EOSC Technical Specification

EOSC Hub Federated Core Services - AAI

Technical Area:	Authentication and Authorization Infrastructure
Version:	0.1
Status:	Final
Document Link:	https://wiki.eosc-hub.eu/display/EOSCDOC/AAI

EOSC-HUB  UNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AG NO. 777536.

DELIVERY SLIP

Date	*Name*	*Partner/Activity*
From:	Michal Prochazka	ELIXIR
	Licia Florio	GEANT
Moderated by:		
Reviewed by:		
Approved by:		

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
	21. 5. 2020	Final version	Michal Prochazka, Licia Florio

TERMINOLOGY

https://wiki.eosc-hub.eu/display/EOSC/EOSC-hub+Glossary

Terminology/Acronym	*Definition*

Table of Contents

Introduction

The EOSC AAI that is being designed and will be further deployed beyond the EOSC-Hub project enables seamless access to research data and services in EOSC in a secure and user-friendly way.

Adopted standards

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 of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to 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
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 "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

Protocol/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
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 SCIM: Protocol, RFC7644, https://tools.ietf.org/html/rfc7644 SCIM: Definitions, Overview, Concepts, and Requirements, RFC7642, https://tools.ietf.org/html/rfc7642

High-level Service Architecture

The EOSC AAI follows the architectural and policy recommendations defined in the AARC project [AARC-Community]. As such, it enables interoperability across different SP-IdP-Proxy services, each of which acts as a bridge between the community-managed proxies (termed Community AAIs) managing the researchers' identity and the generic services offered by Research Infrastructure and e-Infrastructures (termed R/e-Infrastructures or Infrastructures). This is the “community-first” approach to the AARC Blueprint Architecture [AARC-G045], which enables researchers to sign in with their community identity via their Community AAI. A high-level view of the EOSC AAI is provided in Figure 1.

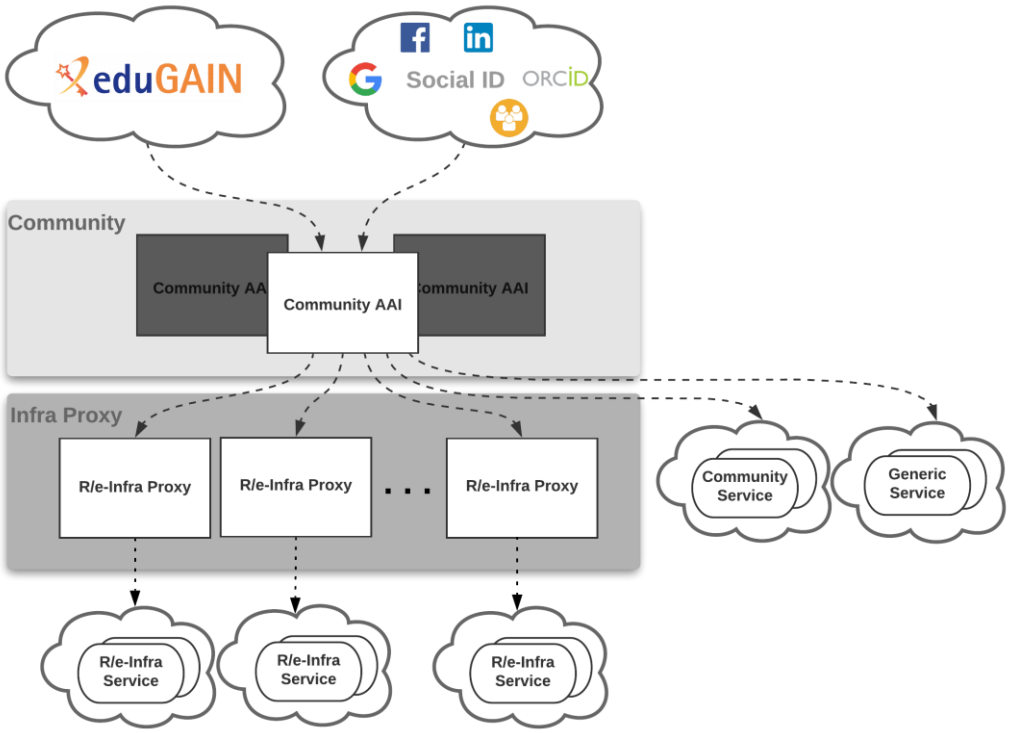

Figure 1. High-level view of AAI architecture for access to EOSC resources: A researcher's perspective following the AARC Blueprint Architecture.

Community-specific services are connected to a single Community AAI, while Infrastructure Services are connected to a single Infrastructure Proxy. Lastly, generic services may be connected to more than one Community AAI. Each Community AAI, in turn, serves as a bridge between external identity providers and the proxies to the e-infrastructure services. Specifically, Community AAIs connect to eduGAIN as service providers but act as identity providers from the services point of view, thereby allowing users to use their credentials from their home organisations. Complementary to this, users without an account on a federated institutional Identity Provider are still able to use social media or other external authentication providers for accessing services.

Research communities can leverage community AAI services for managing their users and their respective roles and other authorisation-related information. At the same time, the adoption of standards and open technologies, including SAML 2.0, OpenID Connect, OAuth 2.0 and X.509v3, facilitates interoperability and integration with the existing AAIs of other e-Infrastructures and research communities. As shown in Figure 2, communities can allow different authentication options for their members and, at the same time, enable access to all or a subset of the Infrastructures. It should be noted that this model also allows users to access resources as members of their home organisation. Being connected to multiple Community AAIs and the upstream institutional/social IdPs requires the Infra Proxies to properly support discovery for both community and home organisation-based access scenarios.

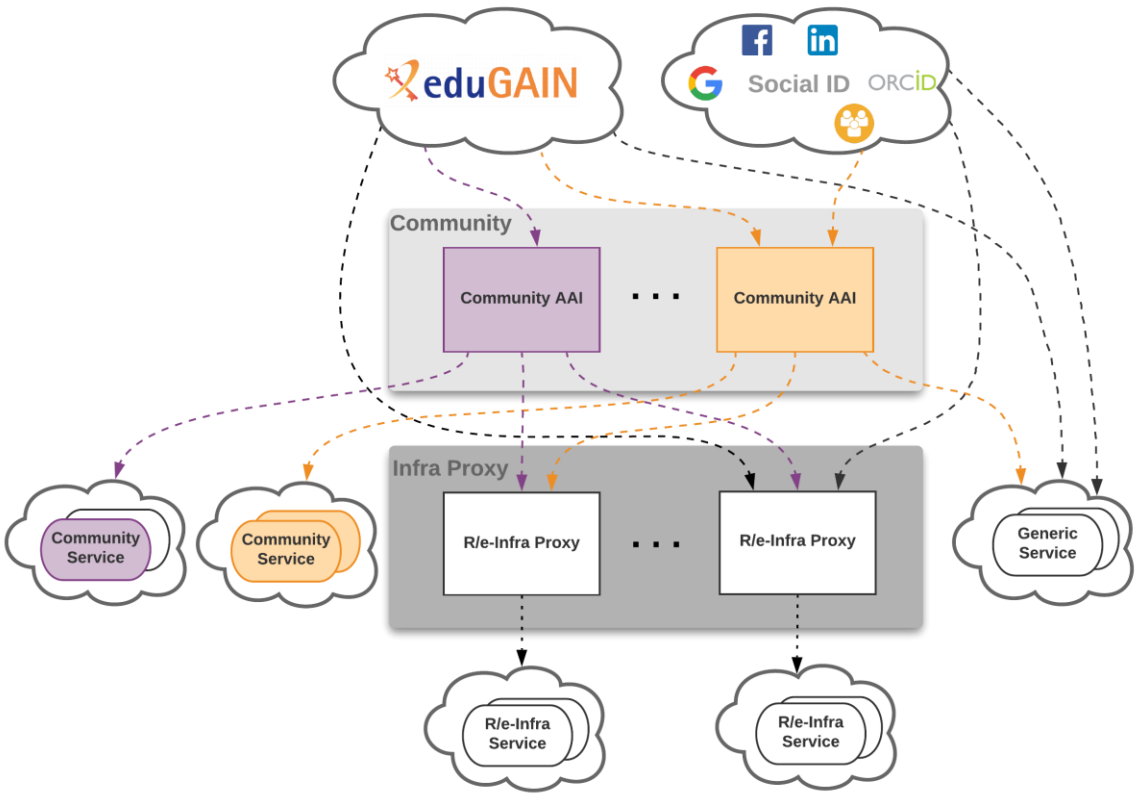

Figure 2. A high-level view of AAI architecture for access to EOSC resources

Interoperability guidelines

Technical interoperability guidelines

- The attributes used to express user information should follow the REFEDS R&S attribute bundle, as defined in [REFEDS-R&S]
- 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 (i) the user's affiliation within their Home Organisation, such as a university, research institution or private company, and (ii) affiliation within the Community, such as cross-organisation collaborations, should be expressed according to [AARC-G025]
- Assurance information used to express how much relying parties 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 Authorisation servers. Extending existing flows, such as the OAuth2 Token Exchange flow [OAuth2-Token-Exchange-draft], will need to be considered for enabling the validation of such externally issued tokens.

Policy interoperability guidelines

- For the EOSC AAI (and for the Community AAIs), compliance with the GÉANT Data Protection Code of Conduct version 1 (DPCoCo-v1) [DPCoCo-v1] is implicit, since it 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 (and for the Community AAIs) registered with eduGAIN should meet the Sirtfi [Sirtfi-v1.0] requirements and express Sirtfi compliance in their metadata in order to facilitate a 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 services and resource providers, the EOSC AAI and the Community AAI services should adopt the WISE Baseline AUP model [WISE-AUP].

Examples of solutions implementing this specification

AAI services:

- B2ACCESS
- Check-in
- eduTEAMS
- INDIGO-IAM

Identity and Access Management:

- Perun
- Comanage

- HEXAA

Token Translation Services:

- WaTTS
- MasterPortal
- RCauth.eu

Procedure to integrate a service with the EOSC Hub AAI

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