AARC Architecture

AARC Architecture WG Area

This is the wiki space of the Working Group in the Architecture Area of the AARC Community and AEGIS. Participation in the working group is open to individuals who are interested in following and contributing to the evolution of the AARC Blueprint Architecture and its supporting Guideline documents. Discussions about the ongoing work of the WG take place in the appint mailing list. The groups holds a biweekly call every other Wednesday at 14:00 CE(ST)

- See latest version of AARC BPA
- Join the appint mailing list

High-level Objectives

- focus on the **integration aspects** of the AAARC Blueprint Architecture
- provide recommendations and guidelines for implementers, service providers and infrastructure operators on implementing **scalable and interoperable AAIs across e-infrastructures and scientific communities**
- work in close collaboration with AEGIS
- work on the **evolution of the blueprint architecture** , with a focus on identity provider / service provider (IdP/SP) proxies, scalable authorisation solutions for multi-service provider environments and other solutions for integrating with R&E federations and cross-sector AAIs

Video Call Calendar

Team Calendars

Active Draft Document

Guidelines

ID	Title	Summary	Links	Status
AARC-G026	Guidelines for expressing community user identifiers	*This document describes how to express community user identifiers such that the values can be transported in an interoperable way across AARC Blueprint Architecture (BPA) compliant Authentication & Authorisation Infrastructures (AAIs).*	Wiki Working doc	FINAL CALL
AARC-G056	AARC profile for expressing community identity attributes	*This document defines a profile for expressing the attributes of a researcher's digital identity. The profile contains a common list of attributes and definitions based on existing standards and best practises in research & education. The attributes include identifiers, profile information, and community attributes such as group membership and role information.*	Google doc	WIP
AARC-G049 v2.0	A specification for IdP hinting	A new version that will supersede AARC-G049 v1.0	Google doc	WIP

Upcoming / Inactive Drafts

Guidelines

ID	Title	Summary	Links	Status
AARC-G025 v2.0	Guidelines for expressing affiliation information	A new version that will supersede AARC-G025 v1.0	Google doc	ON HOLD
AARC-G052	OpenID Connect /OAuth2 token-based access across different infrastructures	*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 AARC BPA works. However, when an agent running on one service needs to access resources on another service which is 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 document specifies an extension to the OAuth2 Token Introspection meant to be a temporary measure until the OIDC Federation Specification is widely available.*	Google doc	ON HOLD
AARC-G053	Specification for expressing user authentication via REFEDS R&S and/or Sirtfi compliant authentication providers		Google doc	CONCEPT
AARC-G054	Specification for expressing authenticating authorities		Google doc	CONCEPT
AARC-I028 (was AARC2-JRA1.2B)	Best practices for integrating OpenID Connect / OAuth2 based end services	*Capture what OIDC-based services need to understand, which schemes to follow in order to benefit from federated identities, that currently are exclusively in the SAML world.* *This will probably include pointers to documents that specify mappings between SAML and OIDC expression of attributes, entitlements or claims.* *OIDC/OAuth2 client registration is covered in AARC-G032*	Wiki doc	ON HOLD
AARC-G038 AARC2-JRA1.4C	Best practises for scalable account (de)provisioning of VO members	*Best practises for scalable account provisioning, management, and deprovisioning, particularly from the perspective of the standard protocols used to manage accounts (such as LDAP, VOOT, SCIM, etc.)*	doc	ON HOLD
AARC-G032 (was AARC2-JRA1.3B)	Guidelines for registering OIDC Relying Parties in AAIs for international research collaboration	*This document describes different ways to accomplish an OpenID Connect client registration, specifically providing guidance for International Research Collaborations that need to implement one of these systems.*	Wiki doc	ON HOLD
AARC-G036 (was AARC2-JRA1.4A)	Roles, responsibilities and security considerations for VOs	DROPPED. Most of the content is now in DJRA1.3; it was proposed to gather the remaining information into a document describing how roles and the requirements on roles be managed (e.g. "there must always be a security contact"); however, we have decided that we will not have enough time to do justice to the topic. Virtual Organisations (VOs) have several roles and responsibilities; some are identified as community responsibilities, and others arise from relations to infrastructures (e.g. security contact, technical contact). Can we minimise the number of places that need this information, in order to improve maintainability and scalability?	Wiki doc	ABANDONED
AARC-G037 (was AARC2-JRA1.4B)	Guidelines for combining group membership and role information in multi-AA environments	*When combining information from several AAs, one needs to consider the different semantics, different levels of assurance, and different purposes of the AAs and their attributes.*	Wiki Doc	ON HOLD

AARC-G030 (AARC2-JRA1.2D)	Requirements and Implementations for Authentication Freshness (was: *Guidelines for step-up authentication via forced reauthentication)*	*This document describes mechanisms for forcing a user to perform an additional login (reauthentication) in order to ensure that the user who is accessing a protected resource is the same person who initially authenticated at the start of the session. Forced reauthentication can therefore provide additional protection for sensitive resources.*	Wiki doc	ABANDONED
AARC2-JRA1.1B	Guidelines for the discovery of authoritative attribute providers across different operational domains			ABANDONED
AARC2-JRA1.1C	Guidelines for handling user registration and user consent for releasing attributes across different operational domains			CONCEPT
AARC2-JRA1.1D	Guidelines for federated access to non-web services across different operational domains			CONCEPT
AARC2-JRA1.3C	Guidelines for AAI interoperability with non-R&E Identity Providers in support of international research collaboration			ABANDONED
AARC2-JRA1.3D	Guidelines for AAI interoperability with eIDAS Identity Providers in support of international research collaboration			CONCEPT
AARC2-JRA1.3E	AAI tools & technologies enabling OIDC for international research collaboration			CONCEPT
AARC2-JRA1.4D	Guidelines for implementing, operating and using VO platforms	it was suggested this incorporate anything from JRA1.4A not included in DJRA1.3 plus guidance on evaluating and selecting a proxy platform. However, as we have too many documents already and not enough time to do them justice, JRA1 have decided to drop this document. However, EOSC Hub is currently (as of March 2019) putting together an evaluation form. It was suggested at the F2F in April 2019 that this document be resurrected?		ABANDONED