31-12-2024

Deliverable 3.1:

Landscape analysis of AARC BPA adoption

Publication Date	[Publish Date]
Due Date:	
Authors:	Marina Adomeit (SUNET), Janos Mohasci (KIFÜ)
Contributors:	Licia Florio (NORDUnet), Sally Chambers (DARIAH), David Groep (Nikhef NWO-I), Christos Kanellopoulos (GÉANT)
Version:	V1.0
Document Code:	AARC D3.1
Publishing Organisation:	NORDUnet/SUNET
DOI:	

Abstract

This document provides an overview about the deployment of Authentication and Authorisation Infrastructures (AAIs) in the research and education community that follow the AARC BPA and on the adoption of AARC Guidelines.

The content of this deliverable builds on the the insights learned from surveys that were conducted during 2024 with the Research Infrastructures and e-Infrastructures participating in the AARC TREE project, AEGIS [AEGIS] and FIM4R (FIM4R]. The findings presented in this deliverable serve as input for the technical (WP1), policy (WP2), which will deliver an updated version of the AARC BPA as well as a revision of the accompanying guidelines (WP4) and for the compendium and recommendations (WP5) work which will start in 2025, which will deliver recommendations for a common long-term strategy for AAI services in pan-European Research Infrastructures in Europe.

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

Table of Contents

1. Introduction

The objective of Work Package 3 (WP3) "Use Cases Collection and Analysis" is to collect the Research Infrastructures (RI)'s requirements and use cases among the Research and e-Infrastructures that participate and operate an Authentication and Authorisation for Research and Collaboration (AARC) Blueprint Architecture (BPA) compliant Authentication and Authorisation Infrastructure (AAI) and to produce a landscape analysis of AAI services (and gaps) to provide input for the technical (WP1) and policy (WP2) work in Year 2, as well as for the compendium work (WP5). The results of the work conducted in WP3 serve as essential input to Architecture (WP1), Policy (WP2) and Validation (WP4) work packages to steer their work on revising the AARC BPA and its guidelines concerning the gathered implementation experience and further requirements.

The aim of the work package is twofold: on one hand, its aim is to assess the deployment of AARC BPA-compliant AAIs as well as the adoption of the AARC guidelines that accompany the BPA; on the other hand, the work package has the objective to collect new requirements the AARC BPA should support. These two different, but complementary, aspects are reflected in two separate deliverables:

- Landscape analysis of AARC BPA adoption (D3.1) due in December 2024
- Use-Case Collection and Analysis (D3.2) due in February 2025

This document is the first deliverable, D3.1, which contains the first result of the work carried out in WP3 and focuses on assessing the adoption of the existing AARC Guidelines.

Milestone M3.1 (and later Deliverable D3.2) describe the approach and methodology taken to conduct the surveys within the Research and e-Infrastructure that have deployed an AARC BPA compliant AAIs.

The body of work is significant. The latest version of the AARC BPA was published in 2019, following its initial publication in 2015; the guidelines have been published between 2017 and 2022. Over the years the AARC BPA (and some of the guidelines) has been deployed by several Research and e-Infrastructures in Europe and beyond.

Over the years, the AARC Engagement Group for Infrastructures (AEGIS) has developed and endorsed additional guidelines. Established after the AARC2 project in 2019, AEGIS brings together representatives from research and e-infrastructures that operate (or are in the process of operating) AAIs that follow the AARC BPA; the chairs of the AARC policy and technical working groups are also in AEGIS. The working groups are open to anyone interested in policy or technical aspects and have been instrumental over the years to ensure continuity of the work over the years even in the absence of funding for AARC.

The survey and the interviews conducted offered valuable insights about their AAI deployments, AARC BPA and guidelines adoption and use cases and gaps. This deliverable focuses on the data collected about the adoption of the AARC BPA guidelines. At the beginning, the document provides an overview of AARC BPA and guidelines and explains their creation and maintenance process. This is

followed by the quantitative data that was gathered during the surveys. Finally, the final part of the deliverable provides an analysis of the collected data and recommendations.

2. AARC BPA Guidelines

The AARC Guidelines complement the AARC Blueprint Architecture (BPA), encompassing both technical and the policy best practices defined by the AARC community and endorsed by the AEGIS, the AARC Engagement Group for Infrastructures.

At the end of the first cycle of AARC in 2017, some guidance was needed to support the deployment of the AARC BPA in a way that would foster interoperability.

The AARC guidelines were created in response to that need. The AARC Guidelines help communities and infrastructures to implement and operate an AAI that follows the AARC BPA and provide the framework to ensure that these AAI are interoperable.

A process has also been defined to ensure that:

- The guidelines are prepared in an inclusive manner.
- Documents with the ambition to become guidelines go through a process that includes several stages of consultation and a final call for comments.
- A DOI is assigned to a document after the Final Call. The DOI, to be obtained from Zenodo unless otherwise given or already assigned, is embedded in the document. All AARC guidelines are deposited in Zenodo.
- Documents become AARC Guidelines after AEGIS endorses them; this ensures that the existing operators of AARC BPA-compliant AAIs can validate the soundness of the guideline and its deployability. Documents that are not endorsed as guidelines but are of general interest are still published as informational AARC documents.

Over the last eight years, the number of guidelines has grown. Some of them have been deprecated and replaced by a new version.

AARC Guidelines are complemented by the AARC Policy Development Kit (PDK)[1]. Defining a set of policy documents that regulate and facilitate trust for users, resource providers, and infrastructures is necessary to operate an identity and access management infrastructure. These policies outline the operational measures undertaken by the infrastructures to provide services properly. The policies principally cover security measures, user management and data protection. AARC PDK offers policy templates to provide a head start for Research Infrastructures that want to deploy the AARC Blueprint Architecture. These policies were not in the scope of this survey, however, the conclusions could be applicable to AARC PDK as well.

[1] https://aarc-community.org/policy/policy-development-kit/

2.1. Overview of AARC Guidelines

There are almost 40 AARC Guidelines including the additional PDK documents. For an easier overview, AARC Guidelines can be divided into several sets, each targeting a specific area of interest. The list of the AARC guidelines divided into thematic sets is provided below.

User Identity:

- How should I integrate Social Media Identity Providers? AARC-G008
- How should users link accounts, and how does that affect Assurance? AARC-G009
- How should services indicate that they would like users to authenticate with multi factor authentication, and how should my proxy forward that information? AARC-G029

Assurance (of identity):

- How should assurance information of external identities be calculated? AARC-G031
- What can I say about assurance of identities from social media accounts? AARC-G041
- How is assurance impacted by account linking? AARC-G009
- How should assurance information be shared with other infrastructures? AARC-G021
- Which Assurance Profiles should I use, there are so many! AARC-I050

Access Protocol Translation:

- Which best practices should I follow for my Token Translation Services? AARC-G004
- How should I translate from Identity Federation information to X.509 certificates? AARC-G010

Proxies:

- How can I ensure that my proxy is able to accurately claim that it supports best practices in Identity Federation? AARC-G015
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user AARC-G026
- How should I express assurance information for users when interacting with another proxy? AARC-G021
- How can my proxy simplify the discovery process for end-users? AARC-G061
- How can my proxy route the user to the correct discovery service? AARC-G062
- How can my proxy provide information about end-services? AARC-G063

Community Attribute Services:

- How should attributes from multiple sources be aggregated? AARC-G003
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user AARC-G026
- What are the best practices for running my Attribute Authorities securely? AARC-G071

- Which Acceptable Use Policy should I use to facilitate interoperability? AARC-I044
- How should I infer the affiliation of a user? AARC-G057

Authorisation:

- How should I manage authorisation information from multiple sources? AARC-G006
- How should group and role information be expressed to facilitate interoperability? AARC-G002
- How should resource capabilities be expressed? AARC-G027

End Users Services:

- My service needs to act on behalf of the user – how should I handle credential delegation and impersonation? AARC-G005
- My services are not web based, how can I use identities from the proxy? AARC-G007
- How should Services hint which Identity Provider (IdP) they would like users to use? AARC-G049
- Which Security practices should I follow? AARC-G014

3. AARC BPA Guidelines Adoption Survey

During April-November 2024, the WP3 AARC team conducted a series of interviews with 22 Research and e-Infrastructures. The details of those interviews are published in M3.1 and the gained insights about the Adoption of AARC BPA Guidelines are presented here.

The AARC guidelines are needed to ensure the interoperability of the Research and e-Infrastructures; there is not a list of mandatory ones, and Research and e-infrastructures choose the ones that are more relevant for them. Thanks to this survey, it will be possible to identify those guidelines that are a must. All AARC guidelines endorsed by AEGIS, were in the scope of the conducted survey and are addressed in this section.

The results of the analysis investigating the adoption of the selected AEGIS AARC BPA Guidelines is presented in Figure 1. In total, 22 infrastructure participated in the survey. From these RIs, four do not yet implement the AARC BPA and one did not provide an answer about the adoption of the AARC BPA Guidelines.

One of the infrastructures that does not implement the AARC BPA is a laser facility where users have to perform experiments on site, and another is an national HPC facility - for both of them AARC BPA was not in focus because of the nature of services where interoperability with other infrastructures was not (yet) a priority. The other two infrastructures that do not implement AARC BPA rely on legacy AAI systems where AARC BPA compliance will be considered when this infrastructure is upgraded.

The feedback received by several interviewees regarding the adoption of the AARC BPA, was that it is not very clear what criteria need to be met to be considered compliant with the AARC BPA. This is an area that would need further clarification. One of the interviewed research infrastructures (SKA) noted that they are extending the definition of the AARC BPA as they are implementing a centralised Attribute Authority, and that they are interested in bringing this use case to the AARC architecture working group.

The remaining 17 infrastructures implementing AARC BPA and related guidelines are diverse in the aspects of their scope and coverage. Some e-infrastructures are offering AAI services to international or national research infrastructures such as GÉANT and EGI.

National infrastructures such as the National Research and Education Networks (NRENs) and other organisations are also offering AAI services to cater for the national research community; this is the case of SURF for example, the Dutch NREN, that with the support of GÉANT has developed a science collaboration platform; similar platforms have been deployed in Germany (NFDI and HIFIS) are offering an AAI platform for the research community that follow the AARC BPA. These e-infrastructures have good coverage of adopting AARC BPA Guidelines, and through providing services to Research Infrastructures, enable a larger footprint for practical reach of these guidelines. Furthermore, five of the interviewed infrastructures are already or about to use GÉANT Core AAI Platform, and one is using EGI CheckIN service.

For these 17 infrastructures, the adoption of the AARC BPA Guidelines has been quantitatively analysed. There are four possible states - an AARC BPA Guideline is either implemented or in evaluation of implementation and therefore shown in shades of green in the chart. Otherwise, the AARC BPA Guidelines are either not implemented or it is out of scope for that infrastructure - shown in red and gray colors respectively. The graph also groups the guidelines by their area of implementation, based on which we will further analyse these results.

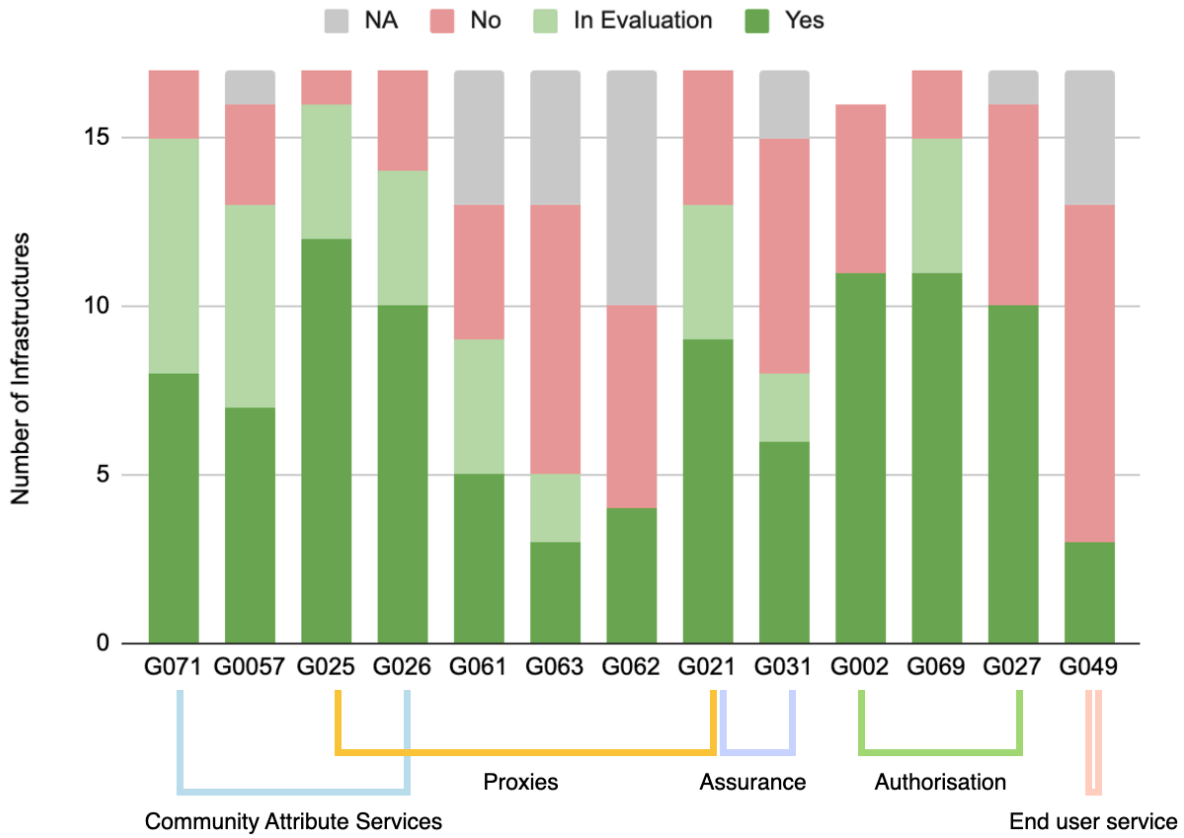

Figure 1: *Adoption of AARC Guidelines among interviewed Research and e-Infrastructures*

Looking at the results, the most implemented guidelines are in the areas of *Community Attribute Services* and *Authorisation*. This is reasonable, because for these two areas infrastructures have to have their solution, as community attributes and authorisation need to be maintained exclusively in the administrative domain of the infrastructure.

Third most adopted Guidelines are in the area of *Assurance*. It can be interpreted that these guidelines are important as infrastructures have requirements to use assured identities for individuals accessing their resources.

The area of *Proxies*-related guidelines is specific as there is some overlap with other areas as presented in Figure 1. The guidelines overlapping with *Community Attribute Services* and *Assurance* are well adopted. The guidelines G061 and G062 about implementation of the discovery services and signaling about the end-user service seem to be not prioritised or relevant.

The least adopted guideline is the one in the *End user service* area that is related to IdP hinting for discovery services, which confirms the results of less adoption of the discovery-related guidelines.

For guidelines that have not been implemented as yet, this could be for a number of reasons: because there is not a use case yet, another approach was implemented before a specific guideline was defined or because its implementation is not of high priority.

Several comments, mostly about the relevance of the Guidelines were received. However, they don't provide enough basis to draw certain conclusions. These comments therefore are not presented in this deliverable, but were shared with the Technical, Policy and Validation work packages for use at their discretion.

4. Conclusions and Recommendations

Based on the information received during the interviews, a number of conclusions and recommendations can be drawn. These are presented below in a numbered format for ease of reference. They provide valuable insights for the further development of the AARC Guidelines and supporting documentation, including the Compendium to be developed by WP5.

Conclusion no.1

For some interviewees it is unclear which are the criteria for declaring compliance with the AARC BPA.

Recommendation no.1

As the Research Infrastructures and e-Infrastructures are performing this evaluation as a self-assessment, it would be advised for AARC to come up with a process or some criteria that would make it easy for research and e-infrastructures to declare compliance with the AARC BPA.

Conclusion no.2

There were large differences between the interviewed Infrastructures. Some are e-Infrastructures providing Identity and Assurance Management (IAM) services to other Research Infrastructures or communities; for them providing these services are core business and they are therefore in a forefront of implementing the AARC BPA and Guidelines. The national and international Research Infrastructures and communities are on the other hand the users of such AAI services, as well as the owners of the use cases for using the AAI services. Such services are either run solely by them or used in conjunction with IAM services provided by e-Infrastructures while, on average, developing IAM expertise is not in their primary business.

Recommendation no.2

Utilising the expertise and evangelists from the champions in implementing the AARC BPA and Guidelines to guide the adoption for infrastructures who are behind the curve, while maintaining close relationship with the ones carrying the business cases would be a good tactic for improving the adoption. This work could be supported by the Compendium and related events being developed in WP5.

Conclusion no.3

Some of the feedback received for both AARC Guidelines and the PDK was that there is a large number of them and that it makes it difficult to comprehend which ones are important and where to

start when implementing them. Also, the feedback was that they are very wordy and comprehensive, which also decreases their clarity.

Recommendation no.3

It would be worth considering providing more guidance on how to use the Guidelines and PDK, categorising them for example by the use cases they support, or by interoperability or legal requirements. It could be also considered if revising and simplifying some of the documents would be feasible, while providing additional practical examples such as reference implementations and implementation guides from experience gathered in the field.

Conclusion no.4

This analysis focused on the subset of Guidelines that are endorsed by the AEGIS community. The Guidelines and PDK are however a larger set of documents for which the adoption and practical use is not clear in each case.

Recommendation no.4

It would be beneficial if a process was defined for the AARC Guidelines (and for the adoption of the PDK as well) that would help to assess how mature the adoption is. For instance some tags could be added to show whether a guideline has never been adopted, or conversely whether it has been deployed by one or more research and/or e-infrastructures. This approach would improve understanding the relevance and practicalities of implementing the guidelines, and introduce a possibility to produce an updated version of the documents after gaining implementation experience.

Conclusion no.5

The analysis of the adoption of the AEGIS endorsed AARC Guidelines, shows that some of the Guidelines are more used than the others. Also, related to Conclusion no. 3, the feedback received was that there is an overwhelming number of Guidelines and PDK documents.

Recommendation no.5

AARC could consider reviewing the Guidelines and PDK and evaluate if there could be some that could be retired. In future, this process could be incorporated into Recommendation no.4 where Guidelines or PDK documents that have no proven use in practice would be declared obsolete after a period of time.

References

[AEGIS] https://wiki.geant.org/display/AARC/AEGIS

[AARC BPA] https://aarc-community.org/architecture/

[FIM4R] https://fim4r.org/