

16-05-2019

Deliverable DNA1.2: Annual Report

Deliverable DNA1.2

Contractual Date: 30-04-2019

Actual Date: 16-05-2019

Grant Agreement No.: 730941

Work Package: 1

Task Item: 1

Lead Partner: GÉANT

Document Code: DNA1.2

Authors: L. Florio (GÉANT), A. Biancini (Reti), D. Groep (Nikhef), C. Kanellopoulos (GÉANT), N. Liampotis (GRNET), A. Terpstra (SURFnet), L. Durnford (GÉANT)

Abstract

This document reports on the work carried out by the AARC2 project, with greater emphasis on the second project year (2018-2019).

© GÉANT on behalf of the AARC2 project.

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Table of Contents

| | |
|---|----|
| Executive Summary | 3 |
| 1 Introduction | 4 |
| 2 Overview of AARC2 | 5 |
| 2.1 AARC2 Objectives | 5 |
| 2.2 AARC2 – Finalising the Work of AARC1 | 5 |
| 3 Summary of AARC2 Results | 8 |
| 3.1 Key Exploitable Results | 9 |
| 3.2 The AARC Blueprint Architecture (BPA) and its Evolution | 12 |
| 3.3 The Role of AEGIS in AARC2 and beyond | 15 |
| 4 Activities by Work Package | 17 |
| 4.1 Work Package NA1 – Project Management and Sustainability | 17 |
| 4.2 Work Package NA2 – Training and Outreach | 18 |
| 4.3 Work Package NA3 – Policy and Best Practices Harmonisation | 19 |
| 4.4 Work Package JRA1 – Architecture for Integrated and Interoperable AAI | 22 |
| 4.5 Work package SA1 – Pilots on the Integrated AAI | 24 |
| 5 Conclusions | 28 |
| Annex I – About AARC2 | 29 |
| AARC2 Partners and Structure | 29 |
| AARC Target Audience | 30 |
| Annex II – Summary of Deliverables and Milestones | 31 |
| References | 34 |
| Glossary | 36 |

Table of Figures

| | |
|--|----|
| Figure 3.1: AARC-BPA at the start of AARC2 | 13 |
| Figure 3.2: AARC BPA 2019 | 14 |
| Figure 3.3: Community-first approach based on the AARC Blueprint Architecture. | 14 |
| Figure 4.1: Overview of AARC2 Pilots with research collaborations | 26 |
| Figure I.1: AARC work packages | 30 |
| Figure I.2: AARC work packages, AEGIS and CEF | 30 |

Table of Tables

| | |
|--|----|
| Table 2.1: Differences between AARC1 and AARC2 | 7 |
| Table 3.1: Summary of AARC2 results | 9 |
| Table 3.2: AARC2 KERs | 12 |
| Table 3.3: Summary of Guidelines produced by AARC2 | 16 |
| Table II.1: List of Deliverables in AARC2 | 32 |
| Table II.2: List of Milestones in AARC2 | 33 |

Executive Summary

The Authentication and Authorisation for Research and Collaboration project, AARC2, builds upon and further expands the work of the previous AARC1 project, focusing in particular on the areas related to championing federated access, supporting global policies, running pilots with research collaborations participating in AARC2, and promoting AARC results and ensuring their sustainability. In addition to its deliverables and milestones, AARC2 has also produced important output in the form of toolkits, policy templates, training modules and guidelines.

The work carried out in the specific areas of focus of the various project work packages, including management of the project (NA1), training and outreach (NA2), policy and best practices (NA3), AAI architecture (JRA1), and pilots (SA1), is described in detail in Chapter **Error! Reference source not found.** of this document.

Specifically, the key outputs of the AARC2 project are:

- The AARC Blueprint Architecture (BPA) which offers a standardised architecture to deploy AAI for research collaborations. The AARC BPA builds on top of eduGAIN and adds the functionality required to support common use cases within research collaborations. The current version of the BPA [[AARC-BPA-2019](#)] focuses on interoperability aspects to address an increasing number of use cases from research communities requiring federated access to resources offered by different infrastructure providers.
- A streamlined policy and security framework including templates, pilots and guidelines to support research infrastructures in the deployment and operation of their AAI particularly on those that follow the AARC BPA.

The AARC projects have created a community representing various parties, such as research infrastructures and e-infrastructures, Federation operators and service providers. The main goal of AARC to enable research collaborations to build an AAI with their preferred components, in such a way as to ensure interoperability, security and privacy, has been achieved.

AARC2 has proved to be very successful and to have considerable impact, particularly for a project of such a relatively small size and brief duration. AARC's legacy and key results will continue to be disseminated and promoted through the #StartWithAARC social media tag and its work carried on through the AARC Engagement Group for Infrastructures (AEGIS).

1 Introduction

This document provides an overview of the overall results of the Authentication and Authorisation for Research and Collaborations (AARC2) project that ran between 2017-2019, with particular focus on the work carried out in the second and final year of the project.

The goal of the AARC2 project was to expand the initial version of the Blueprint Architecture (BPA) developed during AARC1 to support a wider range of technical and policy requirements typical of research collaborations. In this regard, training and the pilots were very important auxiliary elements focusing on aspects relating to the BPA's deployment and on service providers operating within research collaborations and e-infrastructures.

These research collaborations and e-infrastructures, several of which were included as partners in the project, were the primary targets of AARC2.

This report is structured as follows:

- Chapter 2 – presents AARC2's objectives and outlines the main differences between the AARC2 and AARC1 projects, and how AARC2 expands on AARC1's results.
- Chapter 3 – presents AARC2' overall achievements and identifies its key exploitable results.
- Chapter **Error! Reference source not found.** – presents the work carried out in each work package.
- Chapter **Error! Reference source not found.** – summarises the impact of the project and presents some final conclusions.

2 Overview of AARC2

2.1 AARC2 Objectives

The Authentication and Authorisation for Research and Collaboration project, AARC2 (May 2017 – April 2019), builds upon and further expands the work of the previous AARC1 project (May 2015- April 2017). In this document, the AARC2 project will generally be referred to as AARC2; when referring to the previous project the term AARC1 will be used. When talking in more general terms about results, the term AARC may be used, covering both projects.

Specifically, the AARC2 project focused on the following objectives:

- **Championing federated access** – Promoting the use of federated access as the main means of access for eScience by addressing the technical and policy challenges involved.
- **Support global policies** – Developing key policy frameworks to minimise diverging policies and empower interoperable infrastructures.
- **Run pilots with research collaborations participating in AARC2** (and beyond as needed) – Supporting research communities to scope their requirements and deploy matching solutions based on the AARC Blueprint Architecture.
- **Promote AARC results and their sustainability** – AARC results have been promoted via presentations at relevant events where AARC stakeholders would be attending; blog posts and social media contributed to expand the reach. Sustainability aspects had been taken into account since the very beginning: AARC took the view that provisions for the operation of each AAI implementation resulting from the AARC pilots, would be the responsibility of the relevant research infrastructure. Sustainability and exploitation aspects are covered in “Summary of AARC2 Main Achievements and Sustainability and Exploitation Plans” deliverable [\[DNA1.3\]](#).

To learn more about AARC, please see the two-minute AARC video that was created during AARC1. [\[AARC video\]](#).

2.2 AARC2 – Finalising the Work of AARC1

The AARC1 project had the ambitious goal of defining a single architectural model to drive the implementation of AAI in different research collaborations and e-infrastructures. It was acknowledged that for AARC to succeed it would be essential to integrate such a model within the existing environment and adopt existing AAI components whenever possible. It was therefore decided that development would be limited to components that were missing and those related to integration aspects.

This work resulted in the first version of the **AARC Blueprint Architecture** [\[AARC-BPA-2016\]](#). The proposed BPA reflected the architectural patterns found in different research collaborations that were already operating AAI.

The AARC BPA was not only well received but started to play a significant role in the "standardisation" of AAI design among research collaborations. However, the timeline of the AARC1 project meant that it had only two years to engage the project partners as well as key players (research collaborations, e-infrastructures, federation operators and relevant service providers) and produce a model that would be accepted by all.

AARC2 continued the work started in AARC1, refining its scope and including the lessons learned in AARC1. **Two key aspects** in particular were strengthened in AARC2:

- Evolution of the AARC BPA – During AARC2, the AARC-BPA was further developed to expand both its technical and policy aspects and facilitate its deployment by providing guidelines, templates and training modules.
- Deployment of results – AARC2 worked directly with research collaborations participating in the project to pilot versions of the BPA customised to suit their needs; the lessons learned from the pilots informed the further development of the BPA and helped create a number of case studies featured on the 'AARC in Action' web page [[AARC in Action](#)]. The AARC Engagement Group for Infrastructures (AEGIS), initially named Competence Centre, was created to engage research and e-infrastructures and request that they consider endorsing AARC2 guidelines. This resulted in the creation of a forum to **discuss implementation details** and provide useful inputs to AARC2's work. Training and outreach were a key aspect towards achieving this goal.

AARC2 has also contributed significant effort to the **Community Engagement Forum** (CEF), which was proposed with the aim of strengthening engagement with research communities and implemented via [[FIM4R](#)]. Additional differences between AARC1 and AARC2 are highlighted in the table below.

| AARC1 | AARC2 |
|---|---|
| Focused on delivering an integrated AAI (AARC BPA), addressing core security and policy aspects and promoting federated identity management at large. | Focused on enhancing the AARC BPA and on expanding policy frameworks as well as offering guidelines to facilitate the deployment of the BPA. As the project was coming to an end, work was undertaken to identify key results and to make provisions for their sustainability. |
| Various types of pilots to understand which of the existing components would fit in the BPA. | Pilots focused on supporting research collaborations in deploying AAI compliant with the AARC BPA. |
| AARC1 recognised the value of policies and the need for security frameworks for the BPA. To this end, AARC1 developed Snctfi (Scalable Negotiator for a Community Trust Framework in Federated Infrastructures) [Snctfi] and contributed significant effort to Sirtfi (Security Incident Response Trust Framework for Federated Identity) [Sirtfi]. | In AARC2 policy work went further, delivering templates, guidelines and training and packaging it together in the AARC Policy Development Kit [PDK]. This helps research collaborations or e-infrastructures in adopting the policies that regulate the operation of an Authentication and Authorisation Infrastructure (AAI) built in line with the AARC BPA. In addition, this policy work also resulted in provision of guidelines on GDPR, accounting traceability and assurance. |
| Training focused on generic federated identity management concepts. | Training evolved to target service providers operating within research collaborations and e-infrastructures as well as AARC BPA and policy-related aspects. |
| Outreach – focus on AARC1 results and generic federated identity management concepts. | Outreach – Addresses AARC2 results and paves the way for the promotion and exploitation of results beyond AARC2 ('AARC in Action' and '#StartWithAARC'). |

| AARC1 | AARC2 |
|---------------|---|
| Not Available | AARC2 offers consultancy to research collaborations: the AARC2 team works with research communities to analyse their use cases, and derives technical and policy requirements and proposes the most suitable AAI architecture, which is then piloted in AARC2. This function was added after AARC1. |

Table 2.1: Differences between AARC1 and AARC2

3 Summary of AARC2 Results

In addition to deliverables and milestones, AARC2's important outputs also include toolkits, policy templates, training modules and guidelines. These are listed in Table 3.1

| AARC2 Output Produced (Y1 and Y2) | Addressed |
|--|--|
| 2 new versions of AARC BPA: AARC-BPA-2017 and AARC-BPA-2019 | <p>Expands the initial version of the AARC-BPA and offers a reference architecture for implementing an AAI that supports common use cases within research collaborations.</p> <p>The 'community-first' approach adopted focuses on interoperability across BPA-compliant AAls and provides a broader view for addressing an increasing number of use cases from research communities that require access to federated resources offered by different infrastructure providers.</p> |
| AARC Policy Development KIT [PDK] : <ul style="list-style-type: none"> • 9 Template policy documents • 2 Online training packages • 11 Policy-related guideline documents | <p>Offers policies that outline the operational measures undertaken by an infrastructure to properly offer services via an IdP/SP proxy. The policies principally cover security measures, user management and data protection.</p> <p>Addresses attribute release by requiring REFEDS R&S and security by requiring Sirtfi.</p> |
| Snctfi | <p>Supports a community or an infrastructure operating the proxy to assess the characteristics of service providers and of the (IdP-SP) proxies. By addressing the structure of the security policies that bind services 'hiding' behind the IdP-SP proxy, Snctfi allows comparison between proxies.</p> <p>It eases attribute release by research and education federations and ensures that service providers comply with the GDPR.</p> |
| Contributed to Sirtfi and produced reports on security incident simulations | Improves security and facilitates the trust building process across infrastructures. |
| Guidelines: <ul style="list-style-type: none"> • 26 Total guidelines, 11 in AARC2 • 9 Guidelines endorsed by AEGIS • 3 information documents | Support the deployment of the BPA by offering concrete guidance on specific technical and policy aspects. |
| 9 Pilots | Support AARC-BPA deployments in research and e-infrastructures. |

| AARC2 Output Produced (Y1 and Y2) | Addressed |
|--|--|
| Training Modules: <ul style="list-style-type: none"> • 2 OIDC training events • 2 training events for research collaborations (EPOS and Life Science) • PDK online training module • 3 Trainings on how to implement an IdP/SP proxy with SaToSa [TRAINING-SATOSA] • Sirtfi module | Support: <ul style="list-style-type: none"> • adoption of federated access, • deployment of the AARC BPA and related policy frameworks in production environments. |
| Videos and articles: <ul style="list-style-type: none"> • 32 blog post in total (16 in PY2) • 11 CONNECT magazine pages (6 in PY2) • 4 leaflets to disseminate AARC results (2 in PY2) • 2 Webinars • 4 short promotional videos on BPA, AARC in Action (pilot results) and PDK, plus 5 PDK content videos • 1 poster • Social media posts – in PY2: 46 Facebook, 29 LinkedIn, 79 Twitter | Ensure promotion and outreach. |
| AEGIS (AARC Engagement Group for e-Infrastructures) | Supports adoption of AARC results by AAI operators in research collaborations. |

Table 3.1: Summary of AARC2 results

3.1 Key Exploitable Results

In line with what was described in both AARC1 and AARC2 technical annexes, AARC results are better exploited by the research and e-infrastructures, which are best positioned to serve their constituency but also to operate infrastructures in the longer term. Both AARC1 and AARC2 projects took the view that no services would be operated within the project. This was a strategic choice given the temporary nature of the AARC projects and the need to ensure longer term sustainability. The exploitation aspects are discussed in more details in the deliverable DNA1.3.

Because of the very specific focus on AAI aspects within research infrastructures and the specific nature of AARC results, the consortium agreed to follow a non-commercial exploitation approach, based on the following principles:

- *Knowledge transfer*, based on the training modules and online documentation. All AARC1 and AARC2 material has been reviewed during the second year of the project to be used online as much as possible.
- *Community building*, AARC has built a community and has strengthened the relations with and between different research infrastructures and e-infrastructures. AARC2 has also explored synergies with other projects, like GN4-3, EOSC Pilot and EOSC-Hub, that will continue beyond AARC.

- *Research and development*, AARC videos and presentations have been widely promoted at relevant events, webinars and via social media. The material available provides the basis for further research and development activities.

AARC2's Key Exploitable Results (KERs) are shown in Table 3.2 below.

| KER | Description | Impact | Beyond AARC2 | Category |
|---|---|---|--|---------------------------------|
| AARC Blueprint Architecture (AARC BPA) | Provides a reference architecture to guide architects in research collaborations in building interoperable AAls. | The BPA has become the reference model for AAI among research and e-infrastructures worldwide. To date 13 research and e-infrastructures operate an AARC BPA-compliant AAI. EOSC-Hub AAI implementation is based on the AARC BPA. OpenAIRE and ESA are also considering the AARC BPA for their AAls. Some NRENs (currently SURF and Jisc) are considering the AARC BPA to manage their own services. | The BPA is currently hosted on the AARC website. After AARC2 is completed, the BPA will be hosted by AEGIS for future development and maintenance. Resources will be provided by GN4-3, EOSC-Hub projects and other by the research infrastructures participating in AEGIS. | Specification |
| Policy frameworks / 'PDK' | To better support research and e-infrastructures to deploy the AARC policy framework, AARC developed a Policy Development Kit [PDK] including training modules, templates, and documentation on how to adopt Sirtfi and Snctfi. | PDK is being used for the evolution of the e-infrastructure policy suites (e.g. in EOSC-Hub and WLCG), and is expected to become a useful instrument for new research collaborations that plan to deploy an AARC BPA-compliant AAI. The Baseline Acceptable Use Policy developed in AARC through the WISE community has been adopted by multiple infrastructures, at community, national and European levels. | The AARC PDK training module will remain on the GÉANT e-learning platform as well as on the AARC project website; further updates will be jointly supported by WISE, IGTF, GN4-3, EOSC-Hub projects and other interested parties. Sirtfi continues to be hosted and supported by the [REFEDS] Sirtfi Working Group. Snctfi is hosted by [IGTF] . | Specification / training module |
| Pilots results / 'AARC in Action' | Pilots were carried out in collaboration with | The pilots have been a very effective way to engage with different | The sustainability of the pilot results is out of scope for AARC2, as each | Documentation |

| KER | Description | Impact | Beyond AARC2 | Category |
|-------------------------|--|---|---|------------------|
| | research infrastructures to deploy an AARC BPA-compliant AAI. | research communities, and to validate the AARC BPA enhancements and the relevant guidelines, as well as to gain an insight on its deployment aspects. | <p>research infrastructure will decide how to exploit them based on their needs and resources. The lessons learned from the pilots have been turned into case studies and are available on the 'AARC in Action' web page [AARC in Action].</p> <p>The pilot results have been widely promoted at relevant events.</p> | |
| Training modules | Provide general information on key aspects of federated access; offer guidance on how to implement AAls and leverage AARC project results. | AARC2 delivered various training modules, some in the form of online courses, some more tailored to specific communities or aspects of the BPA, and others more for general purposes. | <p>All training modules will remain available via the AARC website.</p> <p>The possibility to build a training programme that spans beyond AARC2 was considered. It was however felt that the income would not be sufficient to secure the availability of trainers as well as to update the material and support any promotional or administrative activities. It was felt more important to ensure that as many interested people as possible could access the training modules and benefit from them free of charge.</p> | Training modules |
| AEGIS | Brings together research and e-infrastructures that operate an AARC BPA-compliant AAI to | At April 2019 there were seven infrastructures participating in AEGIS. | <p>AEGIS will continue some parts of AARC's work. An AEGIS website is under preparation.</p> <p>Research- and e-infrastructures</p> | Forum |

| KER | Description | Impact | Beyond AARC2 | Category |
|-----|------------------------------|--------|---|----------|
| | discuss operational aspects. | | <p>participating in AEGIS provide the effort for their key people to attend AEGIS Calls.</p> <p>The GN4 and EOSC-Hub projects have agreed to support AEGIS beyond AARC.</p> | |

Table 3.2: AARC2 KERs

3.2 The AARC Blueprint Architecture (BPA) and its Evolution

The AARC Blueprint Architecture (BPA) builds on top of eduGAIN and adds the functionality required to support common use cases within research collaborations, such as access to resources based on community membership. The AARC BPA champions a proxy architecture in which services in a research collaboration can connect to a single point, the SP-IdP-Proxy (hereafter termed “proxy”), which itself takes the responsibility for providing the connection to the identity federations in eduGAIN, thus reducing the need for each service having to separately connect to an identity federation/eduGAIN.

The first version of the AARC-BPA [[AARC-BPA-2016](#)] was published during the AARC1 project, with a further evolution published at the start of AARC2 [[AARC-BPA-2017](#)]. The current and latest version of the BPA [[AARC-BPA-2019](#)] also known as ‘community-first’ focuses on interoperability aspects to address an increasing number of use cases from research communities requiring access to federated resources offered by different infrastructure providers. Hence AARC’s ‘community-first’ approach, which introduces the Community AAI. The purpose of the Community AAI is to streamline researchers’ access to services, including those provided by their own infrastructure as well as services shared by other infrastructures. Specifically, according to the community-first approach, three types of services can be connected to the Community AAI:

- Community services – provided to members of a given community only.
- Generic services – provided to members of different communities.
- Infrastructure services – provided by a given research infrastructure or e-Infrastructure to one or more Community AAIs (typically through a dedicated infrastructure proxy).

Authorisation aspects were investigated extensively by analysing of the authorisation architectures from nine different use cases [see [AARC2-DJRA1.2](#)]; three main authorisation models have been identified in [[AARC-I047](#)] that make use of an SP-IdP-Proxy:

1. Centralised Policy Information Point: the proxy aggregates user attributes, such as group membership information and roles, and makes them available to the end-services.
2. Centralised Policy Management and Decision Making: the proxy conveys the authorisation decision to the end-services in the form of capabilities.

3. Centralised Policy Management and Decision Making and Enforcement: the proxy enforces the decision directly at the proxy.

Assurance was an important area of investigation as well. The problem of combining assurance information associated with one or more external identities linked to the community identity is addressed in a dedicated guideline [\[AARC-G031\]](#).

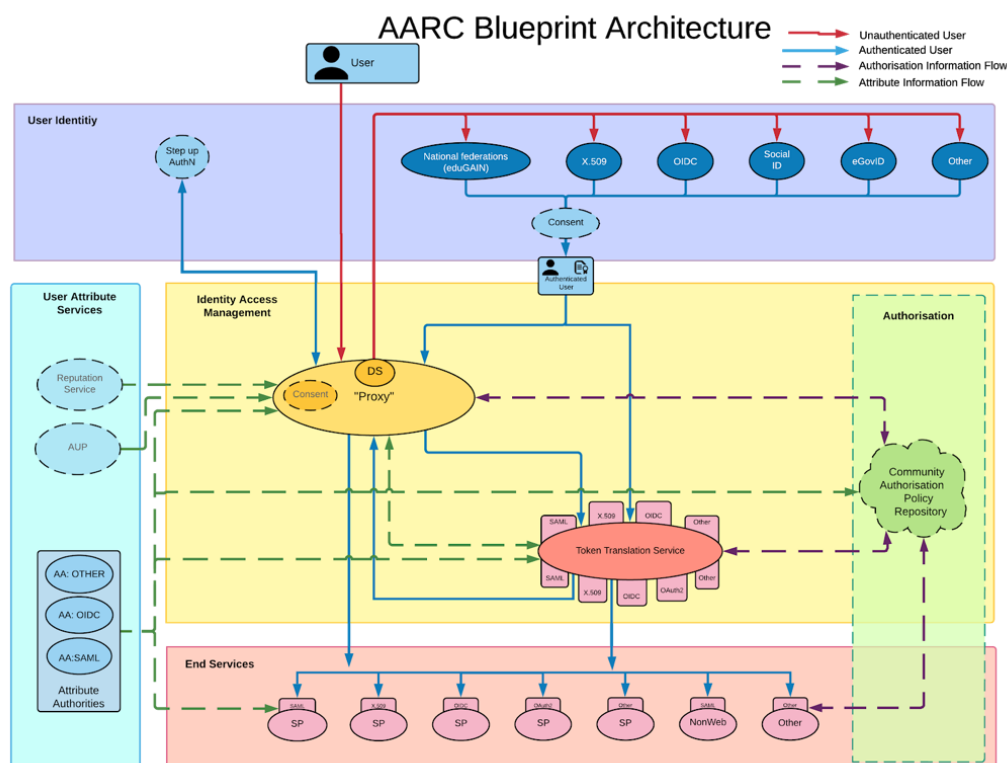


Figure 3.1: AARC-BPA at the start of AARC2

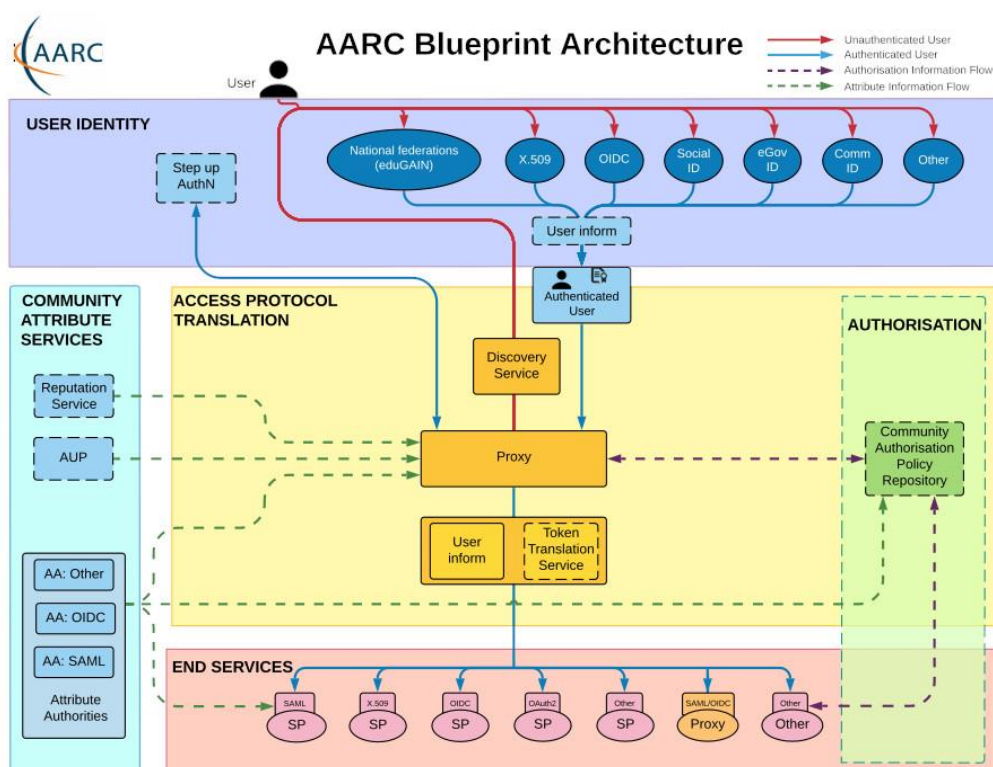


Figure 3.2: AARC BPA 2019

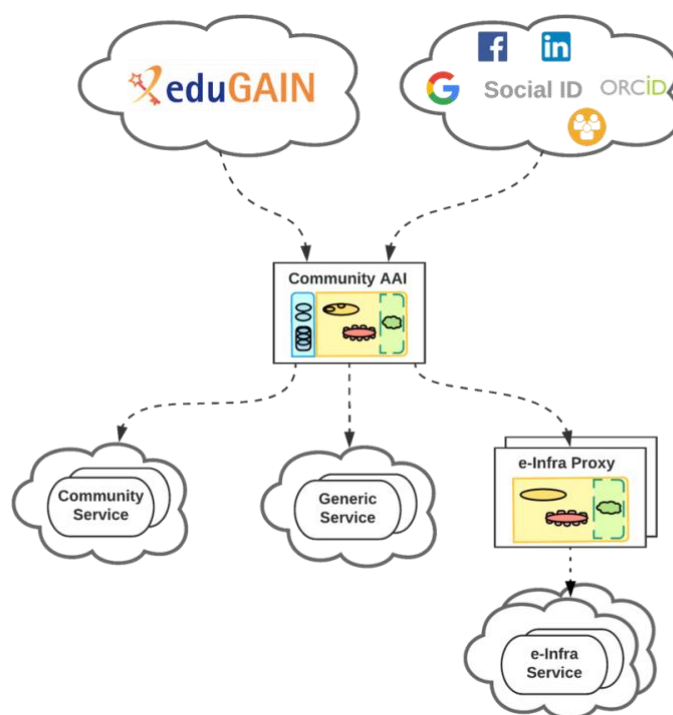


Figure 3.3: Community-first approach based on the AARC Blueprint Architecture.

3.3 The Role of AEGIS in AARC2 and beyond

The AARC Engagement Group for Infrastructures (AEGIS) brings together representatives from research and e-infrastructures, operators of AAI services and the AARC team to bridge communication gaps and make the most of common synergies. Participation in AEGIS is limited to those research collaborations and e-infrastructures that are already operating or piloting an AARC-compliant BPA. The AEGIS group enables AARC to:

- Consult the expertise of participants for feedback on project activities.
- Showcase project results.
- Promote a consistent vision for federated access.
- Facilitate activities that help different infrastructures adopt the AARC results in their production environments.

AEGIS played an important role in validating AARC2 results and helping towards their adoption. By the end of the project, the membership of AEGIS included the AARC2 Work Package leaders and two representatives from each of the participating infrastructures, namely, GÉANT, EUDAT, EGI, Lifescience, PRACE, XSEDE and DARIAH.

As more infrastructures are adopting AARC results, the membership of AEGIS is expected to expand. AEGIS continues beyond the AARC2 lifespan and the aim is to make AEGIS more open whilst ensuring that discussion items on operational AARC-BPA related deployments remain one of the priorities. At the time of writing a charter and an AEGIS website are under preparation. Further work on the AARC BPA and on the guidelines will be hosted by AEGIS, but feedback will be gathered also outside AEGIS.

AEGIS holds a video conference every second Monday of each month. The agenda of each meeting includes potential new guideline documents that might have come out of the project, updates from the work packages regarding recent and upcoming work and discussion items relevant to the AAI interoperability between the infrastructure operators.

An "AEGIS Brief" is compiled and distributed two weeks before every meeting, to allow the infrastructure operators to consult their internal technical and policy experts before deciding whether to adopt the new AARC guidelines and introduce them in their production environments. If a guideline includes operational recommendations, then AEGIS is asked to endorse it. By endorsing the recommendation, the AEGIS members agree to conform to that in the near future. Not all recommendations are meant for endorsement; they may be however shared with the AEGIS group for information. More recently AARC2 produced information documents, that are white papers on specific topics; these are not meant to be endorsed.

| Summary of Guidelines | Document status |
|--|---|
| Guidelines on expressing group membership and role information (updated version produced in AARC2) – [AARC-G002] | Nov 17 (PY1) - endorsed by AEGIS |
| Exchange of specific assurance information between infrastructures – [AARC-G021] | March 2018 (PY1) |
| Guidelines for expressing affiliation – [AARC-G025] | Presented at AEGIS meeting in April 2019 – under approval |

| Summary of Guidelines | Document status |
|--|--|
| Guidelines for expressing resource capabilities – [AARC-G027] | December 2018 |
| Guidelines on stepping up the authentication component in AAls implementing the AARC BPA – AARC-G029 | March 2018 (PY1) |
| Guidelines for evaluating the combined assurance of linked identities – [AARC-G031] | May 2018 |
| Preliminary Proxy Policy Recommendations (application to the Life Sciences AAI) – [AARC-G040] | Not sent to AEGIS – community specific guideline |
| Expression of REFEDS RAF assurance components for identities derived from social media accounts – [AARC-G041] | March 2018 |
| Data Protection Impact Assessment - an initial guide for communities - [AARC-G042] | Not sent to AEGIS |
| Specification for IdP hinting – [AARC-G049] | March 2019 |
| Guidelines for Secure Operation of Attribute Authorities and other issuers of access - granting statements – [AARC-G048] | Endorsed by IGTF |
| Implementers Guide to the WISE Baseline Acceptable Use Policy [AARC-I044] | February 2019 – presented to AEGIS for information |
| Implementing scalable and consistent authorisation across multi-SP environments - Informational doc [AARC-I047] | March 2019 – presented to AEGIS for information |
| Guide to Federated Security Incident Response for Research Collaboration [AARC-I051] | March 2019 – presented to AEGIS for information |

Table 3.3: Summary of Guidelines produced by AARC2

4 Activities by Work Package

The specific activities carried out by the Tasks in each Work Package are described in the sections that follow. The lead organisation for each task is shown in **bold**.

4.1 Work Package NA1 – Project Management and Sustainability

Task 0 - Management

(GÉANT, CERN)

The work of this task focused on supporting various teams to deliver the required outcomes according to project plans. The task managed the AARC2 general meetings and specific meetings with the task leaders and work packages leaders. The task defined the AARC remit and strategic directions and worked closely with the NAs on outreach and results dissemination. This task also supported:

- The Project Board, which met three times per year.
- The Project Management Team (PMT), consisting of the WP leaders – monthly calls with the PMT took place to synchronise the work.
- Periodic project reviews.
- Tools to support the team's day-to-day work (wiki, mailing lists, website etc.).

Task 1 - Finance and Administration

(GÉANT)

Defined reporting procedures and oversaw expenditures.

Task 2 - Global Liaisons

(GÉANT)

Managed liaisons with the EC, other projects and other relevant stakeholders. The AARC2 project worked closely with:

- GN4-2/GN4-3 in the area of OIIC and testing Sirtfi procedures in simulated security incidents.
- REFEDS, in the area of Sirtfi.
- REFEDS and IGTF in the area of assurance specification (the REFEDS assurance WG was created to expose the AARC discussion to a wider audience).
- EOSC pilot project, to provide general support on the AAI architecture.

- EOSC Hub project, to promote adoption of AARC results.
- EC meeting and relevant activities as needed

The task also defined the engagement strategies with relevant initiatives and projects in Europe and beyond. The AARC BPA has been promoted in the US as well as Australia.

Task 4 - Sustainability, Dissemination and Exploitation

(GÉANT, CERN, Reti and DAASI)

The Task identified key exploitable results and, in collaboration with other work packages, defined approaches to ensure these can be maintained beyond the project lifetime. Effort was also allocated to CERN, as well as to RETI and DAASI (the two SMEs involved in the project) to support this work. More information on these activities can be found in the deliverable *Summary of AARC2 Main Achievements and Sustainability and Exploitation Plans* [[DNA1.3](#)].

4.2 Work Package NA2 – Training and Outreach

This WP promoted AARC work and developed and delivered the necessary training modules. The work carried out in NA2 was organised in three tasks. This work package was initially led by GÉANT, but in July 2017 it was agreed to transfer the leadership to Reti.

Task 0 – WP Leadership

(Reti)

Coordination of the activity.

Task 1 – Outreach and Communication

(GÉANT, EGI, LIBER, GARR, DAASI, MKZ)

- Maintained, updated and restructured the project website to showcase project activities and results and to engage with new communities and researchers.
- Supported overall dissemination and communication activities, via case studies (in collaboration with the pilot work package), news and online information.
- Managed the **AARC Engagement Group for Infrastructures** (AEGIS) which supports the adoption of AARC results in research collaborations and e-infrastructures.
- Supported communication and dissemination activities around FIM4R, which is to date the broadest global group where federated identity is discussed among research organisations. AARC2 sponsored key people to attend FIM4R meetings and contribute to effort to produce a second FIM4R white paper. The first paper described the challenges for international research collaborations in deploying federated access and provided a list of recommendations on how to solve them.
- Provided support for the production and dissemination of AARC news and materials across AARC and its partners' channels. The AARC2 team produced 32 news blogs, 9 articles in the GÉANT CONNECT Magazine, 1 article published by GARR and 1 article published by EGI. Four leaflets, a poster and

support to two webinars were provided. Videos to promote the BPA, PDK and AARC in Action were produced.

- Supported the dissemination of AARC2 results via partner channels including newsletters, blog sites, YouTube and social media channels (Facebook, Twitter, LinkedIn).

Task 2 – Training

(GARR, DAASI, CERN, GÉANT, RETI, KIT, MKZ)

- Collected inputs to scope training activities following 6-month update cycles.
- Delivered several training events:
 - OIDC Primer, Rome (in collaboration with GARR), 27 June 2017
<https://eventr.geant.org/events/2694>.
 - OIDC Primer, Rome (in collaboration with GARR), 5 July 2017
<https://eventr.geant.org/events/2698>.
 - [Training for EPOS](#), Lisbon, 14 March 2018.
 - [Training for Life Sciences](#), Munich, 23-24 April 2018.
 - [Hands-on training on Satosa](#) (September 2018, November 2018, April 2019)
 - [Online module for the Policy Development Kit](#) (January 2018) in collaboration with NA3.
- Enriched and updated the training material collection and testimonials for the training section of the AARC website [[AARC-Training](#)].

4.3 Work Package NA3 – Policy and Best Practices Harmonisation

The main focus of this WP is to provide the necessary policy support to those infrastructures that are implementing an AARC BPA-compliant AAI, and to the use cases and pilots in SA1. This WP offers a very effective way to ensure that best practices and relevant policy frameworks are followed when the AARC BPA is deployed. The WP also provides consultancy to those infrastructures that require it and takes care of global policy liaison activities. The work carried out in NA3 is organised in four tasks.

Task 0 – WP Leadership

(Nikhef)

Coordination of the activity.

Task 1 – Operational Security and Incident Response

(CERN, KIT, Nikhef)

The Operational Security task comprised two complementary elements: extending the work on Sirtfi to ensure a coherent operational security capability in both federations and research collaborations; and providing guidance on operational security for the operational elements established by communities for their collaboration:

- Work continued on consolidating the Sirtfi incident response model (communications and mitigating actions) developed in AARC1 by simulating actual incidents. The AARC2 project has benefited from the Blueprint Architecture (BPA) and the increased engagement with user communities to strengthen the collective security posture of the community. The extension of the Sirtfi concept to areas where, for various reasons, organisations cannot join the scheme through their Identity Federation metadata services has been addressed through the Sirtfi Registry concept.

This is supported by the REFEDS [[REFEDS](#)] Sirtfi working group with support from research communities and infrastructures in joint discussions with eduGAIN [[eduGAIN](#)] and federation operators. To validate the model, and to foster operational readiness in the community at large, two security incident exercises were conducted (in March 2018 and a second one in December 2018) both reported in [[DNA3.2](#)].

The report showed that *Sirtfi* in itself is working; points for improvement suggested in the report included the need for federation (not identity-provider level) security contacts and enhancement of the eduGAIN central response capabilities. The proposed best practice was released as a white paper [[AARC-I051](#)] following the second exercise. Since incident response requires collective action across many infrastructures, institutions, and communities – and many of these are performing such communications or readiness challenges – AARC took the initiative for a Security Communications Challenge Coordination working group (SCCC-WG) in the context of WISE, an initiative that was well received in adjacent communities such as the GÉANT Special Interest Group on Information Security Management [[SIG-ISM](#)], REFEDS, and the IGTF.

- In the BPA model, the integrity of the Attribute Authorities and their community membership content is as important as the security of the identities themselves, since access to services is predominantly based on the community membership and roles. Leveraging work of and in collaboration with the IGTF, AARC developed the “*Guidelines for Secure Operation of Attribute Authorities (and other issuers of access-granting statements)*” [[AARC-G048](#)] with configuration and management criteria for secure operation of membership management services by communities. Bearing in mind that communities are likely to use resources across many infrastructures, including those who use access models different from the BPA proxy (e.g. based on direct access to services by users), the guidance addresses both the push and pull models for attribute authorities.

Task 2 – Service-Centric Policies

(KIT, Jülich, Nikhef, STFC)

The need to aid service providers in aligning and harmonising policy was identified already earlier in the project as going beyond supporting the exchange of accounting and ‘bare’ traceability data. Consequently, the service-centric policy activities in task 2 focussed on policy mapping and assessment between collaborating infrastructures and their service providers, supporting them in the exchange of necessary personal data that were collected as a result of the use of services and infrastructure, and targeted guidance for operators of proxies and community infrastructures:

- In addition to the guidance for communities on determining the impact of processing of data by services, guidance was provided on how this applies to proxy and AA operators [[DNA3.2](#)]. The processing basis of legitimate interest was confirmed to be appropriate for processing of data in the proxy and BPA context (and is also the model used by the GÉANT Data Protection Code of Conduct).

- Leveraging the WISE SCI version 2 framework [[WISE-SCIv2](#)] (endorsed by a global range of Infrastructure stakeholders - including EGI, EUDAT, GÉANT, GridPP, HBP, MYREN, PRACE, SURF, WLCG, and XSEDE – an assessment framework was developed to support infrastructures in cross-assessing their ‘policy compatibility’. Based on a consultation process in WISE and the IGTF, a mechanism introducing four maturity levels was decided on that can support a (peer-reviewed) self-assessment. The peer review model, which in a multi-domain distributed infrastructure is more appropriate than conventional information security assessment models that focus on single administrative control like ISO27001, was documented in the WISE SCI WG based on the work from this task.
- Policy guidance for service providers was developed and contributed to the Policy Development Kit [PDK] (further described under the *engagement* task no. 4).

Task 3 – e-Researcher Centric Policies

(STFC, BBMRI, EMBL(CSC), KIT, Nikhef, STFC)

The work of Task 3 focused on the following activities:

- The ‘researcher-centric’ policy work addressed the evolution of the identity assurance profiles and the relationship of assurance frameworks for identity-provider driven profiles, profiles targeted at services and infrastructures, and assurance frameworks from adjacent and complementary domains (such as the Kantara Initiative, or the eIDAS scheme).
- The REFEDS Assurance Framework [[RAF](#)] profiles were also assessed for applicability to highly-sensitive research use bases from the medical domain (especially for human bio-banking), the use cases identified previously in the AARC2 project in need of high-assurance identities. The REFEDS assurance profiles were adapted (in conjunction with the authenticator profiles developed in the GEANT project) and are being gradually deployed for infrastructures (also globally e.g. for CILogon)
- The general complexity of identity assurance mapping (which is also evidenced by the traditional delay in the adoption of such frameworks in the R&E community) was investigated by performing a component-based assurance mapping between the four most prevalent frameworks in Europe: two from the R&E and Infrastructure community (REFEDS RAF and the IGTF Generalised Assurance Profiles), and two from other sectors (Kantara IAF and eIDAS). The eminent complexity and the mapping of vetting elements between these frameworks was untangled in the white paper [[AARC-I050](#)].
- The Acceptable Use Policies [[AUP-Study](#)] comparison study was completed and consensus built around a (global) Baseline AUP by means of the WISE community. The WISE Baseline AUP [[WISE-AUP](#)], a 10-commandment list of key elements which can be augmented by specific requirements from infrastructures and communities, was developed with strong AARC input and has been endorsed by several research infrastructures. In addition, AARC provided implementation guidance [[AARC-I044](#)] on how to incorporate the Baseline AUP and complementary privacy and transparency notices for community-first and user-firm BPA proxy services.
- In close collaboration with the EGI-ENGAGE and EOSC-HUB projects, community framework policies were developed and contributed to the Policy Development Kit (described under Task 4 below).

Task 4 – Policy Development Engagement and Coordination

(STFC, CERN, EMBL (CSC), KIT, Nikhef, Jülich)

A 'Snctfi-complete' Policy Development Kit [\[PDK\]](#) was developed that will act as a repository for infrastructures and communities of current best practice and policy templates. It brings together the experience from established infrastructures, the BPA architecture, and novel guidance from the service-centric, researcher-centric, and operational security developments in a suite of documents that can be adopted (and in some cases used as a template) for all infrastructures. The PDK is accompanied by a training course (developed with the NA2 activity) on how to best apply the PDK to a new Infrastructure.

The FIM4R (Federated Identity Management for Research, see fim4r.org) community, with the input from the AARC project, produced a comprehensive new white paper [\[FIM4Rv2\]](#), which both details the achievements of the federated access mechanisms for research collaboration achieved up till now and, more importantly, sets out the requirements and recommendations to drive further FIM adoption by an even broader (and now global) set of communities in the coming period. Fourteen research fields (and over 50 communities) aligned and provided collective recommendations to the FIM community in five key areas: governance, user experience, operational security, harmonised proxy operations, and sensitive research confidentiality. With its broad reach to communities, FIM4R is also an essential mechanism for the Community Engagement Forum.

The task also supported harmonisation of all AARC outputs through the Guidelines mechanism (now extended to include Informational documents and white papers), which makes policy (and technical) recommendations easier to locate, re-use and apply.

4.4 Work Package JRA1 – Architecture for Integrated and Interoperable AAI

Task 0 – WP Leadership

(GRNET)

Coordination of the activity.

Task 1 – Tools and Services for Interoperable Infrastructures

(EGI, GARR, KIT, GRNET and NIKHEF)

The work of Task 1 focused on the following activities:

- The task evolved the AARC Blueprint Architecture (BPA), while retaining its compatibility with the previous version [\[AARC-BPA-2017\]](#). The new version of the BPA [\[AARC-BPA-2019\]](#) retains the same five layers, each of which includes one or more functional components, grouped by their complementary functional roles. The User Identity Layer, the End Services Layer and the Authorisation Layer are still there, while the User Attribute Services Layer has been renamed Community Attribute Services Layer and the Identity Access Management Layer has been renamed Access Protocol Translation Layer and retains its prominent role in the architecture. Within the Access Protocol Translation Layer, the layout of the Token Translation Service (TTS) has been updated to better visualise the role of the TTS in the flow of attributes between the proxy and the connected services.
- In the context of the evolution of the BPA, the task focused on the interoperability aspects to address an increasing number of use cases from research communities requiring access to federated resources

offered by different infrastructure providers. Hence the “community-first” approach adopted by AARC, which introduces the Community AAI. The purpose of the Community AAI is to streamline researchers’ access to services, both those provided by their own infrastructure and those shared by other infrastructures.

- In the context of the interoperable expression of user attributes, the task looked into the representation of affiliation information. Two different types of affiliation were 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. The attributes for expressing these two types of attributes are specified in a guidelines document [[AARC-G025](#)], which was submitted to AEGIS for endorsement in April 2019. The document also covers the expression of the freshness of affiliation information through the use of assurance attributes that extend the REFEDS Assurance Framework [[RAF-v1.0](#)].

Task 2 – Service Provider Architectures and Authorisation in Multi-SP Environments

(KIT, GRNET, NIKHEF, EGI, PSNC, DAASI, STFC, JUELICH and CESNET)

The work of Task 2 focused on the following activities:

- Based on the analysis of the authorisation architectures from nine different use cases detailed in [[AARC2-DJRA1.2](#)], the task identified three main authorisation models that make use of the SP-IdP-Proxy:
 - Centralised Policy Information Point – the proxy aggregates user attributes, such as group membership information and roles, and makes them available to the end-services;
 - Centralised Policy Management and Decision Making – the proxy conveys the authorisation decision to the end services in the form of capabilities;
 - Centralised Policy Management and Decision Making and Enforcement – the proxy enforces the decision directly at the proxy.

These common models have been used as the basis for providing guidance for managing access across large groups of Service Providers in a consistent, secure and scalable manner, as detailed in the informational document [[AARC-I047](#)], which has been endorsed by AEGIS.

- The task provided 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 authorisation information in a compact form. This specification is defined in the guidelines document [[AARC-G027](#)], which has also been endorsed by AEGIS.
- The task defined a portable and technology-agnostic way to allow services to receive hints about which identity provider to use. This mechanism (termed “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. The IdP hinting specification is defined in another guidelines document [[AARC-G049](#)] endorsed by AEGIS.

Task 3 – Models for the Evolution of the AAI for Research Collaboration

(GARR, GRNET, JUELICH, KIT, STFC, CESNET)

The work of Task 3 focused on the following activities:

- The task looked into best practices for integrating OpenID Connect (OIDC)- and OAuth2-based services, focusing on the expression of user- and community-related information through claims, as well as the different flows (web-based and non-web-based) for supporting R&E use cases. This work was served as input to the newly established OpenID Research & Education working group [[OIDC-RANDE](#)], which is expected to provide specifications for: an OpenID Connect Research and Education Profile; OpenID Connect Research and Education Claims; and an OpenID Connect Entity metadata extension.
- The task provided practical guidance for the implementation of the assurance evaluation methods and compensatory controls that were defined in a guidelines document [[AARC-G031](#)] during PY1. These methods support the evaluation of combined assurance in the case of identity linking and provide guidelines for assessing assurance component values in the absence of assurance information from external identity providers.

Task 4 – Scalable VO Platforms

(STFC, CESNET, EGI, GARR, GRNET, KIT, NIKHEF, SURFnet)

Infrastructures offer a variety of services to enable scientific collaborations for their user base. These infrastructures make use of Virtual Organisation (VO) platforms to improve scalability and reduce the effort required to support these users. Via the VO, an infrastructure can manage a group of users (such as those working on a common project) by interacting with the VO manager (or other appointed people) rather than interacting with users individually. Similarly, the resources allocation can be brokered by the VO, instead of micromanaging resource allocations to individual users.

In deliverable [[AARC2-DJRA1.3](#)], the task provided a list of recommendations pertaining to the VO lifecycle, its operations and the management of attributes by VO platforms.

4.5 Work package SA1 – Pilots on the Integrated AAI

The main objective of this WP was to support research collaborations and e-infrastructures participating in AARC2 to pilot the deployment of the AARC BPA and offer a neutral environment for research and e-infrastructures to test interoperability use cases. The work package also supported service delivery pilots to enable research communities to design and choose an infrastructure provider that can deliver AAI services following the AARC BPA. A significant part of this work is paving the way for work that has now started in the EOSC context.

The work in this WP was organised in 4 tasks.

Task 0 – WP Leadership

(SURFnet)

Coordination of the activity.

Task 1 – Pilots of Solutions with Research Communities

(GARR/GRNET, CSC, KIT, NIKHEF, PSNC, SURFnet, LIGO, EPOS, CTA, CERN, ELIXIR, INSTRUCT, INFRAFRONTIER, BBMRI, DAASI, EISCAT3D, LIFEWATCH)

Before the start of AARC2, eight research community use cases were selected to be piloted in SA1. A ninth use case (DARIAH) was added during Y1, given the involvement of some DARIAH key people in other AARC2 work packages and the similarity of requirements with other research infrastructures. Although the use cases are specific to each community, the common theme for this group of pilots is the implementation of AAI in line with the AARC BPA. Each research community already had some form of AAI in place, with which they offered data or services to their users, but at varying levels of maturity. The AARC BPA offered the additional functionalities they were looking for and offered a more standardised solution to their use cases, which were needed to enable them to handle their growing numbers of users.

To accomplish the goal of building, testing and implementing a pre-production AAI for each community, four different phases were identified, (1) requirements analysis, (2) implementation, (3) testing and (4) finalisation:

1. **Analysis:** During this phase, the AARC team interviewed representatives of each research community to gather requirements and translate them into a specific AAI architecture, based on the AARC BPA.
2. **Implementation:** During this phase, the research communities, with help and advice from the AARC team, built a proof-of-concept AAI based on the design agreed upon in the previous phase.
3. **Testing:** Keeping in mind that all results of the AARC2 project should conform to ‘Technology Readiness Level 8 (TRL8)’, during this phase the pilot infrastructure was tested in a production setting, with (some) actual production SPs and users. Already existing tools and services were tested against the proof-of-concept AAI as well as existing and new workflows.
4. **Finalisation:** During this phase, the focus was on producing all the necessary documentation that is valuable to the research communities in AARC, but also beyond AARC. Other research communities should also be able to benefit from SA1’s work where they intend to build their own AAI.

All pilots were concluded as far as AARC2 was concerned. This however does not mean that the piloted solutions have been moved to production in all cases; each research infrastructure will need to secure skills and manpower to maintain their new AAI and this may take longer in some cases.

Each community gained much valuable knowledge on AAI technologies, the added value on using an IdP-SP proxy, how to deploy such a proxy, and the key policy aspects that should be addressed to guarantee security without impacting the user experience, and in most of the cases will be able to continue work on their AAI without further need for AARC’s support. The AARC2 team will however remain available to answer generic questions.

The results of each research community pilot and their current status have been summarised in deliverable ‘How to deploy pilot results’ [DSA1.5].










| Community | Links | Topics/Focus | Status |
|---|--------------------------------------|---|-----------|
|  | | Connecting services & Brokering Leverage the work done by AARC on policies and architectural blueprints Implementing Sirtfi Using eduGAIN | CONCLUDED |
|  | EISCAT_3D AAI | Move away from IP based access towards federated AAI according to the AARC BPA | CONCLUDED |
|  | EPOS European Plate Observing System | Evolve current AAI towards one that is fully compliant with AARC BPA; support cross infra use cases with EGI/EUDAT/PRACE and delegated federated access (non-interactive) workflows | CONCLUDED |
|  | CTA Cherenkov Telescope Array | Initial implementation of Community IdP/SP proxy, Group/Role based access to resources, SIRTFI and CoCo/GDPR compliance | CONCLUDED |
|  | LifeWatch AAI | Implementation of AAI according to the AARC BPA; access for citizen scientists | CONCLUDED |
|  | CORBEL LifeSciences AAI | Inter compatibility, share a common AAI shaping according to the ideas in Elixir. Also focus on sustainability and operational aspects | CONCLUDED |
|  | WLCG Worldwide LHC Computing Grid | Implementation of IdP/SP Proxy, mainly to provide Token Translation Services to allow end users to login without the need of manually managing X.509 certificates | CONCLUDED |
|  | LSC Ligo Scientific Collaboration | Implement AAI according to AARC BPA | CONCLUDED |
|  | DARIAH AAI | Implementing an AAI according BPA to allow communication between DARIAH and other infrastructures | CONCLUDED |

Figure 4.1: Overview of AARC2 Pilots with research collaborations

Task 2 – Pilots with Infrastructures

(EGI, CESNET, DAASI, EGI, NIKHEF, SURFnet)

The focus of this task was on piloting AAI components and frameworks to enable transparent interoperability between infrastructures in terms of authentication and authorisation.

To accomplish this, JRA1 and NA3 provided recommendations that were tested by the task.

After Y1, the work of this task merged with that of Task 3 (detailed below) and focused on the Life Science AAI pilot.

Task 3 – Piloting Advanced Use-Cases and New Solutions

(GRNET, CESNET, DAASI, GARR, GRNET), KIT, NIKHEF, SURFnet):

The initial expectation as indicated in the AARC2 DoW was to investigate advanced AAI scenarios by setting up a feedback loop with JRA1 and NA3. However, it soon became evident that it would be impossible to draw a clear demarcation line between the various use cases and pilots. Once the Life Science use case was further

detailed, it emerged that the intent was to pilot a solution for a single production AAI for all Life Science communities, specific characteristics that made this pilot unique and very advanced:

- The Life Science communities joined forces and agreed to deploy a community-specific AAI (LS-AAI) that implements the AARC BPA, hence a single AAI that serves many life science collaborations.
- The Life Science communities also agreed to ask e-infrastructures to operate the resulting AAI piloted in AARC2; after reviewing the AAI requirements for this community, the EGI, EUDAT and GÉANT e-infrastructures (who are also either directly participating in or are represented in AARC) responded with a joint proposal. This is the first case of AAI offered as a service.
- The Life Science AAI implements the AARC BPA in a multi-operator context, as various components of the BPA (that is, token translation services, discovery, group management, and IdP-SP proxy) are implemented by three different e-infrastructures (EGI, EUDAT and GÉANT). This also demonstrates that the AARC BPA can be deployed in different ways.
- The pilot carried out in AARC2 resulted in a collaboration between EGI, EUDAT and GÉANT to jointly deliver an AAI based on the AARC BPA. Lessons learned and additional information on this pilot can be found in the deliverables *Final Results of Pilots for Advanced Use Cases and Technologies* [DSA1.4] and *How to Deploy Pilot Results* [DSA1.5]. The work to move from a pilot to a production AAI continues as part of the EOSC-Life EC-funded project that started in March 2019.

Task 4 – Creation of Showcases, Deployment Scenarios and Documentation

(Reti, DAASI)

One of the lessons learned from the AARC1 project was that clear documentation was not always provided for pilots once these were concluded, making it difficult to showcase results. In AARC2, this aspect was addressed from the start, and technical documentation, case studies, training and general-purpose leaflets were produced for each pilot. In line with the AARC2 strategy and as indicated in the AARC2 Description of Work (DoW), the sustainability of the AARC2 pilots rests with each research and/or e-infrastructure, which have to make the necessary provisions.

Nevertheless, materials have been produced to showcase the work done within AARC to give other research communities a head start. More information about this can be found on the [[AARC In Action](#)] page of the AARC website and in deliverable DSA1.5.

The task also worked closely with the training team to provide inputs for delivering training to the research communities in AARC2.

5 Conclusions

At the end of its lifetime, the AARC2 project has achieved all objectives described in its DoW, and in many cases has delivered beyond what was originally proposed. Most project deliverables were submitted on time or with a small delay due to the need to reach consensus on specific topics within the project consortium but also externally with the wider community.

AARC has been instrumental in creating a community representing various parties, including research infrastructures and e-infrastructures, federation operators and service providers. The resulting collaborative approach as well as the use cases provided by the research collaborations, were fundamental in enabling the progress of the work and ensuring that AARC was able to maintain a neutral and independent approach.

The AARC projects have successfully achieved their goal of enabling research collaborations to build an AAI with their preferred components, while ensuring their interoperability, security and privacy. Each proposed solution was validated via AEGIS and was based on the feedback of actual users that will be applying AARC's results in their environments. AARC results are being used by several research collaborations to shape their next generation AAI as well as by relevant EC-funded projects such as EOSC-Hub, OCRE and others.

Overall, AARC2 has proved to be very effective and has had a considerable impact, especially in relation to its limited size and duration.

The key outputs of the AARC2 project can be summarised as follows:

- Its standardised AAI architecture (AARC BPA) that is helping research and e-infrastructures deploy interoperable AAI. This architecture has proved to be agile; it is technology agnostic and it can be implemented by a single operator or by multiple operators.
- A streamlined policy and security framework that provides templates and guidelines to support research infrastructures in the deployment and operation of their AAI.

Pilots, training and dissemination activities were instrumental in developing the AARC BPA and policy framework further. Via the Life Science AAI (LS-AAI) pilot that paved the way, research communities have started to consider the possibility of outsourcing their AAI operations to e-infrastructures (EGI, EUDAT and GÉANT) whilst still retaining control of their policies. This model has the benefit of shifting the operational aspects to a party that already has the required capabilities, so that a research collaboration adopting it would not need to add extensive resources to manage their AAI.

Following the close of the project, AARC's work will be carried on via AEGIS and continue to be promoted with the #StartWithAARC social media tag, so that more research collaborations may benefit from it in future.

Annex I – About AARC2

AARC2 Partners and Structure

The AARC2 project ran from 2017 until 2019 and comprised 25 partners including NRENs, e-infrastructures, research service providers, SMEs and libraries, with GÉANT as project lead, specifically:

- **Five NRENs** with significant expertise in operating identity federations and all participating in eduGAIN (CESNET, GARR, GRNET, PSNC, and SURFnet).
- **e-Infrastructure service partners** including EGI.eu, FOM-NIKHEF, INAF, CERN, STFC, KIT, CYFRONET, Jülich, BBMRI, EMBL, INSTRUCT, Infrafrontier and EISCAT.
- **Partners representing international research collaborations:** Univ. of Cardiff (LIGO), Univ. of Cantabria (LIFE Watch).
- **Two libraries** organisations: LIBER and their partner MZK.
- **Two SMEs:** DAASI and RETI.
- The project was organised in five work packages (WPs):
 - **Management (NA1):** To provide all the necessary tools, processes and procedures to ensure the smooth operation of the project.
 - **Training and Outreach (NA2):** To manage dissemination, training and outreach for knowledge transfer within and beyond the AARC2 project.
 - **Architecture (JRA1):** To enhance the AARC BPA delivered in AARC1 with authorisation and assurance aspects as well as to provide recommendations to ease the deployment of the AARC BPA and the adoption of AARC results.
 - **Policy and Best Practices (NA3):** To define the necessary policies and best practices to ensure the AARC BPA is secure and GDPR compliant and to provide policy recommendations to those deploying AARC BPA architectures.
 - **Pilots (SA1):** To pilot the deployment of AARC BPA and the related policy framework in research collaborations and to pilot cross-infrastructure use-cases.

The figures below illustrate how the various work packages worked together. The research and e-infrastructure requirements were the main drivers and the architecture and policy work packages addressed these. The policy provided security guidelines related to the deployment of the AARC blueprint. The pilots support research communities in AARC to deploy the proposed AARC solutions. Training and outreach make AARC results visible and support their adoption.



Figure I.1: AARC work packages

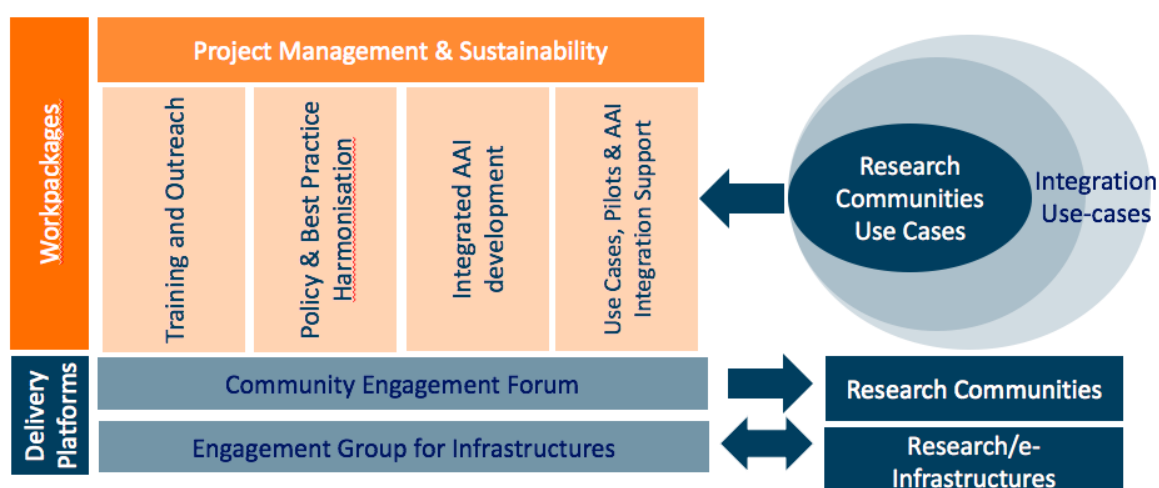


Figure I.2: AARC work packages, AEGIS and CEF

AARC Target Audience

Primary target group

AARC targets international research collaborations and research and e-infrastructures that need to implement and operate AAls following the AARC BPA (i.e. that require an IdP/SP proxy and rely on federated access).

Secondary target group

By deploying an AARC-compliant BPA, researchers' experience improves when accessing services needed to carry out their research (fewer passwords needed, login using their preferred credentials, privacy preserved in line with GDPR).

Annex II – Summary of Deliverables and Milestones

The list of project deliverables and milestones is available online on the [\[AARC website\]](#). All AARC2 documents and deliverables are publicly available under Creative Commons Attributions 4.0. AARC2 deliverables and relevant milestones are listed in the tables below.

| Deliverable Name | Content |
|--|--|
| DNA1.1 Annual Report | This document reports on the progress of the AARC2 project during its first year (2017-2018) |
| DNA1.2 Final Report | This document presents a summary of AARC2 work for each work package |
| DNA1.3 Summary of AARC2 Main Achievements and Sustainability and Exploitation Plans | The document describes the AARC2 project overall dissemination and exploitation strategy and for each key exploitable project result lists the actions that are being proposed to ensure adoption of AARC2 results beyond the project lifetime. |
| DNA2.2 First Advanced Training Material Content | (Github repository) |
| DNA2.3 Summary Report on Training, Communication and Outreach Activities | This document reports on the training, outreach and promotional activities carried out in the AARC2 project, with a particular emphasis on the work done in the second year of the project. |
| DNA3.1/D3.4 Report on the coordination of accounting data sharing among Infrastructures | This report presents the results of the desk study on the evaluation of risks to (personal) data protection as considered in the European General Data Protection Regulation (GDPR), for Infrastructures and their service providers that leverage federated identity management (FIM) to connect research and collaboration users. Specifically, it considers personal data collected as a result of using the infrastructure (not any risks relating to the research data itself, which is a community responsibility) and provides guidance to the Infrastructures concerning Data Protection Impact Assessment (DPIA) in the FIM context. The authors present recommendations to Research Communities for determining the necessity of formal DPIA and guidelines for its execution. |
| DNA3.3/D3.2 Accounting and Traceability in Multi-Domain Service Provider Environments | This report details the service-centric policies that apply to the Blueprint Architecture (BPA) model proposed by AARC, how communities and generic e-Infrastructures can apply the SCI policy framework to their collective service operations, and how this supports the exchange of accounting and traceability information. The report is complemented by the AARC policy guidelines and informational documents, specifically G042, G040, G021, the WISE SCI framework, and the AARC Policy Development Kit. |
| DNA3.2/D3.1 Report on Security Incident Response and Cybersecurity in Federated Authentication Scenarios | This report provides an overview of the current state of security incident response and cybersecurity in Federated Authentication Scenarios, focusing particularly on efforts that have taken place in the past two years related to input from the AARC2 project. |

| | |
|--|--|
| <u>DNA3.4/D3.3 Recommendations for e-Researcher-Centric Policies and Assurance</u> | These Recommendations provide a set of frameworks and guidelines that support, involve, and affect researchers and research communities in order to more effectively use federated identity for accessing services in a blueprint-based proxy architecture. |
| <u>DJRA1.4 Evolution of the Blueprint Architecture</u> | 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. |
| <u>DJRA1.1 Use-Cases for Interoperable Cross-Infrastructure AAI</u> | 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. |
| <u>DJRA1.2 Authorisation Models for Service Providers</u> | This document describes common authorisation models that can be employed by Service Providers (SPs) in order to control access to resources in such an environment. These common models are based on a thorough analysis of use cases collected from the research communities participating in the pilot activities of AARC. The analysis includes describing the different authorisation functions, including management, evaluation and enforcement of policies and their mapping to elements of the AARC Blueprint Architecture. The types of attributes that are commonly used for evaluating authorisation policies are also elaborated on. |
| <u>DJRA1.3 VO Platforms for Research Collaboration</u> | 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. |
| <u>DSA1.1 Results of Pilots with New Communities Part 1</u> | This document provides a general overview of the goals and approach of the Pilots Service Activity ¹ in AARC2. A detailed description including an outline of the use case and the results achieved to date is given for each of the nine Research Community pilots undertaken by SA1 Task 1 in year 1 of the project. The document concludes with some lessons learned so far. |
| DSA1.2 Results of Pilots with New Communities Part 2 | This was a demonstrator about the results of the AARC2 pilots. |
| DSA1.3 Final Results of Infrastructures Interoperations Pilots | This was a demonstrator about the results of the AARC2 pilots. |
| <u>DSA1.4 Final Results of Pilots for Advanced Use-Cases and New Technologies</u> | This was a demonstrator about the results of the AARC2 pilots. |
| DSA1.5 How-to to Deploy Pilot Results | |

Table II.1: List of Deliverables in AARC2

| Relevant Milestones |
|---|
| <u>MNA1.1 Plan to engage with targeted communities and activities</u> |
| <u>MNA3.3 Define and test a model for organizations (IdP) to share information related to account compromises</u> |
| <u>MNA3.4 Identify community accepted frameworks to present to the competence centre</u> |
| <u>MNA3.5 Inventory of high-assurance identity requirements from the AARC2 use cases</u> |
| <u>MNA3.7 Initial Data protection impact assessment on blueprint architecture</u> |
| MSA1.1 Detailed plan of pilots and resources based on the use-cases listed in SA1-Task 1 |
| MSA1.3 Initial plan for piloting advanced use cases and new technologies given input from JRA1 and NA3 |
| MNA1.1 Project website and tools |

Table II.2: List of Milestones in AARC2

References

| | |
|-----------------------|---|
| AARC/AARC2 | https://aarc-project.eu/ |
| AARC-G002 | https://aarc-project.eu/guidelines/aarc-g002/ |
| AARC-G021 | https://aarc-project.eu/guidelines/aarc-g021/ |
| AARC-G029 | https://aarc-project.eu/guidelines/aarc-g029/ |
| AARC-G031 | https://aarc-project.eu/guidelines/aarc-g031/ |
| AARC-G040 | https://aarc-project.eu/wp-content/uploads/2018/03/AARC-G040-Preliminary-Policy-Recommendations-for-the-LSAAI-RandS-and-DPCoCo.pdf |
| AARC-G041 | https://aarc-project.eu/wp-content/uploads/2018/03/AARC-G041-Expression-of-REFEDS-RAF-assurance-components-for-social-media-accounts.pdf |
| AARC-G042 | https://aarc-project.eu/wp-content/uploads/2018/05/AARC-G042-Data-Protection-Impact-Assessment-initial-guidance-for-communities.pdf |
| AARC-I044 | https://aarc-project.eu/guidelines/aarc-i044/ |
| AARC-I047 | https://aarc-project.eu/guidelines/aarc-i047/ |
| AARC-I051 | https://aarc-project.eu/guidelines/aarc-i051/ |
| AARC In Action | https://aarc-project.eu/aarc-in-action/ |
| AUP-Study | https://wiki.geant.org/display/AARC/e-Researcher-centric+policies?preview=%2F123765566%2F123767716%2FAARC2+AUP+study+-+AUP+grid.pdf |
| DNA3.1 | https://aarc-project.eu/wp-content/uploads/2018/04/AARC2-DNA3.1-Accounting-data-sharing-initial-phase.pdf |
| eduGAIN | https://edugain.org/ |
| EPOS Training | https://docs.google.com/document/d/1haTFEOAhaBeGdzvopsXFofO00ma53AW4mX_RqN1e-jg |
| FIM4Rv2 | https://doi.org/10.5281/zenodo.1296031 |
| IGTF | https://www.igtf.net/snctfi/ |
| LS Training | https://drive.google.com/drive/folders/152fEspkl5tH40P7kDep5OAchln10wwh7 |
| MNA1.1 | https://docs.google.com/document/d/1C1af8-7028FddX-WiTdYaMNuplnJIXgkbLAy3Di2rJk/edit |
| MNA2.1 | https://aarc-project.eu/aarc-shop-window-engagement-groups-open-for-business/ |
| MNA2.2 | https://aarc-project.eu/aarc-shop-window-engagement-groups-open-for-business/ |
| MNA3.3 | https://aarc-project.eu/wp-content/uploads/2018/02/MNA3.3-IncidentResponseTestModelForOrganisations.pdf |
| MNA3.5 | https://aarc-project.eu/wp-content/uploads/2018/02/AARC2-MNA3.5-Inventory-of-high-assurance-identity-requirements.pdf |
| PDK | https://wiki.geant.org/display/AARC/Policy+Development+Kit |
| REFEDS | https://refeds.org/ |

Sirtfi <https://refeds.org/sirtfi>

Snctfi <https://aarc-project.eu/policies/snctfi/>

WISE-AUP <https://wiki.geant.org/display/AARC/Acceptable+Use+Policy+and+Conditions+of+Use+-+WISE+Baseline+AUP?preview=/123766285/123773710/WISE-SCI-Baseline-AUP-V1.0.1-draft.pdf>

Glossary

| | |
|---------------------|---|
| AARC/AARC2 | Authentication and Authorisation for Research and Collaboration |
| AAI | Authentication and Authorisation Infrastructure |
| AARC BPA | AARC Blueprint Architecture |
| AEGIS | AARC Engagement Group for Infrastructures |
| CEF | AARC Community Engagement Forum |
| DoW | Description of Work |
| EOSC Pilot | EC funded project |
| FIM4R | Federated Identity Management for Researchers |
| GN4-2 | GÉANT Project |
| IdP | Identity Provider |
| SP | Service Provider |
| IdP-SP Proxy | IdP to SP proxy |
| LS | Life Science research communities |
| LS AAI | Life Science AAI |
| OIDC | OpenID Connect |
| PDK | Policy Development Toolkit |
| REFEDS | Research and Education FEDerations |
| Sirtfi | Security Incident Response Trust Framework for Federated Identity |
| Snctfi | Scalable Negotiator for a Community Trust Framework in Federated Infrastructures – the framework for the IdP/SP proxy that is at the heart of the AARC Blueprint Architecture |