12-09-2016

# Deliverable DNA1.1: Annual Report

**Deliverable: DNA1.1**

| | |
|---|---|
| Contractual Date: | 30-06-2016 |
| Actual Date: | 12-09-2016 |
| Grant Agreement No.: | 653965 |
| Work Package: | NA1 |
| Lead Partner: | GÉANT |
| Document Code: | DNA1.1 |
| **Authors:** | L. Florio (GÉANT) |


The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

**Abstract**

This document provides an overview of the work carried out by the AARC project during its first year (May 2015-April 2016).

# Table of Contents



# Table of Figures

# Table of Tables

# Executive Summary

This document summarises the work carried out by the AARC project and its main achievements during its first year (Y1), from 1 May 2015 to 30 April 2016.

The AARC project is working to define a trust framework that champions federated access and removes the need for multiple accounts, improving user experience while preserving security and privacy. Via this framework, AARC seeks to achieve interoperability and shared service delivery across existing and future R&E authentication and authorisation infrastructures.

The activities of the various work packages during the first year focused mainly on the following areas:

- **Overall project management (NA1)** – Establishing teams and defining processes to ensure smooth operation of the project, including identifying and refining AARC's key messages used for dissemination activities.
- **Libraries' assessment (NA2 and SA1)** – Significant effort during the first year of AARC (more specifically NA2) was spent better understanding libraries' requirements and the challenges that prevent wider adoption of federated access in this community. This work has made it clear that AARC is not best positioned to have a major impact on the adoption of federated access in libraries, owing to the limited presence of libraries in the consortium and the fact that many of the integration aspects need to be further addressed nationally, rather than internationally. However, AARC will continue to monitor this space and to provide training as needed in this area. Based on these findings, SA1 devised a pilot (based on Shibboleth and EZproxies) [Pilot-proxy] which will be offered to interested libraries (outside the AARC consortium) in Y2, while NA2 drew up a Library Factsheet [Factsheet] to make the case for federated access in libraries and prepared and delivered a training module during the LIBER Conference in June 2016.

  **Training and Outreach (NA2)** – the team delivered an information module on basic federated access concepts [Federations 101] and a training module to support service providers [training-sp] to implement federated access.
- **Architecture (JRA1)** – The list of community requirements drawn from the FIM4R paper [FIM4R] and TERENA AAI study [TERENA AAI] were revisited [DJRA1.1] and supplemented with interviews with various research communities. These requirements drove the work to design a blueprint architecture that allows interoperability among existing research infrastructures and e-infrastructures. The first version of the blueprint architecture focuses mainly on authentication, while some of the authorisation aspects will be addressed during Y2 and more in detail during the AARC2 project. The concepts of the blueprint architecture [Draft blueprint] were presented to the AARC partners, federations operators, research infrastructures and e-infrastructures to solicit for inputs.
- **Policy and best practices (NA3)** – The community requirements collected by JRA1 (and previously in the FIM4R document) strongly indicated the need for incident response and assurance in a federated environment.

The team has delivered a baseline assurance profile [MNA3.1] and led the work to define the specification for Sirtfi v1.0 [Sirtfi], a framework to coordinate incident response among federations and service providers.

- **Pilots (SA1)** – Pilots were specified in greater detail after the beginning of the project once requirements became clearer. During Y1, the team worked on the following pilots:
  - A pilot to bridge federated access and IP-based authentication;
  - CILogon for Europe, a token translation pilot that enables federated access for resources that would traditionally require X.509 certificates. This work was carried out jointly by SA1 and NA3 when exploring policy and sustainability aspects.
  - Started work on a number of pilots to support attribute management;
  - Started testing different solutions to provide federated access for non-web-based applications.

There were no major deviations from the plans identified in the AARC Technical Annex [AARC TA] for Y1. 90% of the main deadlines were met on time, and with no more than two months' delay in other cases.

As concerns the use of resources, the project is slightly underspending. It is expected that the underspend will be consumed during Y2.

# 1 Introduction

The AARC project involves 20 partners covering different communities, with GÉANT Association acting as project lead, including:

- Nine NRENs with significant expertise in operating identity federations and all participating in eduGAIN (CESNET, CSC, GARR, PSNC, RENATER, SURFnet, Jisc and DFN).
- e-Infrastructures service partners, including EGI.eu, FOM-NIKHEF, CERN, STFC, KIT, Jülich and SURFsara.
- Libraries, represented by LIBER and their partner MZK.
- One SME (DAASI).

The project's main objectives are:

- To deliver a cross-discipline AAI framework built on federated access to support scientific collaboration and secure access to shared resources. The integrated AAI is referred to as the blueprint architecture.
- To pilot critical components of the blueprint architecture that meet the AARC communities' needs.
- To address policy aspects needed to implement the AARC vision.
- To validate the results of both the research and service activities by engaging with AARC target communities.
- To offer tailored training to increase the uptake of federated access (in terms of more users being able to access services as well as by enabling federated access for services used by the AARC target communities).

This document summarises the work carried out by the AARC project and its main achievements during its first year (Y1), from 1 May 2015 to 30 April 2016.

Section 2 gives an overview of the project's approach and activities over year 1. A summary of the achievements of the project at the end of Y1, as well as links to its main outputs are provided in section 2.2. Section 2.3 shows the project's progress so far in achieving its main KPIs. Section 2.4 describes the work carried out in each work package and section 3 details the resources used by the work packages in Y1. Conclusions and plans for future work are given in section 4.

# 2 Year 1 Activities

## 2.1 Overview

AARC's approach is to build on existing AAIs and related policy frameworks used in the R&E sector (e.g. national federations/eduGAIN, e-Infrastructures and ESFRI cluster AAIs, REFEDS and International Grid Federations etc.). Based on the community's requirements, AARC is designing and piloting missing (technical and policy) components, which will all be reflected in the blueprint architecture. AARC works with research and e-infrastructures to ensure that its results can be integrated in the existing AAI workflows or serve as guidelines for new communities that need AAI functionalities. The diagram below depicts the model followed.

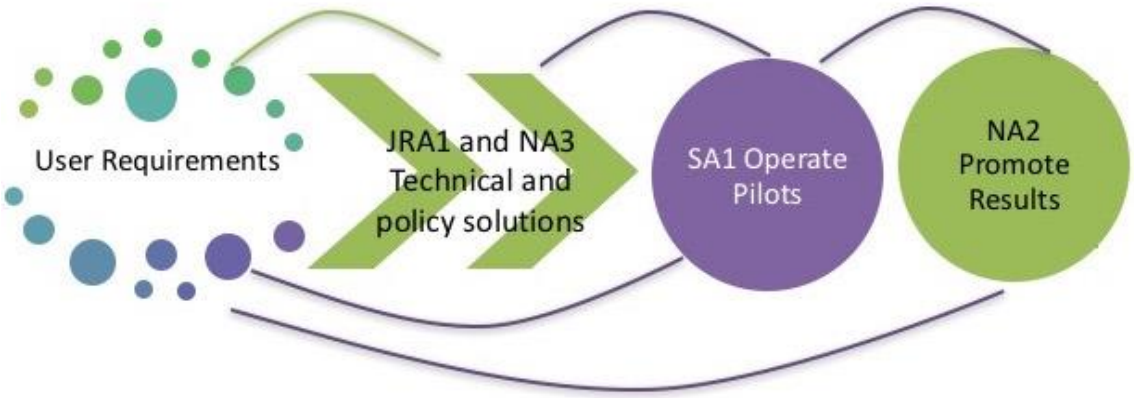


Figure 1: AARC methodology

AARC's work during its first year focused on the following areas:

- **Overall project management** – Establishing teams and defining processes to ensure smooth operation of the project. AARC's key messages were identified and further refined during the year; these have been used for dissemination activities.
- **Libraries' assessment** – This work was carried out mainly by the Training and Outreach WP (NA2), with the support of the architecture WP (JRA1). Significant effort during the first year of AARC was spent better understanding libraries' requirements and the challenges that prevent wider adoption of federated access in this community. Many of the libraries interviewed declared to be satisfied with IP-based authentication; even libraries aware of federated access indicated a lack of a strong driver to adopt it. This has resulted in a better understanding of the problem space as well as in establishing contacts with entities that broker licenses nationally for the libraries. It became clear that to better impact the library sector to move towards federated access it is essential to also involve the national bodies (where they exist) that deal with licenses related to services offered by the libraries Based on these findings, the following actions were taken:

- A pilot (based on Shibboleth and EZproxies) to bridge both federated access and IP-based authentication [pilot-proxy] was devised, which AARC plans to offer to interested libraries (outside the AARC consortium) in Y2, to show how federated access can be introduced without disrupting existing systems.
- A Library Factsheet [Factsheet] to make the case for federated access to decision-makers in the libraries was drawn up.
- A training module for libraries was delivered during the LIBER Conference in June 2016.

This work has made it clear that AARC is not best positioned to have a major impact on the adoption of federated access in libraries. The reasons for this are the limited presence of libraries in the consortium (LIBER as an association can only impact a few of their members) and the fact that many of the integration aspects need to be further addressed nationally, rather than internationally. However, AARC will continue to monitor this space and to provide training as needed in this area.

- **Training and Outreach** – Based on the requirements collected by NA2 at the beginning of the project, the team delivered a basic information module to describe how federated access works [Federation 101]. Plans for Y2 are to use the information collected in the Federations 101 module to provide an online webinar. Further to this, a training module to support service providers [training-sp] to implement federated access was also delivered. The training for service providers was delivered during a dedicated event in March 2016, targeted to ELIXIR and DARIAH service providers (SPs). The feedback was very positive and more of these events are expected to be run during Y2.

- **Architecture** – The list of community requirements drawn from the FIM4R paper [FIM4R] and TERENA AAI study [TERENA AAI] were revisited [DJRA1.1] and supplemented with interviews with the various research communities with which AARC engages. These requirements drove the work to design a blueprint architecture that allows for interoperability among existing research infrastructures, including e-infrastructures. The team has also surveyed existing AAIs [MJRA1.1] and available technologies used to implement federated access, solutions for guest identities [MJRA1.2] and models to integrate attribute authorities [MJRA1.3]. This work has informed the blueprint architecture and has enabled to identify the building blocks needed to implement an AAI. The first version of the blueprint architecture focuses mainly on authentication; authorisation aspects will be addressed during Y2. The concepts of the blueprint architecture [Draft Blueprint] were presented to the AARC partners, federations operators, and research infrastructures and e-infrastructures to solicit for inputs.

- **Policy and best practices** – The community requirements collected by JRA1 (and also previously by the FIM4R document) strongly indicated the need for an incident response framework to be jointly adopted by both federation operators and resource providers, as well as for baseline assurance in a federated environment.

  The team has delivered a baseline assurance profile [MNA3.1] and additionally led the work to define the specification for Sirtfi v1.0 [Sirtfi], a framework to coordinate incident response among federations and service providers. The global Sirtfi working group is hosted by REFEDS [REFEDS]; AARC leads the work within this working group, but all decisions are taken within the global Sirtfi WG, which also benefits from the contributions from international experts. This is a clear example of collaboration between AARC and existing bodies that operate in the same area.

Work was also undertaken to pilot a translation ticket system, CILogon for Europe [CILogonEU], and to address sustainability aspects for the pilot and the underlying certification authority required to generate digital certificates after successful federated authentication [RCauth.eu].

The team has also investigated responsibilities to handle personal data when aggregating accounting data by research infrastructures and e-infrastructures [MNA3.2].

- **Pilots** – Pilots were specified in greater detail after the beginning of the project once requirements became clearer. During Y1 the team worked on the following pilots:
  - Pilot to bridge federated access and IP-based authentication; at the end of Y1, this pilot was nearing conclusion. Its objective is to demonstrate that it is possible to support federated access as well as to cater for users and/or services that rely on IP-based authentication. During Y2, the pilot will be offered to libraries that are not participating in the AARC project. Feedback will be collected and a sustainability proposal delivered and made available to different libraries interested in deploying the pilot.
  - CILogon for Europe, a token translation pilot (carried out in SA1) that enables federated access for resources that would traditionally require X.509 certificates. This pilot is being tested by BBMRI and by Elixir. The CILogon pilot follows the blueprint architecture and it is expected to become one of the building blocks to build an AAI.
  - Started work on pilots to support attribute managements;
  - Started testing different solutions to provide federated access for non-web-based applications. These results will be used to provide guidelines on how different existing solutions (i.e. OpenID Connect, Moonshot, etc.) can support different use cases.

## 2.2 Summary of Achievements

The work carried out during the first year of the AARC project was in line with the content of the project's Technical Annex I [AARC TA]. The table below summarises the main results of the project's activities, the call objectives they meet, and their impact. It also provides links to the project's main outputs.

| Results | Call Objectives | Impact |
|---|---|---|
| **NA1** | | |
| AARC Website, wiki, mailing lists and internal processes.<br><br>AARC remit and key promotional messages agreed with the teams.<br><br>Liaisons with relevant stakeholders established. | NA1 underpins all of the objectives by ensuring smooth operations and consistency with the work plan. | Avoided duplication of efforts by working with existing international initiatives and infrastructures.<br>Ensured coordination across work packages. |
| **NA2** | | |
| Learning needs analysis. | | |

| Results | Call Objectives | Impact |
|---|---|---|
| (Note: library-specific requirements were collected jointly with JRA1).<br><br>Delivered Federations 101 to explain basic concepts of federated access.<br><br>Delivered Training for Service Providers; first training (March 2016) aimed at Elixir and DARIAH service providers.<br><br>Prepared the Library Factsheet | Call objective 1. Facilitate the deployment and promotion of a pan-European identity federation.<br><br>Call objective 2. Lower barriers to entry for organisations to enrol in identity federations<br><br>Call Objective 7. Offer training and outreach for data professionals. | Raised awareness and increased uptake of federated access.<br><br>Developed better knowledge about libraries' needs. |
| **NA3** | | |
| Baseline assurance profile.<br><br>Coordination and implementation of European contributions to the global Sirtfi v1.0 framework (security incident response for federated access).<br><br>Document on data collection for legitimate interest.<br><br>Policy for the RCauth.eu CA for the CILogon for EU pilot and related sustainability plans in collaboration with SA1. | Objective 1. Facilitate the deployment and promotion of a pan-European identity federation.<br><br>Objective 3. Overcome technical, organisational and legal obstacles for the implementation of an integrated and interoperable authentication and authorisation infrastructure.<br><br>Objective 4. Enable the interoperability of different AAIs by researching the use of security token translation services and accounting services. | Addressed identified community requirements for security and legal aspects.<br><br>Improved adoption of federated access for research collaborations by addressing security requirements.<br><br>Facilitated federated access to non-web resources via a token translation service. |
| **JRA1** | | |
| Analysis of user-community requirements (the library requirements were collected jointly with NA2).<br><br>Existing AAI and available technologies for federated access.<br><br>Three iterations for the blueprint architecture.<br>Main concepts presented at: | Objective 1. Facilitate the deployment and promotion of a pan-European identity federation.<br><br>Objective 3. Overcome technical, organisational and legal obstacles for the implementation of an | Addressed identified community requirements.<br><br>Defined identity building blocks and high-level architecture for the blueprint AAI. |

| Results | Call Objectives | Impact |
|---|---|---|
| • EGI Community Conference (November 2015);<br>• GÉANT Symposium (March 2016);<br>• EGI Conference (April 2016).<br><br>Explored approaches and solutions to support guest identities.<br><br>Assessed 3 models for implementing attribute providers. | integrated and interoperable authentication and authorisation infrastructure<br><br>Objective 4. Enable the interoperability of different AAIs by researching support for guest users and attribute providers. | Created a human network to engage with the research and e-infrastructures to adopt a common approach to AAI. |
| **SA1** | | |
| Platform established to execute pilots – The platform offers the same building blocks identified in the AARC blueprint architecture.<br><br>Pilot to bridge IP-based authN and federated access for libraries presented to AARC partners.<br><br>Token Translation service pilot – CILogon for Europe Pilot in collaboration with NA3. The pilot is being tested with Elixir and BBMRI communities.<br><br>Tested additional solutions for non-web access to compare them and provide guidelines on how to best use them. | Objective 1. Facilitate the deployment and promotion of a pan-European identity federation.<br><br>Objective 2. Lower barriers to entry for organisations to enrol in identity federations.<br><br>Objective 3. Overcome technical, organisational and legal obstacles for the implementation of an integrated and interoperable authentication and authorisation infrastructure.<br><br>Objective 4. Enable the interoperability of different AAIs by researching the use of security token translation services and accounting services. | Address identified community requirements.<br><br>Improve adoption of federated access for research collaborations.<br><br>Facilitated federated access to non-web resources via a token translation service.<br><br>Tested the results from JRA and SA1 and advanced the work to deliver the blueprint AAI. |

Table 1: List of outputs and achievements during Y1

## 2.3 Results against KPIs

Table 2 below reports on the progress made towards the main KPIs as described in the project's Technical Annex I [AARC TA]. Only results for which KPIs are applicable are shown.

| Main Results | KPIs for 2 year project/current value |
|---|---|
| Training modules produced and delivered | 90% of satisfied users |
| Engagement with ESFRI, research and e-infrastructures to promote AARC and its results. | Expected to engage with 5/ engaged with 14. |
| Progress with the blueprint architecture | 2 informal consultations with research and infrastructures planned/ 3 done. |
| Sirtfi adoption | Pilot incident response procedures in 5 IdPs/ now 87 in eduGAIN support Sirtfi. |
| CILogon for Europe pilot with Elixir and BBRI | 2 cross-infrastructure use cases delivered/2 |
| Support provided to EGI to design their proxy SP in line with AARC architecture and connect it to eduGAIN. | 3 new SPs selected by the community available in eduGAIN/Work in progress to connect 1/3 SPs |

Table 2: Main results against KPIs

## 2.4 Activities by Work Package

The AARC project includes 20 partners covering different communities, each involved in one or more work packages, as follows:

- **GÉANT Association**, who acts as project lead;
- **NREN partners** – There are a total of nine NRENs involved in AARC, who all have significant expertise in operating identity federations, integrating services within their national federations and offering storage services. They all participate in eduGAIN. These are:
  - CESNET, involved in JRA1 and SA1;
  - CSC, leading the training for service providers in NA2 and the assurance work in NA3;
  - GARR, leading the training on Identity Providers in NA2, and who will lead the work to implement attribute providers in JRA1 and the pilots for guest users in SA1.
  - GRNET, leading JRA1;
  - PSNC, leading the non-web federated access work in SA1;
  - RENATER, contributing to NA3.
  - SURFnet, leading SA1.
  - Jisc and DFN, who are participating unfunded to support AARC in its dissemination work.
- **e-Infrastructures service partners** – There are several different R&E e-infrastructures involved and/or represented in AARC, namely:

- **EGI.eu**, leading the user requirements work JRA1 and the pilots on attribute management solutions in SA1;
- **FOM-NIKHEF**, leading NA3;
- **CERN**, leading the work on Sirtfi;
- **STFC**, leading the work on scalable policy negotiations in NA3 and the work on guest identities in JRA1;
- **KIT,** leading the work on the blueprint architecture in JRA1 and the data accounting in NA3;
- **Jülich** and **SURFsara,** to represent the requirements for PRACE.

- **Libraries** – These are represented by LIBER and by their partner MZK
- **One SME** – DAASI

The sections that follow provide details of the work carried out in each work package in Y1 of the project.

### 2.4.1 NA1 – Management

GÉANT Association (formerly TERENA) is the leading and sole partner working on NA1. During the first year of the project, NA1 focused on defining procedures to monitor effort and expenditure and to implement tools to support teamwork (i.e. wiki, mailing lists, website etc.).

Additionally, NA1 offers support for AARC meetings, including AARC project board meetings, and engages directly with the EC and with other relevant stakeholders. AARC stakeholders include research infrastructures and e-infrastructures that operate internationally for eScience purposes and are interested in establishing an authentication and authorisation infrastructure.

NA1 has also worked closely with the other work packages to fine-tune the AARC remit and define key promotional messages.

NA1 also managed AARC's presence at main events, such as Internet2 conferences, RDA, TNC16 etc.

#### Exploitation and Dissemination

As indicated in the project's technical annex [AARC TA], it is expected that AARC's results will be exploited by existing research infrastructures and e-infrastructures that are already operating AAIs, and integrated with their own systems. AARC is committed to delivering a more detailed plan at the end of the AARC project to offer recommendations on how best to integrate its findings in a format that is 'deployable' for these infrastructures, so as to ensure their adoption.

AARC has already delivered two results in Y1, for which sustainability/exploitation plans have been made – CILgon for Europe and Sirtfi:

- **CILogon for Europe** is a token translation pilot (carried out in SA1) that enables federated access for resources that would traditionally require X.509 certificates. The associated reference policies and integration with the e-Infrastructures (such as EGI) and the R&E Federations and IdPs (including eduGAIN as well as selected IdPs of last resort) are being developed by NA3 (see 2.4.3). NA3 also surveyed the various sustainability models that could accompany a production deployment of the

AARC CILogon pilot, and made these proposed models available on the AARC wiki [AARC wiki] at the end of Y1. Further discussion with interested parties willing to operate the service will take place in Y2.

- In January 2016, the **Sirtfi v1.0 framework** was published following a REFEDS community consultation. This assurance framework comprises a list of assertions that an organisation can attest in order to be declared Sirtfi-compliant. A package [sirtfi-faq] was created to prepare organisations that want to adopt Sirtfi. GN4-2 is working with AARC to facilitate the deployment of Sirtfi within eduGAIN.

As more pilots are finalised, it is expected that more sustainability studies will become available.

Specific dissemination and training activities have been carried out for libraries, resource providers and research communities and e-infrastructures. AARC participants have attended various events to promote the AARC results. The list of presentations can be found online in the documents section of the AARC website [AARC documents].

Mechanisms to ensure that AARC results are widely disseminated include availability of dissemination material and presentations via the AARC website [AARC]. Development is also underway of blogs, social media channels and general PR material (the latter began in Q4 Y1 with more material expected to be produced in Y2).

### 2.4.2 NA2 – Training and Outreach

The work carried out in NA2 during the first year was organised in five tasks. Besides management of the overall work package, activities focused on the following areas:

- **Learning needs analysis** – this task, led by GÉANT, produced a deliverable [DNA2.1] to report on the training requirements of the identified target groups. The requirements were collected following a twofold approach: a survey, sent to libraries and life science, arts and humanities, and high-energy physics organisations that do not support federated access, and interviews. NRENs as representative of national federations and a broad set of institutions were also queried to understand the needs and requirements of their constituencies. A total of 25 organisations answered the survey. The main results are described below:
    - Information material for decision-makers and users – One of the main findings of the survey as well as from the meetings is that in many cases decision-makers are unable to clearly understand costs versus benefits. AARC has started work to produce a value proposition for federated access to support institutional decision-making.
    - Increased uptake of federated access within different research communities by addressing the main technical and policy challenges that prevent implementing identity management systems – REFEDS and R&E identity federations have worked over the years to define best practices to address this point. AARC will complement this effort with further training and dissemination activities and by working with the research communities to help them design and deploy inter-operable AAIs.
    - Operational security and technical training for IdP and SP operators and standardised approaches to incident response to support the assurance needs of research collaborations – AARC is investing significantly in this area, by offering training and supporting Sirtfi.
    - Improved central eduGAIN support that guides resource providers to join eduGAIN and also highlights the benefits of using eduGAIN – AARC will support the GÉANT project, under which

eduGAIN operates, to promote any new enhancements made to eduGAIN to address this requirement.

- Ready-to-use solutions as needed (i.e. IdM as services etc) – AARC will investigate the feasibility of possible solutions via pilots with the communities and will make the necessary recommendations for their deployment.

- **Outreach and dissemination** – this task, led by GÉANT (with the support of DAASI, GARR, CSC, LIBER, MZK and KIT), produced the "**Federations 101**" module [Federations 101], as well as the "Federated access to digital resources at libraries" Factsheet [Factsheet] and additional material for training events highlighting how federated access preserves users' privacy (based on the eduGAIN Code of Conduct). Federations 101 is a dynamic module that is updated frequently and offers basic information on federated access.
- **Training for Resource Providers** – the task, led by CSC, prepared an SP-tailored "**Training Module for SPs**" to support new SPs to join national federations; the first training was delivered in March 2016 for Elixir and DARIAH communities. This module, developed in collaboration with SWITCH, was designed to support scientific service providers to enable federated access.
- **Training for Identity Providers** – this task, led by GARR, worked to produce a module to identify tools and procedures for federations to support attribute release for IdPs. The module builds on the work previously done by REFEDS [REFEDS] to define an approach to group similar services under a category (Research and Scholarship). IdPs would in turn release the same set of attributes to all services in that category. The package was prepared in anticipation of a dedicated event to be held during TNC16 (June 2016), after which the material will be revised on the basis of the feedback collected.

### 2.4.3 NA3 – Policy Harmonisation

The work carried in NA3 during the first year was organised in six tasks. Besides overall work package management, work focused on the areas below:

- **Development of best practices for Levels of Assurance** – this task, led by CSC, delivered the baseline assurance profile [MNA3.1]. The aim of this document is to define requirements for a minimal assurance level that is still relevant for low-risk research use cases. In a federated AAI, the user's Home Organisation issuing and managing user's credentials determines the assurance level available for the user identity. For the risk management of the research services relying on the federated AAI, it is important to determine the assurance level available for the authenticated users. Some of this work was coordinated with the GN4-1 project to assess federation and organisation assurance level feasibility.
- **Incident Response** – this task, led by CERN, resulted in the publication of Sirtfi v1.0 specifications [Sirtifi]. The global Sirtifi working group is hosted via REFEDS [REFEDS]; the AARC project provides funding for coordination support. Sirtfi addresses the reluctance of research organisations to participate in eduGAIN based on the lack of well-defined and shared security practices to handle potential security incidents. The assertion statements in Sirtfi describe practices and attributes that identify an organisation as being capable of participating in collaborative incident response. The framework stipulates preventative measures to protect an organisation from attack, and behaviour to adopt in the event of an incident. Compliance with Sirtfi is expressed in metadata.

- **Recommendations for service operational models for enabling cross-domain sustainable services** – the task, led by DAASI, produced the sustainability model study for CILogon for Europe [RCauth.eu]. The task also produced a document with considerations regarding sustainability models for guest IdPs [sustainability-guestIdP]. The document surveys different operational and cost models to deploy guest IdPs. Clearly, there are different possible approaches, which depend on the institutions, the specific use cases and the existing technical infrastructures.
- **Scalable policy negotiation mechanisms** – this task, led by STFC, is working to develop a policy framework for bridging (IdP-to-SP proxy) multiple eduGAIN IdPs to connect to the CILogon Pilot for Europe and comply with the "RCauth.eu" Policy and Practice Statement.
- **Accounting and processing of data** – the task, led by KIT, reported on the role and responsibilities for personal data protection in the aggregation of accounting data by research infrastructures and e-infrastructures [MNA3.2];

### 2.4.4 JRA1 – Architecture

The work carried out in JRA1 during the first year was organised in five tasks to cover different areas, in addition to overall work package management. These areas are:

- **Analysis of Requirements** – The aim of this task was to review the existing requirements for the research collaborations as drawn from the FIM4R paper [FIM4R] and TERENA AAI study [TERENA AAI]. The results of this work revealed that some of the requirements had already been addressed while some were still a challenge, but also new emerging requirements. The results informed the work on the architecture, on policies (NA3) and on the pilots (SA1). The task was led by EGI and was carried out by engaging with several research communities, most of which were previously engaged in FIM4R. Its findings were presented in deliverable DJRA1.1 [DJRA1.1]. A list of existing tools in use to date was also prepared [MJRA1.1].
- **Blueprint architecture** – the goal of this task, led by KIT, was to identify proven technical solutions and/or implementation patterns to help e-infrastructure operators and technical architects and implementers in the various research communities to enable secure, scalable, and interoperable federated access to their resources. The first draft version of the architecture, presented in April 2016, identifies four component layers:
  - **The User Identities Layer** contains services for identification and authentication of users.
  - **The Attribute Management & Enrichment Layer** groups services that provide additional information about the users. Services like these exist in all of the mentioned authentication technologies.
  - **The Gateway Proxy & Translation Layer** addresses the frequent necessity of having central policy control and support for multiple authentication technologies on the services side.
  - **The End Services Layer** contains the actual services that the research communities are using in order to collaborate and share resources. These can range from simple web services, such as wikis, to portals for accessing computing and storage resources, and non-web based resources such as Big Data access and management, interactive shell access etc.

The result of this work is a major achievement for the AARC project. This blueprint will guide (existing and emerging) research collaborations to build AAIs that meet their requirements but are interoperable with each other, as they will all implement the AARC blueprint architecture principles.

- **Models to support guest identities** – this task, led by STFC, explored possible models for the assessed guest Identities. Initial considerations are described in a document published on the AARC website. [MJRA1.2];
- **Models for implementing attribute providers** – this task, led by GARR, analysed possible models for designing and integrating Attribute Authorities in a scalable manner [MJRA1.3]. The document analyses models to implement Attribute Authorities and examines cases where IdPs act as such, as well as the usage of a dedicated third party built using existing software (i.e. VOMS, COmanage, Perun, etc). Lastly, it presents harmonisation aspects when using different tools and describes mapping mechanisms between key technologies used in the AAI space (i.e. SAML-to-X.509, SAML-to-OpenID Connect, etc.). This work will inform Y2 pilots that focus on specific cross-collaboration use cases that require attributes from multiple sources.

Furthermore, the team (mostly GRNET) is following the developments in eIDAS and gaining an understanding on the penetration of Gov eIDs in the EU Member States. Previous work done in the context of GN4-1 and STORK2.0 [STORK2.0] was analysed in the light of the changes between STORK2.0 and eIDAS. AARC is investigating the possible use of eIDs as a means for stronger authentication.

### 2.4.5 SA1 - Pilots

The work carried out in SA1 during the first year was organised in four tasks. Besides overall work package management, work focused on the following areas:

- **Pilots of solutions for guest users** – this work, led by GARR, focused on testing solutions to bridge SAML authentication with IP-address-based access control. The pilot builds on EZproxy (which is a software widely used in libraries), to enable both federated and IP-based access to library resources. The interface built on top of the EZproxy uses a shibboleth back-end to generate a SAML assertion by converting the information provided when users log in using IP-based authentication. This is meant to showcase how federated access can be introduced without disrupting existing environments. Plans for Y2 are to produce supporting documentation and to invite a limited number of libraries (reached via LIBER and the NREN partners) to use the pilot and report on their experience.
- **Pilots of an attribute management framework** – this work, led by EGI, in Y1 focused on sketching the first outlines for pilots to manage authorisation on a central level to facilitate the sharing of resources and regulate service access authorisations. Two pilots were started:
  - A first with EGI, to investigate and pilot the usability of SAML-based AAI components to use externally managed attributes to provide and restrict access to cloud services. For this pilot PERUN, COmanage, SimpleSAMLphp, and OpenConext aggregator were used.
  - A second, with BBMRI-ERIC to pilot a full-fledged standardised AAI infrastructure for the BBMRI ERIC community, to enable access and authorisation to shared biomedical resources with appropriate level(s) of assurance.
- **Pilot to improve access to research and education and commercial services** – this task, led by PSNC, worked to demonstrate that existing AAIs can be leveraged to access (non-web) resources that are

offered by different e-infrastructures. The team started to test the readiness of the existing solution to implement federated non-web access. The initial findings of this work were presented during the AARC face-to-face meeting in May 2016. The work will continue during Y2 [Solutions for non-web federated access].

Work to support commercial service providers in the area of pay-per-use has been postponed to Y2; this will allow the team to evaluate the work done outside the AARC project and to better understand what additional inputs AARC can offer.

# 3 Use of Resources

With the exception of NA1, at the end of project Y1 all WPs are slightly underspending. This is due to the following reasons:

- As planned, the work on SA1 was more accurately scoped once the deliverable on requirements was available. The team then started to explore the possible technical platforms to use to test the AARC pilot without disrupting production systems.
- Most of the underspent effort was in the first months of the project, due to difficulties in recruiting qualified team members:
  - CSC lost two key members of staff due to parental leave (impact on NA2 and NA3);
  - EGI experienced difficulties with its internal recruitment process (impact on JRA1 and SA1);
  - LIBER experienced internal delay in recruiting new staff to better support NA2;
  - RENATER saw people involved in the project leave the organisation (impact on NA3);
  - SURFnet experienced internal delay in recruiting a non-EU specialist.
- Additionally, PSNC had national funding to carry out the work for the first months, so although they did contribute to the work they have not claimed effort (impact on SA1).

It is expected that the underspend will be consumed during Y2. A breakdown of the use of resources per work package is provided in Table 3 below.

| WP | Total MM | Y1 Forecast | Actual |
|---|---|---|---|
| **NA1** | 14 | 7 | 7,3 |
| **NA2** | 75 | 30 | 28,5 |
| **NA3** | 66 | 28 | 20,2 |
| **JRA1** | 75 | 37 | 32,8 |
| **SA1** | 96 | 40 | 38,0 |
| **TOTAL** | 326 | 142 | 126,8 |

Table 3: Use of resources

# 4 Conclusions

The first year of the AARC project has produced a number of very good results in line with its plans. The AARC teams were created and started to work jointly towards common goals; meeting with all different parties to engage with them as much as possible was an important result.

AARC's funding has clearly contributed to facilitating the involvement and commitment of the parties, as without AARC it would not be possible to engage with research and e-infrastructures to align architecture and policies. The results of Y1 and the lessons learnt have informed the Y2 detailed work plan, specifically:

- With regard to its work with libraries, AARC will continue to monitor this space, to provide training as needed in this area and to promote the pilot to bridge both federated access and IP-based authentication among libraries.
- Work on building a diversified set of training modules was started in Y1, with the production of the Federations 101 set of information material to explain federated access and the training module for service providers. During Y2, it is planned to add more self-explanatory video materials both on Federations 101, to finalise the training on identity providers, and to promote AARC relevant results.
- The pilots were specified in greater detail after the beginning of the project once requirements became clearer. A number of pilots were delivered during Y1 (CILogon Pilot, the pilot to bridge federated access and IP-based authentication) including the pilot platform and an initial matrix to map different solutions to implement federated access for non-web applications to use-cases.
- With the blueprint architecture delivered, the JRA1 team can work with different research infrastructures including e-infrastructures to use this as a model to implement AAIs. This approach was already followed with EGI, and resulted in the EGI-AAI. During Y2, the team will refine the different building blocks and test their integration in existing AAIs.
- On the policy side, the task has delivered a baseline assurance profile, has led the work on Sirtfi, has delivered a first draft on requirements to process data on users and services usage and has defined policies for the CILogon Pilot. Work on sustainability has started and produced two main outputs (the CILogon sustainability plans and the sustainability models for guest IdPs). More work in this area is expected in Y2 as more results mature.

# References


| | |
|---|---|
| [AARC] | https://aarc-project.eu/ |
| [AARC documents] | https://aarc-project.eu/documents/ |
| [AARC TA] | https://aarc-project.eu/wp-content/uploads/2015/04/technical_annexB_chap1_3_v1_0-FINAL.pdf |
| [AARC wiki] | https://wiki.geant.org/display/AARC/AARC+Home |
| [CILogonEU] | https://aarc-project.eu/digital-certificates-behind-the-scenes-the-aarc-cilogon-pilot/ |
| [DJRA1.1] | https://aarc-project.eu/wp-content/uploads/2015/10/AARC-DJRA1.1.pdf |
| [DNA2.1] | https://wiki.geant.org/download/attachments/47908391/AARC-DNA2.1.pdf?version=1&modificationDate=1465290595899&api=v2 |
| [Draft blueprint] | https://wiki.geant.org/display/AARC/AARC+Architecture |
| [EGI] | https://www.egi.eu/ |
| [Factsheet] | https://wiki.geant.org/display/AARC/Fact+Sheet%3A+Federated+access+to+digital+resources+at+libraries |
| [Federations 101] | https://aarc-project.eu/workpackages/training-and-outreach/training-modules/federations-101/ |
| [FIM4R] | https://cdsweb.cern.ch/record/1442597 |
| [Library requirements] | https://wiki.geant.org/display/AARC/Training+needs+at+libraries+-+interviews+with+decision+makerS |
| [MJRA1.1] | https://aarc-project.eu/wp-content/uploads/2016/01/MJRA1.1-Existing-AAI-and-available-technologies.pdf |
| [MJRA1.2] | https://aarc-project.eu/documents/milestones/ |
| [MJRA1.3] | https://aarc-project.eu/documents/milestones/ |
| [MNA3.1] | https://aarc-project.eu/wp-content/uploads/2015/11/MNA31-Minimum-LoA-level.pdf |
| [MNA3.2] | https://aarc-project.eu/wp-content/uploads/2015/11/MNA3.2-AccountingDataProt-20151130.pdf |
| [Pilot-proxy] | https://wiki.geant.org/x/JgV3Aw |
| [RCAuth.eu]: | https://wiki.geant.org/display/AARC/Models+for+the+CILogon-like+TTS+Pilot |
| [REFEDS] | https://refeds.org/ |
| [Sirtfi] | https://refeds.org/sirtfi |
| [sirtfi-faq] | https://refeds.org/sirtfi/sirtfi-faqs |
| [Solutions for non-web federated access] | https://aarc-project.eu/wp-content/uploads/2015/08/Maciej-Michal-Non-web-access-Utrecht-05.2016.pptx |
| [STORK2.0] | https://www.eid-stork2.eu/ |
| [sustainability-guestIdP] | https://wiki.geant.org/display/AARC/Sustainability+models+for+Guest+IdPs |
| [TERENA AAI] | http://www.terena.org/publications/files/2012-AAA-Study-report-final.pdf |
| [training-sp] | https://aarc-project.eu/workpackages/training-and-outreach/training-modules/training-for-service-provider-operators/ |

# Glossary

| | |
|---|---|
| **AAA** | Authentication, authorisation, and accounting |
| **AAI** | Authentication and Authorisation Infrastructure |
| **AARC** | Authentication and Authorisation for Research and Collaboration |
| **eduGAIN** | education Global Authentication INfrastructure |
| **eID** | Electronic identification |
| **eIDAS** | EU REGULATION No 910/2014 on electronic identification and trust services for electronic transactions in the European internal market |
| **ESFRI** | European Strategy Forum on Research Infrastructures |
| **IdP** | Identity Provider |
| **IP** | Internet Protocol |
| **KPI** | Key performance indicator |
| **R&E** | Research and Education |
| **REFEDS** | Research and Education FEDerations group |
| **SAML** | Security Assertion Markup Language |
| **SP** | Service Provider |
| **WP** | Work Package |