Authentication and Authorization Infrastructure - AAI

The EOSC-hub Authentication and Authorisation Infrastructure (AAI) enables seamless, authenticated access to services and research data in EOSC. The EOSC-hub AAI enables service providers to control access to their services from users holding identities (usernames and passwords) from a very broad set of academic, community or social Identity Providers (IdPs). The EOSC-hub AAI brings together these IdPs, the EOSC-hub service providers (SPs) and intermediary identity management proxies into a single, interoperable infrastructure.

Why to use it

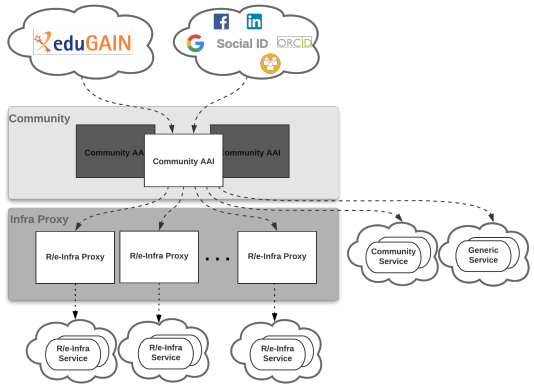
If Your service or dataset requires authenticated access, or if you want to track usage at the level of individual users, then the EOSC-hub AAI offers a simple way for user authentication and authorisation. The AAI enables users to get from the EOSC Portal into your service with a single identity, which they already hold from their university, institute or preferred social network. The EOSC-hub AAI can recognise this identity and pass you a trusted token to enable access for the service you offer.

Features

- Support for different authentications providers, including:
  - institutions from national identity federations in eduGAIN
  - social media (e.g. Google, Facebook, LinkedIn)
  - other external authentication providers such as ORCID or community-operated identity providers
- Access to resources using different login credentials (e.g. institutional and social) via identity linking
- Access to multiple heterogeneous (web and non-web) services and resources using different technologies
  - Non-web-browser based use cases include APIs and command line access (e.g. via SSH or OAuth2)
- Aggregation and harmonisation of authorisation information (e.g. groups and/or roles) from multiple sources
- Adoption of standards and open technologies, including SAML 2.0, OpenID Connect, OAuth 2.0 and X.509v3 to facilitate interoperability and integration with the existing AAIs of e-Infrastructures and research communities
- Adoption of policies compliant with global frameworks (e.g. REFEDS Research and Scholarship entity category and Sirtfi) in order to:
  - support services in receiving and processing consistent user attributes in compliance with the minimal disclosure principle
  - ensure good practices in operational security
  - enable the coordination of incident response across federated organisations
- Expressing the level of trust in the user identity assertions using standard frameworks such as the REFEDS Assurance Framework

High-level service architecture

The EOSC-hub AAI follows the architectural and policy recommendations defined in the AARC project. 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 enables researchers to sign in with their community identity via their Community AAI. A high-level view of the EOSC-hub AAI is provided below.



As shown in the high-level view of the architecture, Community-specific services are connected to a single Community AAI, while Infrastructure Services can be connected to a single Infrastructure Proxy. Lastly, generic services are typically 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 the EOSC-hub 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. 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.

Service overview

The EOSC-hub AAI comprises different AAI services, namely B2ACCESS, Check-in, eduTEAMS and INDIGO-IAM. Research communities can leverage these services for managing their users and their respective roles and other authorisation-related information. The suite of EOSC-hub AAI services also includes Perun, which can be used for managing users within organisations and projects, as well as managing access rights to the services. There are also Token Translation Services such as WaTTS and MasterPortal, which provide mechanisms that enable translation between different protocols or technologies. The RCauth.eu service, in particular, is an Online CA that can on-the-fly identify entities based on federated credentials and issue to them PKIX credentials in real-time, focussing on converting SAML-to-PKIX.

Service documentation

For end-users

The links below cover topics related to managing your community identity, including initial registration, linking of additional institutional/social authentication providers and more:

- B2ACCESS

- Check-in
- INDIGO-IAM

For resource providers

The links below explain how to integrate your service with the EOSC-hub AAI:

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

For community managers

The links below describe how community managers can manage members in their community, organise them in groups, assign roles, access rights and more:

- Check-in
- eduTEAMS
- Perun
- INDIGO-IAM