AARC Handbook

AARC

The AARC-TREE project is co-funded by the European Union under the HORIZON-INFRA-2023-DEV-01 call

Publication Date 28 Feb 2026

Editors: H. Short (CERN), S. Chambers (DARIAH)

Version: 1.0

Table of Contents

1 Introduction

The Authentication and Authorisation for Research and Collaboration (AARC) Handbook is intended as an introductory guide to implementing federated identity management for research collaborations, based on the AARC Blueprint Architecture (AARC BPA).

This guide provides an introduction to Authentication and Authorisation Infrastructure (AAI). A glossary of key terms and their definitions is provided, as well as a list of Frequently Asked Questions (FAQs).

The compendium covers a number of different topics, including what is the AARC Blueprint and why has it been developed, how to implement an AAI service outlining several implementation scenarios. An overview of the landscape of existing AAI solutions is provided including commonly used software and services as well as hosted services.

Specific topics such as technical requirements, security, data protection and policy related issues are covered, including how to build the necessary bridges between legal, policy and technology.

2 Audiences

This guide is written with several audiences in mind. Wherever relevant, information is presented in multiple ways to best suit these audiences.

- Research Community Management **AUDIENCE: RESEARCH COMMUNITY MANAGEMENT**
- AAI Implementors and Operators **AUDIENCE: AAI IMPLEMENTORS AND OPERATORS**
- Funding Agencies **AUDIENCE: FUNDING AGENCIES**
- All **AUDIENCE: ALL**

Please note: the AARC Handbook was originally known as the AARC Compendium but has renamed following feedback from the AARC-Community.

3 What is an AAI and why is it relevant for Research Collaborations?

AUDIENCE: ALL

AAI stands for Authentication and Authorisation Infrastructure. It is a set of software systems that help users to login to services easily. Like any good infrastructure, you should barely notice an AAI system, until it is not available.

Examples of common AAI use cases for research communities include:

- **Accessing research services and repositories**: Logging in to web platforms such as Zenodo or the Social Sciences and Humanities (SSH) Open Marketplace to add or edit records.
- **Network connectivity**: Connecting to Wi-Fi services like eduroam across participating institutions.
- **High-performance and cloud computing**: Logging into computing systems (e.g., HPC clusters) to run workflows via the command line.
- **Secure handling of sensitive datasets**: Granting controlled access to protected computing platforms and data (particularly important for health data or copyright-protected datasets), whilst ensuring compliance with security, legal and ethical requirements.

It is not enough for an AAI to simply grant access - it must enable researchers to securely access trusted services, comply with required policies and experience minimal friction throughout the process. Without an AAI to connect services and researchers, each service may require its own separate account and authorisation process, frustrating users and reducing security and efficiency as identity management tasks are duplicated.

Research collaborations are typically ***federated***; the researchers' identities are managed by their home organisations (e.g. universities) but their authorisation in the research context is managed within the collaboration itself. The systems they use may be hosted by multiple institutes but should share a common access control mechanism. There are even scenarios where AAIs themselves must be federated, i.e. each AAI in a federation trusts the users and attributes released by the others. As a result of these requirements, research AAIs must support many workflows not commonly found in commercial systems that primarily serve single organisations. Over the years, the AARC community has developed best practices to support such scenarios.

Ideally, an AAI is one of the first systems established in a new research community, allowing other services to plug in directly and benefit from unified identity and access management from the outset. If your community missed that opportunity, the second-best time to adopt an AAI is now. **Read on to learn from communities who have already navigated the challenges so you can avoid their mistakes and get your AAI running smoothly.**

AUDIENCE: AAI IMPLEMENTORS AND OPERATORS

Certain research requirements are not supported by common commercial software (i.e. enterprise Identity and Access Management (IAM) systems or Single Sign-Ons) that you would use in a single-domain organisation. For example: globally federated access; verified membership management; token translation and compatibility with other research collaborations.

4 What is the AARC Blueprint Architecture?

AUDIENCE: ALL

The **AARC Blueprint Architecture** (BPA) is a reference framework designed to address the complex identity and access management challenges faced by international research collaborations. Developed through the AARC (Authentication and Authorisation for Research and Collaboration) project series, the BPA provides a set of interoperable architectural building blocks that enable access to research resources across different organisations and infrastructures.

The AARC BPA addresses these challenges by introducing a "community-first" approach to identity and access management. Rather than forcing researchers to navigate multiple institutional boundaries, the architecture enables research collaborations to use federated identities while managing their own access policies and rights. This approach encourages interoperability with institutional identity providers and infrastructure services.

The latest version of the AARC BPA (2025) included the following layers:

Authentication

- Manages authentication via trusted Identity Providers (IdPs) using e.g. SAML (Security Assertion Markup Language) & OIDC (OpenID Connect)
- May include proxies

Attribute Services

- Manages user attributes

Access Protocol Translation

- Includes Service Provider (SP)-IdP-Proxy and Discovery Service
- Manages notice presentation for privacy policies, Acceptable Use Policies

Authorisation

- Controls access to Services
- Centralises complex authorisation decisions
- Reduces complexity for services

Services

- Protected services (e.g. wikis, APIs, compute resources)
- Supports web-based and non-web-based resources
- May include proxies for cross-infrastructure access

For further details about the AARC BPA, see: https://aarc-community.org/architecture/

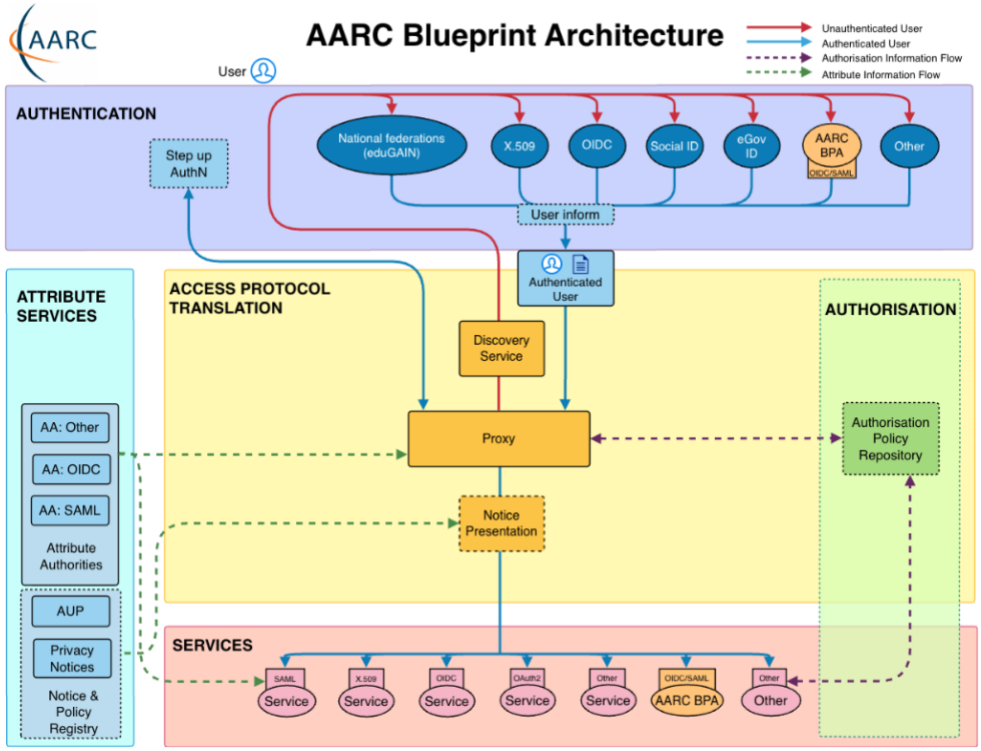


Figure 1 AARC Blueprint Architecture, 2025

5 Benefits and Value Proposition

AUDIENCE: RESEARCH COMMUNITY MANAGEMENT

5.1 Why should Research Communities invest in AARC compliance?

The AARC Blueprint Architecture (BPA) provides a proven, interoperable framework for Authentication and Authorisation Infrastructure (AAI) that supports scalable, secure and sustainable access to research services.

- **For Researchers:**
  Simplified access through single institutional credentials, eliminating multiple accounts and reducing authentication friction so that researchers can focus on research.
- **For Research Collaborations:**
  Managed membership and access policies independent of institutional boundaries, supporting both small projects and large international infrastructures.
- **For Service Providers:**
  Reduced integration effort via a proxy-based model that hides federation complexity and enables advanced access control without bespoke authorisation logic.
- **For Infrastructure Operators:**
  A scalable, multi-tenant AAI model that supports multiple communities efficiently while sharing operational costs and maintaining appropriate isolation.
- **For Security and Risk Management:**
  Centralised policy enforcement, logging and incident response; support for assurance frameworks; cryptographically secured trust relationships.
- **For Funders:**
  Avoids duplicated effort by scarce identity experts, enables scalable policy and technology standards, and supports European and global collaboration.
- **For the Research Ecosystem:**
  Enables true interoperability across research infrastructures, breaking down silos and supporting cross-infrastructure access. The architecture is sufficiently flexible to integrate emerging identity technologies such as European Digital Identity Wallets and OpenID Federation.

Overall, the AARC BPA is a mature, widely-adopted solution that underpins sustainable, interoperable identity management for modern, international research collaboration.

Recommendation

Research Collaborations should **prioritise establishing an AARC Compliant AAI as an early cornerstone in the development of their infrastructure**. As the pressure for researchers to engage with research infrastructures increases, it will be tempting to adopt sub-optimal AAI mechanisms that will ultimately impact research productivity. Early investment in a common, AARC-compliant AAI significantly reduces long-term costs, operational complexity and disruption, compared to retro-fitting identity solutions once communities are already established.

AUDIENCE: FUNDING AGENCIES

5.2 Why should Funding Agencies support common AAI solutions?

An Authentication and Authorisation Infrastructure (AAI) manages digital identities, authenticates users, and controls access to protected resources. However, implementing and operating an AAI goes far beyond technical components.

From an organisational perspective, establishing an AAI requires substantial coordination across multiple stakeholders. Institutions must align their identity management policies, agree on common attribute schemas, and establish trust relationships with partner organisations. This process often involves lengthy negotiations between legal, privacy and technical teams to ensure compliance with various regulatory frameworks whilst maintaining operational flexibility.

The organisational overhead of AAI management includes ongoing responsibilities for user lifecycle management, policy enforcement, incident response and compliance monitoring. Organisations must establish clear governance structures to manage identity federation relationships, handle disputes, and adapt to changing community and legislative requirements. The complexity increases significantly in international collaborations where different cultural norms, legal frameworks, privacy regulations and institutional policies must be negotiated.

Furthermore, AAIs require ongoing investment in staff training, system maintenance and security monitoring. Organisations must maintain expertise in identity federation protocols, security best practices and regulatory compliance, whilst managing the operational burden of supporting diverse user communities with varying technical capabilities and access requirements.

The AARC Community recommends continued and strengthened support for shared AAI solutions (hosted services or open-source software) because they deliver system-wide benefits:

- **More research, less overhead:**
  Seamless AAI reduces time spent managing accounts and access.
- **Improved security and accountability:**
  Centralised access control and logging simplify incident detection and response.
- **Efficiency and reuse:**
  Shared solutions prevent duplication and accelerate project set-up.
- **Better use of expertise:**
  Service providers focus on research services, while AAI specialists improve shared identity infrastructure. This is especially critical for cross-domain resource sharing.
- **Policy agility:**
  Common AAIs provide a central point for enforcing and communicating evolving funding and compliance policies.

- **Lower costs and sustainability:**
  Shared investment reduces duplication and ensures long-term viability.
- **Alignment with public values:**
  Community-governed AAIs reduce reliance on commercial providers and preserve academic control and resilience.
- **Stronger global collaboration:**
  Trusted, cross-border access mechanisms amplify the impact of funded infrastructures across the global research ecosystem.

Recommendation

Funding agencies should not only **fund shared AAI solutions and hosted services** but also **require early involvement of AAI operators in grant proposals**, ensuring best practices are followed and avoiding delays or sub-optimal implementations due to late or unfunded AAI integration.

6 AARC Guidelines and Compliance

AUDIENCE: RESEARCH COMMUNITY MANAGEMENT

AUDIENCE: AAI IMPLEMENTORS AND OPERATORS

6.1 AEGIS

The AARC Engagement Group for Infrastructures (AEGIS) is the approval body that reviews and endorses AARC guidelines, giving them official status within the research infrastructure community. It serves as the governance mechanism that ensures AARC specifications meet the practical needs of infrastructure operators and maintains quality standards for the guidelines that become part of the AARC framework. AEGIS has adopted several AARC guidelines (see full list here), which are mandatory for interoperable infrastructures. Support for AARC guidelines that are not required by AEGIS is optional, but their adoption will improve interoperability.

6.2 When is an AAI AARC Compliant?

An AAI becomes AARC compliant when it implements the architectural principles and technical specifications defined in the AARC Blueprint Architecture (BPA) and adopts the AARC Guidelines that have been approved by AEGIS. AARC compliance is characterised by several key features:

Layered Architecture: AARC-compliant AAIs implement a layered architectural model comprising of: User Identity, Community Attribute Services, Access Protocol Translation, Authorisation and Service layers. In most implementations, some of these layers blend together rather than being discrete. The separation of responsibility boundaries, however, supports a clearer description and implementation of the architecture.

Proxy-Based Design: Central to AARC compliance is the implementation of Service Provider-Identity Provider Proxies (SP-IdP-Proxies) that serve as intermediary services between identity providers and service providers. These proxies handle protocol translation, attribute aggregation and policy enforcement, whilst presenting a unified interface to both users and services.

Community Identity Support: AARC-compliant systems must support community identities - user identities enriched with community-specific attributes such as group memberships and project roles. This enables fine-grained access control based on community participation rather than solely institutional affiliation.

Interoperability Standards: Compliance requires adherence to established standards for several topics crucial for interoperability (e.g. attribute expression, assurance frameworks, federation protocols, etc.).

Trust Framework Integration: AARC-compliant AAIs must integrate with established trust frameworks and support mechanisms for expressing and evaluating identity assurance levels, enabling risk-appropriate access decisions.

To be considered AARC Compliant, AAIs must support the following AEGIS endorsed guidelines. Please see the sections on Technical Requirements and Policy Requirements for further information.

AEGIS Endorsed Guidelines for AARC Compliance			Guideline
Proxy-Based Design	✅	AARC Blueprint Architecture 2019, My AAI includes a SP-IdP-Proxy that presents a unified interface to users and services.	AARC-G045
Community Identity Support	✅	Expressing group and role information	AARC-G069 (supersedes AARC-G002)
	✅	Inferring and constructing voPersonExternalAffiliation	AARC-G057
	✅	Guidelines for expressing affiliation information	AARC-G025
	✅	Guidelines for expressing community user identifiers	AARC-G026
Interoperability Standards	✅	Specification for expressing resource capabilities	AARC-G027
	✅	Exchange of specific assurance information between Infrastructure	AARC-G021
	✅	A specification for IdP hinting	AARC-G061 (supersedes AARC-G049)
	✅	Specification for hinting an IdP which discovery service to use	AARC-G062
	✅	A specification for providing information about an end service	AARC-G063
	✅	*(Under approval) Proxied Token Introspection*	AARC-G052
Trust Framework Integration	✅	Guidelines for Secure Operation of Attribute Authorities	AARC-G071
	✅	Guidelines for evaluating the combined assurance of linked identities	AARC-G031
	✅	*(Under approval) Recommendations for Token Lifetimes*	AARC-G081
	✅	*(Under approval) Trust framework for proxies and Snctfi research services*	AARC-I082

6.3 Policy Guidelines

AUDIENCE: RESEARCH COMMUNITY MANAGEMENT

Many of your questions will not be solved by defining your technical stack - arguably some of the most difficult issues relate to policy. Regardless of what software you choose, those responsible for your research community will need to be able to show that the following considerations, among others, have been addressed:

- How are members identified, verified and removed from the collaboration?
- Are all services within the AAI implementing security patches?
- What will happen when there is a security incident?
- Who has access to user data?

AARC's Policy guidelines are a compilation of best practices and recommendations that help research and e-Infrastructures to implement scalable and cost-effective policy and operational frameworks for their AARC BPA compliant AAIs. These documents aim to ensure three core capabilities for Research Infrastructures: Operational Security, Trustworthy Membership Management and Data Protection.

The set of necessary policies has been reviewed in AARC-I082 following several years of experience of running the AARC BPA in practice. This document addresses trust across the entire chain of AAI components and aims to remove difficulties in tracing back any information to its original source. Establishing trust becomes more challenging when it is not possible to see which link in the 'chain' asserts which information and how trustworthy that link is.

6.3.1 Practical steps for adopting AARC's policy recommendations

Please visit the Policy Development Kit.

Recommendation

We strongly suggest leveraging the Policy Development Kit for the following reasons:

- **Save time** - the templates have been well-researched and adopted in production AAIs by many research communities
- **Speak for the AAI** - all components should be bound by a common set of policies to allow you to make accurate statements on security and data protection for the entire infrastructure
- **Enable access for researchers** - some research communities require evidence of the adoption of policies by researchers' Identity Providers in order for them to be granted access
- **Limit interoperability inconveniences to end users** - by adopting common policies, such as the Acceptable Use Policy, together we can decrease the number of clicks required by end users to access services

6.4 Technical Guidelines

AUDIENCE: AAI IMPLEMENTORS AND OPERATORS

Building an AARC-compliant AAI is achieved through the principles of the AARC Blueprint Architecture (BPA) and by following the guidelines formally approved by AEGIS. These guidelines provide the reference set for achieving interoperability across infrastructures. AEGIS approval ensures that specifications have been reviewed for operational feasibility and community consensus, making them key enablers of interoperability for research collaboration. The following requirements are presented thematically, reflecting the main technical functions needed to support interoperability.

- Harmonised Identity Representation
- Authorisation and Access Control
- Interoperability Architecture
- Discovery and User Experience

6.4.1 Harmonised Identity Representation

Guidelines in this group define how identity attributes are expressed in a consistent way. By harmonising subject identifiers, affiliation information, group membership, and assurance, they ensure that users can be reliably recognised and their attributes correctly interpreted by different infrastructures.

AARC-G026 – Community User Identifiers

Defines globally unique, persistent, and opaque identifiers for users. Expressed as:

- OIDC claim: `voperson_id claim` (in ID token and UserInfo endpoint)
- SAML attribute: `voPersonID`
- Identifiers must not be reassigned and should be permanent where possible

AARC-G025 – Affiliation Information

Specifies how to express the user's affiliation within their `Home Organisation`, such as a university or research institution.

- Affiliation is typically based on the `eduPersonScopedAffiliation attribute` released by the user's Home Organisation
- Expressed as:
  - `OIDC claim: voperson_external_affiliation`
  - `SAML attribute: voPersonExternalAffiliation`
- Includes freshness requirements expressed through `eduPersonAssurance`

AARC-G057 – Inferring Origin Affiliation

Provides rules for constructing `voPersonExternalAffiliation` when not directly asserted by the user's `Home Organisation`.

- Inference may use `eduPersonAffiliation`, metadata, or community registries
- If no reliable inference can be made, the affiliation value must be set to unknown@<issuer>. This guarantees that the `voPersonExternalAffiliation` SAML attribute or `voperson_external_affiliation` OIDC claim is always present for downstream services.

AARC-G069 – Group Membership and Roles

Defines a URN-based syntax for expressing groups, subgroups, and roles.

- Example: `urn:example.org:group:team:subteam:role=member`
- Expressed as:
  - OIDC claim: entitlements (RFC 9068)
  - SAML attribute: `eduPersonEntitlement`
- Supports implied membership (subgroup ⇒ parent group)
- Provides encoding and normalisation rules to avoid clashes across collaborations

AARC-G021 – Assurance

Specifies how Proxies express identity assurance information.

- Uses REFEDS RAF profiles (Cappuccino, Espresso) and supplementary IGTF profiles (BIRCH, DOGWOOD).
- Introduces the AARC-Assam profile for identities partially based on social IdPs, with compensatory proxy controls.

Assurance expressed as:

- OIDC claim: `eduperson_assurance`
- SAML attribute: `eduPersonAssurance`

AARC-G031 – Combining Assurance

Provides methods for proxies to evaluate assurance when linking identities.

- Uses REFEDS Assurance (RAF) components: Identifier uniqueness (ID), Identity Proofing (IAP), Attribute Freshness (ATP)
- Defines compensatory controls (e.g. email verification, Research & Scholarship entity category) when values are missing.

AARC-G056 – Attribute Profile *(in development)*

Defines a harmonised AARC attribute profile consolidating subject identifiers, names, email, affiliation, assurance, groups memberships and roles, and resource capabilities. Once approved, it will provide a single reference profile for attribute release across AARC-compliant infrastructures.

6.4.2 Authorisation and Access Control

Authorisation can rely on identity attributes such as group membership and roles, affiliations, and assurance (described in the identity representation guidelines). Alternatively, it can be based on community- or service-defined capabilities. For token-based workflows, this information may be included directly in the token (e.g. as claims or scopes) or retrieved indirectly via token introspection. The guidelines in this group provide mechanisms to represent resource capabilities and to validate tokens in multi-proxy environments.

AARC-G027 – Resource Capabilities

Introduces a URN syntax for representing what actions a user can perform on a resource.

- Format:
  `<NAMESPACE>:res:<RESOURCE>[:act:<ACTION>[,<ACTION>]...]#<AUTHORITY>`
- Supports hierarchical resource structures and explicit action scopes, enabling fine-grained, interoperable expression of access rights.

AARC-G052 – Proxied Token Introspection *(under final consultation)*

Extends OAuth 2.0 Token Introspection (RFC 7662) to multi-proxy environments.

- Allows an OAuth 2.0 Authorization Server (AS) to proxy introspection requests to the token's authoritative issuer
- Ensures tokens can be validated securely, even when multiple proxies and ASes are involved

6.4.3 Interoperability Architecture

At the architectural core of AARC is the SP-IdP-Proxy model, which reduces integration complexity and supports collaboration-driven identity management.

AARC-G045 – Blueprint Architecture (2019)

Introduces two key proxy roles, namely, the Community AAI and the Infrastructure Proxy.

- The Community AAI, operated by or on behalf of a research community, which manages user enrolment, group membership, roles, and other community-managed attributes
- The Infrastructure Proxy, operated at the infrastructure level, which acts as the single integration point for services. It connects to different Community AAIs and enforces infrastructure policies

- Layered model allows communities to manage their users and authorisation independently, while infrastructures provide the trusted integration point for services
- Services connect only to the Infrastructure Proxy, reducing integration complexity for service providers
- Together, Community AAIs and the Infrastructure Proxy provide a scalable and interoperable foundation for connecting communities, infrastructures, and services

AARC-G080 – Blueprint Architecture 2025 *(in development)*

Updates the BPA to reflect current practices and introduces a capability-based view

structured around four areas:

- Identity Management – covers authentication, identity lifecycle, and integration with external IdPs
- Collaboration Management – enables management of groups, roles, and collaboration-driven authorisation
- Infrastructure Integration – enriches identities with infrastructure-specific attributes (e.g. resource capabilities, infrastructure roles)
- Site-local Integration – connects federated identities to local services and enforcing site-specific policies

AARC-G081 – Token Lifetime Recommendations *(under final consultation)*

Provides recommendations for operational lifetimes of access tokens and refresh tokens. Consistent practices are essential for reducing the risk of misuse while supporting cross-infrastructure interoperability.

- Access tokens verified offline (non-revocable):
- Default: 1 hour – typically long enough for login and use of a protected resource.
- Max: 6 hours – in line with incident response times.
- Access tokens verified online (revocable):
- Default: 1 hour – consistent with SAML session lifetimes.
- Max: 25 hours – allows for running short jobs and next-day result checks.
- Refresh tokens:
- Default: 30 days – chosen as roughly the geometric mean between a day and a year, balancing usability and security
- Max: 400 days – ensures periodic proof of user involvement.

AARC-G100 – Establishing Trust with OpenID Federation *(in development)*

Defines how AARC-compliant AAI services –such as Infrastructure Proxies and Community AAIs– establish trust using the OpenID Federation 1.0 specification.

- Relies on Trust Authorities (Trust Anchors and Intermediates) to provide authoritative statements about federation participants.
- Defines two trust models:
- G100.1 Basic Trust Model – based on registration of proxies with Trust Authorities and validation of trust chains.
- G100.2 Fine-grained Trust Model – adds use of Trust Marks and metadata policies to indicate compliance with frameworks such as REFEDS Assurance, Sirtfi, or Data Protection Code of Conduct
- Enables dynamic trust establishment without bilateral agreements, supporting both explicit and automatic client registration.
- Complements guidelines such as AARC-G052 (Proxied Token Introspection) by enabling secure trust paths between proxies in a scalable way.

6.4.4 Discovery and User Experience

These guidelines improve the usability of federated login by helping users find their Identity Provider and understand which services are available, reducing login friction and confusion, and supporting smoother end-user journeys. Additionally, the accessibility of federated logins needs to be considered in line, for example, with the latest W3C Accessibility Guidelines (WCAG).

AARC-G061 – Identity Provider Hinting

Defines the aarc_idp_hint parameter, allowing services or proxies to guide users to the correct authenticating IdP or upstream proxy.

- Supports nested hints for complex routing

AARC-G062 – Discovery Service Selection

Defines the `aarc_ds_hint` parameter for suggesting which Discovery Service to use.

- Enables community- or infrastructure-specific discovery experiences

AARC-G063 – End Service Information

Introduces the `aarc_service_hint` parameter to signal to a Discovery Service which end-service the user is accessing.

- Allows Discovery Services to present context-specific IdPs (e.g. filtering based on assurance requirements)
- Improves clarity in multi-proxy login flows

7 5. How to implement an AARC Compliant AAI

AUDIENCE: AAI IMPLEMENTORS AND OPERATORS

AUDIENCE: RESEARCH COMMUNITY MANAGEMENT

Implementing an Authentication and Authorisation Infrastructure (AAI) that is compliant with the AARC Blueprint Architecture (BPA) requires navigating a range of technical, policy, and organisational decisions. This section provides practical guidance for prospective implementers - whether you are a research community, infrastructure operator, or service provider - based on maturity level, available resources, and interoperability goals.

7.1 Step 1: Define Your Research Community's Requirements

Before choosing an architecture or software stack, clarify:

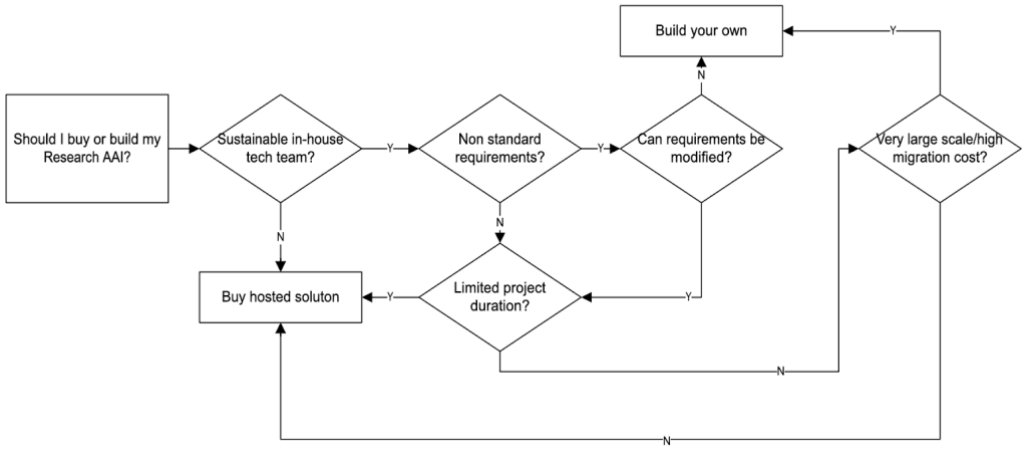
- **User Base**: Who are your users? Are they affiliated with institutions in eduGAIN, external (e.g. guest, citizen science), or a mix?
- **Access Requirements**: Does the sensitivity of your research require additional access approval mechanisms? Do you need fine-grained access control, or is basic authentication sufficient?
- **Scale:** How many services do you plan to connect to your AAI? Which protocols do they require? What is a realistic estimate of effort required to migrate all users and services from one AAI to another in case of a crisis?
- **Existing Infrastructure**: Do you have an identity provider (IdP) or group management service already?
- **Sustainability**: Can you commit operational resources, or do you need a hosted service? For how long will your AAI be required? Will your available support level be able to increase with growth of participating institutes or services?
- **Environment specific requirements**: Do you need any physical connectivity to dedicated networks? Are IT interventions restricted to fixed time windows? Do you have any other unusual requirements that may not be supported by off the shelf solutions?
- **Governance:** Who will take responsibility for policy decisions regarding your AAI? Do they have enough authority over your research community to make high level statements and decisions, e.g. for data protection, security policy requirement etc?

7.2 Step 2: Define your Policies

Further guidelines are provided in the policy section. For practical steps for adopting AARC's policy recommendations, please visit the Policy Development Kit.

7.3 Step 3: Choose an Implementation Path

The following flow chart may help you frame the necessary questions to understand whether to use a hosted AAI platform or run your own.



7.3.1 Option 1: Complete AAI Platform, hosted by a third party supplier

Wherever possible, the AARC community recommends using a hosted platform to benefit from the points mentioned previously.

- **Use Cases**: University collaborations in fixed duration projects, temporary research endeavors, research collaborations with limited technical staff. Please see later sections for examples of hosted solutions.
- **Pros**: Faster deployment and configuration, AARC compliance out of the box, integration with eduGAIN
- **Cons**: Less flexibility for local policy enforcement or custom attribute handling

Visit the section on existing hosted services.

7.3.2 Option 2: Self-Hosted Proxy Architecture

Ideal for communities needing more control over attributes, group management, or federation strategy. May be more suitable for communities that already operate an internal AAI and are seeking to interoperate with the wider community.

- **Use Cases**: Certain conditions may require a research community to host their own AAI such as; network connectivity requirements (i.e. connecting to a protected physical network for experiment operations), having full control over the release cycle (i.e. needing to only upgrade at certain times of year to align with research needs) or to

mitigate the cost of a future migration (migrating from an AAI to another can be a very slow process and you may choose to host your own AAI to mitigate the risk of migrating high numbers of services).

- **Pros**: Full flexibility, modular architecture, greater control over hosting location and update schedule
- **Cons**: Requires DevOps expertise and maintenance; policy coordination across proxies can be complex; higher costs

Visit the section on existing software solutions and ensure AARC Compliance with Technical Guidelines.

7.4 Step 4: Plan for Operations and Sustainability

- **Staffing**: Assign roles for technical ops, security, policy coordination, and user support. Ensure adequate personnel are in place for technical assistance.
- **Monitoring**: Track login flows, token issuance, and service usage
- **Updates**: Stay aligned with emerging AARC TREE recommendations (e.g. support for OIDC Federation, digital wallets)
- **Governance**: Ensure stakeholders agree on responsibilities, especially if federating across institutions or countries
- **Funding**: Secure ongoing resources (vs. project-based funding) for operational continuity.

8 Available Software and Services

AUDIENCE: AAI IMPLEMENTORS AND OPERATORS

Choosing software to construct your AAI can be a minefield. You have probably heard of many names of software and services but are not sure what they do or whether you need them. The sections below do not provide an exhaustive list but strive to demystify the words and include lessons learned by our community. **Please note:** be aware the resources listed below are curated by the AARC-Community. ***Ongoing input is welcome!***

Many items below receive support through the European Commission and/or NRENs, highlighting the importance of sustainable funding models for AAI.

- Complete AAI Solutions
    - Hosted
    - Self Hosted
- Commonly used Software and Service Components

8.1 Complete AAI Solutions

Several software solutions can provide all, or nearly all, of the components that you will need for your AAI. Care must be taken to configure them in a way that supports the AARC guidelines.

The NFDI project completed a feature comparison between several offerings that may be useful for further information https://www.nfdi-aai.de/community-aai-software/#feature-matrix

8.1.1 Hosted

Some of the following are offered free of charge whilst others operate on a paid subscription. The best place to start to see whether you are eligible is often your national NREN.

Service	Community Notes
CILogon	Significant experience in running AAIs that support AARC guidelines
EGI Check-In	Significant experience in running AAIs that support AARC guidelines
GEANT Core AAI (MyAccessID, MyAcadmicID)	Significant experience in running AAIs that support AARC guidelines

B2ACCESS	Primary target: users of the B2 Suite from EUDAT
MyAccessID	The MyAccessID Identity and Access Management Service is provided by GEANT with the purpose of offering a common Identity Layer for Infrastructure Service Domains (ISDs).
NFDI AAI	Primary target: DE
SURF Research Access Management (SRAM)	Primary target: NL
UK-IRIS	Primary target: UK
LS AAI	Primary target: Life Sciences. LS AAI is one of the instances powered by AARC-based Perun AAI solution. LS AAI targets Life Science RIs, offering community management and integrated computational platforms and data services. It is operated jointly by Masaryk University and CSC, which also provide user support and CSIRT.
EU 1+MG framework	Components for data quality, data standards, and technical infrastructure standards and APIs needed to federate sensitive health data access in genomics. Depends on Life Science Login.
didmos-as-a-service	A multi-tenant capable hosted Community AAI. Provides VO management supports SAML and OIDC and includes a proxy to interact with other proxies, like eduID or generic infrastructure proxies. See also didmos below. Primary target: DE but some customers outside
RCIAM	The RCIAM solution by GRNET is a suite of open-source IAM tools, aligned with the AARC Blueprint Architecture. It includes a multi-protocol Service Proxy (based on a Keycloak fork) supporting OAuth2, OpenID Connect, and SAML; a Keycloak group management extension enabling authorisation; and a service management portal for onboarding and managing services (based on the RCIAM Federation Registry). It is used, for example, by EGI Check-in and the EOSC EU Node Infrastructure Proxy for EOSC Core Services.

8.1.2 Self Hosted

If you plan to host your own AAI we strongly suggest benefiting from the AARC Community's existing knowledge of the following software solutions. Reinventing the AAI wheel can be a long and painful process and the AARC Community is here to help. Contact information is available at https://aarc-community.org/

Software	Community Notes
Keycloak	Most experience is with the community version rather than the Redhat build, which offers a support model. Keycloak has been found to be highly performant but is geared towards common industry use cases, i.e. service and identity provider integration is managed manually by Keycloak admins with the expectation that there is a fairly low number of them. Community experience with Keycloak highlights the following adaptations that are often made: • Keycloak does not support multilateral federation but you can use a secondary proxy (e.g. Satosa or SimpleSAMLphp) as a bridge between Keycloak and eduGAIN. • Several communities have developed AARC extensions for Keycloak e.g. to support the AARC recommended attribute formats • Several communities have developed secondary software to allow end users to register services (known as clients in Keycloak) in a managed way. See RCIAM above or Keycloak REST Adapter
INDIGO IAM	Built-in support for AARC guidelines is being developed. INDIGO IAM provides backwards compatibility features for VOMS Proxy authorisation required by some legacy grid infrastructure. Note that there is no support for SAML services, only OAuth.
MidPoint	Provides features beyond AARC AAI, including account provisioning in LDAP which is out of scope for many research communities. Initially built as an open source alternative to Microsoft MIM.
didmos (NFDI, DAASI)	didmos is a modular open-source Identity and Access Management framework by DAASI International that provides flexible authentication and authorization services through components like the Authenticator (supporting SAML/OIDC protocols through Satosa or an integration with Shibboleth IdP), Core (for access control), and Federation Services, enabling organisations to implement customized IAM solutions. Import of users and attributes from databases can be configured, e.g. from an ERP or SAP. Support can be configured for command line workflows. SAML and OIDC/Oauth2 are supported for SSO integration. The company DAASI International can offer assistance with service setup and support.
Unity (B2Access, HIFIS, NFDI)	Unity IDM is an open-source identity and access management platform that serves as the core technology behind B2ACCESS, supporting federated authentication through SAML, OAuth2, and X.509 protocols to enable single sign-on across European research infrastructures operated by EUDAT and hosted at Forschungszentrum Jülich.
RegAPP (NFDI)	RegApp is an open-source federated identity management system developed at KIT's SCC that provides authentication and authorization infrastructure (AAI). Regapp supports SAML, OpenID Connect, LDAP protocols and two-factor authentication

REMS	Resource Entitlement Management System (Finland) - in CSC Github (https://github.com/CSCfi/rems)
AcademicID (NFDI)	Academic ID is an authentication service developed and operated by GWDG that provides single sign-on access to their Cloud platform and various IT services for universities and research institutions in Lower Saxony through federated authentication via DFN-AAI. AcademicID can be self-hosted, but is also is a solution hosted by GWDG.
Perun AAI	Perun AAI is a comprehensive open-source AAI solution based on community standards (like AARC and REFEDS) and focused on supporting research infrastructures. Its two main components are Perun IdM for user identity and access management, including the capability to (de)provision local service access; and Perun ProxyIdP for SSO, attribute enrichment and service level access control. Additional side components are available for specific use cases. Perun AAI is co-developed by ISO27k-certified teams at CESNET and Masaryk University which also host and operate most instances, the largest in the 10-100k user range and hundreds of services.
CoManage	The software behind CILogon. Actively developed with support from Incommon.

8.2 Commonly used Software and Service Components

The following table is included to demystify some of the software or service terms you may come across in AARC BPA inspired AAIs. It is not an exhaustive list and input is welcome.

Software or Service	AARC BPA Component	Purpose	Community Notes
eduGAIN	Authentication (SAML as of 2025 - and OIDC in the future)	User authentication from home organisation to your Research Community	To use eduGAIN you will need to join a national federation. Some national federations may offer additional services, such as a hosted Identity provider, that you may find useful. OpenID Federation is a work in progress
ORCID	Authentication (OIDC)	User authentication using their self-managed ORCID account	Many communities offer ORCID as a way for users to authenticate (or to add their ORCID ID as another attribute to their user object). ORCID supports OpenID.
Decentralised Identity	Authentication	User authentication use	There is little current experience with using Decentralised Identity (e.g.

		their self-managed identity	Wallets). This is being explored in the AARC TREE project.
Trusted Certificate Services (TCS)	Authentication (X.509)	User authentication with an end-user X.509 certificate. Required for some legacy grid workflows (e.g. for the physics community)	Only available to members of participating NRENs.
Seamless Access Discovery Service	Access Protocol Translation "Discovery Service"	Users select their home organisation for authentication, which is persisted in their browser to improve usability.	You can use the hosted service or run it yourself (the underlying software is thiss-js). You can optionally configure a filter to show a limited set of identity providers.
PyFF	Access Protocol Translation "Metadata Query"	A store of SAML metadata that is trusted by your Research Community and used by your discovery service	PyFF is recommended as a tool for filtering metadata but no longer as a Metadata Query engine
thiss-mdq	Access Protocol Translation "Metadata Query"	A store of SAML metadata that is trusted by your Research Community and used by your discovery service	An implementation of the metadata query protocol (MDQ) for JSON metadata only. Explore only if you are running a standalone instance of thiss-js and pyFF.io or similar and have performance challenges.
Satosa	Access Protocol Translation "Proxy"	A configurable proxy for translating between different authentication protocols such as SAML2, OpenID Connect and OAuth2.	Other Identity Python modules are typically run alongside Satosa, such as the consent service, Seamless Access and/or PyFF.
SimpleSAMLphp	Access Protocol Translation "Proxy"	A PHP based proxy with many extensions available.	Many research institutions run SimpleSAMLphp as the basis for their AAI. Despite the name it supports many protocols including OIDC. It can also be used as both an Identity or Service Provider supporting various protocols.

Shibboleth IdP	Access Protocol Translation "Proxy"	Java based Identity Provider with proxy support	Shibboleth Identity Provider is a SAML Identity Provider (IdP) with proxy support. Combined with the OpenID Connect Provider (OIDC OP) and OpenID Relying Party (OIDC RP) plugins, it acts as a full access protocol translation proxy. Plugins for OpenID Federation (OIDFed), OpenID for Verifiable Credential Issuance (OID4VCI) and OpenID for Verifiable Presentations (OID4VP) are under development.
Lighthouse	Services (OIDC)	OpenID Federations Trust Anchor	
OFFA	Services (OIDC)	OIDFed for services	Forward Authentication to add OIDFed to existing (OIDC) services
mytoken	Services (OIDC)	Access Tokens for long running jobs	(see also htgettoken & vault - to be added)
ssh-oidc	Services (SSH)	SSH with federated identities	Multiple solutions exist. ssh-certificates seem to be preferable over PAM solutions. • ssh-oidc at KIT • WAYF-SSHCA
oidc-agent	Services (OIDC)	Enable command line OIDC workflows	oidc-agent is a set of tools to manage OpenID Connect tokens and make them easily usable from the command line.
mod_auth_openidc	Services (OIDC)	Protect end services using the OpenID Connect protocol	OpenID Connect Relying Party module for the Apache web server Also add: other plugins, also for OAuth2 Resource servers and for NGINX: https://www.openidc.com/#software
Shibboleth SP	Services (SAML)	Protect end services using the SAML protocol	Shibboleth Service Provider is a SAML Service Provider (SP). In this context it is most interesting to research communities as a way to protect their end services using SAML without having to implement SAML oneself. See also Shibboleth IdP above.

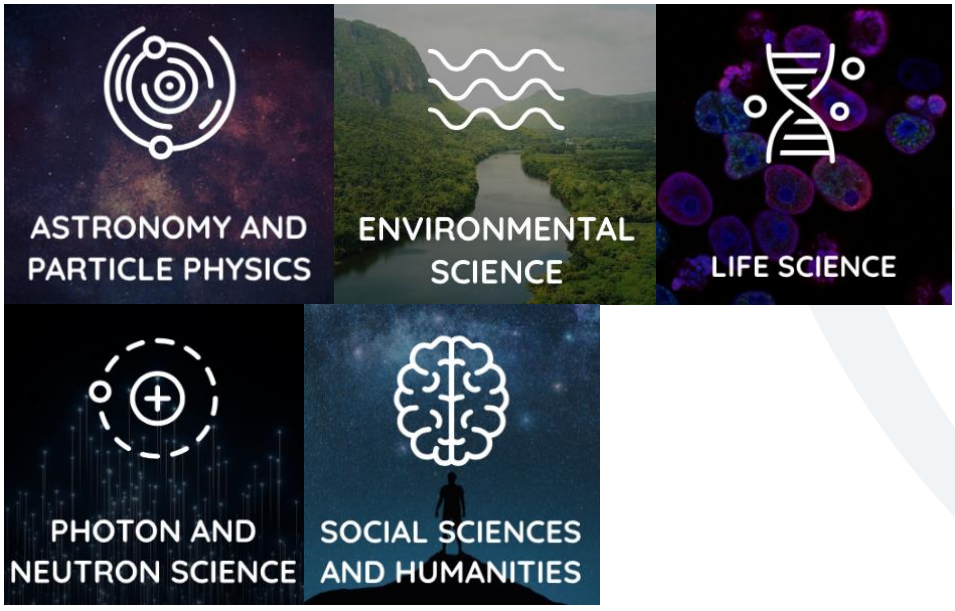
REMS	Authorisation	Authorisation/Data access management support support (can be federated)	Resource Entitlement Management System is a service component that organises and harmonises and communicates (SAML, OIDC, GA4GH) resource access application process. Requires (federated) identity service. Similar to COManage and Perun?

9 AARC in Action: Case Studies

Research Collaborations vary in terms of requirements, meaning that each AAI architecture will look different. The AARC Handbook is intended to be used as a practical tool to foster the uptake and use of the AARC-compliant AAI by different research communities. To reach this goal, a series of varied case studies is being compiled over time. These case studies are intended to service as real-life examples of how different research collaborations have set-up AARC-compliant AAI. They will include lessons learned, tips and tricks and reference implementation examples to help other communities setting up their own AAI. Further contributions from Research Collaborations are welcome!

Research Infrastructures and Communities

To provide a framework for this outreach campaign, we are collaborating with the five Science Clusters in the framework of the Open Science Clusters' Action for Research and Society (OSCARS) project. The aim of OSCARS is to foster the uptake of Open Science in Europe by advancing and integrating FAIR research data and cross-disciplinary services within the European Open Science Cloud (EOSC). This collaboration with the Science Clusters, kick-started through a joint workshop, has provided the basis for creating a series of case studies in the domains of:



9.1 AARC in Action: Case Studies

The success of the AARC Blueprint Architecture (BPA) is largely determined by its uptake and use within research collaborations. Through our AARC in Action outreach campaign, we will raise awareness of the AARC Handbook with research infrastructures and their communities regarding their AAI-requirements and implementation. This will not only help us to update and improve the AARC Handbook, but will help us develop a series of AARC in Action Case Studies, to help others to implement an AARC-compliant AAI. As the AARC Case Studies are developed, we will publish them as real-life AAI-implementation in the AARC in Action section of this handbook.

Here is an initial list of AARC in Action Case Studies:

- **Astronomy and Particle Physics:**
    - Case Study: CERN laboratory
- **Social Sciences and Humanities**
    - Case Study: Philosophy: Medieval Fallacy project

These case studies will be coordinated by the AARC Handbook Editorial Team. Further case studies will be added as they become available. Case Study contributions from Research Collaborations are welcome!

To ensure comparability, each case study will use the AARC in Action Case Study template provided below.

9.1.1 AARC in Action: Case Study Template

Domain	Which research field are you serving?
User Base	Who are your users? Are they affiliated with institutions in eduGAIN, external (e.g. guest, citizen science), or a mix?
Access Requirements	Does the sensitivity of your research require additional access approval mechanisms? Do you need fine-grained access control, or is basic authentication sufficient?
Scale	How many services do you plan to connect to your AAI? Which protocols do they require? What is a realistic estimate of effort required to migrate all users and services from one AAI to another in case of a crisis?
Existing Infrastructure	Do you have an identity provider (IdP) or group management service already?
Sustainability	Can you commit operational resources, or do you need a hosted service? For how long will your AAI be required? Will your available support level be able to increase with growth of participating institutes or services?

Environment specific requirements	Do you need any physical connectivity to dedicated networks? Are IT interventions restricted to fixed time windows? Do you have any other unusual requirements that may not be supported by off the shelf solutions?
Governance	Who will take responsibility for policy decisions regarding your AAI? Do they have enough authority over your research community to make high level statements and decisions, e.g. for data protection, security policy requirement etc?

9.2 Particle Physics: CERN laboratory

Domain	Which research field are you serving?	Particle Physics
User Base	Who are your users? Are they affiliated with institutions in eduGAIN, external (e.g. guest, citizen science), or a mix?	A mixture of verified researchers (CERN account holders), and collaborators (eduGAIN, social logins)
Access Requirements	Does the sensitivity of your research require additional access approval mechanisms? Do you need fine-grained access control, or is basic authentication sufficient?	Fine grained access control per service
Scale	How many services do you plan to connect to your AAI? Which protocols do they require? What is a realistic estimate of effort required to migrate all users and services from one AAI to another in case of a crisis?	12,000 OIDC clients. 250 SAML service providers.
Existing Infrastructure	Do you have an identity provider (IdP) or group management service already?	Yes
Sustainability	Can you commit operational resources, or do you need a hosted service? For how long will your AAI be required? Will your available support level be able to increase with growth of participating institutes or services?	In house technical support for the foreseeable future of the laboratory
Environment specific requirements	Do you need any physical connectivity to dedicated networks? Are IT interventions restricted to fixed time windows? Do you have any other unusual requirements	Many. Upgrades must be performed in specific windows. Specific network requirements for experiment hardware. Truly global user base, independence from any one sovereign

	that may not be supported by off the shelf solutions?	state is paramount. Client/service management must be self-service for trusted users.
Governance	Who will take responsibility for policy decisions regarding your AAI? Do they have enough authority over your research community to make high level statements and decisions, e.g. for data protection, security policy requirement etc?	Clear governance model exists for the laboratory

9.2.1 Chosen AAI

The best option for this laboratory was to run their own AAI. Keycloak was chosen as a core technology with custom applications supporting CERN specific workflows. Not all AARC guidelines are followed to date (February 2026).

Impact

The AAI is fully operational. Due to not following all AARC Guidelines fully, occasionally challenges with interoperability are encountered and must be handled on a case by case basis.

9.3 Social Sciences and Humanities: Philosophy: Medieval Fallacy Project

Domain	Which research field are you serving?	Philosophy
User Base	Who are your users? Are they affiliated with institutions in eduGAIN, external (e.g. guest, citizen science), or a mix?	15 eduGAIN IdPs
Access Requirements	Does the sensitivity of your research require additional access approval mechanisms? Do you need fine-grained access control, or is basic authentication sufficient?	Basic membership approval is sufficient
Scale	How many services do you plan to connect to your AAI? Which protocols do they require? What is a realistic estimate of effort required to migrate all users and services from one AAI to another in case of a crisis?	20 OIDC services (small scale)
Existing Infrastructure	Do you have an identity provider (IdP) or group management service already?	No
Sustainability	Can you commit operational resources, or do you need a hosted service? For how long will your AAI be required? Will your available	Required for 6 years minimum (duration of EC project). Small amount of

	support level be able to increase with growth of participating institutes or services?	IT support funded through the project.
Environment specific requirements	Do you need any physical connectivity to dedicated networks? Are IT interventions restricted to fixed time windows? Do you have any other unusual requirements that may not be supported by off the shelf solutions?	None
Governance	Who will take responsibility for policy decisions regarding your AAI? Do they have enough authority over your research community to make high level statements and decisions, e.g. for data protection, security policy requirement etc?	Project governance

9.3.1 Chosen AAI

The best option for this project was a hosted solution. The IT support approached 2 European hosted AAI providers and was eligible to use one.

9.3.2 Impact

By using a hosted solution, researchers have been able to authenticate with very few obstacles. The time taken to gain access to a hosted solution was too long for many researchers, impact their ability to work. The solution has been well received and other similar communities are showing interest.

10 Recommendations

An overview of recommendations for each of our target audiences are provided below:

AUDIENCE: RESEARCH COMMUNITY MANAGEMENT

Research Collaborations should **prioritise establishing an AARC Compliant AAI as an early cornerstone of their infrastructure**. As the pressure for researchers to become active increases it will be increasingly tempting to adopt sub-optimal AAI mechanisms that will ultimately impact research productivity. Early investment in a common, AARC-compliant AAI significantly reduces long-term costs, operational complexity, and disruption, compared to retrofitting identity solutions once communities are already established.

Wherever suitable, the **adoption of a hosted AAI solution is encouraged** to minimise overhead and ease future interoperability between AAIs.

Translating the AARC guidelines into practical recommendations that can be widely implemented across research infrastructures and their communities is essential. For this, the AARC Handbook is an important step forward. However, this needs to be complemented by an investment in AAI-specific **capacity building, training, and knowledge exchange mechanisms.**

AUDIENCE: FUNDING AGENCIES

It is crucial that funding agencies recognise **AAI as Critical Infrastructure for Research and Education and promote the AARC BPA as the reference model for AAIs in the research and education community.**

To complement this, funding agencies should not only **fund shared AAI solutions and hosted services** but also **require early involvement of AAI operators in grant proposals**, ensuring best practices are followed and avoiding delays or suboptimal implementations due to late or unfunded AAI integration.

Ongoing **funding for Research AAI communities of best practice** (such as the AARC Projects or FIM4R) is essential. These are critical resources for new or evolving research collaborations who require customised guidance to navigate this complex, specialised domain and identify the best AAI solution for their unique requirements.

Additionally, **supporting the expansion of the AARC BPA to ensure it can also address the education use-cases**, is a natural next step for the AARC Community.

AUDIENCE: AAI IMPLEMENTORS AND OPERATORS

Organisations providing complete AAI solutions should focus on **optimising the setup time for research collaborations**. This includes easy to follow documentation, quick-start guides, responsive support and clear information on pricing and/or eligibility.

AUDIENCE: ALL

The wider Research AAI community should remain active and responsive to requests for guidance from new or evolving research collaborations.

11 9. Glossary

The AARC Glossary provides an overview of terms and acronyms frequently used in the AARC Community, alongside their definitions. Further suggestions of glossary terms are welcome.

Additional terms can be found in https://aarc-community.org/guidelines/aarc-g045/

Terminology / Acronym	Definition
2FA	Two-Factor Authentication (2FA) is a type of authentication in which there are two steps to authenticate, usually a username/password plus a physical token generator.
AAI	Authentication and Authorisation Infrastructure. A service that enables authenticated and authorised access to resources.
Attribute	Metadata about the end-user, the service, or other entities. Attributes are used by Service Providers for service provision, including authentication, authorisation, and accounting operations. They may also assist end-user systems in selecting appropriate services.
Attribute Authority	A component containing attributes about users and entitled to make statements about entities and assign attributes to them. Attribute authorities can be part of the AAI, an infrastructure proxy, or elsewhere in the federation.
Authentication	The process by which a system recognises who you are. When you log in to your university network, you are authenticated. Authentication checks user credentials against an authorised database or authentication server.
Authorisation	The process of determining what services or resources a user is permitted to access, based on policies from service providers or relevant authorities. It enforces access control decisions after authentication.
Collaboration	A bounded collection of universities, laboratories, institutions, or similar entities that adhere to collaboration policies and offer research infrastructure to a community.
Collaboration management	Boards, committees, groups, and/or individuals mandated to oversee and control the collaboration.
Collaboration policy	Policies governing the management, operations, and security of the collaboration, including operational security, membership management, and data protection.
Community	A group of users organised around a common purpose and jointly granted access to a collaboration. It may mediate access between users and resources.

Terminology / Acronym	Definition
Community AAI	An AAI service managed by a community or its representative, used to assign user roles, rights, and community-specific attributes.
Community / Infrastructure ID	A user identity enriched with community or infrastructure attributes for user management at the community or infrastructure level.
Community management	A management body responsible for a community, its sub-groups, and the lifecycle of user membership.
Community membership policy	A policy governing community membership and access rules. It does not supersede infrastructure or service membership policies.
eduGAIN	A SAML inter-federation combining multiple national federations to enable global trust. It publishes metadata of trusted IdPs and SPs, enabling cross-border access to research infrastructure services.
Federation	A group of Identity Providers (IdPs) and Service Providers (SPs) that trust each other through shared policies and contracts, enabling authentication, identity verification, and access control.
Identity and Access Management (IAM)	A general term for systems that manage digital identities and access, including provisioning, de-provisioning, single sign-on, and authorisation.
Identity Assurance	The process of ensuring that a user account corresponds to a real-world identity, combining identity vetting and authentication strength (e.g. MFA usage).
Identity Provider (IdP)	An entity responsible for storing, managing, and securing user identities and providing identity services to relying applications within a federation or distributed network.
Infrastructure	IT hardware, software, networks, data, facilities, and processes required to develop, deliver, and support services, often with governance and integration across services.
Infrastructure service	A service provided by a research infrastructure or e-infrastructure to members of one or more communities, typically receiving user attributes through an infrastructure proxy.
MFA	Multi-Factor Authentication, an authentication method requiring two or more independent verification factors.
OAuth 2.0	An open standard authorisation protocol that allows applications limited access to user resources without sharing login credentials, using secure token-based access.
OIDC	OpenID Connect, an interoperable authentication protocol built on OAuth 2.0 that enables identity verification and retrieval of user profile information.
OIDFed	OpenID Federation, a federation protocol enabling OpenID Connect to leverage identity federations such as eduGAIN.

Terminology / Acronym	Definition
RAF	REFEDS Assurance Framework, which defines assurance levels for identity attributes.
REFEDS	The Research and Education FEDerations group, which develops recommendations and best practices for operating identity management federations.
Role Based Access Control / Management (RBAC / RBAM)	An access control model in which permissions are assigned to roles rather than individual users, simplifying access management and ensuring consistency.
SAML	Security Assertion Markup Language, a standard for exchanging authentication and authorisation data between Identity Providers and Service Providers.
SAML Federation	A collection of SAML entities whose metadata is curated and published by a federation, typically organised at a national level.
Service (End Service)	A collaboration or infrastructure element that fulfils a user need, such as computing, storage, networking, or software systems.
Service Provider (SP)	An entity responsible for the management, deployment, operation, and security of a service.
Single Sign-On	A system allowing users to authenticate once and access multiple services within a session.
SP-IdP-Proxy	A component that sits between service providers and identity providers, simplifying trust relationships by acting as a single intermediary.
User	An individual authorised to access and use services.
User identifier	An attribute that uniquely identifies a user within a specific domain or system. A user may have multiple identifiers across domains.
WAYF	“Where Are You From”, an AAI component allowing users to select their authentication source (e.g. home organisation). Also known as a Discovery Service.

12 FAQ

Answers to a series of Frequently Asked Questions (FAQs) are provided below. If you have a question that is not mentioned in the list and you would like an answer, please let us know!

What is the difference between AAI and Federated Access?
Federated Access is authentication across separate administrative domains by relying on shared technologies and policies - i.e. users from one organisation accessing services from another. AAI encompasses both **scalable** Federated Access and access control, such as user management and authorisation.
How can I let researchers authenticate to the services in my infrastructure with eduGAIN?
You will need to run a SAML Service Provider (this is typically the entry point to your AAI) and publish its metadata to a federation that is part of eduGAIN. See https://edugain.org/participants/how-to-use-edugain/
How can my researchers authenticate to services in eduGAIN?
You will need to publish a SAML Identity Provider into eduGAIN. Ensure that you are authoritative for each attribute that you issue about a user - see technical guidelines below for how to aggregate information from researchers' home organisations and your own sources.
How can I use the European Open Science Cloud (EOSC)?
By this question you may mean **"How can I log into the EOSC EU Node and get credits to use its services".** If that's the case please see https://open-science-cloud.ec.europa.eu/support/frequently-asked-questions/user-credits. In short - your Identity Provider will need to 1) be trusted for authentication to EOSC e.g. via eduGAIN and 2) assert that you are a Faculty or Employee/Staff of your Home Organisation by using the eduPersonAffiliation attribute. If you are acting as a proxy to users coming from a different home organisation that will be accessing EOSC using your own IdP you may want to propagate these values. Please see "AARC-G003 Attribute aggregation" for guidance on aggregation of scoped attributes https://aarc-community.org/guidelines/aarc-g003/ Alternatively you may mean "**How can I enrol my AAI and research services as an EOSC Node?**" and enable cross-node authentication and authorisation. At the moment a first stage enrolment of 13 communities are being enrolled and a second phase will start shortly. More information will be provided in the future. It is already a good idea to build your AAI keeping in mind its future interoperability needs, though, so try to support the AARC guidelines to get a head start.
Isn't SAML considered "dead"?
Generally, yes. OIDC has surpassed SAML for granting access to services - particularly because it supports non-web and API use. SAML, however, is still necessary for the connection between SAML Home Organisations (i.e. those in eduGAIN) and AAIs. A new OIDC equivalent for scalable identity federation is under active development but is not yet widely adopted.
Should I require users to register for MFA?

Some Home Organisations in eduGAIN already assert whether an authentication was performed with MFA or not. Wherever possible this should be accepted as proof of MFA to avoid your researchers managing multiple MFA tokens. Other home organisations, however, do not. If you want to ensure that all researchers use MFA (perhaps you are required to for legal reasons or simply as a good security practice) you will need to also provide your own MFA registration workflow.

Why should my community implement an AAI?

When a research community sets up a common AAI, people can use their university or institute login to access services in the community. It makes working across institutions feel a lot less complicated, because you don't have to ask for new logins or wait around for someone to approve your access. There's also a level of trust that comes with it. If everyone is on the same system, you know the same rules and security standards apply everywhere and you can introduce things like two-factor authentication in a uniform way without every service having to figure it out on their own. For the people running services, it's a big relief too. They don't have to spend time and money building their own user management and login systems or maintaining separate user databases. They just connect to the shared infrastructure, and it grows naturally as new services join. On a bigger scale, this kind of common AAI ties the community into international infrastructures. It makes data and services more interoperable and that means research outputs stay accessible for the long term, and the whole ecosystem becomes more sustainable.

How do I convince my home organisation that federated AAI can be trusted?

Historically Identity Providers have been hesitant to release user attributes to services in eduGAIN if there are no bilateral agreements in place. There are various trust marks that have been set up to address this problem. Entities in eduGAIN can assert Sirtfi to declare their support of good practices in operational security and incident response. At the AAI level a similar trustmark has been established, Snctfi, that asserts that the AAI and all services behind it comply with a set of policies. Additionally, it is up to service (and AAIs) to ensure that they do not request more attributes than strictly necessary - the Research and Scholarship attribute bundle has been developed for this purpose https://refeds.org/category/research-and-scholarship .

Which groups or mailing lists can I join to stay connected to other communities?

We strongly recommend following FIM4R (Federated Identity Management For Research) https://fim4r.org . This group has been active since 2012 and spanned multiple different projects that have come and gone.

Is there a financial benefit to using an AARC compliant AAI and avoiding a common commercial AAI?

Although difficult to quantify, in many situations the long term costs may be reduced. Using a common commercial AAI solution (such as those provided by Google or Microsoft) can expose you to certain risks:

- **Lack of open access:** Research is often global and neutral, allowing researchers to collaborate despite wars or political perspectives. Relying on a commercial product may put this at risk due to lack of control over the network access or terms of use. In the event of incompatibility, a workaround may be costly or impossible - putting the research itself at risk.

- **Vendor lock-in:** The cost to migrate from one AAI to another is substantial and frequently underestimated. One large scale research community took 6 years to migrate their 12,000 services from one AAI to its successor, incurring a significant cost to that community due to time spent configuring systems. The AAI and the unique identifiers it provides should be viewed as a valuable asset to a research community. Being exposed to vendor lock-in in an AAI is a significant risk - if prices are suddenly increased a research community will have to find the technical resources to migrate or pay the fee.