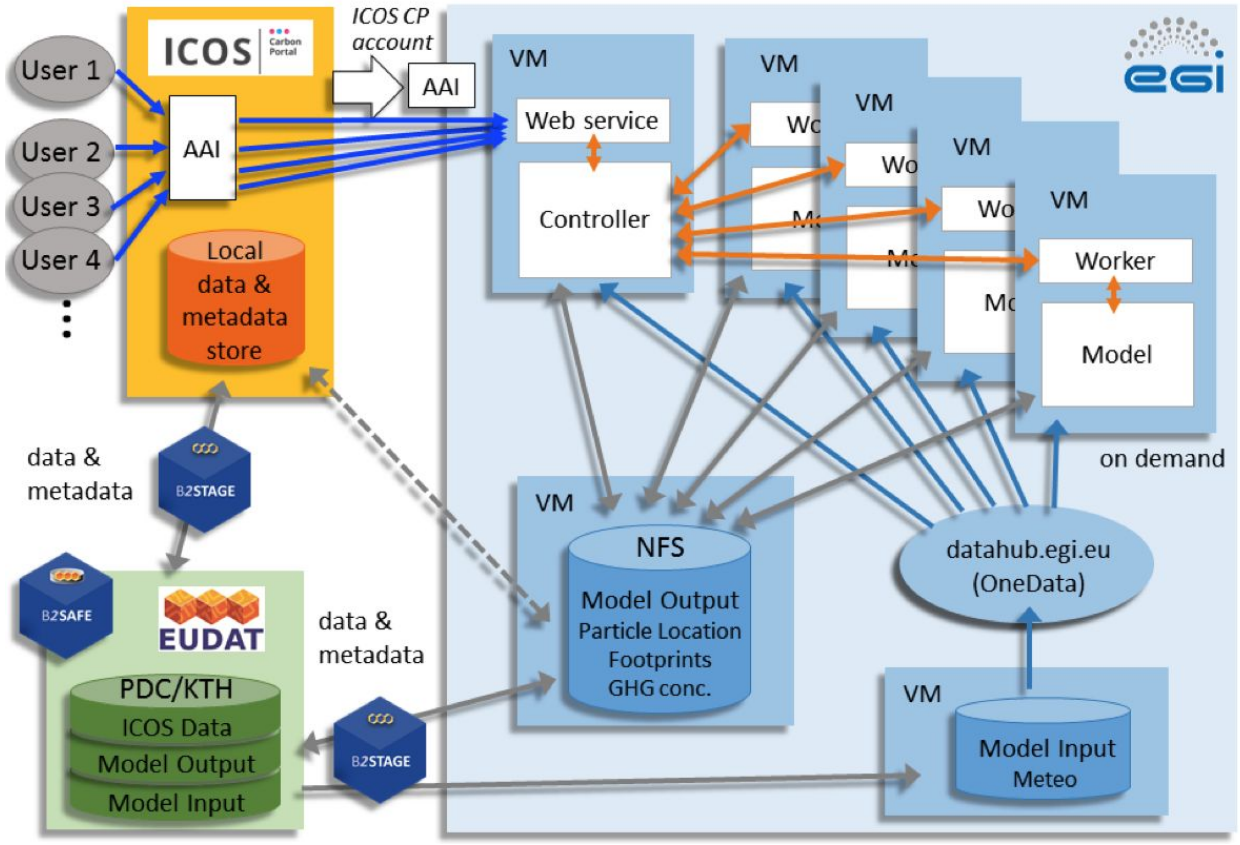
## High-level Service Architecture

# Example use case

## ICOS Carbon portal (Credit to Maggie Hellström)

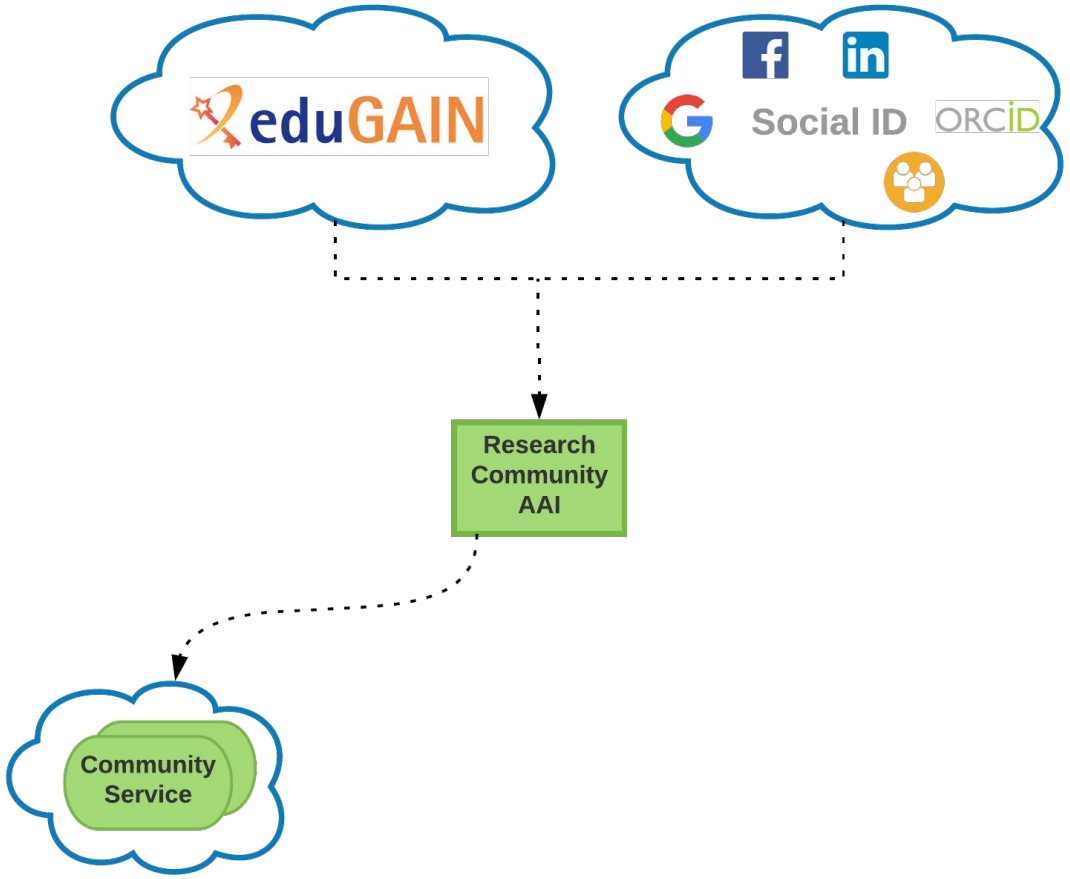
- Characteristics:
  - Access & orchestration from a community portal/framework
  - Underpinned by EGI services (e.g. Cloud; DIRAC; OneData, …)
  - Underpinned by EUDAT services (B2STAGE, B2SAFE, B2DROP, …)

- Requirements:
  - SSO through the portal/framework with community userIDs (e.g. LS AAI) or with public ID (e.g. EduGAIN)
  - Seamless translation of identities among underlying services



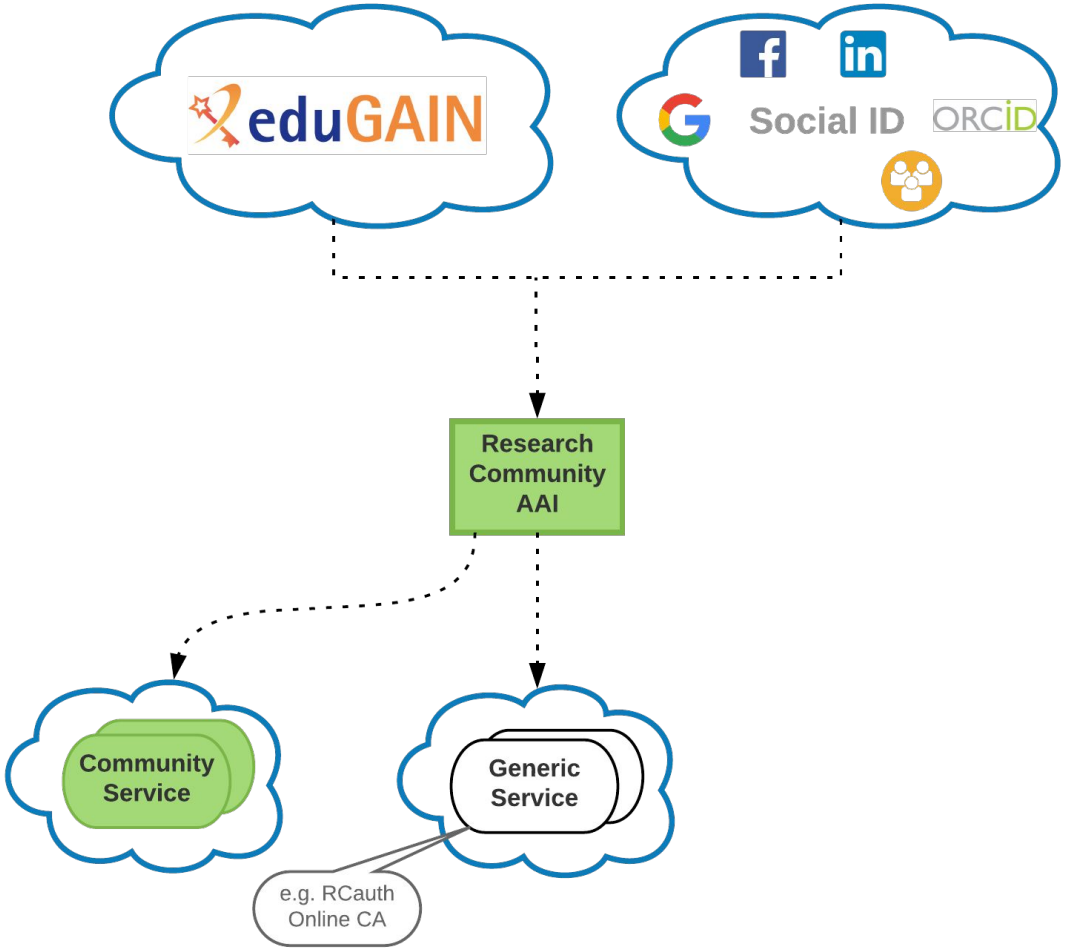
# Generic AAI use case

## Accessing community services



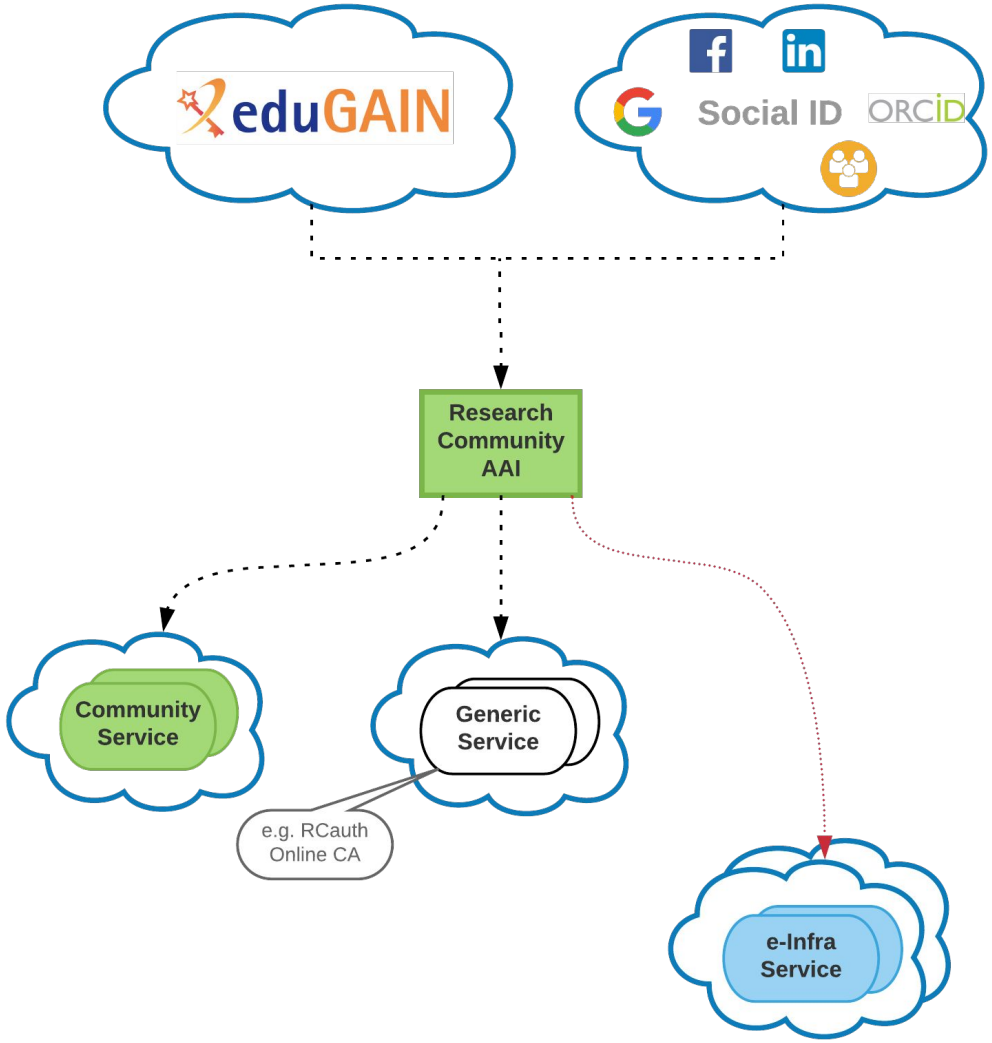
# Generic AAI use case

## Accessing generic services

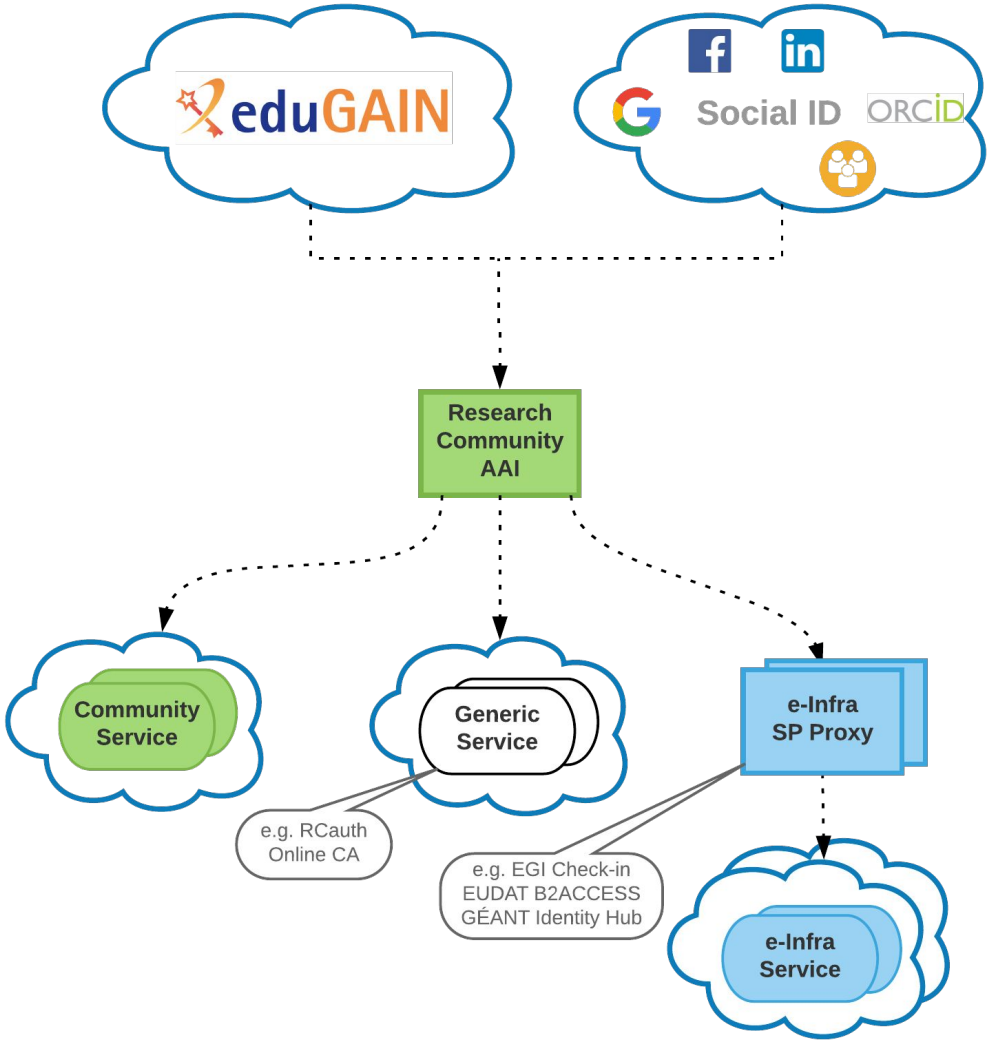


# Generic AAI use case

## Accessing EOSC resources



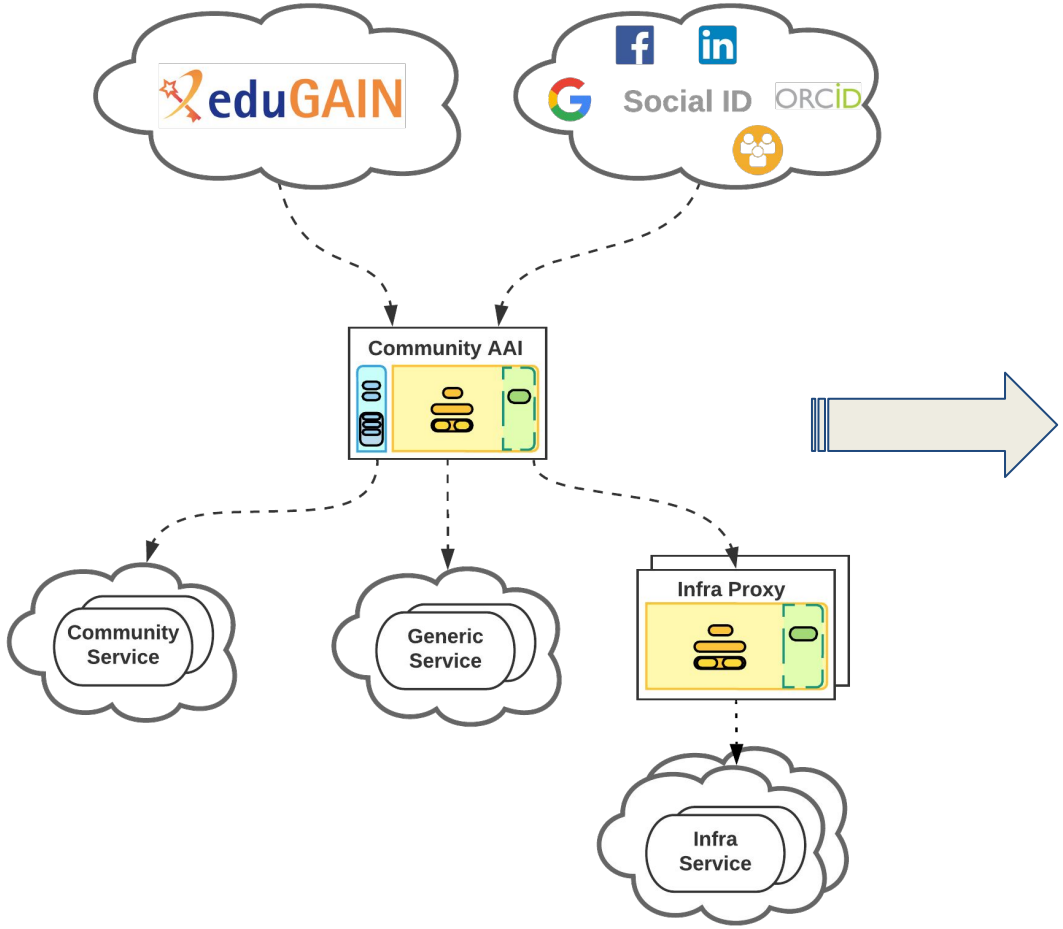
# EOSC-hub AAI
## High-level Architecture

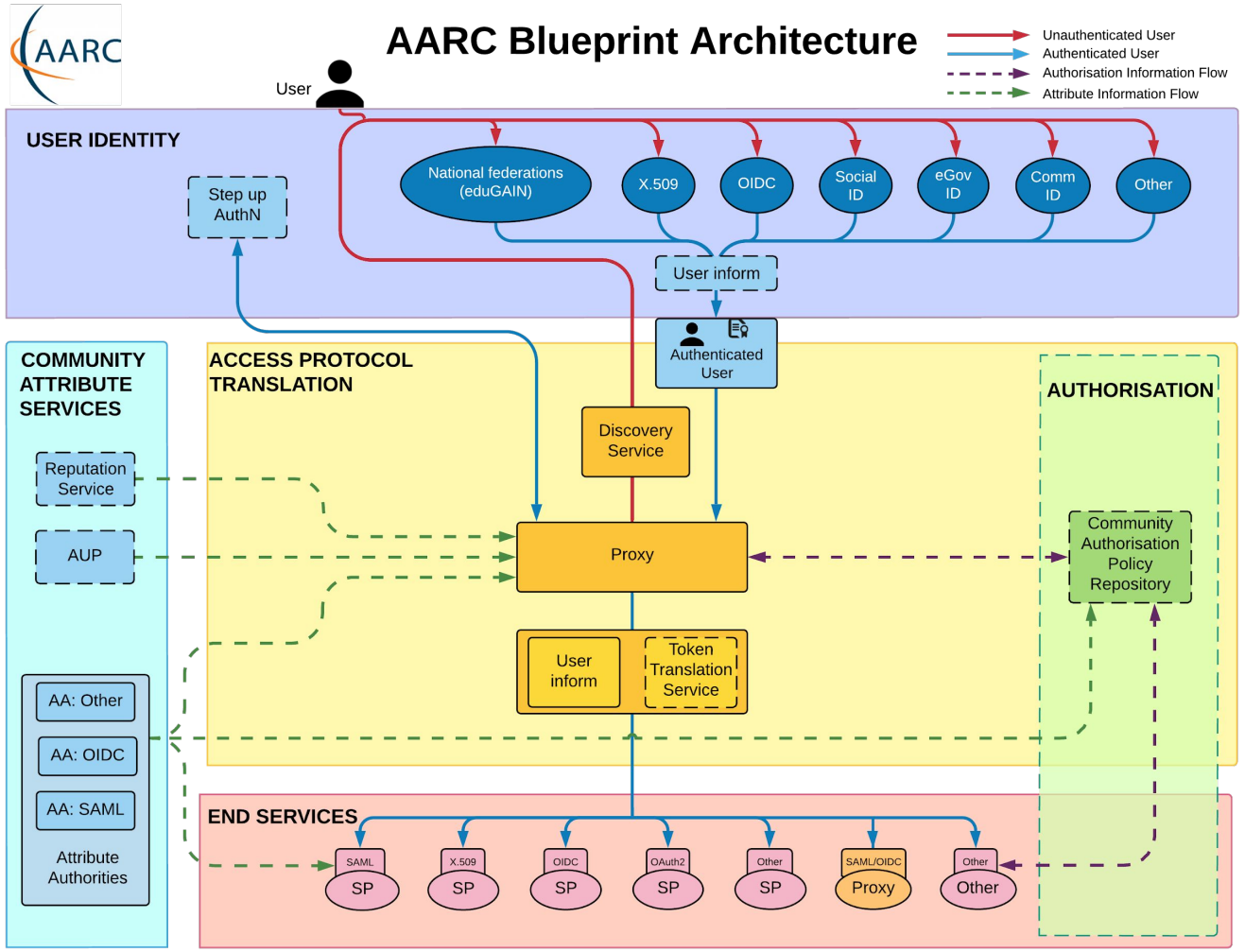



- Researchers register once with with their Community AAI
- Researchers always sign in via their Community AAI
- Community-specific services are connected to a single Community AAI
- Generic services (e.g. RCauth.eu Online CA) may be connected to more than one AAI proxies
- General-purpose e-Infra services are typically connected to a single e-infra SP proxy

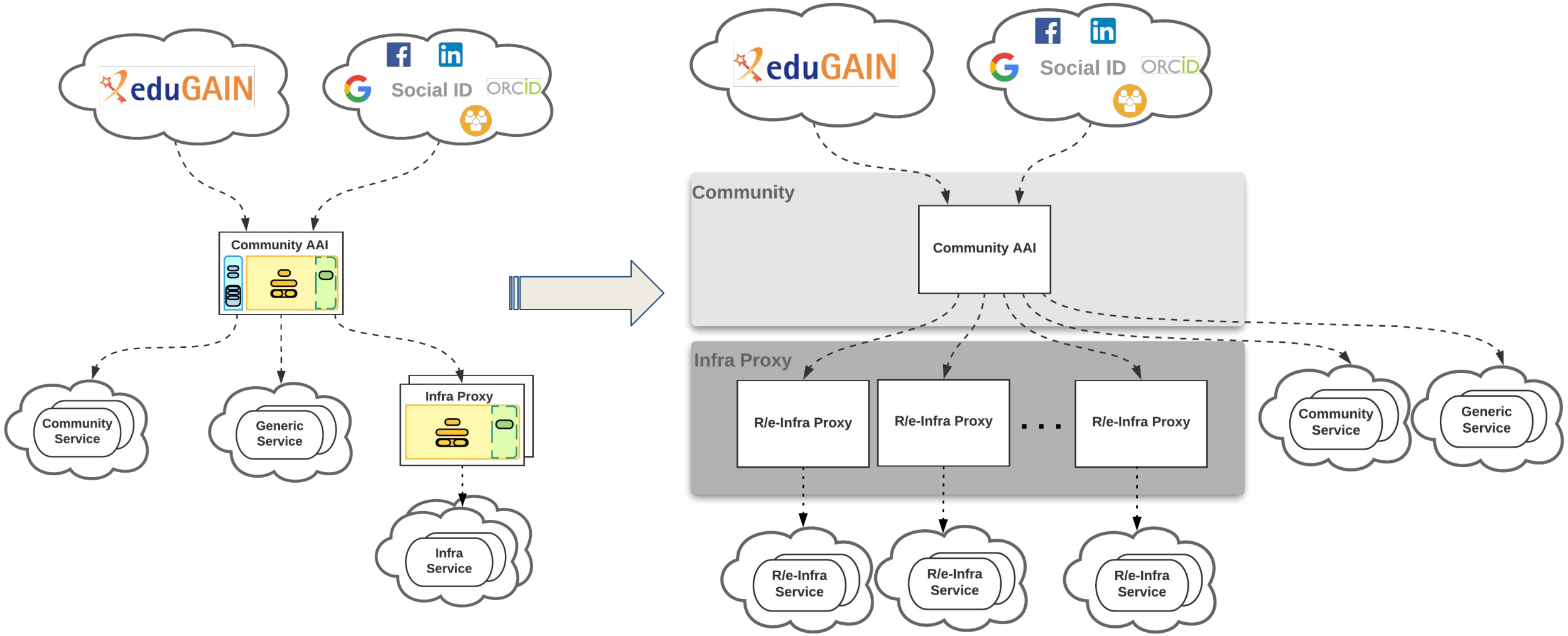
# EOSC-hub AAI

## Implementation of the AARC BPA

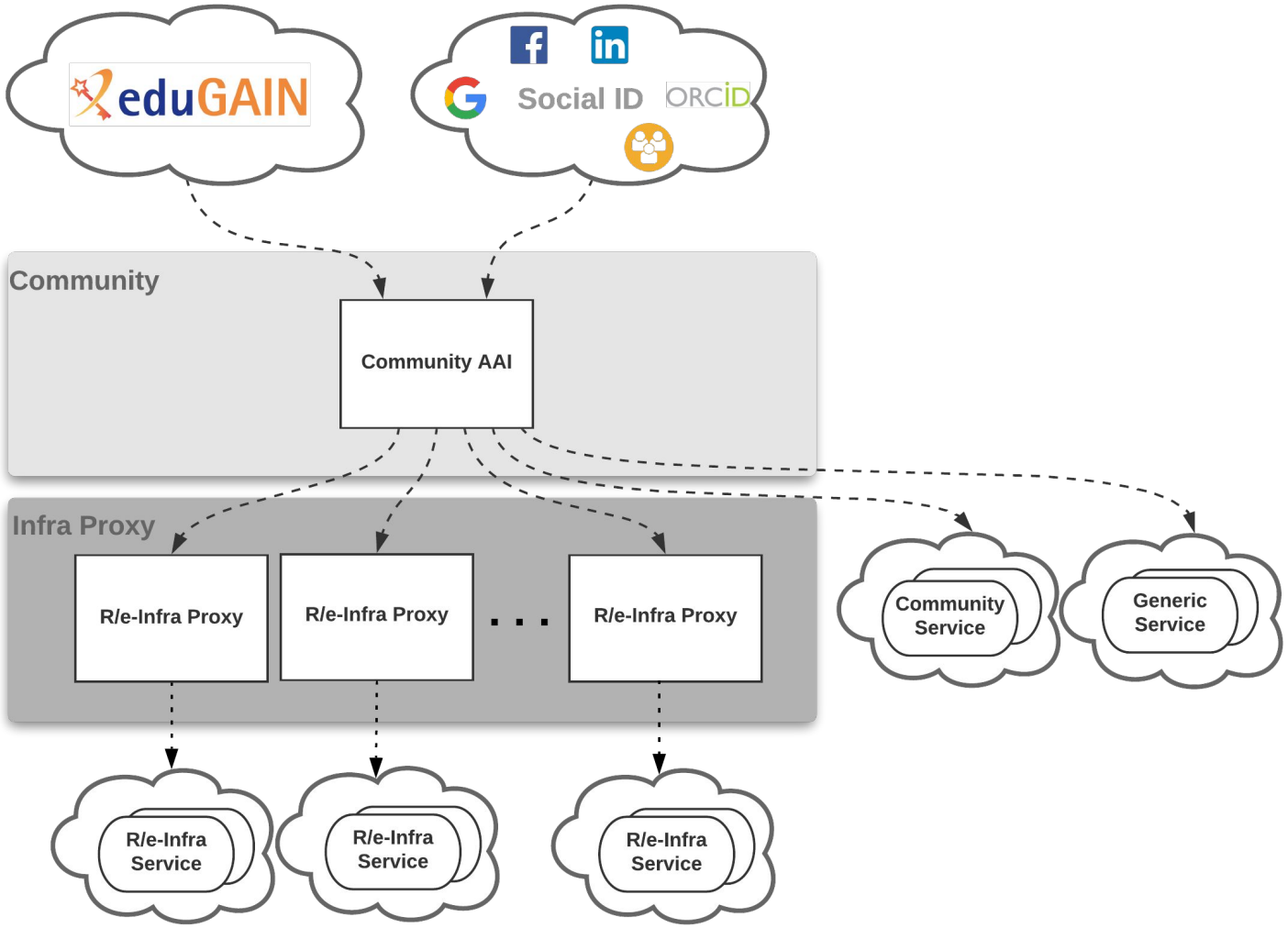


# Impl. of the AARC BPA “Community-first” approach



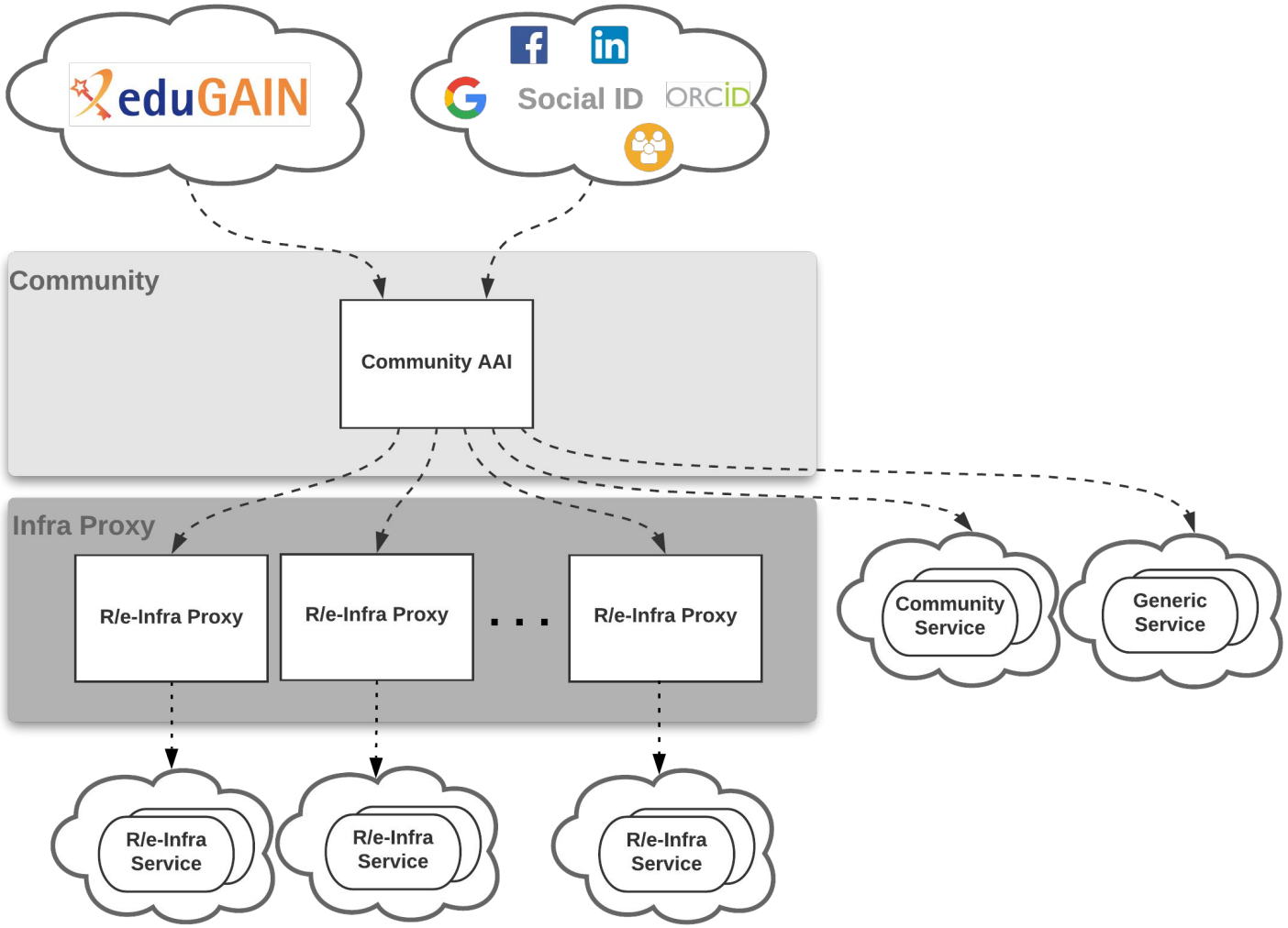
# EOSC-hub AAI
## Layers




- **Community:** Enables the use and management of community identities for access to EOSC resources
- **Infra Proxy:** Enables access to resources offered by Service/Resource Providers connected to the R/e-Infrastructures.

# EOSC-hub AAI

## Use cases




- For communities without an AAI:
  - EOSC-hub AAI provides different Community AAI service offerings:
    - B2ACCESS
    - Check-in
    - eduTEAMS
    - INDIGO-IAM
- For communities with an AARC BPA-compliant Community AAI
  - They can connect to the Infra Proxy layer to gain access to EOSC resources
- For infrastructures with an AARC BPA-compliant Infra Proxy:
  - They can connect to the Infra Proxy layer to make their resources available to different communities

# EOSC-hub Authentication & Authorisation Infrastructure

## Standards & interoperability guidelines

# Standards & APIs

| Standard | Short description | References |
|---|---|---|
| Security Assertion Markup Language (SAML) 2.0 | OASIS standard for exchanging authentication and authorisation data between parties. | https://www.oasis-open.org/standards#samlv2.0 |
| OAuth 2.0 | Standard for authorisation that enables delegated access to server resources on behalf of a resource owner | "The OAuth 2.0 Authorization Framework", RFC 6749, https://www.rfc-editor.org/info/rfc6749 |
| OpenID Connect 1.0 | Identity layer on top OAuth 2.0. Enables Clients to (i) verify the identity of the End-User based on the authentication performed by an AS; (ii) obtain basic profile information about the End-User in an interoperable and REST-like manner | “OpenID Connect Core 1.0”, https://openid.net/specs/openid-connect-core-1_0.html |

# Standards & APIs (Cont.)

| Standard | Short description | References |
|---|---|---|
| X.509 | ITU-T standard for a public key infrastructure (PKI), also known as PKIX (PKI X509) | "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, https://www.rfc-editor.org/info/rfc5280<br>"Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile", RFC 3820, https://www.rfc-editor.org/info/rfc3820 |
| Lightweight Directory Access Protocol (LDAP) | Provides access to distributed directory services that act in accordance with X.500 data and service models | https://tools.ietf.org/html/rfc4511 |

# Standards & APIs (Cont.)

| API | Short description | References |
|---|---|---|
| OAuth 2.0 Token Introspection | Protocol that allows authorised protected resources to query the authorisation server for determining the set of metadata for a given OAuth2 token, including its current validity. | https://tools.ietf.org/html/rfc7662 |
| OAuth 2.0 Token Exchange | Protocol for requesting and obtaining security tokens from OAuth 2.0 authorization servers, including security tokens employing impersonation and delegation | https://tools.ietf.org/id/draft-ietf-oauth-token-exchange-14.html |

# Standards & APIs (Cont.)

| API | Short description | References |
|---|---|---|
| OAuth 2.0 Device Authorization Grant | Enables OAuth 2.0 clients on input-constrained devices to obtain user authorisation for accessing protected resources without using an on-device user-agent | https://tools.ietf.org/html/draft-ietf-oauth-device-flow-15 |
| System for Cross-domain Identity Management (SCIM) 2.0 | Open API for managing identities | SCIM: Core Schema , RFC7643, https://tools.ietf.org/html/rfc7643<br>SCIM: Protocol, RFC7644, https://tools.ietf.org/html/rfc7644<br>SCIM: Definitions, Overview, Concepts, and Requirements, RFC7642, https://tools.ietf.org/html/rfc7642 |

# Technical interoperability guidelines

- **Expressing Authentication information:**
  - Attributes for expressing **user information** should follow the REFEDS Research & Scholarship attribute bundle [REFEDS-R&S]
- **Expressing Authorisation information:**
  - **VO/group membership and role information**, which is typically used by relying parties for authorisation purposes, should be expressed according to [AARC-G002]
  - **Capabilities**, which define the resources or child-resources a user is allowed to access, should be expressed according to [AARC-G027]
  - Affiliation information, including
    - user's **affiliation within their Home Organisation** (e.g. university, research institution or private company)
    - **affiliation within the Community**, such as cross-organisation collaborations, should be expressed according to [AARC-G025]

# Technical interoperability guidelines (Cont.)

- Assurance information used to express how much relying partins can trust the attribute assertions about the authenticating user should follow:
  - REFEDS Assurance framework (RAF) [RAF-version-1.0]
  - Guideline on the exchange of specific assurance information [AARC-G021]
  - Guideline for evaluating the combined assurance of linked identities [AARC-G031]
  - Guideline Expression of REFEDS RAF assurance components for identities derived from social media accounts [AARC-GO41]
  - Guidelines for expressing the freshness of affiliation information, as defined in [AARC-G025]
- OAuth2 Authorisation servers should be able to validate tokens issued by other trusted Authorisaton servers → requires extending existing flows (e.g. OAuth2 Token Exchange flow [OAuth2-Token-Exchange-draft])

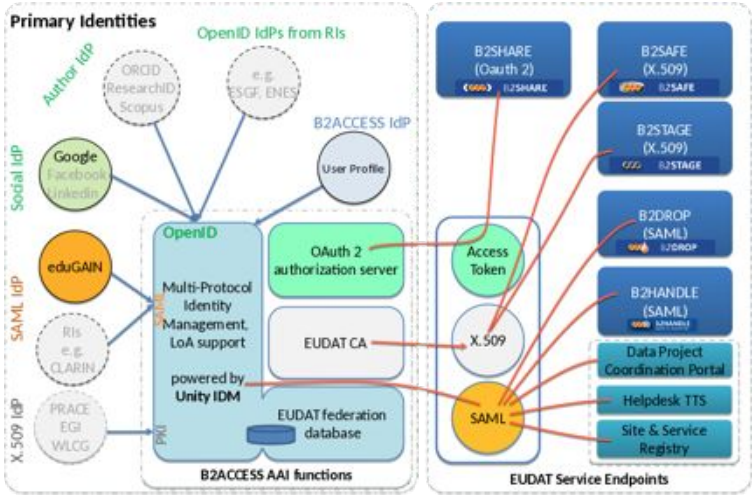
# Policy interoperability guidelines

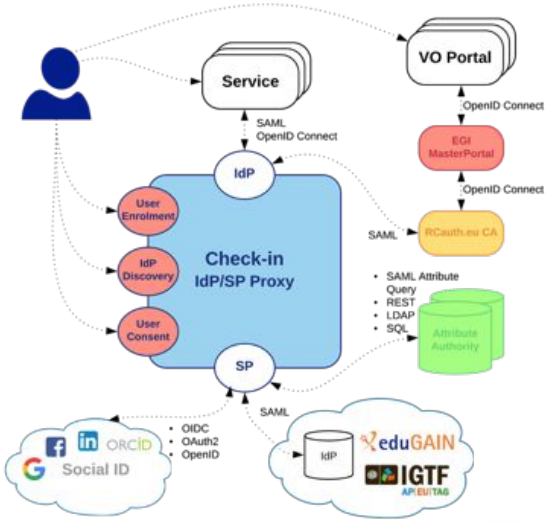
- Compliance with the GÉANT Data Protection Code of Conduct version 1 (DPCoCo-v1) [DPCoCo-v1] → reflects the **Data Protection** Directive and means compliance with applicable European rules (see [AARC-G040])
  - To explicitly declare compliance with DPCoCo-v1, the privacy notice of each EOSC AAI service should include a reference to DPCoCo-v1
- The entities of the EOSC AAI registered with eduGAIN should meet the Sirtfi [Sirtfi-v1.0] requirements and express Sirtfi compliance in their metadata in order to facilitate **coordinated response to security incidents** across organisational boundaries.
- To reduce the burden on the users and increase the likelihood that they will read the AUP as they access resources from multiple service and resource providers, the EOSC AAI services should adopt the WISE Baseline AUP model [WISE-AUP]

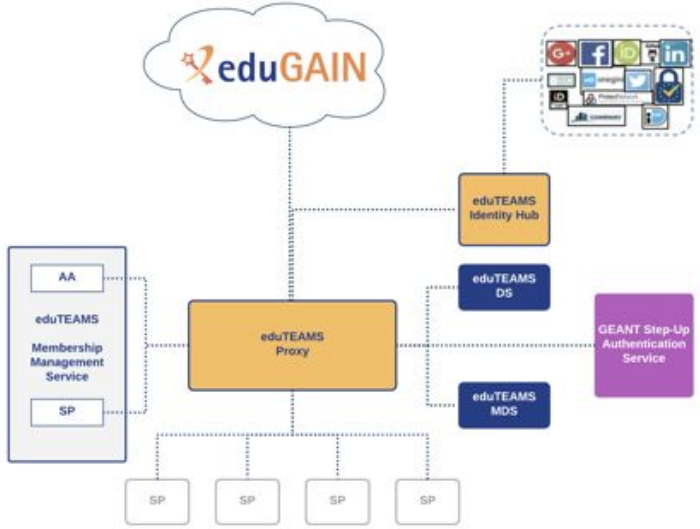
# EOSC-hub Authentication & Authorisation Infrastructure

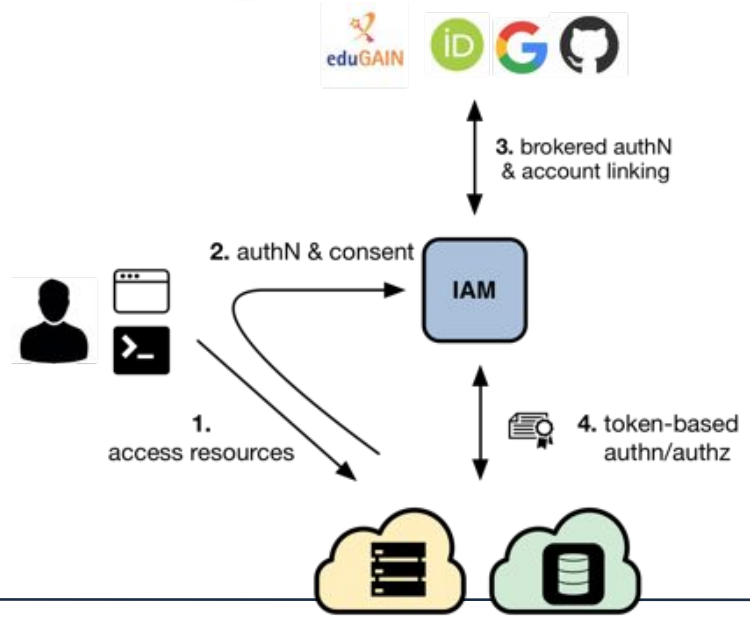
## Solutions

# EOSC-hub AAI services



# EOSC-hub AAI Solutions

- AAI services:
  - B2ACCESS
  - Check-in
  - eduTEAMS
  - INDIGO-IAM
- Membership Management Services:
  - Perun
  - COmanage Registry
  - HEXAA
- Token Translation Services:
  - WaTTS
  - MasterPortal
  - RCauth.eu

# EOSC-hub AAI integration guides

- B2ACCESS
- Check-in
- eduTEAMS
- INDIGO-IAM
- Perun
- COmanage
- WaTTS
- MasterPortal
- RCauth.eu

# EOSC-hub Authentication & Authorisation Infrastructure

## Future plans

# AAI Roadmap

https://confluence.egi.eu/display/EOSC/Roadmap

# Thank you for your attention!

*Questions*?

## Contact

nliam@grnet.gr

EOSC-hub

eosc-hub.eu @EOSC_eu