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 aarc-architecture mailing list. The group holds a weekly call every other Monday at 14:00 CE(ST)

- See latest version of AARC BPA
- Join aarc-architecture mailing list
- View shared folder with guideline documents

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-G052	OAuth 2.0 Proxied Token Introspection	*This specification extends the OAuth 2.0 Token Introspection (RFC7662) method to allow conveying meta-information about a token from an Authorization Server (AS) to the protected resource even when there is no direct trust relationship between the protected resource and the token issuer. The method defined in this specification, termed "proxied" token introspection, requires access tokens to be presented in JWT format containing the iss claim for identifying the issuer of the token. Proxied token introspection assumes that the AS which is trusted by the protected resource has established a trust relationship with the AS which has issued the token that needs to be validated.*	Google 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	FINAL CALL
AARC-I058	Methods for establishing trust between OAuth 2.0 Authorization Servers	*This document explores different approaches for establishing trust among entities such as OAuth 2.0 Authorization Servers (AS) and Resource Servers (RS) residing in distinct domains. These interactions are facilitated through trusted third parties referred to as Trust Anchors, which are entities issuing authoritative statements about entities that participate in an identity federation.*	Google doc	FINAL CALL

AARC-G073	Guidelines for refreshing tokens between proxies	*This document explores the refresh token flow in a scenario where client applications interact with resource servers through interconnected OpenID Providers (OIDC). Specifically, it focuses on the case where an AARC-compliant Infrastructure Proxy [AARC-G045] acts as an intermediary between the client and a Community AAI. To address challenges related to refresh token handling in this configuration, the document specifies a secure refresh token flow that leverages introspection to ensure the validity of refresh tokens before issuing new access tokens. The document describes the flows for both obtaining and using refresh tokens.*	Google doc	IN PROGRESS
AARC-G080	AARC Blueprint Architecture 2025	*The AARC Blueprint Architecture (BPA) provides a set of building blocks for software architects and technical decision makers who are designing and implementing access management solutions for international research collaborations. This document describes the evolution of the AARC Blueprint Architecture, starting with a summary of the changes since AARC-BPA-2019.*	Google doc (Initial Revision)	IN PROGRESS
AARC-G081	Recommendations for Token Lifetimes	*This document provides an overview over various types of tokens, or more generally, about assertions used to identify and authorise users. We analyse the different properties of tokens and categorise available authorisation patterns to give recommendations about the life times of tokens associated with specific properties and authorisation levels.* The document is between policy and architecture working group	Google doc	IN PROGRESS

Upcoming / Inactive Drafts

Guidelines

ID	Title	Summary	Links	Status
AARC-G058	Establishing trust between OAuth 2.0 Authorization Servers	*Specification for establishing trust among OAuth Proxies (based on AARC-I058)*		ON HOLD
AARC-G079	AARC Community-based Access Entity Category	*This document provides guidelines for using the Community-based Access Entity Category to support the release of attributes to Service Providers that have a proven need to receive a set of community-managed information about their users in order to effectively provide their service to the users.*	Google doc	ON HOLD
AARC-G059	Guidelines for expressing affiliation information	*The goal of this document is to define how affiliation information should be expressed when transported across AARC BPA-compliant AAIs. Two different types of affiliation have been identified, namely Affiliation within the Home Organisation, such as a university, research institution or private company; and Affiliation within the Community, such as cross-organisation collaborations. Both affiliation types should be communicated to the service providers that rely on affiliation information in order to control access to resources.* Will supersede AARC-G025	Google doc	ON HOLD Waiting for feedback from voPerson schema (see voPerson issue#40)
AARC-G060	A framework for IdP hinting		Google doc	ON HOLD
AARC-G064	A specification for hinting which IdPs to show in discovery		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-JRA 1.2 B)	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-JRA 1.4C	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-JRA 1.3 B)	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-JRA 1.4 A)	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-JRA 1.4 B)	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-JRA 1.2 D)	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-JRA 1.1B	Guidelines for the discovery of authoritative attribute providers across different operational domains			ABANDONED
AARC2-JRA 1.1C	Guidelines for handling user registration and user consent for releasing attributes across different operational domains			CONCEPT
AARC2-JRA 1.1D	Guidelines for federated access to non-web services across different operational domains			CONCEPT
AARC2-JRA 1.3C	Guidelines for AAI interoperability with non-R&E Identity Providers in support of international research collaboration			ABANDONED
AARC2-JRA 1.3D	Guidelines for AAI interoperability with e IDAS Identity Providers in support of international research collaboration			CONCEPT
AARC2-JRA 1.3E	AAI tools & technologies enabling OIDC for int ernational 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