

05-06-2018

Deliverable DNA1.1: Annual Report

Deliverable <DNA1.1 >

Contractual Date:	30-06-2018
Actual Date:	Error! Reference source not found.
Work Package:	1
Task Item:	1
Lead Partner:	GÉANT
Document Code:	DNA1.1
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 progress of the AARC2 project during its first year (2017-2018).

© 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	5
1 Overview of AARC2	6
1.1 AARC2 Objectives	6
1.2 From AARC1 to AARC2: What Has Changed?	6
1.3 AARC Target Audience	9
1.4 AARC2 Partners and Structure	9
1.5 The Role of AEGIS	10
2 Overview of AARC2 Results in Y1	12
2.1 Summary of Deliverables and Milestones for Y1	14
3 Work Carried Out per WP	17
3.1 Work Package NA1 – Project Management and Sustainability	17
3.2 Work Package NA2 – Training and Outreach	18
3.3 Work Package NA3 – Policy and Best Practices Harmonisation	20
3.4 Work Package JRA1 – Architecture for Integrated and Interoperable AAI	22
3.5 Work package SA1 – Pilots on the Integrated AAI	24
4 Impact 27	
4.1 Overview of KPIs as per DoW	27
5 Conclusions and Plans for Y2	29
References	30
Glossary	31

Table of Figures

Figure 1: Current version of the AARC BPA	7
Figure 2: AARC work packages	10
Figure 3: AARC work packages, AEGIS and CEF	10
Figure 4: Example AEGIS Brief	11
Figure 5: AARC2 Pilots with research collaborations	25

Table of Tables

Table 1: Differences between AARC2 and AARC1	8
Table 2: Summary of AARC2 Y1 results	13
Table 3: Summary of Guidelines produced by AARC2	13
Table 4: List of Deliverables in Y1	14
Table 5: Overview of KPI	28

Executive Summary

This document reports on the progress of the second Authentication and Authorisation for Research and Collaborations ([AARC2](#)) project during its first year (2017-2018).

The first chapter presents the structure of AARC2, its objectives, and explains the main differences between this and the AARC1 project, funded between 2015-2017. AARC2 took as input AARC1 results and in particular the AARC Blueprint Architecture (BPA). **AARC2 focuses on implementing the AARC BPA** within research collaborations in line with their needs, whilst at the same time the BPA itself and the initial policy framework continue to evolve and expand to encompass more aspects.

AARC2 has also strengthened the way of interacting with e-infrastructures and research infrastructures in what concerns the adoption of AARC1/AARC2 results. To this end, the AARC Engagement Group for Infrastructures (**AEGIS**) was created. AEGIS members represent the research- and e-infrastructures that deploy an AARC BPA-compliant authentication and authorisation infrastructure (AAI) that are interested in adopting AARC technical and policy guidelines. AEGIS validates AARC2 guidelines, but also provides a forum for its members to discuss implementation details.

Research collaborations are the primary target in AARC2, as demonstrated by the high number in the project consortium: 9 research collaborations in a total of 25 partners.

Chapter 2 describes in more detail the work carried out by each Work Package.

Chapter 3 presents the impact of AARC2 so far.

Chapter 4 concludes the document and presents an overview of the Y2 plans.

1 Overview of AARC2

1.1 AARC2 Objectives

The Authentication and Authorisation for Research and Collaboration project, AARC2, 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.

AARC2 focuses on:

- **Championing federated access** - Make federated access the main access means for eScience by addressing technical and policy challenges and promoting its usage.
- **Support global policies** - Develop key policy frameworks to minimise diverging policies and empower interoperable infrastructures.
- **Run pilots with research collaborations participating in AARC2** (and beyond as needed) - Support research communities to scope their requirements and deploy matching solutions based on the AARC Blueprint Architecture.
- **Promote AARC results and make them sustainable** - By entrusting operations with existing research and e-infrastructures whenever possible.

To learn more about AARC, please refer to the two-minute [AARC video](#).

1.2 From AARC1 to AARC2: What Has Changed?

The AARC1 project had an ambitious goal: to define a single architectural model to drive the implementation of AAI in different research collaborations. This resulted in the first version of the **AARC Blueprint Architecture (BPA)**. The proposed BPA reflected the architectural patterns found in different research collaborations that were already operating AAI. The **AARC BPA has played a significant role in "standardising" the AAI architecture and turning it into a reference model**. By design, the AARC BPA adopted existing AAI components whenever possible, so that new areas of development would be limited to components that were missing and to integrating the various components.

At the start of the AARC1 project, there were a number of technical and policy challenges that needed addressing (such as token translation services, use of guest identity providers, security aspects etc.) to make the BPA work in practice and for different use-cases. Work was undertaken in AARC1 to address these challenges and provide technical and policy solutions for the BPA. For this reason, in AARC1 different technology-driven pilots were needed.

A graphical representation made it easier to identify the various BPA components and the functions each of them performs. The impact of the AARC BPA exceeded expectations (probably also thanks to the graphical representation) and it soon became a reference document for AAI architects.

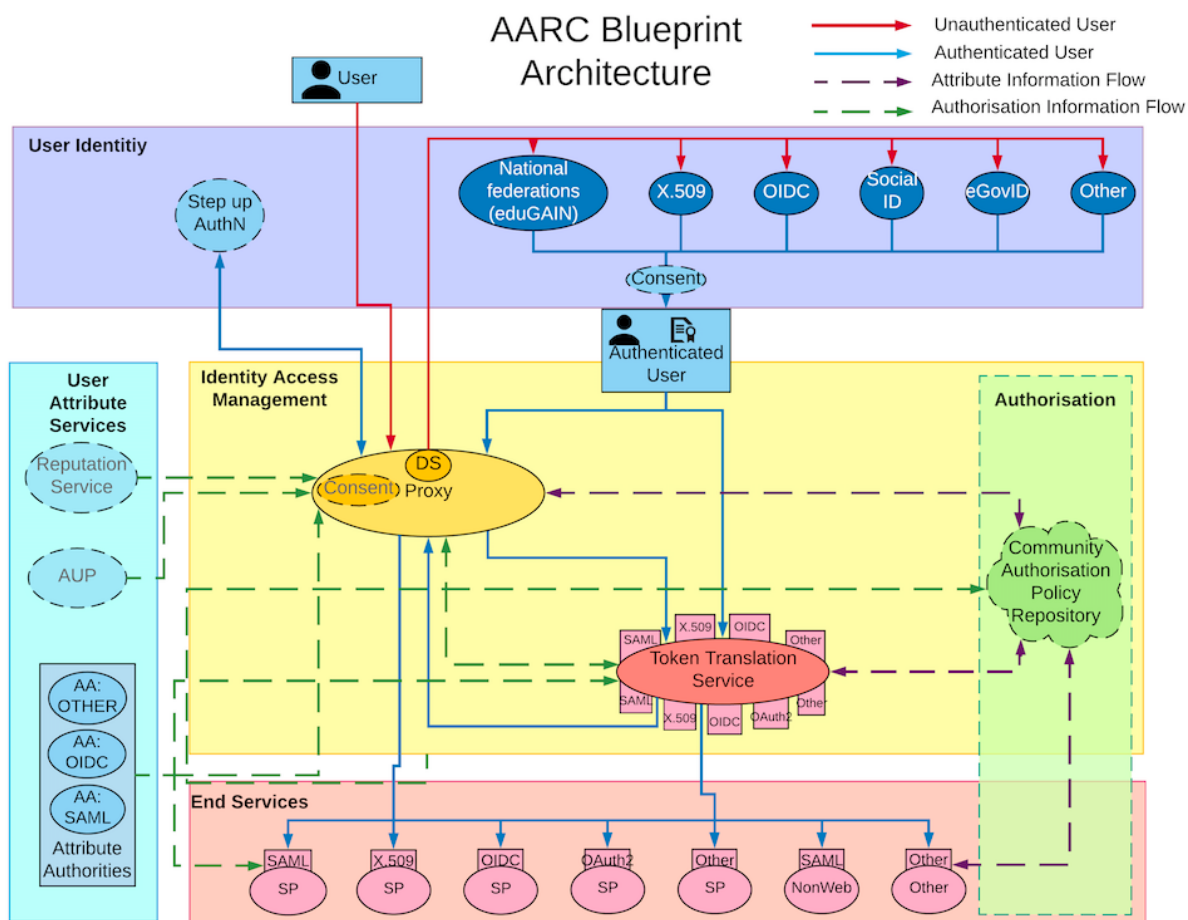


Figure 1: Current version of the AARC BPA

The lessons learned in AARC1 were used to better scope the plan for AARC2. **Two key aspects** in particular were strengthened in AARC2:

- **AARC2 focuses much more on implementation aspects of the AARC BPA and on research collaborations**, in fact many of them (9 research collaborations) participate in the AARC2 project with the purpose of implementing their AAls in a way that follows the AARC BPA. This is also reflected in the pilots that have a clear focus on deployment.
- The competence centre proposed in the AARC2 technical annex has been implemented under the name '**AEGIS**'. (The original name was too generic and, given the existence of other 'competence centres', it would have created confusion). AEGIS (AARC Engagement Group for Infrastructures) is proving to be extremely useful, not only because it validates AARC guidelines, but also to provide a forum for research collaborations and e-infrastructures to **discuss implementation details**.
- A **Community Engagement Forum (CEF)** has been introduced. CEF strengthens the engagement with research communities in AARC2 and beyond, and meets within [FIM4R](#). The role of CEF is to create a bi-directional channel between the AARC2 project and research communities to receive requirements and feedback on AARC2 proposed results.

Additional differences are highlighted in the table below.

AARC1	AARC2
AARC1 main goal was to deliver an integrated AAI (AARC BPA), address core security and policy aspects and promote federated identity management at large.	The focus in AARC2 is on enhancing the AARC BPA, offering policy and technical guidelines to facilitate its deployment, taking into account aspects such as ownership by the communities and cross-infrastructure use of resources.
A number of technology-driven pilots were necessary in AARC1 to understand which of the existing components would fit in the BPA. Pilots in AARC1 had a broader scope.	Pilots in AARC2 focus on supporting research collaborations in deploying AAI that implement the AARC BPA and that meet their collaboration needs.
The BPA focused mostly on authentication aspects; authorisation aspects were only looked at towards the end of AARC1.	AARC2 technical work focuses on defining concrete guidelines on different aspects that are critical for interoperability and deployment, such as authorisation models for service providers in research collaborations and e-infrastructures, on step-up authentication and assurance aspects.
AARC1 recognised the value of policies and contributed effort to build two main frameworks: Sirtfi (Security Incident Framework in Federated Infrastructures) and Snctifi (framework for the IdP/SP proxy that is the heart of the AARC Blueprint Architecture).	In AARC2 the policy work goes further, providing concrete guidelines and a policy toolkit for research collaborations. Guidelines cover assurance, GDPR considerations for research infrastructures and security aspects.
Not available	AARC2 offers consultancy to research collaborations: the AARC2 team works with research communities to analyse their use cases, derives technical and policy requirements and proposes the most suitable AAI architecture, which is then piloted in AARC2. This function was added after AARC1.
Libraries were a key targeted community in AARC1.	In AARC2 libraries are not in scope - however the project continues to support the promotion of AARC1 results in this space.

Table 1: Differences between AARC2 and AARC1

1.3 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).

1.4 AARC2 Partners and Structure

The AARC2 project runs from 2017 until 2019 and comprises 25 partners including NRENs, e-infrastructures, research service providers, SME 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 work together. The research and e-infrastructure requirements are the main drivers; the architecture and policy work packages address these. The policy provides 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 2: AARC work packages

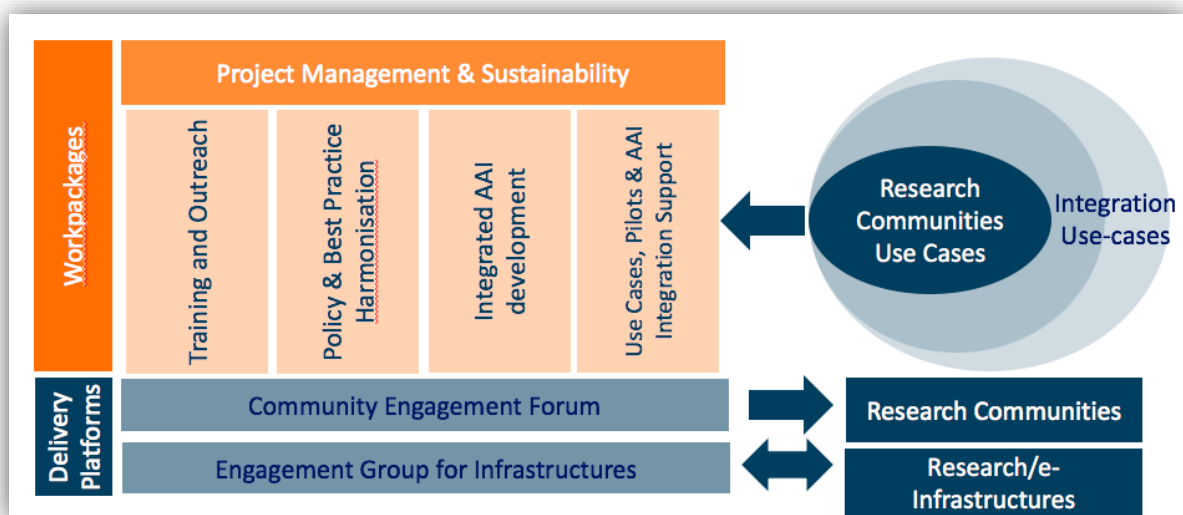


Figure 3: AARC work packages, AEGIS and CEF

1.5 The Role of AEGIS

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. AEGIS is part of NA2, however given its importance, it is the focus of a dedicated chapter in this document.

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 plays an important role in validating AARC2 results and helping towards their adoption. Plans are for AEGIS to continue beyond the AARC2 lifespan.

Currently, the membership of AEGIS includes the AARC2 Work Package leaders and two representatives from each of the participating infrastructures, namely, GÉANT, EUDAT, EGI, ELIXIR, PRACE, XSEDE and DARIAH. As more infrastructures are adopting the AARC results, the membership of AEGIS will expand. We are also in contact with the cluster of the Life Sciences communities participating in the CORBEL project, with CLARIN, LIGO, and NIH from the US.

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.

2018-05-14 AEGIS BRIEF

Created by [Christos Kanellopoulos \(GÉANT\)](#), last modified on Apr 30, 2018

Documents for consideration

i This section includes documents that have been developed by the AARC community and which are considered to be ready for adoption. Infrastructure representatives in AEGIS are requested to review these documents and consult with technical and policy experts within their infrastructures. At the next AEGIS meeting we will discuss the adoption of these documents in the production environments of the member infrastructures.

AARC-G031 Guidelines for evaluating the combined assurance of linked identities

The Research Infrastructures (from now on just Infrastructures) that follow the AARC Blueprint Architecture [AARC-BPA] set up their own AAI to grant access to their services. The AAI is typically based on a central IdP-SP proxy that act as a gateway for the Infrastructure services and resources. In order to assign an identity to the users of the research collaboration or the community they serve, Infrastructures rely on external Identity Providers and employ identity linking strategies.

The Infrastructures also define one or more assurance profiles, or a combination of assurance components, tailored to a specific risk assessment [AARC-G021].

In order to assign an assurance profile to a user, the Infrastructure shall evaluate the assurance components of the linked identity, or identities, used to register to the Infrastructure's AAI or used during authentication at the infrastructure proxy. These guidelines provide a method to combine assurance information and to compensate for the lack of it.

[\[MS Word\]](#) | [\[PDF\]](#)

Figure 4: Example AEGIS Brief

During the first year of the AARC2 project, AEGIS members endorsed two guidelines documents:

- [Guidelines on expressing group membership and role information \(AARC-G002\)](#) – endorsed in November 2017.
- [Exchange of specific assurance information between Infrastructures \(AARC-G021\)](#) – endorsed in March 2018.

2 Overview of AARC2 Results in Y1

Beside deliverables and milestones, AARC2 produces also toolkits, templates, and guidelines which are critical outputs to ensure adoption of AARC1/AARC2 results. The guidelines, in particular, are validated via a broad consultation beyond the AARC2 boundaries, before they reach AEGIS for feedback and endorsement.

Y1 Result	Addressed
6 new Guidelines (see Table 3) 1 AARC1 guideline updated	Deployment of AARC BPA and interoperability of AAls
First version Policy Development Kit	Adoption of Snctfi when deploying AAls that comply with the AARC BPA
Tested response model (MNA3.3) developed in AARC1 Incident simulation report	Improved responsiveness for actual incidents
Study on existing Acceptable Use Policies (AUP) with first version AUP template for research collaboration.	Baseline AUP among e-infrastructures
High assurance requirements (MNA3.5)	To inform assurance guidelines
9 pilots started	Deployment of AARC BPA in research collaborations to meet collaboration requirements
Identify training topics for research collaborations (MNA2.5)	

2 OIDC Training events	Supported deployment of OIDC among service providers in research collaboration
2 training events for research collaborations (EPOS and Life Science)	Presented FIM concepts, BPA key concepts and deployment benefits
Launched AEGIS	Adoption of AARC results by AAI operators
Launched CEF (Community Engagement Forum)	Research communities' requirements
5 Deliverables (see table 4)	Different topics as per AARC2 DoW

Table 2: Summary of AARC2 Y1 results

Summary of Guidelines
AARC-G002 Guidelines on expressing group membership and role information – endorsed by AEGIS Produced during AARC1, it was updated after the AEGIS consultation.
AARC-G021 Exchange of specific assurance information between infrastructures – endorsed by AEGIS
AARC-G029 Guidelines on stepping up the authentication component in AAls implementing the AARC BPA
AARC-G031 Guidelines for evaluating the combined assurance of linked identities
AARC-G040 Preliminary Proxy Policy Recommendations (application to the Life Sciences AAI)
AARC-G041 Expression of REFEDS RAF assurance components for identities derived from social media accounts
AARC-G042 Data Protection Impact Assessment - an initial guide for communities

Table 3: Summary of Guidelines produced by AARC2

2.1 Summary of Deliverables and Milestones for Y1

The list of deliverables and milestones for Y1 is available online on the [AARC wiki](#) for more convenient access: as well as on the [AARC website](#). All AARC2 documents and deliverables are publicly available under Creative Commons Attributions 4.0. The list of deliverables and milestones is shown in the tables below.

Deliverable Name	Led by	Type	Due Date
NA2			
Initial Information Package on AARC2 and Website Update (DNA2.1)	GÉANT	Website	M1
NA3			
Initial recommendations coordinated with infrastructures on accounting data sharing (DNA3.1)	KIT	Report	M12
JRA1			
Use-Cases for Interoperable Cross-Infrastructure AAI (DJRA1.1)	EGI	Report	M10
Authorisation Models for SPs (DJRA1.2)	KIT	Report	M11
SA1			
Results of Pilots with New Communities Part 1 (DSA1.1)	SURFnet	Report	M12

Table 4: List of Deliverables in Y1

Milestone Name	Type	Due Date
NA1		
Plan to engage with targeted communities and activities (MNA1.1)	Google Doc	M2

Milestone Name	Type	Due Date
Period review of WPs plans, KPIs, results, finances, request for sustainability plans and AARC2 participation at external events (MNA1.2a, MNA1.2b)	Internal doc on the wiki	M6, M12
NA2		
Kick start the Community Engagement forum (MNA2.1)	News Item	M2
Kick start the Competence Centre (now known as AEGIS) (MNA2.2)	News Item	M3
Review the content of the basic training material and plan new modules as needed (MNA2.3)	Google doc	
Identify topics for training with research collaborations (MNA2.4)	EPOS and Life Science training events delivered	M7
NA3		
Yearly plan	Information on the wiki information on the wiki	M1, M12
Define and test a model for organisations (IdP) to share information related to account compromises (MNA3.3)	Document	M9
Inventory of high-assurance identity requirements from the AARC2 use cases (MNA3.5)	Document	M9
JRA1		
JRA1 yearly plan (MJRA1.1a, MJRA1.1b)	Internal wiki page	M1, M12
SA1		
Detailed plan of pilots and resources based on the use-cases listed in Task 1 (MSA1.1)	Information on the wiki	M1
Detailed plan of the integration pilots with infrastructures in Task 2 (MSA1.2)	Information on the wiki	M2

Milestone Name	Type	Due Date
Initial plan for piloting advanced use cases and new technologies given input from JRA1 and NA3 (MSA1.3)	Information on the wiki	M3
Kick start and plan the year's work for Task 4 in collaboration with NA2 (MSA1.4)	Work started – documentation produced for Life Science and CTA pilots	M3

3 Work Carried Out per WP

3.1 Work Package NA1 – Project Management and Sustainability

The organisation that led each task is shown in **bold**. The work in this WP focused on:

Task 0 - Management (**GÉANT**, CERN)

- The work of this task focuses on supporting various teams to deliver according to plans. Following the kickoff meeting in June 2017, a meeting with Task Leaders and WP leaders was organised in September 2017 to identify points of collaboration across teams to avoid overlap. This task also manages:
 - the project board, which meets three times per year;
 - the Project Management Team (PMT), consisting of the WP leaders - monthly calls with the PMT take place to synchronise the work, while the board meets three times per year;
 - organisation of project meetings and project periodic reviews;
 - tools to support team day-to-day work (wiki, mailing lists, website etc.).

The task also defines the AARC remit and strategic directions and works closely with NAs on outreach and results dissemination.

Task 1 - Finance and Administration (**GÉANT**) - Defines reporting procedures and oversees expenditures.

Task 2 - Global Liaisons (**GÉANT**)

- Manages liaisons with the EC, other projects and other relevant stakeholders. The AARC2 project works closely with:
 - GN4-2, in the area of OIHC 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.

The task also defines strategies to engage 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):

- Identifies key exploitable results and defines approaches to ensure they can be maintained beyond the project lifetime. Effort is allocated to CERN, as well as to RETI and DAASI (which are the two SMEs in the project) to also work on this. **Work on this task started in March 2018** and will

continue in 2019. This will be an essential part of the work of NA1 during Y2; it is important to ensure that AARC key results can be maintained beyond 2019.

3.2 Work Package NA2 – Training and Outreach

This WP promotes AARC work and develops and delivers the necessary training modules. The work carried out in NA2 is organised in three tasks. This work package was initially led by GÉANT; in July 2017 it was agreed to transfer the leadership to Reti. The organisation that led each task is shown in **bold**.

Task 0 – WP Leadership (**Reti**):

- Coordination of the activity.

Task 1 – Outreach and Communication (**GÉANT**, EGI, LIBER, GARR, DAASI, MKZ):

- Maintains and updates the project website to showcase project activities and to engage with new communities and researchers.
- Supports the overall dissemination and communication activities, via case studies (in collaboration with the pilot work package), news and online information.
- Manages the **AARC Engagement Group for Infrastructures** (AEGIS) which supports the adoption of AARC results in research collaborations and e-infrastructures.
- **The Community Engagement Forum (CEF)** aims to raise awareness about AARC2's results among the wider research community. Exposes research collaborations participating in AARC2 and new research collaborations to the works of FIM4R, which is to date the broadest and most global group where federated identity is discussed among research organisations. AARC2 sponsored key people to attend FIM4R meetings and contribute to the 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.
- Provides support for the production and dissemination of AARC news and materials across AARC and partners' channels. AARC2 team has produced 14 blog posts, 3 articles published via the GÉANT Connect Magazine, 1 article published by GARR and 1 article published by EGI.
- Supported the dissemination of AARC2 results via social media.

3.3 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. The organisation that led each task is shown in **bold**.

Task 0 – WP Leadership (**Nikhef**):

- Coordination of the activity.

Task 1 – Operational Security and Incident Response (**CERN**, **KIT**, **Nikhef**):

- This task extends Sirtfi work and adoption to research collaborations. In Y1 the focus was on testing the Sirtfi incident response model (communications and the mitigating actions) developed in AARC1 by simulating actual incidents. In particular, cross-federation and cross-community aspects were evaluated: the simulated incident involved different research infrastructures (WLCG, LIGO) and a generic e-infrastructure service (RCauth.eu), and spanned four identity federations and two continents (to see the effect of time-zone differences on communications). The report showed that Sirtfi in itself is working, yet also highlighted points for improvement: it raised awareness of the procedures, the need for federation (not identity-provider level) security contacts, and suggests enhancement to the eduGAIN central response capabilities.
- Sirtfi adoption was supported by both training and specific consultancy, so that it has become a basic element of complementary policy efforts. (It is e.g. incorporated verbatim in the work done by GN4-2 on the Data Protection Code of Conduct, and in the LS AAI Policy Recommendations).
- The extension of operations security elements to community services (attribute authority operations) and to the operation of proxies has been targeted for Y2.

Task 2 – Service-Centric Policies (**KIT**, **Jülich**, **Nikhef**, **STFC**):

- When targeting data protection in traceability and in sharing of accounting records, it became clear in Y1 that many of the research infrastructures involved in AARC2 actually needed guidance on personal data protection and GDPR issues at an earlier stage in the process. ‘Resource usage accounting’ is the most visible place where personal data is collected and stored for a longer period of time; the same (but still limited) set of attributes is processed prior to infrastructure use. In the initial phase the task provides guidance and methodology for performing the required risk assessment for processing of personal data by the research Infrastructures. This is a fundamental ingredient in the balancing test required when using legitimate interest as the basis for processing (which is the model used by the GÉANT Data Protection Code of Conduct).
- Despite a significant amount of uncertainty about the interpretation of GDPR at the moment (and different member states still giving conflicting and confusing guidance even about the processing in academia and research collaborations), the scoped deliverable DNA3.1 (initial

phase) supports the execution of the risk assessment by communities and infrastructures and helps them explain decisions to their users.

- Guidance for proxy operations and cross-infrastructure harmonisation was developed to complement the work in JRA1. This includes specific **recommendations on how to use assurance profiles between infrastructures** (G021), the **treatment of social identities** (G041), and **targeted guidance for LS AAI Proxy operators** – supporting the SA1 pilot – in “Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)” ([G040](#)).

Task 3 – e-Researcher Centric Policies (STFC, BBMRI, EMBL(CSC), KIT, Nikhef, STFC):

- Work on assurance levels was performed in the context of the REFEDS Assurance Framework (RAF) working group. Aiming to define assurance components as well as a limited set of ‘profiles’ incorporating a specific combination of identity assurances, this framework has to balance community and infrastructure requirements against the feasibility of getting assurance components expressed by institutional identity providers through federations. Additionally, it has to work within the constraints of a standards ecosystem that separates authentication strength (single- or multi-factor tokens) from other assurance elements (identity vetting, unique identifiers, freshness of information). Although the high-level concept is well developed, and significant effort has been put into coordination with the REFEDS SFA and MFA specification work, the work is still ongoing. In order to gain operational experience, a pilot has been started with both European and US institutions to evaluate the deployment feasibility of the RAF assurance elements in existing home organisations.
- An extensive study of existing Acceptable Use Policies (AUP) was undertaken to perform a gap and complementarity analysis. The intended outcome of the study is an aligned AUP that allows a layered approach, in which the AUP presented to the end-user (at community enrolment or later) comprises a generic AUP component that is common to all e-infrastructures, plus a section with community-specific additions. The study is available (<https://wiki.geant.org/pages/viewpage.action?pageId=86736956>) and will be the basis for international consensus work on what is intended to be a joint AUP text.
- The assurance model and community-specific parts of the AUP (or ‘terms and conditions of use’) was also evaluated against sensitive data use cases in particular in the context of BBMRI. This specifically clarified targeted guidance for the operators of the Life Sciences AAI as to which elements of the AUP to present at which stage of the user enrolment process.
- In close collaboration with the EGI-ENGAGE and EOSC-HUB projects, two community framework policies were developed that support research infrastructures in securely managing the community attribute repositories, and in aligning community membership management processes so that users can seamlessly use generic e-infrastructures without the need for explicit sign-up (<https://wiki.geant.org/display/AARC/Community+Policy+Framework+Development>).

Task 4 – Policy Development Engagement and Coordination (STFC, CERN, EMBL (CSC), KIT, Nikhef, Jülich):

- To promote policy baselines and interoperability across infrastructures, a **Policy Development Kit (PDK)** was built in support of training activities and to act as a repository for infrastructures and communities to use as a source of current best practice templates (<https://wiki.geant.org/display/AARC/Policy+Development+Kit>).

- The PDK is in continuous evolution and will continue to be an important activity also in Y2, during which it will be trialled with specific European as well as national communities.
- Bringing together work from the other tasks within NA3, but also looking further afield at work in WISE (wise-community.org), EGI, EUDAT, PRACE, REFEDS, and CTSC (and the US NSF initiative), this task uses a process to identify and classify the community to determine policy needs, and it develops training modules (jointly with NA2) and targeted consultancy where appropriate.
- Collaboration with the IGTF has brought additional support and expertise in policy assessment methodology (leveraging structured peer review and assessment matrices), and has renewed the development of security and operational policies around attribute authority operations and trusted credential stores – which were applied to the BPA proxy elements for token translation and credential management for RCauth.eu-issued PKI user credentials. REFEDS continues to provide a key mechanism for both the adoption of AARC policies and concepts and as an important source of input to gauge the feasibility of policies directed towards identity federations and home organisations.
- The FIM4R (Federated Identity Management for Research, see fim4r.org) group was strongly reinvigorated with support from NA3, resulting in a new white paper bringing together FIM requirements from a much broader range of research infrastructures (from the ‘Arts and Humanities’ to the ‘Virtual Atomic and Molecular Data Centre’). This collaborative effort with inputs from many individuals and projects is essential for AARC’s harmonisation effort, and the new white paper provides both a basis for targeting new activities as well as a means of measuring the results of the technical and policy alignment achieved. As such, FIM4R is an essential mechanism for AARC2 and NA3 to steer developments, as well as to for CEF – which more than justifies the effort invested in bringing these very disparate communities together in expressing their AAI and policy requirements.
- The task also supports harmonisation of all AARC outputs through the Guidelines mechanism, which makes policy (and technical) recommendations easier to locate, re-use and apply.

3.4 Work Package JRA1 – Architecture for Integrated and Interoperable AAI

The aim of this WP is to expand the initial version of the blueprint architecture delivered during the AARC1 project by elaborating further on authorisation aspects and adding assurance elements. The WP also provides a number of technical recommendations aimed at infrastructures to facilitate their BPA deployment. The work in this WP is organised in five tasks. The organisation that led each task is shown in bold.

Task 0 – WP Leadership (GRNET):

- Coordination of the activity.

Task 1 – Tools and Services for Interoperable Infrastructures (EGI, GARR, KIT, GRNET and NIKHEF):

- Analyses and standardises user- and community-related information that needs to be communicated across infrastructures. In this context, the task refined the URN-based scheme that was proposed in AARC1 for standardising the way group membership information is expressed. The proposed scheme supports: indicating the entity that is authoritative for each

piece of group membership information, expressing VO membership and role information, and representing group hierarchies. It is worth noting that the related guidance document ([AARC-G002](#)) has been endorsed by AEGIS. The task has also investigated the various different user identifiers currently used by research infrastructures and e-infrastructures and has been working on a document (AARC-G026) for providing guidelines for expressing user identifiers when transported across AARC BPA-compliant AAls. Different strategies for generating these identifiers are also proposed.

- The task evolves the AARC BPA, focusing on cross-AAI interoperability aspects in support of the increasing number of use cases from research communities that require access to federated resources offered by different infrastructures. The refined version of the BPA offers a broader view that supports cross-AAI workflows.
- Collects feedback and requirements from SA1 and the research communities about cross-infrastructure use cases. Based on the analysis of specific use cases, the task has identified a set of generic cross-AAI flows (DJRA1.1). These generic flows will serve as inputs for extracting technical requirements that will drive the design of the new version of the blueprint architecture.

Task 2 – Service Provider Architectures and Authorisation in Multi-SP Environments (KIT, GRNET, NIKHEF, EGI, PSNC, DAASI, STFC, JUELICH and CESNET):

- Step-up authentication guidance ([AARC-G029](#)) – this document provides guidelines for stepping up the authentication component. It covers requirements and implementation recommendations, describes a proposed authentication step-up model, and outlines related work and documentation.
- Analyses the authorisation schemes that are currently in use or in development by infrastructures. The goal was to identify common authorisation models that have been documented in DJRA1.2. These common models will be used as the basis for providing guidance for managing access across large groups of Service Providers in a consistent, secure and scalable manner.

Task 3 – Models for the Evolution of the AAls for Research Collaboration (GARR, GRNET, JUELICH, KIT, STFC, CESNET):

- Analysed evaluation methods and compensatory controls that can be employed by infrastructures for assessing the assurance components associated with the identities used for registration and authentication. These methods support the evaluation of combined assurance in the case of identity linking. It should be noted that the guidance document ([AARC-G031](#)) has been endorsed by AEGIS.
- Study of existing registration processes and policies for the registration of OpenID Connect clients. The task has been investigating the use of the upcoming OIDC federation for infrastructures in support of a scalable and trusted registration scheme for the growing number of OIDC-based services.

Task 4 – Scalable VO Platforms (STFC, CESNET, EGI, GARR, GRNET, KIT, NIKHEF, SURFnet):

- Analysed roles and responsibilities in Virtual Organisations (VOs). The purpose was to investigate technical requirements arising from these responsibilities, in particular scalability issues and other technical issues such as the need for shared authorisation, or delegation (see [AARC-G036](#)).

3.5 Work package SA1 – Pilots on the Integrated AAI

The main objective of this WP is 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 supports 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 started in the EOSC context.

The work in this WP is organised in 4 tasks. The organisation that led each task is shown in bold.

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. 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 AAI in place, with which they offered data or services to their users, but at varying levels of maturity. However, none of the solutions was perfect; the AARC BPA offered a standardised approach to simplify integration of community-specific services (via the IdP/SP proxy) and to deploy federated access for them.
- To accomplish the goal of building, testing and implementing a pre-production AAI for each community, four different phases were identified, (1) requirements discussion, (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, selected the necessary AAI on the basis of community know-how and already-adopted tools.
 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.
 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 the SA1 work if they intend to build their own AAI.
- The results of each research community pilot and their current status has been summarised in deliverable [DSA1.1](#) – *Results on pilots with new communities* part 1.














Community	Links	Topics/Focus	Status
		Connecting services & Brokering Leverage the work done by AARC on policies and architectural blueprints Implementing Sirtfi Using eduGAIN	CONCLUDED
		Cross infrause case integration with EGI/EUDAT/PRACE Controlled, granular access to resources. Need for a good LoA scheme for AuthZ	IMPLEMENTATION
		Cross infra use case integration with EGI/EUDAT/PRACE Delegated federated access (non-interactive) Workflows	IMPLEMENTATION
	CTA Cherenkov Telescope Array	Initial implementation of Community IdP/SP proxy, Group/Role based access to resources, SIRTFI and CoCo/GDPR compliance	IMPLEMENTATION
		Integration, access for citizen scientist	IMPLEMENTATION
	CORBEL LifeSciences AAI	Inter compatibility, share a common AAI shaping according to the ideas in Elixir. Also focus on sustainability and operational aspects    	TESTING
		Non webstuff (SAML-X509) Implementation of Sirtfi stuff Solution for a persistent unique ID (ORCID?)	ANALYSIS
		Non web scenarios + enrolment workflows	IMPLEMENTATION
		Implementing an AAI according BPA to allow communication between Dariah and other infrastructures	IMPLEMENTATION

Figure 5: AARC2 Pilots with research collaborations

Task 2 – Pilots with Infrastructures (EGI, CESNET, DAASI, EGI, NIKHEF, SURFnet):

- The focus of this task is to enable researchers to access services offered by two or more e-infrastructures without the need for separate accounts for each of them (SSO across e-infrastructures). To accomplish this, JRA1 and NA3 work together to provide recommendations which will be tested in this task (SA1.2).
- Some work to this end started already in AARC1, with two cross e-infrastructure pilots: EGI-EUDAT and EUDAT-PRACE. During Y1 of AARC2, three new pilots were identified: GÉANT/eduTEAMS - EUDAT/B2Access; GÉANT/eduTEAMS - EGI/CheckIn; and DARIAH - EGI. The AARC2 pilots with infrastructures comprise both e-infrastructure interconnections as well as those with and between research infrastructures. Building on the two AARC1 cross-e-infrastructure technology pilots, in Y1 of AARC2 the team put these into the context of community use cases. Both the joint Life Sciences AAI (also known as the Corbel pilot) and DARIAH bring together generic e-infrastructures and research infrastructures, and were selected as AARC2 pilots. In support of the Life Sciences AAI, interoperability between the GÉANT eduTEAMS and EUDAT B2ACCESS as well as between eduTEAMS and EGI CheckIn were

added to the interoperability demonstrator. In the DARIAH context, a pilot was initiated that connects their community AAI to EGI (CheckIn). The GÉANT-EUDAT and GÉANT-EGI pilots subsequently formed the basis for the prototype Life Sciences AAI that was co-developed with the e-infrastructures for the benefit of the Corbel community. See the next task for more information.

Task 3 – Piloting Advanced Use-Cases and New Solutions (GRNET, CESNET, DAASI, GARR, GRNET), KIT, NIKHEF, SURFnet):

- As indicated in the AARC2 DoW, within this task, solutions are piloted that complement the nine AAI use cases provided by the research communities (piloted within Task 1) and the cross e-infrastructure integration issues addressed by task 2. Task 3 investigates advanced AAI scenarios by taking into consideration the results of AARC1 and building a feedback loop with JRA1 and NA3. Bearing in mind that it is difficult to have a clear demarcation line across the various use cases and pilots, the team felt that only the CORBEL pilot (now renamed as Life Science AAI) would be a good match for this task. There are some specific characteristics that make this pilot unique and very advanced:
 - the Life Science communities joined forces and agreed to deploy a community-specific 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, 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, IdP/SP proxy) are implemented by 3 different e-infrastructures (EGI, EUDAT and GÉANT). This also demonstrates that the AARC BPA can be deployed in different ways.

Task 4 – Creation of Showcases, Deployment Scenarios and Documentation (Reti, DAASI):

- One of the lessons learned from the AARC1 project was that pilots do not always have clear documentation once they are concluded. This poses some challenges with regards to their sustainability and adoption. In AARC2, this aspect is addressed from the start as for each pilot, technical documentation, case studies, training and general purpose leaflets are produced. This task also links to the more general sustainability work done in NA1. Material has been produced for the Life Science AAI, CTA and EPOS pilots.
- The task also works closely with the training team to provide inputs for delivering training to the research communities in AARC2.

4 Impact

The AARC1 project was particularly successful in creating an independent forum to enable research and e-infrastructures in Europe and beyond to get together and address shorter and medium-term interoperability aspects. AARC2 continues to support this facility and in fact makes this aspect stronger and more structured via AEGIS. AARC2 keeps encouraging alignment and integration of e-infrastructures' AAI offerings and services for the benefit of AARC2 use cases and communities. As a result of which communities are less inclined to build their own tools, but they prefer to relay on a limited number of building blocks (which are already used by other research collaborations) when selecting their AAI components. The key impact of the AARC2 project can be summarised as follows:

- Standardised AAI architecture (AARC BPA) to help 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.
- Streamlined policy and security framework by providing templates and guidelines to support research infrastructures in the operation of their AAI re
- Provided guidelines aimed at the AAI operators within research and e-infrastructures to support various needs.
- Supported research communities in analysing their use-cases and helping them design an AARC-compliant AAI that is suited to their needs and that they can manage.

4.1 Overview of KPIs as per DoW

The table below reports on the KPIs progresses as per AARC2 Description of Work.

Planned KPIs	Status	Impact
Deliver 3 pilots via SA1 in the first 10 months.	9 pilots ongoing: 1 concluded, 7 in development and 1 (Life Science) in testing/acceptance phase.	Makes it easier for different communities to benefit from the service offering of various e-infrastructures. Leverages AARC2 work to enable federated access in research communities.
Establish competence centre (AEGIS) with at least 3 infrastructures.	7 infrastructures in AEGIS to date	Ensures adoption of AARC results among AAI operators.

Planned KPIs	Status	Impact
Number of AARC recommendations adopted by infrastructures.	<p>6 new guidelines produced; 2 endorsed by AEGIS</p> <p>14 r/e-infrastructures deploying AARC BPA</p> <p>20 research communities in FIM4R endorsing the AARC BPA as 'the standardised' AAI reference architecture</p>	Ensures adoption of AARC results and advance technology to support open science and open access.
Number of MoUs signed with infrastructure providers.	2 MoUs in draft state (EOSC pilot and GN4).	Supports adoption of AARC results beyond AARC2 project
1 meeting per year of the Community Engagement forum within FIM4R.	CEF meets within FIM4R (3 meetings in Y1)	Bridges the gap between adjacent but unconnected scientific communities and promotes wide access to scientific data.
Offer 4 training instances on key aspects related to federated access and AARC2 results.	<p>2 training events delivered: to EPOS and Life Science communities.</p> <p>2 training events on OIIC aimed at SPs also delivered.</p>	Improves penetration of federated access in research communities and know-how about building an AARC-complaint AAI.
One common policy framework piloted by 3 infrastructures.	<p>2 available policy frameworks – Sirtfi and Snctfi.</p> <p>1 Policy Development Kit</p>	Reduces duplication of efforts in developing services common to various e-infrastructures.

Table 5: Overview of KPI

5 Conclusions and Plans for Y2

As reported in the document, the team has made significant progress towards the implementation of the AARC2 description of work. There have been some delays particularly with regards to the work in JRA1 and the related deliverables; this was due to the fact that JRA1 was impacted the most by personnel changes resulting from key people leaving their organisations. Furthermore, some topics required longer discussions to reach consensus than was initially envisaged.

During Y2, the team will focus on the following:

- NA1 will lead the sustainability work and have a clear roadmap for the post-AARC2 phase. Furthermore, NA1 will make sure that the MoUs with other projects are finalised and a report on the collaboration work carried out will be presented.
- NA2 will continue to deliver training that will focus on supporting SPs in the research collaborations in AARC2 to connect to the AAls resulting from the pilots. Also NA2 will continue to support the general outreach and promotion of all AARC results. To this end, specific training for the LS AAI community (to present the new AAI) is planned. The training will support service providers in connecting to the new AAI and existing AAI operators in migrating to it.
- NA3 will focus on the cross-infrastructure policy mapping framework, and on the development of an assessment methodology based on the Security for Collaboration among Infrastructures (SCI) framework. NA3 will also work on data protection for complex communities (i.e. communities with internal structure and intra-community control requirements) and aggregations of accounting data. The high-assurance use cases and validation of the intra-infrastructure and REFEDS RAF assurance profiles for working in research communities dealing with sensitive (human) data are scheduled for Y2. Further work on community policy alignment and baseline AUP will also continue.
- JRA1 will produce a new version of the BPA where the research communities are at the heart of the research collaboration, providing a so-called "community-first approach". The two main principles driving the new version of the AARC BPA are that (i) a user should be able to register once and then be able to access and share any resources available within a specific collaboration and (ii) a service provider should be able to connect its services to one point, if it chooses to do so, and make its services available to any community that it supports. JRA1 will continue to work to finalise the technical guidelines that are a key aspect in the adoption of the BPA and the big step forward towards the interoperability of AAls.
- SA1 will finalise all pilots and provide the necessary documentation and make it available for the benefit of other research collaborations. SA1 will also explore pilots with OIDC federations from the SPs point of view. The team will liaise with GN4-2 and other relevant groups.

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
DNA3.1	https://aarc-project.eu/wp-content/uploads/2018/04/AARC2-DNA3.1-Accounting-data-sharing-initial-phase.pdf
DSA1.1	https://aarc-project.eu/wp-content/uploads/2018/06/DSA1.1-v1.1FINAL.pdf
EPOS Training	https://docs.google.com/document/d/1haTFEOAhaBeGdzvopsXFofO00ma53AW4mX_RqN1e-jg
LS Training	https://drive.google.com/drive/folders/152fEspki5tH40P7kDep5OAchIn10wwh7
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

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
B2Access	EUDAT AAI service offering compliant with the AARC BPA
CEF	AARC Community Engagment Forum
eduTEAMS	GÉANT AAI service offering compliant with the AARC BPA
CheckIn	EGI AAI service offering compliant with the AARC BPA
EOSC Pilot	EC funded project
FIM4R	Federated Identity Management for Researchers
GN4-2	GÉANT Project
JRA1	AARC2 Joint Research Activity on Architecture
IdP	Identity Provider
SP	Service Provider
IdP/SP Proxy	IdP to SP proxy
LS	Life Science research communities
LS AAI	Life Science AAI
NA1	AARC2 Network Activity on Project Management
NA2	AARC2 Network Activity on Training and Outreach
NA3	AARC2 Network Activity on Policy Development
OIDC	OpenID Connect
PDK	Policy Development Toolkit
REFEDS	Research and Education FEDerations
SA1	AARC2 Service Activity on Pilots
Sirtfi	Security Incident Framework in Federated Infrastructures
Snctfi	Framework for the IdP/SP proxy that is the heart of the AARC Blueprint Architecture.