AARC Architecture

AARC Blueprint Architecture (BPA)

The purpose of the AARC Blueprint Architecture (BPA) is to provide set of interoperable architectural building blocks for software architects and technical decision makers, who are designing and implementing access management solutions for international research collaborations.

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

High-level Objectives

- focus on the **integration aspects** of the 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 the policy, pilots, and the training and outreach activities of AARC2
- 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

Documents

Final

Guidelines

ID	Title	Summary	Links	Status
AARC-G002 Supersedes: AARC-G001 (June 13, 2017) Other identifiers: AARC-JRA1.4A)	Guidelines on expressing group membership and role information	*This document standardises the way group membership information is expressed. It defines a URN-based identification scheme that supports: indicating the entity that is authoritative for each piece of group membership information; expressing VO membership and role information; representing group hierarchies.*	AARC-JRA1.4A (201710) [PDF] Older versions AARC-JRA1.4A (1.0) [PDF]	FINAL AEGIS
AARC-G021	Guideline on the exchange of specific assurance information between Infrastructures	*Infrastructures and generic e-Infrastructures compose an 'effective' assurance profile derived from several sources, yet it is desirable to exchange the resulting assurance assertion obtained between Infrastructures so that it need not be re-computed by a recipient Infrastructure or Infrastructure service provider. This document describes the assurance profiles recommended to be used by the Infrastructure AAI Proxies between infrastructures.*	Wiki doc Website	FINAL AEGIS
AARC-G027	Specification for expressing resource capabilities	*This document provides a specification for expressing resource-specific capabilities using entitlements. A capability defines the resource or child-resource a user is allowed to access, optionally specifying certain actions the user is entitled to perform. Capabilities can be used to convey - in a compact form - authorisation information.*	PDF	FINAL AEGIS

AARC-G031	Guidelines for the evaluation and combination of the assurance of external identities	*The Research Infrastructures (from now on just Infrastructures) that follow the AARC Blueprint Architecture [AARC-BPA] set up their own AAI to grant access to their services. The AAI is typically based on a central IdP-SP proxy that act as a gateway for the Infrastructure services and resources. In order to assign an identity to the users of the research collaboration or the community they serve, Infrastructures rely on external Identity Providers and employ identity linking strategies.* *The Infrastructures also define one or more assurance profiles, or a combination of assurance components, tailored to a specific risk assessment [AARC-G021].* *In order to assign an assurance profile to a user, the Infrastructure shall evaluate the assurance components of the linked identity, or identities, used to register to the Infrastructure's AAI or used during authentication at the infrastructure proxy. These guidelines provide a method to combine assurance information and to compensate for the lack of it.*	Wiki pdf working doc	FINAL AEGIS
AARC-G049	A specification for IdP hinting	*This document defines a generic browser-based protocol for conveying - to services - hints about the IdPs or IdP-SP-proxies that should be used for authenticating the principal. This protocol, colloquially referred to as Identity Provider (IdP) hinting, can greatly simplify the discovery process for the end-user, by either narrowing down the number of possible/IdPs to choose from or by making the actual selection process fully transparent.*	doc pdf	FINAL AEGIS

Informational documents

ID	Title	Summary	Links	Status
AARC-G003 Other idenftifiers: AARC-JRA1.4B	Guidelines on attribute aggregation	*This document discusses attribute aggregation scenarios applied in international research collaborations. Attribute aggregation can take place at proxy, SP or TTS services, in-line with the Blueprint Architecture.*	PDF	FINAL
AARC-G004 Other idenftifiers: AARC-JRA1.4C	Guidelines on token translation services	*This document discusses attribute aggregation scenarios applied in international research collaborations. Attribute aggregation can take place at proxy, SP or TTS services, in-line with the Blueprint Architecture.*	PDF	FINAL
AARC-G005 Other idenftifiers: AARC-JRA1.4D	Guidelines on credential delegation	*In distributed environments it is often necessary for a remote service to access other services on behalf of a user, or for a software agent to act on behalf of the user. This guidelines consider delegation of credentials based on signed assertions, session tickets, "tokens" of various types, and proxy certificates.*	PDF	FINAL
AARC-G006 Other idenftifiers: AARC-JRA1.4E	Best practices for managing authorisation	*This document provides best practices for a range of models for Authorisation policy enforcement that apply at service providers end-points, even if not always solely on the resource SP alone, e.g. in the case of an IdP/SP proxy.*	PDF	FINAL
AARC-G007 Other idenftifiers: AARC-JRA1.4F	Guidelines on non-browser access	*Overview of non-web access mechanisms in common use for both interactive (command-line) access and for API based access. Mechanisms based on ssh, PKIX/X.509, API keys and OIDC are reviewed and placed in context.*	PDF	FINAL

AARC-G008 Other idenftifiers: AARC-JRA1.4G	Guidelines for implementing SAML authentication proxies for social media identity providers	*This guidelines provides recommendations and best practices for implementing authentication proxies that can connect social media identity providers with federated SAML 2.0 service providers.*	PDF	FINAL
AARC-G009 Other idenftifiers: AARC-JRA1.4H	Account linking and LoA elevation use cases and common practices for international research collaboration	*In Identity linking (account linking) the user's infrastructure identity is associated with external identities, i.e. created and assigned outside of the administrative boundaries of the infrastructure, such as institutional IdPs or social media IdPs. This linking may be either implicit or explicit to the user. The document reviews use cases and considers consistency of representation, accounting, and traceability of linked identities.*	PDF	FINAL
AARC-G010 Other idenftifiers: AARC-JRA1.4I	Best practices and recommendations for attribute translation from federated authentication to X.509 credentials	*This guideline suggests the common way to encode authentication and authorization in X.509 credentials, to increase the re-usability and interoperability of X.509 credentials generated by token translation services.*	PDF	FINAL
AARC-G029	Guidelines on stepping up the authentication component in AAIs implementing the AARC BPA	*A number of research community use cases require users to verify their identity by using more than one type of credentials, for instance using password authentication, together with some physical object such as a phone or usb stick that generates tokens /pins, etc. At the same time, there are services that may require an already logged in user to re-authenticate using a stronger authentication mechanism when accessing sensitive resources. Authentication step-up is then needed to improve the original authentication strength of those users. This document provides guidelines on step-up of the authentication component. It covers requirements and implementation recommendations, describes a proposed authentication step-up model, and outlines related work and documentation.*	Wiki Website	FINAL
AARC-I047 (was AARC2-JRA1.2A)	Implementing scalable and consistent authorisation across multi-SP environments	*The purpose of this document is to provide information to infrastructures for efficiently implementing access restrictions that are required by the individual communities and e-Infrastructures. The suggestions are given within the setting of the AARC BPA. In this scenario, user communities make use of an SP-IdP-Proxy (including User Attribute services) in order to manage access to resources (end services). The suggestions given address two different topics. One is about providing an interoperable schema to use for expressing authorisation information. This is an extension of the recommendations provided in AARC-G002 - Expressing group membership and role information and AARC-G027 - Specification for expressing resource capabilities. The other topic concerns the organisational architecture for conveying authorisation information. All information within this latter area are derived from the more detailed Deliverable DJRA1.2 on authorisation models.*	Wiki pdf	FINAL

Deliverables

ID	Title	Summary	Links
AARC2-DJRA1.2	Authorisation Models for SPs	*This deliverable describes possible authorisation models for SAML-SPs and OIDC-RPs in a proxied environment. We provide an overview about available and upcoming technologies currently in use or development for community and research infrastructures.*	pdf
AARC2-DJRA1.1	Use-Cases for Interoperable Cross-Infrastructure AAI	*The researchers' need to access online services and resources offered by different research and e-infrastructures has increased over the last years. Through federated access, researchersshould be able to seamlessly and securely access resources across these infrastructures using their existing credentialsfrom their home organisations. AAI interoperability a key requirement to support this. The AARC blueprint architecture has been designed to address this need, aiming to improve the user experience when accessing and sharing resources provided by different infrastructures. To this end, this document analyses research community use cases that require access to services and resources across infrastructures. The research community specific use cases have been mapped to a set of generic use cases of cross-infrastructure AAI flows. These flows will serve as input for further refining and complementing where needed the AAI interoperability aspects of the AARC Blueprint Architecture.*	pdf
AARC2-DJRA1.3	VO Platforms for Research Collaborations	*In order to scale the users' use of research infrastructures, cyber- and e-infrastructures, it makes sense to introduce a "virtual organisation" (VO) that can unify users with a shared purpose or research activity. This document investigates this use of the VO and makes recommendations for the platform which maintains this VO information, both for the VO's own use but particularly for the VO's members' use of the infrastructure.*	pdf

AARC2-DJRA1.4	Evolution of the AARC Blueprint Architecture	*This document describes the evolution of the AARC Blueprint Architecture, starting with a summary of the changes since AARC-BPA-2017. It also describes the community-first approach which enables researchers to use their community identity for accessing services offered by different infrastructures.*	pdf

Active Drafts

Guidelines

ID	Title	Summary	Links	Status
AARC-G025 (AARC2-JRA1.1E)	Guidelines for expressing affiliation	*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.*	Wiki Working doc pdf	FINAL CALL
AARC-G045	Evolution of the AARC Blueprint Architecture and best practices to support cross-infrastructure AAI interoperability	*This document provides the first iteration of the AARC Blueprint Architecture (AARC-BPA-2018) including the "community-first" approach.*	Working doc	FINAL CALL
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

Upcoming / Inactive Drafts

Guidelines

ID	Title	Summary	Links	Status
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 AARC 2-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 (AARC 2-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
AARC 2-JRA1.1B	Guidelines for the discovery of authoritative attribute providers across different operational domains			ABANDONED
AARC 2-JRA1.1C	Guidelines for handling user registration and user consent for releasing attributes across different operational domains			CONCEPT
AARC 2-JRA1.1D	Guidelines for federated access to non-web services across different operational domains			CONCEPT
AARC 2-JRA1.3C	Guidelines for AAI interoperability with non-R&E Identity Providers in support of international research collaboration			ABANDONED
AARC 2-JRA1.3D	Guidelines for AAI interoperability with eIDAS Identity Providers in support of international research collaboration			CONCEPT
AARC 2-JRA1.3E	AAI tools & technologies enabling OIDC for international research collaboration			CONCEPT
AARC 2-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