AAI Roadmap

This page describes the future plans for the EOSC-hub AAI. These include alignment activities across the EOSC-hub AAI services which can be classified into technical and policy-related activities.

Technical alignment activities

The following technical alignment activities have been identified:

- **Alignment of user attributes:** The attributes used to express user information should follow the REFEDS R&S attribute bundle, as defined in [REFEDS-R&S]
- **Alignment of VO/group membership and role information:** VO/group membership and role information, which is typically used by relying parties for authorisation purposes, should be expressed according to [AARC-G002]
- **Alignment of resource capabilities information:** Capabilities, which define the resources or child-resources a user is allowed to access, should be expressed according to [AARC-G027]
- **Alignment of affiliation information:** 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]
- **Alignment of assurance information:** 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 token validation across multiple domains:** There are use cases requiring a service agent to be able to act autonomously, on behalf of the user, consuming services and resources. If the services consumed by the agent are behind the same proxy, the EOSC-hub AAI architecture works. However, when an agent running on Service A needs to access resources on Service B, which might be connected by a different proxy, then there is no straight-forward solution at the moment. So, currently, services need to trust the same proxy to support those use cases. The AARC community is working on "AARC-G052: Recommendations for OpenID Connect/OAuth2 token-based access across different infrastructures", which is meant to be a temporary measure until the OIDC Federation Specification is widely available.

The table below lists the identified technical alignment activities and their status. A green checkmark indicates a complete activity, otherwise the expected time of implementation is provided.

Activity	B2ACCESS	Check-in	eduTEAMS	INDIGO-IAM
Alignment of user attributes				
Alignment of VO/group membership and role information				
Alignment of resource capabilities information				
Alignment of affiliation information		M34		M36
Alignment of assurance information (including freshness of affiliation information)	M36	M35		M36
OAuth2 token validation across multiple domains (multi-proxy connection workaround)				
OAuth2 token validation across multiple domains (interim implementation based on OAuth2 introspection)	M36	M36	M30	

Policy-related integration activities

The following policy-related alignment activities have been identified:

- **Alignment of privacy statements:** For the EOSC-hub AAI, 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-hub AAI service should include a reference to DPCoCo-v1.
- **Alignment of operational security and incident response policies:** The entities of the EOSC-hub 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.
- **Alignment of Acceptable Use Policies (AUPs):** 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].

The table below lists the identified policy-related activities and their status. A green checkmark indicates a complete activity, otherwise the expected time of implementation is provided (M21 is September 2019).

Activity	B2ACCESS	Check-in	eduTEAMS	INDIGO-IAM
Alignment of privacy statements		M34		
Alignment of operational security and incident response policies				
Alignment of Acceptable Use Policies (AUPs)		M34		

Integration of EOSC-hub AAI services

This section presents the integration roadmap of the EOSC-hub AAI services. The expected time of implementation is described in the table below. Integrations which have already been established are marked with a check mark. The currently identified integration gaps are included in the known issues list.

	EUDAT	EGI	GEANT	INDIGO-IAM
B2ACCESS			M36	M36
Check-in			M36	
eduTEAMS				M36
INDIGO-IAM	M36		M36	

Known issues

- **Multiple IdP discovery steps:** The EOSC-hub AAI is based on the AARC BPA “community-first” approach, whereby users often need to go through multiple IdP discovery steps: (a) to select their Community AAI and (b) to select their Home Organisation. During this process, users don’t need to re-enter their login credentials as long as their Single Sign-On session is active, however the IdP selection can be frustrating in some cases. The discovery process needs to be simplified by either narrowing down the number of possible IdPs to choose from or by making the actual selection process fully transparent (see also “IdP hinting” protocol proposed in AARC-G049).
- **OAuth2 token validation:** The current EOSC-hub AAI architecture works very well when the user is consuming services directly. However, there are use cases requiring a service agent to be able to act autonomously, on behalf of the user, consuming services and resources. If the services consumed by the agent are behind the same proxy, the current architecture works. For those cases, though, where an agent running on Service A needs to access resources on Service B, which might be connected by a different proxy, then there is no straight-forward solution at the moment. So, currently, services need to trust the same proxy to support those use cases. A solution for dynamically establishing trust in a distributed environment will be provided by the OpenID Connect Federation specification v1.0 (draft). The AARC community is working on “AARC-G052: Recommendations for OpenID Connect/OAuth2 token-based access across different infrastructures” that is investigating an extension of the OAuth2 Token Introspection specification as an interim solution measure until the OIDC Federation Specification is widely available.