AARC
Technical Annex Part B

Research and Innovation actions

Authentication and Authorisation for Research and Collaboration (AARC)

List of Partners

Participants N	Participant organisation name	Country
1 (coordinator)	Trans-European Research and Education Networking Association (TERENA)	Netherlands
2.	Organisation Européenne Pour la Recherche Nucléaire / European Organisation for Nuclear Research (CERN)	Switzerland
3.	CESNET, zajmove sdruzeni pravnickych osob	Czech Republic
4.	CSC	Finland
5.	DAASI International GmbH	Germany
6	Verein zur Foerderung eines Deutschen Forschungsnetzes e. V. (DFN)	Germany
7.	European Grid Initiative (EGI)	Netherlands
8.	Consortium GARR	Italy
9.	Greek Research and Technology Network (GRNET)	Greece
10.	The JNT Association (JANET)	United Kingdom
11.	Forschungszentrum Jülich (FZJ)	Germany
12	Karlsruhe Institute of Technology (KIT)	Germany
13.	Association of European Research Libraries (LIBER)	Netherlands
14.	Moravská zemská knihovna v Brně, (MZK)	Czech Republic
15.	Stichting voor Fundamenteel Onderzoek der Materie (FOM-NIKHEF)	Netherlands
16.	Instytut Chemii Bioorganicznej Pan (PSNC)	Poland
17.	Groupement d'Intérêt Public Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche (RENATER)	France
18.	Science and Technology Facilities Council (STFC)	United Kingdom
19.	SURFnet B.V.	Netherlands
20.	SURFsara	Netherlands

Table of Contents

Figures

PART B

1. Excellence

1.1 Objectives

Collaboration and sharing of resources is critical for research. Authentication and authorisation play a key role in providing access to resources. During the last decade, national Identity Federations [FIM] for Research and Education have emerged across the whole of Europe and beyond. Based on the information available from REFEDS,[1] as of May 2014 there were 31 Identity Federations in production and 17 in a pilot phase operating for the R&E community worldwide. Thanks to the growth of national identity federations and to eduGAIN [eduGAIN] (the interfederation framework), federated access is gaining momentum as demand for it increases. The advantage of federated access is that the identity of users is verified by the institution that issues the users' credentials. Users can access different services with the same credentials [Single Sign-On] and research e-Infrastructures can offer resources in a more controlled and consolidated way.

Besides eduGAIN [eduGAIN] and national identity federations, various Authentication and Authorisation Infrastructures (AAIs) have been used to date in the R&E community. Known examples are eduroam [eduroam] (federated access to networks), AAIs operated by various research and education collaborations and e-Infrastructures[2] [e-Infrastructures] (EGI-AAIs, PRACE-AAI and so on) and Project Moonshot (to enable federated access to non-Web-based resources and services).

The lack of seamless integration among the different AAIs operated by the various research collaborations and e-Infrastructures, the non-ubiquity of federated credentials and technical and policy challenges are ultimately hindering the sharing of knowledge across the European and global research collaborations.

In addition to interoperability, functional gaps also exist. These aspects include support for aggregating information (attributes) needed for authorisation purposes from multiple attribute providers, better support for Single Sign-On [FIM] for non-web applications, and a diverse training package to cover both technical, legal and policy matters.

Although technical progress towards the integration of different AAIs has been made, the resulting pilots were primarily technical in focus and not organisational nor production oriented therefore their deployment did not proceed further.[3] To complement the technical aspects, integration of AAIs requires significant efforts to define a common policy framework that is supported by all e-Infrastructures to cover the necessary legal and operational best practices for those issuing users credentials, for those providing attributes and for the resource providers and for those in charge of managing interoperability between subjects previously listed, i.e. federation operators.

---

[1] REFEDS is the Research and Education Federations group led by TERENA.

[2] In the context of AARC the e-Infrastructures targeted are GÉANT, EGI, EUDAT and PRACE as well as the ESFRI cluster projects such as DARIAH and ELIXIR.

[3] Examples of this are various translation credentials pilots to convert SAML assertion [SAML] to x.509 certificates [X.509], integrated tools to manage groups, and solutions to support guest users.

The goals of the Authentication and Authorisation for Research and Collaboration (AARC) project address these challenges of interoperability and functional gaps. The objectives are based on the increasing expectation of researchers to be able to work flexibly and securely outside the walls and facilities of their own campus and the need to reduce administrational burden. The main goals of this project are:

1. **To develop an integrated cross-discipline AAI framework, built on production and existing federated access services (National Identity Federations and eduGAIN),** to serve researchers, students and educators. Scientific, educational and research collaboration is rapidly migrating to electronic environments. The ability to securely share and access resources and services across organisations has become a requirement. Although these groups may appear different, they have similar needs to securely and reliably access resources anytime anywhere with as few credentials as possible. All work-packages address this aspect from different angles. As significant work has already been invested by national identity federations and user communities to build and integrate with eduGAIN, eduGAIN should be seen as the anchor of the AAI framework for future developments.

2. **To increase the uptake of federated access within different research communities** by addressing the main technical and policy challenges that prevent seamless interoperability of existing AAIs , by supporting a wider range of (commercial) resources and services relevant to the R&E community and by tailored training. AARC has already identified a number of user communities with which to engage. Some of these communities are represented by the project partners, such as libraries (LIBER and MKZ), arts and humanities such as DARIAH [DARIAH] (represented by DAASI), bio-medical such as ELIXIR [ELIXIR] (represented by CSC) and high-energy physics (represented by CERN) and more are represented through the e-Infrastructures like EGI. It is the intention that other user communities will be consulted about the outcomes of the project as they mature. All of AARC's final results will be open for adoption by any interested community.

   This goal will be addressed by offering tools and tailored training for IT professionals to improve the adoption of federated access, both in terms of increasing the number of users that can obtain federated credentials and in terms of the number of services that can be accessed in a federated fashion.

3. **To pilot critical components of the proposed integrated AAI where existing production services do not address user needs**; results from the research activity and the network activity on policy harmonisation will be demonstrated via specific pilots in the service activity.

4. **To validate the results of both the research and service activities by engaging with the research communities** (e.g. FIM4R[FIM4R]/ SiG Federated Identity Management under the Research Data Alliance [RDA]) during the test phase. Feedback from the user-communities as well as from the research e-Infrastructures will be sought on both the technical aspects as well as on the policy and operational framework proposed by AARC.

To achieve these goals, AARC will:

- Define a trust framework for identities and attributes, with eduGAIN as the reference infrastructure, that can be supported and adopted by all stakeholders for international collaboration;
- Work with national identity federations and eduGAIN towards better harmonisation of national policies to ease cross-community collaboration and access to commercial service providers;
- Pilot solutions for group management/attribute providers, by integrating existing technical solutions;
- Offer support by means of outreach and training in the area of federated access and more in general on the main technologies, policies and legal aspects (including EU data protection laws [EU data protection]) underlying an integrated AAI;
- Increase the number of resources and services users can access once they obtain their institutional credentials;
- Improve interoperability between AAIs by defining adequate policies and procedures;
- Lower the thresholds for new user-communities to access resources offered by one of the research e-Infrastructures;
- Enable researchers to collaborate within secure and trusted virtual research environments where scientific resources and content can be accessed, used, stored and shared on a pan-European basis.

The technical work proposed for this project builds on the work delivered by the GÉANT project (in particular eduGAIN). It takes as input the FIM4R documents,[4] which identify the challenges for the wider adoption of federated access, the results of the study on "Advancing Technologies and Federating Communities",[5] and the output of the AAI workshop[6] held in April 2014 in Brussels, where identity providers and federations, content/community providers and research e-infrastructure providers met to express their requirements. This approach ensures user-community engagement, avoids duplication of efforts by reusing existing AAI systems, and creates the conditions to enhance them to meet the community requirements.

1.2 Relation to the work programme

As identity becomes a key priority for all e-Infrastructures, and the number of mature AAI systems in deployment increases, there is a consensus to work towards more integrated interoperability of existing AAIs, by developing interfaces between them and a common operational framework.

By focusing on technical integration and on the policy harmonisation of existing AAIs, the AARC project will facilitate access to resources and services and will improve collaboration between scientists in Europe and beyond.

AARC's goals fit with the technical and policy objectives of the EINFRA-7 call Horizon2020 as indicated below.

Call objective 1. **Facilitate the deployment and promotion of a pan-European identity federation for researchers, educators and students**.

4 https://cdsweb.cern.ch/record/1442597
5 http://www.terena.org/publications/files/2012-AAA-Study-report-final.pdf
6 http://www.terena.org/activities/AAI-Workshop/

- AARC will design and validate an AAI framework that will build on federated access and on the evolution of eduGAIN's interfederation approach. This not only achieves the cost-effectiveness of using existing AAI solutions, but will also offer an opportunity to enhance them to better support emerging requirements, hiding the complexities of different infrastructures from researchers and resource providers.

- AARC has budgeted for extensive training and outreach activities, with the aim of promoting federated access among libraries, institutions and resource providers. The content will take into consideration the results on the penetration of federated access in various research communities and where relevant and possible include developments from outside the research sector.

Combined, these actions will facilitate the deployment and promotion of a pan-European identity federation for researchers, educators and students, in compliance with existing identity interfederation efforts.

Call objective 2. **Lower barriers to entry for organisations to enrol in identity federations**

This objective will be achieved by:

- Identifying and demonstrating ways to offer ready-to-use solutions (whether commercially available or developed by participating partners) to easily create an Identity Provider [IdP] for institutions where manpower or know-how are limited. Possible target groups are small research institutes, small higher education organisations, libraries, museums, small data centres and their equivalents.

- Identifying and demonstrating ways to facilitate users who are not able to receive credentials from an institution (also known as guest users), such as independent researchers, or researchers from not (yet) federated organisations.

- Delivering technical support and training to make it easy for resource providers to offer federated access and to join a national federations.

A few key scientific community service providers (SPs), both commercial and non-commercial, will be technically supported by the project. These SPs are expected to join a national federation and enable federated authentication at the end of the AARC project. The goal is to engage actively with high-profile scientific community efforts (like the biomedical ESFRI cluster, EGI and the WLCG[7]) to produce a generalised best-practice for the use of federated access needed by, for example, scientific data SPs, and disseminate the results in training events organised by the AARC project.

Call objective 3. Overcome technical, organisational and legal obstacles for the implementation of an integrated and interoperable authentication and authorisation infrastructure

- One of the biggest challenges to implementing an integrated AAI is the orchestration of existing components to be integrated with cross-border and cross-organisational workflows, such as those of eduGAIN. A major aspect of the integration work will focus

[7] The Worldwide Large Hadron Collider computing Grid (WLCG) is the computational system to exchange the data generated during the experiments at the Large Hadron Collider at CERN.

on organisational, policy and legal aspects that must be acceptable to all stakeholders in Europe. AARC aims to create an ecosystem where users, identity and attribute providers, and resource providers meet efficiently and securely.

- Research will be conducted to offer solutions to scale beyond bilateral policy agreements that currently pose an unacceptable burden for those in charge of policy management within a research infrastructure; to use identifiers to collect attributes from multiple sources and to link them to the same person in a consistent manner and in line with the privacy laws.

- The combined set of policies and best practices addresses resource and service providers, research e-infrastructures, IdPs and federations. These policies are to be sufficient for addressing the identity management requirements associated with any research task.

Call objective 4. Enable the interoperability of different AAIs by researching the use of security token translation services and accounting services

This objective will be addressed as follows:

- To enable interoperability within e-Infrastructures, it is necessary to provide ways to offer collective services and to aggregate their accounting information via accounting services. AARC will develop recommendations for the processing of accounting data applicable within the whole AAI framework.

- It is also necessary to exchange authentication and authorisation tokens across heterogeneous environments; security token translation services make this process easy without disrupting existing AAIs. AARC will address this need through pilots of security token translation services and similar credential translation services to connect AAIs of different R&E e-Infrastructures and offer seamless authentication for the user.

Call objective 5. Allow for public access at large

The AARC proposal will achieve this objective by offering support to reduce the effort for institutions to join a national federation, support for guest users that are not be able to obtain federated credentials, and by identifying use cases that can be supported by social credentials (i.e. where usage-tracking is only required for statistical purposes etc.).

Call objective 6. Assess the penetration of existing identity federations at national level

An assessment of the penetration of existing identity federations is planned at the very beginning of the project (JRA1) to identify the user groups that are not using federated access. These user groups will constitute one of the important target audiences for the AARC project.

Call Objective 7. Offer training and outreach for data professionals

Training and outreach is a key activity for AARC. Different forms of training are foreseen as part of the project (NA2):

- Training for institutions (IdPs) on the key concept of data protection laws to ease the release of attributes;

- Training for scientific resource and service providers to understand what it takes to join a federation and to offer federated access;
- Training for libraries to enable them to replace IP-based access control;
- Training and dissemination of AARC's results;
- Reaching out to main user communities (e.g. ESFRI cluster projects) to obtain feedback on AARC's progress.

The training and outreach material will not be designed from scratch. Instead, existing materials created by the GÉANT project, NRENs and other e-Infrastructures will be reused and enhanced as needed. This material will be disseminated both by making it available on the AARC website and through face-to-face training as part of NA2.

1.3 Concept and approach

1.3.1 Concept

AARC work is driven by the principle to support the collaboration model across institutional and sectoral borders encountered by large-scale research initiatives and to advance mechanisms that will improve the experience for users and guarantee their privacy and security.

The concept behind the AARC project is to build on existing AAIs used in the R&E sector (i.e. national federations, eduGAIN, ESFRI cluster's AAIs, International Grid Federations and so on), to analyse them in light of user requirements, integration aspects and security, and to design, test and pilot missing components and integrate them with existing working flows.

There is a consensus that most of the technical components have already been developed and, to a certain extent, tested. The main research work in AARC will focus on verifying whether their integration in the existing workflows is possible and cost-effective and whether the harmonisation of their operations is achievable.

AARC's exploitation plans foresee that existing e-Infrastructures (such as GÉANT and EGI) will deploy AARC's results in their production services. This is a strategic choice, based on the consideration that existing e-Infrastructures are better positioned to deploy services, to operate infrastructures and to implement any recommendations and best practices to guarantee sustainability and support for their communities.

AARC will take advantage of the fact that different stakeholders are jointly participating in the project to benefit from their expertise in operating services according to the requirements of their user constituency. By bringing together in one consortium different e-Infrastructure providers, as well as libraries and user-communities, AARC will engage at equal level with all stakeholders to ensure the proposed integrated AAI framework can support their needs.

AARC's results will be beneficial for various stakeholders in the R&E sector, which are also represented in the consortium and depicted in Figure 1, namely:

- e-Infrastructures, eduGAIN (GÉANT), EGI, EUDAT and PRACE to facilitate federated access to the resources they offer;
- Libraries, to empower them to deploy federated access and therefore help increase the penetration of federated identity;
- ESFRI cluster projects (DARIAH, ELIXIR, etc.);

- Individual research communities to enable them to reduce the number of credentials they need to manage in order to access e-Infrastructure services;
- Individual researchers, students and educators, who will benefit equally from a framework where identity provisioning is already an integral part of establishing pervasive AAI for researchers' use cases.

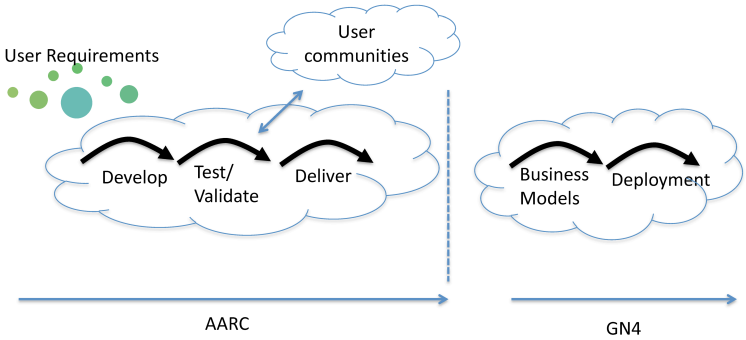

Figure 1: AARC's organisational concept

1.3.2 Approach

The consortium has set the following principles to guide the execution of the plan:

- Drive the work based on the community requirements and demonstrate flexibility in satisfying these requirements;
- Take eduGAIN as the starting-point and enhance it to make it the foundation of the next-generation AAI to support libraries, ESFRI cluster projects, existing and new research communities in their daily work.
- Build the integrated AAI on eduGAIN but also allow for interoperability with existing AAIs in relation to the use-cases;
- Consider the issues related to data privacy, intellectual property and cultural barriers to pertain to the sharing of data generated through the use of federated AAI. The AARC project considers the issues related to sharing of research data to be the remit of dedicated research data management projects;
- Adopt a collaborative approach when delivering AARC results, both between partners within the Consortium and with external partners;
- Make all AARC results available on a public website or wiki, to make optimal use of public funds;
- Deliver AARC results to existing e-Infrastructures for sustainability and future operations.

The AARC project has been conceived as an exploitation project aiming to build on the developments and deployments in the AAI areas that led to the current AAI frameworks in use to date in the R&E community. While previous projects have addressed a specific community and, based on their requirements, have delivered the most suitable AAI, AARC will work horizontally. Federated access is considered the most effective way to share resources across borders as well as across Europe. There is consensus in favour of using eduGAIN as the main building block of any future AAI, due to the investments made so far, the experience gained

with it, and its ongoing uptake beyond Europe.[8] At the same time, there is a need to interoperate with the other AAIs in use to date in the R&E area, and to mediate among heterogeneous requirements that call for easy-to-use solutions, for high level security and privacy, and for the support of different technologies.

The project has been structured as follows:

- A networking activity on "Project Management" (NA1) to:
    - offer the overall management support tools to ensure that AARC goals are met;
    - deliver an exploitation plan and an overview of the main achievements of the project at its end.

- A Networking Activity on "Training and Dissemination" (NA2) to:
    - disseminate, reach out and offer different types of training to the communities targeted by AARC (libraries, arts and humanities, universities, ESFRI cluster projects and FIM4R);
    - support external communications, promotion and liaison with other groups and projects.

- A Networking Activity on "Best Practices and Policies Harmonisation" (NA3) to:
    - define a cost-effective operational and policy framework to create a secure framework in line with resource providers' requirements, national identity federations frameworks and compliant with privacy laws, and to integrate it with the technical framework.

- A Joint Research Activity on "Integrated architectures for R&E AAI" (JRA1) to:
    - deliver the design of the integrated AAI framework, by enhancing eduGAIN and researching ways to integrate additional technical components to support a wider range of use-cases than to date.

- A Service Activity on "Integrated architectures for R&E AAI" to:
    - pilot and validate the results of JRA1 and NA3. All demonstrations and pilots will be carried out in the SA, which will be influenced by, and will influence, the final results of both JRA1 and NA3. All pilots will be tied to concrete user requirements, ensuring that these are represented consistently throughout the innovation process. User communities will be asked to engage during the pilot phase.

The proposal has activities in all areas relevant to ensuring that technical and policy work to design an AAIs framework can be achieved, that support for pilots targeted at users across the R&E community can be supported, and that training and outreach can be delivered.

[8] The GN3plus project is working together with REFEDS to expand the policy framework of eduGAIN to facilitate the exchange of personal data outside Europe.

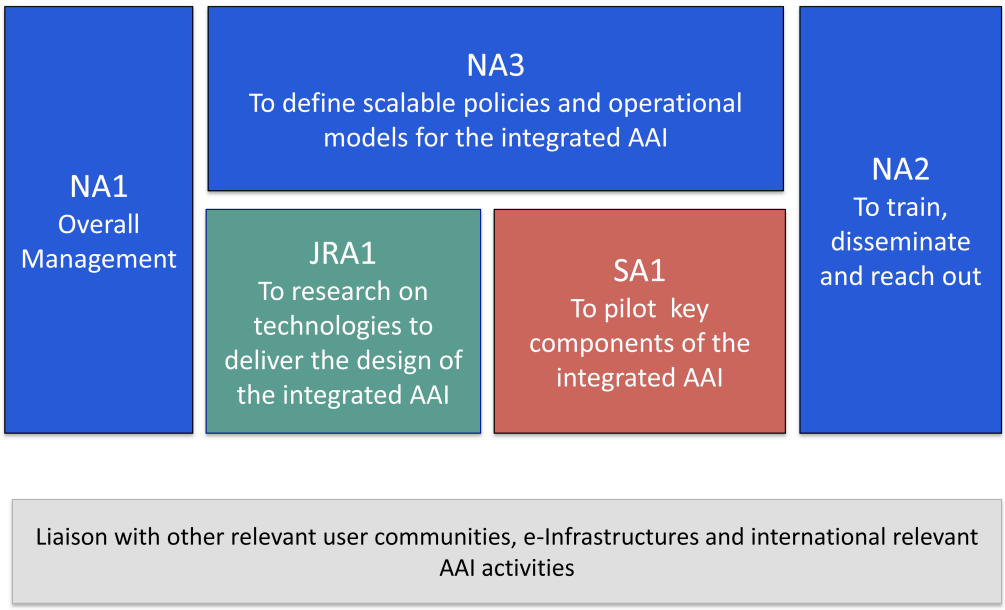

Figure 2: Approach

1.3.3 Relation to the GÉANT Project, EGI, PRACE and EUDAT

GÉANT
This proposal has been conceived to complement the work carried out in other areas, most notably the GÉANT project, which is being prepared at the same time as AARC.

GÉANT's mission is to deliver world-class services with the highest levels of operational excellence to research and education communities within Europe and beyond, helping to develop talent and providing opportunities for communication across the divides of resources and distance, and so promoting the free, unimpeded movement of scientific data and knowledge.

Besides including a sub-set of the NRENs that are also participating in GÉANT this proposal also includes user communities and other e-Infrastructures. It seems obvious that whenever results are expected to be deployed at federation level, the involvement and support of the eduGAIN team will be required.

The primary difference between AARC and GÉANT is that the E-INFRA-7 call offers a greater ability to directly support user communities, to access key experts across the various research and education communities, and to reach out to more elements in the supply chain. As opposed to the GÉANT project, which caters to one community (the NRENs), the AARC project is, by design, cross-disciplinary (as shown by the profile of its consortium), has a strong focus on integration rather than on research to enhance a specific product (i.e. eduGAIN), and has the budget to offer training aimed at different stakeholders. The success of AARC pilots

are assessed based on user community feedback, which will indicate how AARC-proposed solutions impact on the success of their operations. This feedback will then be documented and integrated with eduGAIN.

Specific items of work that will be delivered in coordination with the GÉANT project include:

- Training and outreach – GÉANT (along with national identity federations) already has material that can be made available for wider outreach. AARC will produce additional material to address specific user-community requirements and to promote and validate the results of the pilots. While GÉANT is directly aimed at NRENs and funding is allocated for that purpose, AARC will support training for libraries, research communities and institutions.

- Incident Response – AARC is well positioned to make an inventory of the existing documented practices in the R&E federations, as well as on the community requirements and to propose recommendations for an operational framework for security and incident response. AARC will carry out the research and pilots implementation aspects to that extent, whilst GÉANT will transition applicable results to the production of eduGAIN services. The work in this area will be anchored to the SCI requirements to which PRACE has contributed. This work will therefore satisfy some of PRACE's requirements as well.

- Levels of Assurance (LoA) – This work will map the R&E identity federation supported assurance levels with the requirements of the initial set of resource and service providers and e-infrastructures (enhancing the work done in the Gn3plus project by the Enabling Users). The result, a framework adopted by the R&E community, will be a minimum assurance level that is needed to offer a trustworthy framework. This assurance level will be validated by REFEDS and the GÉANT project will look at the business model and deployment implications for eduGAIN.

EGI

The **European Grid Initiative**, EGI, is a high throughput and cloud infrastructure distributed across 40 countries in Europe and beyond. The EGI partners provide resources and services to diverse research disciplines from high energy physics to life sciences, computational chemistry and the humanities. EGI's participation in AARC will ensure that the requirements of the communities served by EGI are supported.

PRACE

The **Partnership for Advanced Computing in Europe**, a project co-funded by the EC, offers world-class computing, data management resources and services open to all European publicly-funded researchers. Although not directly participating in the AARC project, they are represented by SURFsara and Jülich partners.

EUDAT

The project will liaise with EUDAT, the EC-funded multi-domain project to tackle the problem of data deluge. AARC will carefully evaluate the results of EUDAT with regard to the integration of heterogeneous AAIs to access data resources and take their experience into account. Liaison with EUDAT will be established via joint partners.

1.3.4 Engagement with REFEDS

REFEDS (Research and Education FEDerations) is the international body led by TERENA to coordinate Identity Federation processes, practices and policies and to discuss ways to manage interfederation work. REFEDS has a global membership of R&E federation operators.

As the scope of the work carried out in AARC relates to identity federations REFEDS is the best forum to disseminate AARC results and to obtain feedback on these results from the global federation community. AARC results must be shared with the wider, global stakeholder community to give them the ability to participate, criticise and endorse the results prior to any handover to operational contexts such as eduGAIN.

Additional advantages of this approach are:

- More efficient use of available people and travel time within the community
- Better engagement with the community
- Increased ability to contribute to standards as REFEDS documents plan to enter the IETF RFC process.

1.3.5 Engagement with other relevant groups: RDA, FIM4R, ESFRI cluster projects

FIM4R

FIM4R, the Federated Identity Management for Research group is a collective body of eResearch infrastructures with consistent and well-specified requirements for AAI. They are currently also forming a Special Interest Group within the Research Data Alliance [RDA]. There are existing relationships with this group, which will be maintained. AARC will seek collaborations/pilot participants for services within this group as a body representing many user communities engaged in AAI. These collaborations will be coordinated with the work of the GÉANT project.

RDA

The Research Data Alliance, RDA, together with the FIM4R group will offer a good platform to publish results and to engage with user communities with a special focus on the operations.

ESFRI

The European Strategy Forum on Research Infrastructures, ESFRI, is a strategic instrument to develop the scientific integration of Europe and to strengthen its international outreach. Their mission is to support a coherent and strategy-led approach to policy-making on research infrastructures in Europe. In the strategy report on European Research Infrastructure roadmap [ESFRI], ESFRI has identified 44 research infrastructure projects from the broad disciplines of Social sciences and humanities, Environmental sciences, Energy, Biological and medical sciences, Materials and analytics facilities and Physical sciences and engineering.
AARC will liaise with this group via common partners. AARC will particularly collaborate with the ELIXIR [ELIXIR] biomedical project and DARIAH.

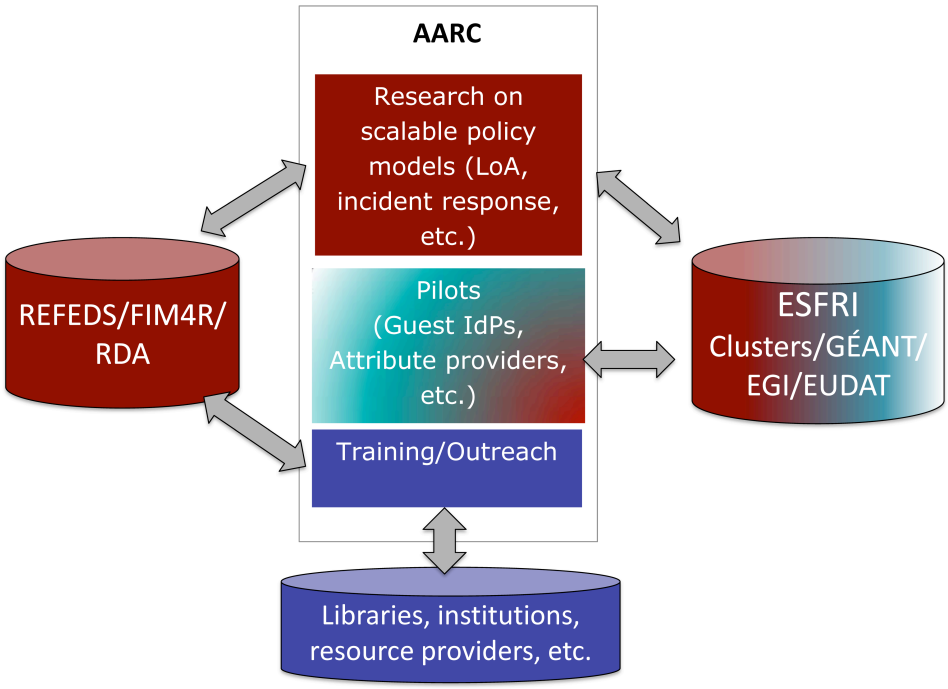

Figure 3: Relationship between AARC and other relevant groups

1.4 Ambition

The ambition of AARC is to avoid a fragmented future, where different e-infrastructures and new research collaborations develop and operate separate and independent AAIs, hindering cross-discipline interoperability and introducing extra costs.

AARC recognises also that there is a long history of user familiarity with existing AAIs and considerable valuable investment made to date, and that a greenfield approach is therefore inappropriate. By designing and validating a model for an integrated AAI framework to serve researchers, students and educators, AARC will move towards the implementation of its vision to allow researchers to use their existing credentials to access a wide range of services offered by existing research e-Infrastructures and other service providers.

As stated above, the AARC project will contribute to delivery of the enhanced version of eduGAIN, meeting requirements of a wider audience so that libraries, ESFRI research infrastructures and research communities can depend on it as part of their computing models for the future.

This will be achieved by using a more distributed approach to handle authentication and attribute provisioning and to define procedures to assess the quality of the attributes.

AARC will prioritise aspects in the design of the integrated AAI that address use-cases and will demonstrate them via pilots. These include (i) testing the integration of distributed group management/attribute providers with the (e-infrastructure) services to implement attribute-based authorisation; (ii) showcasing and testing solutions for guest identities; (iii) providing

proof of concept to improve federated access to e-Infrastructure resources and services, including non-web services and offerings by commercial service providers.

The main criteria underlying AARC development can be summarised as follows:

- Make access to resources easy for users by reducing the number of credentials and by using mechanisms to hide complexity and to transparently translate credentials among the systems.
- Create the conditions to allow identity to become a core element of e-infrastructures, as has been the case for network connectivity for many years already.
- Harmonise policies among e-Infrastructures to make it easy for resources and services providers to offer their services on a cross-border and cross-organisation basis.

2. Impact

2.1 Expected impacts

The impact of AARC is targeted based on the assumption of a two-year project.
The main impacts of the AARC project and their related Key Performance Indicators (KPIs) are summarised below:

1. **Facilitate sharing of research results across disciplines**
   KPI: A research service is available across three disciplinary communities.

2. **Harmonise procedures and policies to ease cross-discipline collaboration**: KPI: Pilot the adoption of incident response procedures in 5 IdPs.

3. **Facilitate the integration of (commercial) resources and services** that are deemed critical for the R&E community
   KPI: 3 new SPs available in eduGAIN.

AARC's contribution to the additional key impacts set out in the call for proposals is described below.

Call Impact 1. Interoperability of e-Infrastructures is improved

AARC will improve **the interoperability of e-Infrastructures** by delivering the design of the integrated AAI for R&E, which will lay the foundations to harmonise and integrate existing AAIs. Key aspects that will be analysed and researched include:

- Scalable models for authorisation, which will facilitate access to services available in different e-Infrastructures;
- Innovative operational models to meet resource providers' requirements and to create a secure ecosystem for researchers, students and educators;
- Innovative business models in the context of level of assurance (LoA) to design a cost-effective LoA framework by either using existing framework or adapting them to meet resource providers and institutions requirements.
- Advance the work to improve single sign-on for non-Web applications, by deploying the results coming from the GN3plus project (and other relevant R&E projects) and applying operational considerations.

- Work towards the adoption of common policies among e-Infrastructures. The lack of shared policies as well as the lack of harmonised procedures among different e-Infrastructures is one of the factors that hinder interoperability.

KPI:

- At least one generic attribute provider pilot;
- Adoption of the incident response procedure at 5 IdPs.

Call Impact 2. Reduced duplication of efforts for developing services common to various e-Infrastructures

AAI has become a critical service for all the e-infrastructures as well as for any collaborative groups. Developing different solutions per user community is not an option, as this increases development and operational costs, duplicates the users management and has an impact on interoperability. For example, the provision of secure controlled access to data is a requirement for many biomedical or linguistics datasets. At present, users must repeatedly fill in similar, but service- and data-specific paper forms to apply for access to these independently controlled data sets; the service providers need to keep track of the these users and their affiliations over the time period for which data access is granted. This paper process would benefit from a more consistent electronic approach, where federated AAI solutions (including access control and accounting) would make the whole process more efficient (see ELIXIR preparative work[9]).

Although the situation to date does not yet allow for seamless usage of credentials across e-Infrastructures, AARC's work will offer mechanisms to leverage the authentication process among different e-Infrastructures, to retrieve additional information about users via attribute providers or group management and to feed this information to the resource for authorisation purposes. In practice, this will distribute the management of identities between identity providers and attribute providers, reducing the overall service management costs.

KPI:

- 2 successful cross-infrastructure use cases delivered.

Call Impact 3. Contribution to the creation of an Europe-wide single sign-on framework to enable research

As highlighted in the FIM4R report and in the AAI workshop, there is increased consensus for using eduGAIN as the authentication framework for the R&E community. AARC will work to address the key areas identified during the AAI workshop[10] to design a Europe-wide single sign-on for Europe. AARC will build workflows, interfaces and solutions to optimise the existing AAI platforms and provide an operational and security framework with shared procedures to handle incidents.
In this context, AARC will also identify opportunities and challenges to leverage R&E credentials with eIDs (work planned for JRA1).

By delivering an integrated AAI framework, AARC will improve access to digital libraries, data and computing facilities worldwide. This will make it easier for researchers to contribute to

[9] http://tnc2013.terena.org/getfile/870
[10] These areas are: attribute release, level of assurance, Single-Sign-On for non-web applications, improve cross-discipline collaboration.

large or small, global or European research projects with a minimum of administrative overheads.

KPI:

- Enable federated access in at least each community represented in the project (libraries, arts and humanities, biomedical). At last 2 resource or services to be available via eduGAIN at the end of the project.

Call Impact 4. Expanding the coverage of federated access to support a wider range of resource providers

This impact will be achieved via different types of actions, namely:

- By researching and piloting solutions to make it easier for institutions to create an identity provider and to support guest users;
- By offering training on key aspects that are related to federated access;
- By working with resource providers in different R&E fields (ELIXIR, EGI, etc.) to enable federated access;
- By integrating some commercial service providers in the area of pay-per-use and contracted services.

KPI:
At least 3 new SPs and at least 3 new IdPs.

Call Impact 5. Social-Economic Impact

With the recognised importance of research and education for the future economy of Europe and hence for the social well-being of our societies, the socio-economic impact of AARC concept will be significant.

The AARC project will meet the key requirements of the research and education community in Europe and beyond by providing a framework to manage identities, including the use of personal identifiers, to offer interoperability of different user credentials. This will create a dynamic environment where identity and attribute providers and resource providers efficiently and securely meet.

The socio-economic impacts of AARC will be realised as follows:

- A secure, privacy-protecting and easy-to-use AAI framework to facilitate international collaboration and data sharing by increasing the quantity and quality of research outputs.
- Research is in general carried out internationally. An enhanced AAI framework will empower researchers to share their findings by retaining ownership and defining different access rights regardless of the geographic locations.
- AARC's results will also reinforce Europe's position as a hub for global research, thus creating the best possible conditions for European researchers to work on collaborations that span beyond Europe.

In summary, AARC's AAI framework will play an incremental role in the transformational impact for the international scientific and educational communities as user mobility increases and the amount of relevant data proliferates. No matter where they are, researchers can have access to the same rich set of supporting services from the network as at their home institution, including access to data and computing services, allowing them to contribute to

large or small research projects across Europe and the rest of the world with a minimum of administrative overheads and without worrying about geography.

With such impacts, AARC will open up new prospects for advanced services for science and education and for building trust to share research data.

2.2 Measures to maximise impact

2.2.1 Dissemination and exploitation of results

The main objective of the AARC project is to serve the research and education community in Europe and beyond by designing and validating an integrated AAI framework to facilitate world-class research. It is expected that the AARC results will be exploited by the existing e-Infrastructures already operating AAIs, integrated with their own plans. At the end of the project AARC will deliver an exploitation plan to offer recommendations on how best to integrate AARC's results in the existing AAI workflows and also to propose any additional collaboration with commercial parties that may be useful for reaching out to communities. AARC partners are represented in European and global initiatives dealing with technology, standards and future service visions relevant to the delivery of federated services to the R&E community.

One of the target candidates to exploit AARC's results is GÉANT due to the impact on eduGAIN; national identity federations are also expected to endorse and deploy AARC's best practices with regards to incident handling and policy best practices. Lastly, identity providers are expected to follow AARC's best practices with regards to level of assurance and attribute release policies.

All AARC results (apart from exceptional cases) will be freely, easily and openly accessible not only to AARC partners but also to the wider R&E community. The results from the project will be disseminated through the partners' channels to peers, industry and other e-infrastructure endeavours worldwide. AARC will engage with other groups (REFEDS, RDA, etc.) to reach as many communities as possible beyond consortium members. This broad participation is also the main channel for the project to disseminate the results and to wield global influence on future standards and developments.

Specific dissemination activities have been planned for libraries, resource providers and research communities to promote the AARC results, as well as to deliver training on the main AAI best practices and tools in use to date. Mechanisms to ensure that the training and outreach are widely disseminated include availability of this material via the AARC website, using popular social media and developing PR material for the general public.

All property rights will be managed via the consortium agreement and in line with the call by using an industry-friendly open source license for software and "CC-BY" type of license for documents.

NA2 will also ensure that AARC is represented at key global networking events and manage contacts with relevant international bodies. The objective of these dissemination activities is to deliver information about AARC results in a coordinated fashion. AARC's results will also reinforce Europe's position as a hub for global research, thus creating the best possible conditions for European researchers individually, in international research.

2.2.2 Communication activities

The AARC project will hold different types of communication events, as listed below. These activities will target different audiences of stakeholders to address their specific needs.

- Participation at main conferences to report on AARC's results as appropriate, i.e. TERENA Conference, RDA conference, LIBER conference, EGI events etc.;
- Thematic training events, whether delivered online as webinars or face-to-face;
- Dedicated meetings with research communities and resource providers (one to take place at the start of the project) to engage with them to shape the format and the content of the training and to prioritise the work to undertake and the services to support. Ideally this event could be co-located with REFEDS or RDA meetings;
- Project meetings, where all partners will be asked to participate to disseminate and discuss progress and achievements.

3 Implementation

3.1 Workplan — Work packages, deliverables and milestones

The work of this proposal will be carried out through a complementary set of activities: networking activities, a research activity and a unifying service activity.

The structure of the project (depicted in figure 3) has been constructed to support AARC's main goals (i) to design the integrated AAI framework to support user-community use cases, (ii) to validate the key components, engaging with the communities that provided the requirements and (iii) to provide extensive training, outreach, and dissemination on both technical and policy aspects.

These will be supported by a management work package (NA1) and a dissemination, outreach and training work package (NA2). An exploitation plan will be provided at the end of the project.
The overall project governance has been kept simple, to reduce overheads as much as possible without compromising the overall coordination. The work package leaders together with the project coordinator will have regular virtual meetings to report on progress, issues, new opportunities, deviations from the work plan and so on, whilst the day-to-day work is left in the hands of the work packages and task leaders.

A short description of the key tasks of each work-package is provided below.

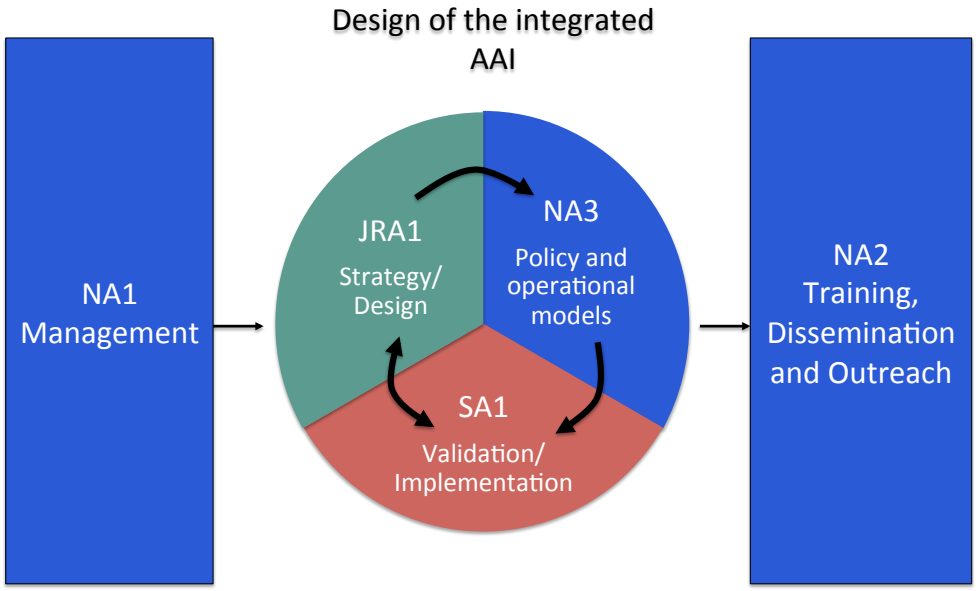

Figure 4: Work packages

NA1: Management

This activity is in charge of the overall project management, overall planning, organisation, resourcing and quality control of the project to ensure that the goals are achieved, optimising costs, time and resources. NA1 will also be in charge of organising the main project meetings and ensuring the web presence and day-to-day working tools are available to all partners.

The goal of NA1 is to coordinate and manage the consortium to accomplish desired goals and objectives using available resources efficiently and effectively.

The oversight of project activities is devolved to the activity leaders and task leaders. Coordination among the various tasks will be ensured via regular contact among the activity leaders and task leaders and coordinated via NA1.

NA2: Training and outreach

A primary objective of this project is to promote and further deploy federated access for researchers, educators and students. Dedicated training and outreach material should help to lower barriers to entry for organisations not already participating in identity federations.

Whilst the national deployment is the responsibility of the NRENs and/or equivalent organisations in a country operating the national identity federations, there are some common challenges that can be tackled at European level as identified in the Study on “Advancing Technologies and Federating Communities” and the AAI Workshop held at the EC premises in April 2014.

This NA will focus on a set of key aspects to address based on these common challenges. Phase one of the training plan will focus on these challenges with the initial target communities

(ELIXIR, EGI and WLCG); Phase two of the training plan expects that additional training and outreach will be needed in the second year to disseminate the results of JRA1, NA3 and SA1.

The research communities targeted in this project will take responsibility for the training and outreach in that specific community.

This NA has two main objectives:

1. To offer training following the train-the-trainers model, on the technical and policy aspects of federated access and addressing specific challenges. The trained people will in turn organise training for their community or their country.
2. To create an outreach package to promote the results coming from JRA1, NA3 and SA1, particularly concerning support for guest IdPs and attribute release.

NA3: Policy and Best Practices Harmonisation

The diversity in practices between the R&E federations across Europe (and the even wider assurance divide between R&E federations and social media identities) makes it hard for resource providers (as well as user communities) to offer pan-European services with a single known 'risk' level. This diversity is addressed by NA3.

NA3 will produce operational and security aspects as well as policies to complement the technical research work carried out in JRA1. This work package will deliver a set of recommendations and best practices to implement a scalable and cost-effective policy and operational framework for the integrated AAI.

Specific topics for this activity include:

- the creation of a level of assurance framework;
- identifying a minimal set of policies to enable attribute aggregation;
- enabling consistent handling of security incidents when federated access is enabled;
- exploring policy and security aspects to enable the integration of attribute providers and of credential translation services;
- develop support models for (inter)federated access to commercial services;
- developing guidelines to enable exchange of accounting and usage data.

The work is driven by user community requirements, but will by necessity include considerations of the cost of (especially higher) assurance levels for the IdPs and R&E federations. Prior work by REFEDS, the Interoperable Global Trust Federation [IGTF], the Kantara Initiative's assurance framework [Kantara] and other relevant work will be taken into account in all aspects of the work.

The activity will also address policies and best practices for the identified gaps in the system, such as incorporation of guest identities, credential translations etc. It is essential that this work is validated in production and trusted virtual research environments; results from this activity will be applied to the pilots developed in SA1 and evolved based on the experience gained therein.

The recommendations on policy and best practice will be developed with the objective of adoption by and integration into the existing AAI federations (through eduGAIN), e-infrastructures (such as EGI, PRACE, and others) and virtual research environments.

JRA1: Architectures for an integrated and interoperable AAI

Existing AAIs serve the needs of the R&E community worldwide on a segmented basis. These are well established within their local communities, but individually they lack the ability to form an interoperable AAI. Some examples of these include

- eduGAIN to offer Single Sign-On for web applications;
- Libraries that still use IP-based access;
- PRACE and EGI that use digital certificates,
- Government spaces that rely on national e-IDs and STORK. A citizen who is also a student or an educator could in principle link a government identity with an educational one, with the possibility to access different context providers during the different ages, i.e. at the education stage and at the university stage.

This work package will investigate the obstacles that prevent users, educators and researchers from using their credentials to access services offered by the various e-Infrastructures, libraries and research communities.

This work package will carry out research to:

- Facilitate access to resources and collaboration between researchers, students and educators;
- Reduce duplication of efforts for developing and deploying AAI services common to many e-infrastructures;
- Explore the technical elements needed for the integrated AAI: attribute frameworks and deployable non-web technologies;
- Expand the coverage of national identity federations for network, services and applications by supporting research institutions with low levels of technical or organisational preparedness by delivering easy-to-use solutions for them to enable federated access.

The output of this work package will be the technical design of the integrated AAI framework. All research aspects and architectural design will be carried out in this JRA1, NA3 will provide the necessary policies, while any implementations and pilots are done in SA1. The JRA1 final results will be informed by feedback from SA1's pilot results.

SA1: Pilots on integrated R&E AAI

Ensuring that digital credentials issued in the R&E community can be used to access services offered by different e-Infrastructures or research communities is a key goal to achieve the vision of an integrated AAI.

Key areas for pilots include:

- Providing access to shared resources for all users, including guests, participating in a virtual collaboration;
- Testing with different levels of trust associated with the credentials;
- Providing scalable mechanisms to handle authorisation at resource level;
- Enabling federated access for (commercial) resources and services;
- Piloting the introduction of attribute management services.

The main goal of this SA is to demonstrate the feasibility of the proposed architecture for the integrated AAI. By validating the key components designed in JRA1, with the integration of the operational, security and policy framework designed in NA3, SA1 will demonstrate that a European-wide single sign-on infrastructure is possible. This infrastructure will enable collaboration within an accessible but secure and trusted virtual research environment where scientific resources and content can be accessed, used, stored and shared.

3.1.1 Work schedule

The duration of this project is two years, which is an appropriate timescale for delivering the design framework of the integrated AAI. At the end of two years AARC will deliver a coherent framework with the appropriate recommendations to the existing e-Infrastructures to support and integrate it.

The picture below shows the timing of the various tasks.

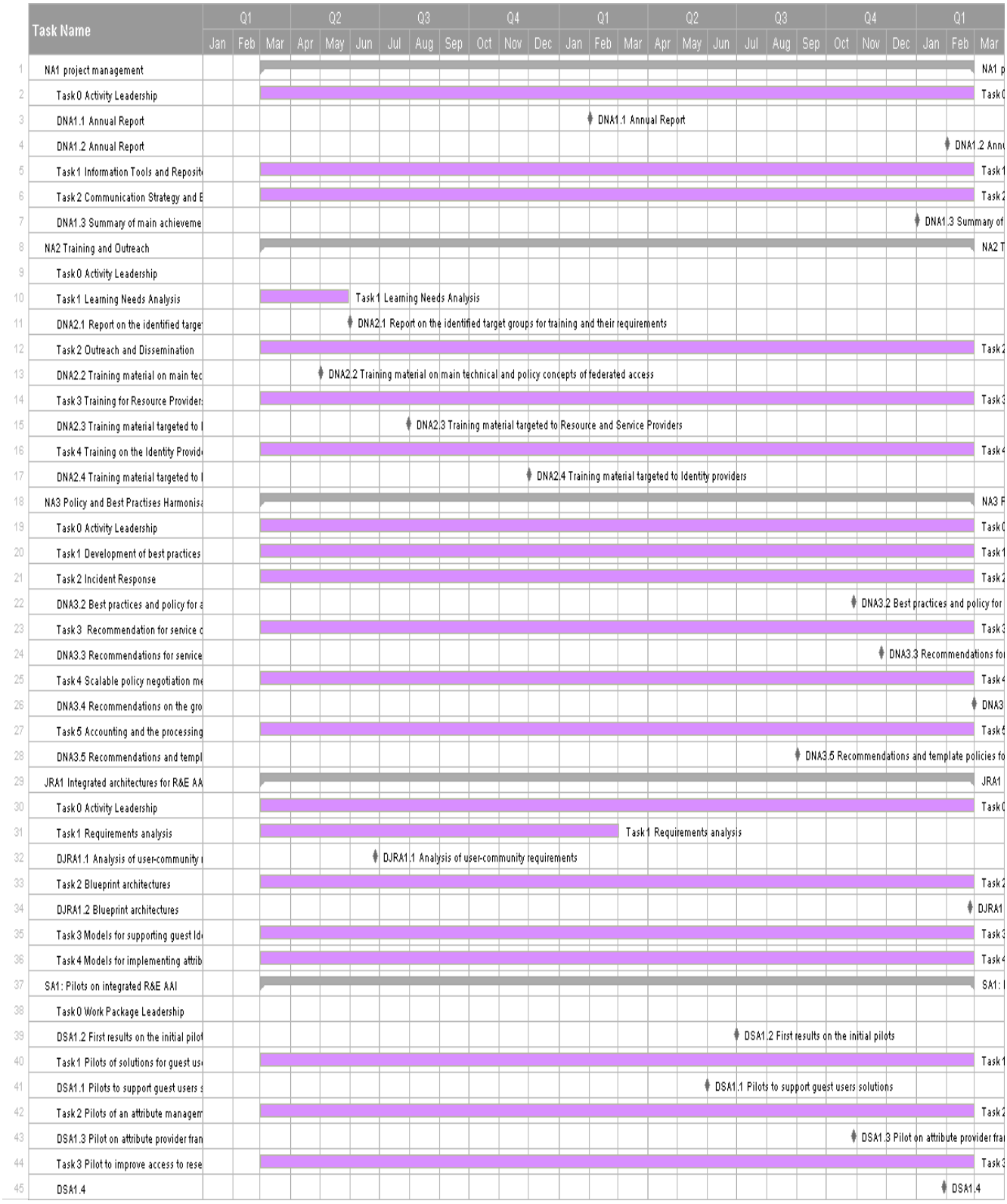

Figure 5: AARC GANTT

3.2 Management structure and procedures

The project management is organised via three main bodies as indicated in the picture below.

Project Assembly is the supervisory body of the project as well as its ultimate decision-making body. Each partner will appoint one voting member to represent them in the assembly. The project coordinator is also member. The Project Assembly decides on matters related to:

- General supervision of the progress made by the AARC project with regards to its deliverables and main objectives;
- Approval of major deviations regarding the AARC project plan or its expenditures;
- Acceptance of new participants as well as the exclusion of participants (subject to the approval of the EC);
- Request from the participants for modifications to the Consortium Agreement;

Coordinator is responsible for the overall management of the project. In particular the coordinator will:

- Represent the project during communications with the EC or with other relevant bodies;
- Ensure that the project plan is executed;
- Ensure that project reports and expenditures are provided and are in line with the AARC project plan;
- Identify issues that need to be escalated to the project assembly.

Project Management Team is the body that comprises the activity leaders. This body will ensure the smooth execution of the project plan. Some of their key tasks include but are not limited to:

- Report on the work on each activity;
- Detect risks and discuss measures to mitigate them;
- Propose and provide feedback for technical works, workshops and similar.

The work will be coordinated via regular progress meetings, where progress and issues are managed.

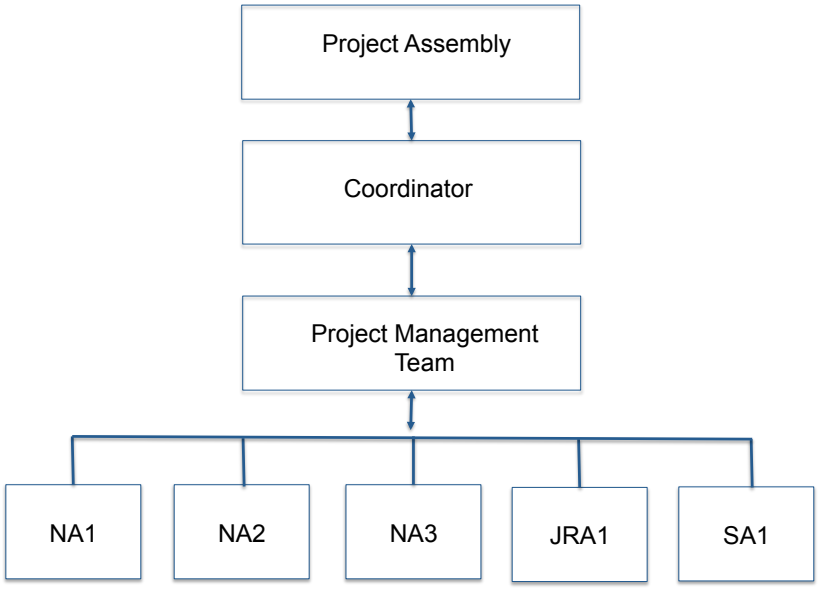

Figure 6: Project Structure and Management

To ensure that work is carried out efficiently, but with the aim to reduce travel costs, the project participants will meet face-to-face twice per year; it is expected that during these meetings each activity will also organise their own meetings. The use of video tools is encouraged to carry out the day-to-day work.

The goals of AARC are based on the increasing expectation of researchers to be able to work flexibly and securely outside the walls and facilities of their own campus. This change in how R&E operates is the key anchor in the innovation management strategy for this consortium, with technology progressing through the stages of the innovation process based on these user needs for federated identity.

Innovation Management

The innovation management process will take as inputs user requirements, available solutions and potential new solutions and technologies. Via complementary JRA and NA activities, these will be refined. The SA will operate pilots tied to concrete user requirements, ensuring that these are represented consistently throughout the innovation process.

Gateways between the JRA1, N3 and SA, including flexible feedback loops will be managed by NA1. In addition, NA1 will also produce sustainability recommendations for the future long term positioning of solutions. More details about the exploitation plans are provided in section 2.2.1.

Figure 7: Innovation Management in AARC

3.2.1 Milestones

The table below shows the main and most important milestones for the project. These milestones will ensure that the interim results of AARC, particularly those upon which other work relies, will be available on time.

Milestone Number	Milestone Name	Description	Related WP	Delivery Date (project month)	Means of Verification
MNA1.1	Project website	Project Website and project tools available to all partners	NA1	M1	Site up and running
MNA1.2	Kick Off Meeting	First meeting with the whole consortium	NA1	M1	News item
MNA2.1	Guideline document for AARC training materials	A document to define the guidelines for all AARC training material	NA2	M3	Document published on the web site
MNA2.2	First SP training delivered	First SP training delivered	NA2	M9	Event scheduled and carried out. Material online
MNA2.3	First IdP Training delivered	Training for identified IdPs	NA2	M14	Event scheduled and carried out. Material online
MNA3.1	Recommendation	A document the	NA3	M7	Report

	on minimal assurance level relevant for low-risk research use cases	describe a possible level of assurance framework			online. This document will be used as input for SA1 work
MNA3.2	Requirements on data to protect from AAI, community, resource providers and e-infrastructure	A document to describe the requirements from different communities on data to process and protect	NA3	M7	Report online. This document will be used as input for SA1 work
MJRA1.1	Existing AAI and available technologies for federated access.	Assessment on the technologies operated R&E AAIs, including about a list of existing group management tools and translation credentials systems	JRA1	M08	Online report to be shared among the partners.
MJRA1.2	Design for deploying solutions for “Guest Identities”	A document that will describe the possible options for supporting guest identities and alternative methods of identification	JRA1	M12	Report on line. This document will be used as input for SA1 work.
MJRA1.3	Design for the integration of an Attribute Management tool	A document that describes the existing solutions for attribute management and release and delegated authorisation management	JRA1	M12	Report online. This document will be used as input for SA1 work
MJRA1.4	First Draft of the blueprint architecture	A document to detail the first version of the blueprint architecture.	JRA1	M15	Report online. This document will be used as input for SA1 work
MSA1.1	Specify the work to be undertaken in collaboration with JRA1 and NA3	Detailed workplan	SA1	M3	Online document
MSA1.2	Report on the user testing and future recommendations	Brief report about the tests done on the pilots	SA1	PM24	Online document

Table3.2a List of Main Milestones

3.2.2 Critical Risks

The risks for the AARC project are shown in the table below.

Description of risk	Work package(s) involved	Proposed risk-mitigation measures
Research Community and Federation Community resistance to the adoption of shared infrastructure/AAI solution (not invented here problem) Likelihood: Medium Impact: High	All	Continuous engagement and opportunities for feedback into the development of solutions so that communities feel comfortable that their needs are incorporated.
Consortium disruption - A partner withdraws or fails to deliver their commitments (e.g. delay in delivery of user stories, overall architecture, best practices for LoA) Likelihood :Low Impact: High	All	As part of the management of the overall projects mechanisms will be in place to monitor the work and identify possible issues in a timely fashion.
Dependencies on the results from JRA1 and NA3 for SA1 to start the work. Likelihood: Medium Impact: Medium	SA1	SA1 can commence basic work based on the existing inputs from the study on Advancing Technologies and Federating Communities, the FIM4R report and the results from the AAI EC workshop. More advanced work can start when NA3 and JRA1 deliver their mid results (M7, M8 and M12) milestones and results are available.
Despite reaching the technological goals, the legal limitations might prevent the consistent deployments of the solution Likelihood: Low Impact: High	All	Involve legal experts, who can (if required) provide recommendations to the European policy makers to address the legal aspects.
The developments of pilots takes longer than expected Likelihood: Low Impact: Medium	SA1	The delivery of the pilots is critical for user testing. For this reason the partners within SA1 will adequately prioritise the functionalities to be implemented, to keep the effort focused and the overall plan sustainable. Moreover, all the partners have a solid background on software design, development and production deployment, which lower this risk.

Undiscovered interoperability aspects that hinder final integrations and deployment Likelihood: high Impact: high	JRA1, NA3, SA1	Continuous engagement with the research communities and the research e-Infrastructures particularly during the pilot phase. Ensuring that the testing is done at the earliest possible stage.
The results of the pilots do not meet the requirements of the user communities. Likelihood: Low Impact: Medium	SA1, JRA1 and NA3	The pilots will be carried out in close collaboration with the user communities, with user testing and feedback carried out at frequent intervals and in several iterations. The potential inadequacy, feasibility and expectations will therefore be managed in a timely fashion.
Limited uptake of federated access in the targeted communities despite the training and the supporting tools provided Likelihood: Medium/high Impact: High	NA2, NA1	Budget significant (and thus funded) contributions to support research communities and libraries to engage with AARC. Use the train-the-training model to ensure wide penetration of the training. This will ensure that AARC can deliver value over existing community engagement initiatives (i.e. REFEDS).
Limited ability of Identity Providers to offer richer functionality due to constrained funding and manpower Likelihood: Medium/high Impact: High	All	Within AARC, work with IdP communities who are well resourced to deliver. Beyond the lifespan of AARC, national funding initiatives encouraged by the EC are likely to be required for large-scale deployment.

Table3.2b Critical Risks for Implementation

3.3 Consortium as a whole

The design and deployment of a pan-European integrated AAI will be done jointly with a consortium of 20 partners that represent the National Research and Education Networks (NRENs), libraries, ESFRI cluster projects, international collaborations and e-Infrastructures. Each of the partners brings the required position and access to various e-infrastructures as well as to the communities that each e-Infrastructure supports.

The project will be coordinated by TERENA, which for many years has been offering a forum to collaborate, innovate and share knowledge in order to foster developments in technology, infrastructure and services to be used by the research and education community. TERENA is well positioned to mobilise the expertise and experience of hundreds of professionals in the research and education networking area and industry thanks to TERENA's involvement in key middleware activities.

Within the framework of this project each partner will bring a key expertise to achieve the objectives of the project, as described below:

- **NRENs [NREN]** – There are a total of 9 NRENs involved in AARC. They all have significant expertise in operating identity federations, in integrating services (also commercial services) as well as in offering storage services. They all participate in eduGAIN and some of them are involved in Project Moonshot as well. In particular:
    - CESNET has been working extensively on solutions to support group management and on the development of Project Moonshot,
    - CSC has been for years supporting AAI development for important projects like ELIXIR, CLARIN[11] and EUDAT. They have been involved on the eduGAIN policy side as well as on levels of assurance. They will lead tasks in NA2 and NA3.
    - GARR have been engaging for years to deliver solutions to facilitate the adoption of federated technologies across various research and education communities (i.e. biomedicine, arts and humanities, in schools as well as in universities). They will lead tasks in NA2, JRA1 and SA1.
    - GRNET is operating the national identity federations and is actively involved in interoperability pilots between e-Governments and R&E AAIs. They will lead JRA1.
    - PSNC has extensive experience on integrating commercial and cloud services; they will a task in SA1.
    - RENATER has significant experience with group management solutions.
    - SURFnet was amongst the first NRENs to deploy federated access for their users. They are pioneers in integrating (commercial) services into their federation and offering a flexible environment to support groups. They will lead SA1.
    - JANET, although they are participating without claiming any costs, will offer their expertise based on operating one of the biggest federations in Europe and their work on Project Moonshot.
    - DFN, although they are participating without claiming any costs, will support AARC in the dissemination work.

- **e-Infrastructures service partners** – There are several different R&E e-infrastructures involved and/or represented in AARC, namely:
    - **EGI.eu**, the coordination body of the European Grid Infrastructure, will liaise with the EGI service providers to gather feedback on policy and technical solutions. They will lead different tasks in the project that include requirements gathering and deployment of proofs of concept. EGI.eu will bring the experience that the EGI collaboration gained in federating resources and user communities in a cross-national infrastructure. EGI.eu will also bring the experience of the Technical Outreach team for requirement analysis to liaise with potential new customers.
    - **FOM-NIKHEF** has extensive experience in coordinating international policy efforts in light of their role as leader of the IGTF. They will lead NA3.
    - **CERN** represents the WLCG collaboration and its services, the Large Hadron Collider experiments, as well as the larger international High Energy Physics user community, with specific requirements for security. They will offer their expertise in NA3 to address the operational and security aspects

[11] http://www.clarin.eu

    - **KIT** will offer their expertise in the integration of federated non-web SSO and access the expertise in legal aspects of attribute release.
    - **Jülich** and **SURFsara** that represent the requirements for PRACE.

- **Libraries** – They are represented by LIBER and by their partner MZK. They will articulate the requirements and challenges for the libraries and will be instrumental for the training in that community.
- Liaisons via the partners with the wider community.

Subcontracting will be used only for specialised functions (i.e. high quality printing, video material, etc.).

3.4 Resources to be committed

Table 3.4a: Summary of staff effort

	NA1	NA2	JRA1	NA3	SA1	Total Person/ Months per Participant
1 TERENA	14	22				36
2. CERN		9		15		24
3.CESNET			6		8	14
4. CSC		9	2	8	4	23
5.DAASI International		8	6	3	7	24
6. DFN						0
7. EGI		4	9		11	24
8. GARR		9	7		6	22
9 GRNET		1	15	8	6	30
10. JANET						0
11. FZJ			3			3
12. KIT		2	8	6	8	24
13. LIBER		6	1	2		9
14 MZK		5	2		1	8
15. FOM-NIKHEF			3	9	10	22
16. PSNC			6		12	18
17. RENATER				6		6
18. STFC		0	6	6		12
19. SURFnet B. V.			1		23	24
20. SURFsara				3		3
Total Person/Months		75	75	66	96	326

Table 3.4b: 'Other direct cost' items (travel, equipment, other goods and services, large research infrastructure)

The table below shows the participants for whom the sum of the costs for 'travel', 'equipment', and 'goods and services' exceeds 15% of the personnel costs for that participant (according to the budget table in section 3 of the proposal administrative forms). The amount listed here does not include the overhead.

1/TERENA	Cost (€)	Justification
Travel	17920	As coordinator and leader for the NA2, TERENA is expected to have some additional travel costs.
Equipment		
Other goods and services	120000	These include meeting costs, printing material as well as training costs.
Total	137920	

8/GARR	Cost (€)	Justification
Travel	12800	Travel has been calculated on the assumption that GARR will offer three task leaders and they are expected to have additional trips. GARR person costs are also lower than other partners.
Equipment		
Other goods and services		
Total	12800	

14/Moravian library	Cost (€)	Justification
Travel	2560	Travel costs are based on the assumption of two people travelling for AARC.
Equipment		
Other goods and services		
Total	2560	

19/SURFnet	Cost (€)	Justification
Travel	43520	The calculation has been made on the assumption of three people travelling for AARC.
Equipment		
Other goods and services		
Total	43520	

3.5 Work Packages Description

Table 3.1a: Work package description

NA1: Project Management

Work package number	**NA1**		**Start Date or Starting Event**						M1 of the project
Work package title	**Project Management**								
Participant number	1	2	3	4	5	6	7	8	9	10
Short name of participant	TERENA	CERN	CESNET	CSC	DAASI	DFN	EGI	GARR	GRNET	JANET
Person/months per Participant:	14	-	-	-	-	-	-	-	-	-
Participant number	11	12	13	14	15	16	17	18	19	20
Short name of participant	JÜLICH	KIT	LIBER	Moravian Library	FOM-NIKHEF	PSNC	RENATER	STC	SURFnet	SURFsara
Person/months per participant	-	-	-	-	-	-	-	-	-	

Objectives
NA1 represents the overall management of the project.

The goal of NA1 is to bring people together to accomplish the desired goals and objectives of the project using the available resources efficiently and effectively.
The list of objectives is provided below:

- To provide an efficient management framework to enable project participants to deliver efficiently and effectively, to identify challenges and overcome obstacles in the project;
- To coordinate the activities of the project, such as reports, project-participant meetings, overall project promotion;

- To raise awareness about the project's goals and to coordinate AARC presence at relevant events;
- To monitor expenditure;
- To ensure the project builds on the results achieved by other projects or initiatives, such as GN3plus, REFEDS and FIM4R;
- To liaise as necessary with the European Commission and with other relevant initiatives, such as GN4, EUDAT, FIM4R, REFEDS etc..

Description of work

The work in this work package has been broken down into several tasks:
Task 0: Work Package Leadership
Task 1: Information Tools and Repositories
Task 2: Communication Strategy and Exploitation

Task 0 – Work Package Leadership

Task Leader organisation: TERENA

Objectives

This task is to lead the project as a whole. The task will offer:

- a framework to ensure that work in the project is done smoothly, reported and monitored in accordance with the workplan. Part of the work will cover the support for the project management as a whole, its governance, the support for the Activity Leaders and Task Leaders with day-to-day management tasks in their respective areas;
- support for the financial and administrative management (such as time reports, costs reports and so on) to facilitate the delivery, monitoring and tracking of the project's objectives;
- logistical support to organise two internal project meetings per year - the organisation of additional events that may be relevant for the project shall be discussed within the consortium on a case-by-case basis and in relation to the budget and manpower required.

Task 1: Information Tools and Repositories

Task Leader organisation: TERENA

Objectives

This task will offer tools and infrastructure required for AARC teams to do their work efficiently. This task will offer the project web presence, communication and collaboration tools, CRM, repositories, document storage, meetings and events registration and calendars.

Task 2: Communication Strategy and Exploitation

Task Leader organisation: TERENA

Objectives

The goal of this task is to define the communication and marketing strategy for the AARC project as a whole to ensure that information and promotion about the project and its goals is consistent and successful. This task will ensure that AARC is represented at the most relevant events, that news items about project events and

achievements are promptly issued and that the project website is up-to-date. This task will also manage news items for the whole project.

Part of the work of this task will cover the exploitation of the AARC project, to ensure that recommendations and detailed information are available to the existing e-Infrastructures to deploy AARC's results.

Deliverables
DNA1.1 and DN1.2 – Annual Reports M14, M24
DNA1.3 – Summary of main dissemination activities and Exploitation Report M23

NA2: Training and Outreach

Work package number	NA2		Start Date or Starting Event				M1 of the project		
Work package title	**Training and Outreach**								
Participant number	1	2	3	4	5	6	7	8	9	10
Short name of participant	TERENA	CERN	CESNET	CSC	DAASI	DFN	EGI	GARR	GRNET	JANET
Person/months per Participant:	22	9	-	9	8	-	4	9	1	-
Participant number	11	12	13	14	15	16	17	18	19	20
Short name of participant	JÜLICH	KIT	LIBER	Moravian Library	FOM-NIKHEF	PSNC	RENATER	STC	SURFnet	SURFsara
Person/months per participant	-	2	6	5	-	-	-	-	-	

Objectives

This work package will:

- Provide general purpose material with the aim of transferring solutions about how to overcome technical, organisational and legal obstacles to make federated access more pervasive;
- Document and disseminate best practice in enabling SAML support in application;
- Provide training to IdP-enabled organisations with a low level of technical expertise or limited manpower;
- Support targeted service providers to ensure the uptake of e-Infrastructures' AAI services;
- Develop training activities for data professionals on issues related to AAI-enabled collaboration and data sharing (data privacy, intellectual property, cultural barriers, etc.);
- Develop promotional materials for (commercial) SPs explaining how to work with R&E federations;
- Provide promotional material, best practices and training for identified AARC user

groups (ESRI clusters, libraries, arts and humanities) to optimise the uptake of federated identities in accessing electronic resources together with other library services;
- Perform training workshops.

Description of work
The work in this work package has been broken down into several tasks as detailed below:
Task 0: Work package Leadership
Task 1: Learning Needs Analysis
Task 2: Outreach and Dissemination
Task 3: Training for Resource Providers
Task 4: Training on the Identity Providers

Task 0 – Work package Leadership
Task Leader organisation: TERENA

Objectives
This task is to lead the activity as a whole and to provide the necessary support to deliver training efficiently as well as to define and produce materials, together with the project partners, to promote federated access.

Task 1: Learning Needs Analysis
Task Leader organisation: TERENA

Objectives
This task will identify the knowledge and skills gaps among target groups including libraries setting the competencies required for the project goals to be successful, and assessing the current knowledge and skills levels in order to prepare effective training to meet those needs. This will include setting clear guidelines and standards for all parties responsible for producing training materials and defining strategies.
Furthermore this task will ensure that once the material is ready it is indeed consistent with the guidelines provided.

Task 2: Outreach and Dissemination
Task Leader organisation: TERENA

Objectives
The objective of this task is to reach out targeted user communities and promote the use of federated access. The approach of the task will consider different aspects:

- Technical aspect: Various existing technical materials from NRENs, pioneer projects and communities will be evaluated, repackaged to convey a coherent message, and stored in a central repository for use by project partners when talking to different user groups. As federations' technical implementations and specific policy conditions differ, the results produced will be rather high-level. The material will be used to approach selected user communities to persuade them to join their national federation. The way in which these events will be organised will depend on the results of task 1.

- Legal aspect: There have been significant efforts to enable the exchange of user data within the federations in compliance with the law. National federations have all prepared guidelines for their users, explaining how federated access in fact preserves users' privacy. At European level the eduGAIN team has invested resources to implement and deploy a Data protection Code of Conduct for Service Providers [CoC] and to promote the key messages of this approach. This task will work closely with national federations and the eduGAIN team to prepare materials for distributed training to targeted communities. This will help institutions utilise the potential of federated AAI for their users.

- Liaison with other projects/communities: Many existing projects and communities already focus on reaching out to user communities. Working closely with some of them will enable this task to have a bigger impact in terms of outreach, and will minimise duplication of effort across the whole spectrum. It is a component of this task to analyse and define target communities in order to ensure a multitude of community types can be reached by dissemination. The consortium partners' existing relationships, networks, and communication channels will be used to maximise the true impact.

- General Dissemination about AARC results: All AARC results will be promoted via NA2.

Task 3: Training for Resource and Service Providers
Task Leader organisation: CSC

Objectives
This task will enable e-Infrastructure providers to meet scientific service providers and, with the support of key people known to these providers, explain how to implement SAML-based services. This may result in the gathering of new requirements and recommendations with regards to implementation and operational costs.

Targeted service providers to implement federated access will initially include, but not be limited to:

- The European biological, and biomedical user community represented by ELIXIR-ESFRI.[12] Considering the importance of federated authentication and access for sensitive data management and processing, this community provides a practically-driven environment to develop and disseminate training materials to streamline uptake of federated AAI services within the biomedical community. The training material developed for this community will be used to derive guidelines for other service providers in other communities as well, allowing those communities to evolve the initial material following their requirements and needs.

- The European Grid Infrastructure. EGI represents a very diverse ecosystem that needs flexible authentication and authorisation mechanisms to support both big and structured collaboration and the users of the long tail of science. The training activities will be focused on dedicated sessions during the EGI main events, which are attended by a large number of EGI resource provider representatives and user communities. The goal of these workshops for resource providers will be to

[12] This group is submitting a proposal in response to the EINFRA-4 call. Liaisons between AARC and this project are envisaged if both projects are approved.

disseminate the technical solutions and policies produced by the project, to raise awareness and trust in the framework designed by the AARC and to foster the integration of such technologies. For the user communities the target of the training will be to expand the use of standard-based attribute provider services to manage the authorisation, and to promote the use of federated identities to access EGI.

- The Worldwide LHC Computing Grid. The WLCG community makes use of a production infrastructure spanning hundreds of resource providers, serving a community of more than 10,000 physicists around the world with near real-time access to LHC data, and the power to process it. The current architecture relies on X.509, which involves a number of drawbacks. It would be highly beneficial both for the users whose organisations are participating in eduGAIN and for the LHC experiments to enable identity federation for the WLCG services. An objective of this task is to enable significantly easier and more convenient access to a number of WLCG services using federated identities issued by eduGAIN Identity Providers.

- Another series of activities address the needs of Digital Humanities e-infrastructure communities. DARIAH has established an AAI solution and a proven record of resources that have been made available for federated access. However, on a European scale, many valuable humanities resources are not yet accessible via federations. This task will identify and address further resource providers and their training needs in order to extend the number of available resources.

Task 4: Training for Identity Providers
Task Leader organisation: GARR

Objectives
One of the goals of this project is to offer solutions for the easy creation of Identity Providers for targeted user groups and for libraries and other institutions willing to optimise the uptake of federated identities. This task will promote the solutions developed as part of the project. Part of the task is also to analyse the requirements of these institutions pertaining to all essential aspects of federated Identity Management. Because the type of solutions will depend on the results of JRA1 and SA1, a more detailed description of this work will only be possible at a later stage.

Deliverables

DNA2.1 – Report on the identification of target groups and their requirements, M3
DNA2.2 – Training material on the main technical and policy concepts of (inter)federated access, M5
DNA2.3 – Training Material for resource providers M9
DNA2.4 - Training Material for Identity Providers M14

NA3: Policy and Best Practices Harmonisation

Work package number	**NA3**		**Start Date or Starting Event**			M1 of the project			
Work package title	**Policy and Best Practices Harmonisation**								
Participant number	1	2	3	4	5	6	7	8	9	10
Short name of participant	TERENA	CERN	CESNET	CSC	DAASI	DFN	EGI	GARR	GRNET	JANET
Person/months per Participant:	-	15	-	8	3	-	-	-	8	-
Participant number	11	12	13	14	15	16	17	18	19	20
Short name of participant	JÜLICH	KIT	LIBER	Moravian Library	FOM-NIKHEF	PSNC	RENATER	STFC	SURFnet	SURFsara
Person/months per participant	-	6	2	-	9	-	6	6	-	3

Objectives

This activity will develop recommendations for best practice in the areas of identity and attribute assurance, and identify the minimal set of policies and best practices that permits grouping of identity and attribute providers.

The main objectives are:

- To provide a level of assurance (LoA) framework that meets the requirements of resource providers and can at the same time be supported by institutions (identity providers);
- To identify a distributed approach to handling security incidents in a federated environment;
- To specify scalable policy negotiation mechanisms between identity providers, attribute providers and service providers to facilitate resource providers;
- To investigate terms of usage for delivering commercial services.

Description of work

The work has been broken down into the following tasks:

Task 0: Work Package Leadership
Task 1: Development of best practices for Levels of Assurance
Task2: Incident Response
Task 3: Recommendation for service operational models for enabling cross-domain sustainable services
Task 4: Scalable policy negotiation mechanisms
Task 5: Accounting and the processing of data

Task 0 Work Package Leadership
Task Leader organisation: FOM-NIKHEF

Coordinate the activities of the other tasks and communications with the other WPs. Ensure the coordination with external policy development stakeholders and customers.

Task 1 Development of best practices for Levels of Assurance
Task Leader organisation: CSC

This task will collect the current set of policies in use within the R&E federations and derive the main 'effective' assurance levels that are available today. These will be compared to the assurance requirements of the initial set of resource providers and e-infrastructures, and with those of the identified user communities. Based on the comparison, the minimal assurance level which is still relevant for low-risk research use cases will be defined. This will be then available for dissemination and training activities in NA2.

Based on the architectural design defined in JRA1 and the experience of the proof-of-concept virtual research environments in SA1, this will be developed into a limited set of differentiated assurance level recommendations. These recommendations will reflect the options for distribution of responsibilities amongst the three identified participant roles: researchers and research communities, resource and e-infrastructure providers, and identity federations and their constituent IdPs. (DNA3.1).

During the project the recommendations will evolve to take into account results from JRA1 and SA1 and a final recommendation will be published.

Task 2 Incident Response
Task Leader organisation: CERN

Since the R&E federations and their underlying IdPs have a long-standing operational tradition, they have also developed a computer security incident response capability to deal with both accidental and deliberate violations of system and network security. However, although computer security incident response procedures often exist at the national level, they are rarely formally specified for federations and there is no best practice guidance for security incidents involving several federations spreading across multiple administrative domains.
This task will review existing documented practices and propose recommendations for security incident response, in the form of a generic security incident response procedure for federations.
This procedure will be documented as deliverable DNA3.2, and disseminated via appropriate channels to relevant groups outside of AARC and TERENA, so that it can

serve other projects, infrastructures, and federations, such as the RDA FIM4R Interest Group.

Task 3 Recommendation for service operational models for enabling cross-domain sustainable services
Task Leader organisation: DAASI International

This task will identify the current set of policies and practices in use within the R&E federations, and having identified the elements necessary for enabling the initial set of use cases, specify operational recommendations for federations to streamline their policies.

This task will make these baseline recommendations available for adoption by operational infrastructures such as eduGAIN. The recommendations developed in this task will directly support the proof-of-concept implementations of SA1.

It is also clear that the sustainability model for federated services will evolve: translation services, guest identity providers, and attribute authorities must have a model that permits them to be supported by different entities (e-infrastructures for credential translators or as hosts of attribute authorities, research communities that are self-sustained and will operate their own services, etc.).

A recommendation for possible operating models meeting the requirements for a sustainable cross-domain collaboration will be developed in this task.

Task 4 Development of scalable policy negotiation mechanisms
Task Leader organisation: STFC

The bi-lateral negotiation of policies between SPs and IdPs/AAs does not lead to timely results and the only viable option for differentiated policy and LoA will be through the definition of a very limited set of these, as will be done in TNA3.1. A classification of all participants in the identity and attribute ecosystem (identity providers, attribute providers, and translation services) and expressing these technically will result in the necessary scalable policy negotiation mechanisms.

The first work will be the identification of the entities that need to be classified and expressed, such as the specific categorisation that may be needed for non-identity attribute providers and for credential translators. (MNA3.4)
Once the initial policy and best practice groupings are available after MJRA1.2, this task will proceed to formulate recommendations on the grouping of entities and on the actual deployable mechanisms that can be evaluated in the proof-of-concepts of SA1.
The final recommendations will then be provided to the operational infrastructures and federations. (DNA3.4)

Task 5 Accounting and the processing of data
Task Leader organisation: KIT

Collaboration across different administrative domains and across borders in Europe and beyond needs to address the management of personal information. Most of the research use cases and all of the cross-domain resource providers and e-infrastructures will have to process such data in order to measure usege and allocate resources. Because of the

inherently distributed nature of the AAI – including attribute authorities – this includes persistent unique identifiers that are likely to (implicitly) identify the user involved. This data must be protected, and at the same time be made available to those who have a legitimate reason to view and process it.
To develop the appropriate recommendations for processing these data, the relevant participants in the AAI infrastructure as well as in the user communities, at the resource providers and in the collective shared-service e-infrastructures must be identified and their roles made explicit (MNA3.5)

The task will develop recommendations and template policies for the processing of personal data for each of the identified participants with the aim of providing recommendations that can be applied across the entire infrastructure – bearing in mind the current state of European legislative efforts and the implementation thereof in the member states. It will identify the minimal sets of information needed by the participants in the prevalent use cases and those foreseen for the proof-of-concepts in SA1 (DNA3.5).

Deliverables
DNA3.1 - Differentiated LoA recommendations for policy and practices of identity and attribute providers, applicable to research use cases, M23
DNA3.2 - Best practices and policy for attribute authorities and credential stores in the area of collective security incident response, M20
DNA3.3 - Recommendations for service operational models for enabling cross-domain sustainable services, M21
DNA3.4 - Recommendations on the grouping of entities and their deployment mechanisms in scalable policy negotiation, M24
DNA3.5 - Recommendations and template policies for the processing of personal data by participants in the pan-European AAI, M18

JRA1: Architectures for an integrated and interoperable AAI

Work package number	**JRA1**		**Start Date or Starting Event**				M1 of the project		
Work package title	**Architectures for an integrated and interoperable AAI**								
Participant number	1	2	3	4	5	6	7	8	9	10
Short name of participant	TERENA	CERN	CESNET	CSC	DAASI	DFN	EGI	GARR	GRNET	JANET
Person/months per Participant:	-	-	6	2	6	-	9	7	15	-
Participant number	11	12	13	14	15	16	17	18	19	20
Short name of participant	JÜLICH	KIT	LIBER	Moravian Library	FOM-NIKHEF	PSNC	RENATER	STFC	SURFnet	SURFsara
Person/months per participant	3	8	1	2	3	6	-	6	1	-

Objectives

Identify and overcome technical, organisational and legal obstacles that hinder seamless interoperability and user experience among existing AAIs. To achieve this, the work package will:

- Analyse how much has been developed to leverage federated access with other authentication systems used in the R&E communities, in the eGov space and in the commercial sector;
- Research a possible solution to link identities in the contest of higher levels of assurance, attribute providers and guest identities;
- Assess existing technologies to provide SSO for non-Web applications (cloud, storage and so on) and offer recommendations for their usage;
- Develop a risk-based model for existing AAI solutions;
- Propose models for supporting guest identities (NRENs' in-house solutions vs commercially-offered solutions should be explored);
- Define a blueprint architecture to enable web and non-web SSO capabilities across different infrastructures, integrating attribute providers/group management tools operated by user-communities;

Provide models for federated authorisation: how to integrate attributes and permissions from diverse communities, making them available at the federation level in a consistent and secure way.

Description of work

Federated access is a main requirement both for users and resource providers. At the same time distributed collaborations and R&E e-infrastructures developed and deployed mechanisms for the management of the authorisation based on information provided from the final user communities to the service providers.

This work package will investigate the obstacles that prevent users, educators and researchers to use their credentials to access services offered by the various e-Infrastructures, libraries and research communities, and produce a blueprint document that defines a possible workflows and the tools to make possible the deployment of SSO capabilities across e-infrastructures.

This work package contains five main tasks as detailed below.

- **Task 0:** Work Package Leadership
- **Task 1:** Requirements analysis
- **Task 2:** Blueprint architectures
- **Task 3**: Models for supporting guest Identities and alternative methods of identification
- **Task 4**: Models for implementing attribute providers and token translation services

Task 0: Work package Leadership
Task Leader organisation: GRNET

- Coordinate and monitor the evolution the tasks in the JRA1
- Report on the progress of each task and of the work package as a whole
- Ensure the cooperation with the other work packages and with the project leadership

Task 1: Requirements analysis
Task Leader organisation: EGI

This task will capture and analyse the requirements for pan-European identity federation for researchers, educators and student. It will identify gaps that hinder seamless interoperability of existing e-Infrastructure AAIs and it will investigate the obstacles in using federated credentials to access resources operated both in the R&E sector and commercially.

Findings from previous studies and ongoing work in GÉANT, EUDAT and EGI will be used.

The aims of this task are to:

- Describe the authentication and authorisation technologies used by the different e-Infrastructures, including research communities, libraries and educational service providers and identify the existing gaps that prevent their interoperability.

Explore how the current e-Infrastructures can support broader cross-domain collaboration, for instance when dealing with commercial services and or with e-Government initiatives.

- Prioritise the work to undertake on the basis of the community requirements, results of pilots carried out by the GN3plus project and FIM4R group and on the technical analysis of existing pilots to support groups, token translation and SSO for non-web.
- Explore how the current e-Infrastructures can support broader cross-domain collaboration, for instance when dealing with commercial services and or with e-Government initiatives.
- Gather information on the penetration of AAIs and eduGAIN in R&E sector, libraries and e-Government.
- Gather information on the interoperation experiments between R&E federations (including eduGAIN) and eGOV in the different European countries. Determine the maturity level and portability of the solutions enabling non-Web SSO, which is important when access to computing and storage services in several e-Infrastructures and cloud is considered.
- Document relevant standards bodies and other interoperation activities and their role in supporting AAI

Task 2: Blueprint architectures
Task Leader organisation: KIT

The aim of this task is to produce a set of blueprint architectures for an interoperable pan-European AAI. The first version of the blueprint will provide a reference architecture, which will fill the gaps identified by Task 1. In the second version of the blueprint, the outcome of the work performed in Task 3 and Task 4 will be incorporated in order to produce the final reference architecture.

The aims of this task are:

- To produce a blueprint architecture for a pan-European integrated AAI for web and non-web access and propose sustainability models for some of the systems listed in the blueprint by leveraging the outcome of tasks 1, 3 and 4;
- To explore the use of guest identities;
- To research how attribute providers fit into the blueprint, such that user attributes can be aggregated from multiple authoritative sources;
- To assess the integration of security token translation services to offer seamless authentication among heterogeneous systems;
- To explore models to elevate the LoA by linking federated credentials with e-Government credentials

Task 3: Models for supporting guest Identities
Task Leader organisation: STFC

One of the main requirements reported by different research and education communities as identified in the FIM4R paper and in the AAI Workshop held in April 2014, is to offer support for guest identities. The support should serve nomadic users (those without a “home” organisation, such as “long-tail” researchers) as well as users belonging to an institution that is not able to operate an Identity Provider (IdP), or one which operates a stand-alone IdP which is not part of an established federation. Also, community IdPs are considered, since many communities have established practices independently of their

home organisations. Finally, it has been argued (in FIM4R) that many younger researchers, having grown up with social media, may expect to continue to use social media in their research roles.
This task will explore models for supporting guest identities, including solutions to ease the creation of an identity provider. Commercially available solutions will also be considered in relation to solutions built by NRENs.

The aims of this task are to:

- investigate and propose solutions for Guest Identities;
- investigate the use of alternative methods of identification (e.g. social networks etc);
- investigate the usefulness of the IdMaaS model (IdP-in-the-Cloud);
- define a strategy to permit broad public access at large to services, including libraries via AAIs;
- collaborate with NA3 for the definition of the levels of assurance relevant for European federated AAI, based on the existing levels when possible,
- investigate the risks associated with implementing delegation of credentials
- develop a risk-based model for assessing the suitability of identities for infrastructure provisioning.

Task 4: Models for implementing attribute providers and token translation services
Task Leader organisation: GARR

As emerged in several occasions (FIM4R, VAMP workshop, TERENA Conference) the model in which identity provider manages all attributes about a user does not scale for all use-cases. The trend is to move to a scenario where different attributes are managed by different entities and then aggregated and offered to the services. This work will build on the finding of relevant work in this area at the time the project starts.

Furthermore, this task will build upon the outcome of Task 1 and on the experiences and knowledge of partners in the consortium to investigate the needs and possible solutions for Token Translation Services as a potential mechanism for exchanging authentication and authorisation tokens across heterogeneous technical implementations. Example of existing token translation services to convert SAML credentials and X.509 are: CILogn, TERENA Certificate Service Portal, EUDAT software, EMI STS and so on. Mechanism to support OpenId Connect and OAuth2 will also be explored.

The aims of this task are to:

- Provide a model for implementing attribute providers and guidelines for improving attribute release This work, in turn, will in part build on existing grid guidelines for the operation of an attribute authority [attribute authorithy] as well as SAML guidelines and tools about delegated attribute management;
- Define an architecture to integrate attribute providers operated by user-communities or other third parties with the current identity federations. This will have to take into account how account linking will be performed in order to collect attributes from different sources and also to grant user-centric long-lived identities;
- Define a model and vocabulary for translation of authorisation-related information from group memberships of a user into authorisation attributes to be used by Service Providers;
- Research the use of token translation services to enable seamless access across

technical barriers;

- Research the technologies necessary to support delegation of authorisation management. (e.g. GSI proxies, OAuth and SAML based solutions etc)
- Provide best practices for managing authorisation using the attributes providers, achieving interoperable authorisation across e-infrastructure and between user communities.

Deliverables

DJRA1.1 - Analysis of user-community requirements, M4

DJRA1.2 – Blueprint architectures (this document will take into account the results from the pilots in SA1) M24

SA1: Pilots on the integrated R&E AAI

Work package number	SA2		Start Date or Starting Event						M1 of the project
Work package title	Proof of concepts on cross sector SSO								
Participant number	1	2	3	4	5	6	7	8	9	10
Short name of participant	TERENA	CERN	CESNET	CSC	DAASI	DFN	EGI	GARR	GRNET	JANET
Person/months per Participant:	-	-	8	4	7	-	11	6	6	-
Participant number	11	12	13	14	15	16	17	18	19	20
Short name of participant	JÜLICH	KIT	LIBER	Moravian Library	FOM-NIKHEF	PSNC	RENATER	STC	SURFnet	SURFsara
Person/months per participant	-	8	-	1	10	12	-	-	23	

Objectives

The objectives of this SA are to:

- Facilitate researchers to collaborate in a secure and trusted virtual research environment, by providing the tools to support collaborative research in a distributed environment.
- Demonstrate through pre-production services that existing AAIs can be leveraged to access (non-web) resources that are offered by different e-Infrastructures enabling SSO capabilities for the users.
- Demonstrate through pre-production services the integration of distributed group managers/attribute providers with the (e-infrastructure) services to implement attribute-based authorisation capabilities to user communities and service providers.
- Support commercial service providers in the area of pay-per-use and contracted services.
- Showcase test solutions for guest identities and to ease the deployment of non academic identity providers.

Description of work

The work in SA1 will be driven by use-cases that will be selected as a result of the work of JRA1 and in consultation with the user communities and e-Infrastructure providers. The pilots will have to demonstrate that the solutions proposed by JRA1 and NA3 are effective in addressing the requirements of both users communities and different service providers (commercial and non-commercial) in terms of usability, security, reliability and provided functionalities. Some of the SA1 work will start in parallel with JRA1 and NA3, based on the already known requirements; the other part of the work will commence when the interim results of both JRA1 and NA3 are available. SA1 feedback from the pilots will be taken into account for NA3 and JRA1 to refine their final results.

The proof of concepts will involve services from the main e-infrastructures in Europe (e.g. EGI, EUDAT, PRACE, eduGAIN), as well as libraries and ESFRI cluster projects (ELIXIR, DARIAH and so on). Service providers will include both academia and industry, and both web-based and non-web based services.

This work package contains the following tasks:
Task 0: Activity leadership to coordinate the overall work
Task 1: Pilots of solutions for guest users
Task 2: Pilots of an attribute management framework
Task 3: Pilot to improve access to research and education relevant resources and (commercial) services

Task 0: Work Package Leadership
Task Leader organisation: SURFnet

The aim of this task is to:
- Coordinate the activities of the other tasks and the communications with the other WPs
- Support the definition of a test bed infrastructure together with all relevant parties
- Plan demonstrators at relevant events.
- Provide technical feedback and other activities to pilot the work of JRA1 and NA3

Based on results of user testing, recommendations for production deployment within the enhanced version of eduGAIN.

Task 1: Pilots of solutions for guest users
Task leader organisation: GARR

The aim of this task is to:
- Lower barriers for entry of organisations not already participating in identity federations. Solutions (i.e. IdP in the cloud) to support institutions that are not able to run an Identity Provider will be piloted. The integration aspect of these solutions with existing national federation workflows and eduGAIN will be evaluated as well.
- Showcase viable solutions whether commercially available or R&E community supported for guest access to shared resources
  Based on requirements from JRA1, several approaches will be investigated. Scenarios are likely to include identities from social providers, government e-IDs and community provided identities and to address models for linking accounts. After

determining feasibility, viable solutions will be tested. In collaboration with NA3 policy and trust implications will be evaluated.

- Showcase ways to support scalable LoA for guest users.
  JRA1 will provide requirements for LoA whereas NA3 will provide guidelines for the implementation of LoA in relation to guest identities. This activity will evaluate requirements and recommendations with at least one user case driven pilot.
- Showcase AAI Approaches for research libraries.
  University libraries need to service a broad community of users from outside the academia. The need to deal with these creates a number of unique use cases for this sector. Together with LIBER, MKZ and the other interested University libraries, AAI issues in the domain of research libraries will be identified as part of JRA1. After the requirements analysis a pilot will be conducted. The solution will make use of existing AAI approaches. In collaboration with NA3 policy and trust implications will be evaluated.

Task 2: Pilots of an attribute management framework
Task Leader organisation: EGI

Objectives
Based on the scenarios for an attribute management framework as described in JRA1 this activity will deploy pilots for the tools and methodology identified by JRA1 for deploying attribute management frameworks for collaborative SSO scenarios. The pilots will focus on maximising the interoperability of the tested solutions. This includes:

- Attribute management
  Identify tools and services that better support the registration and management of attributes by the research communities. Based on the requirements, as defined in JRA1, at least two tools will be selected for a pilot. The tools should support standard interfaces to be used by user communities and e-infrastructure service providers.
- Attribute aggregation
  Multiple scenarios for attribute aggregation are expected to result from the attribute framework definition. This work item will validate at least two basic models, a hub model and a mesh model. From a protocol perspective the same open standards can be used to engage in attribute distribution. This work item will investigate feasibility, security and privacy implications of at least two protocols.
- Attribute based authorisation
  Service providers will base authorisation on a combination of IdP and community provided attributes. This work item validates the investigations done in JRA1 with at least two real service providers as they exist in participating R&E communities. In collaboration with NA3, LoA requirements with regard to authorisation attributes will be considered and tested.

Task 3: Pilot to improve access to research and education relevant resources and (commercial) services
Task Leader Organisation: PSNC

Objectives
The aim of this task is to:

- To provide AAI mechanisms to access (non-web) resources relevant for the R&E communities (e.g. FIM4R)
- To pilot mechanisms identified in JRA1 to integrated services that are not yet

accessible via the federated framework.

- To pilot SSO access for commercial (cloud) services for research communities and consider both technical/architectural solutions (in collaboration with JRA1) and legal and policy aspects (in collaboration with NA3). This work will build on the results of the service activity “Support to cloud that is part of the GN3plus”

The goal of this activity is to demonstrate how the credentials owned by the users and the information of the attributes provided by the tools of Tas2 are compatible with the different technologies used by the e-infrastructures and service providers

Demonstrate how the tools deployed in Task 1 and 3 can effectively bridge the usage of user credentials between two or more e-infrastructures and interconnects the e-infrastructure service providers with IdPs and attribute authorities. As part of this activity the common attribute requirements for non-web SSO, authorisation and provisioning will be investigated.

The commercial services will be selected together with the user community and we will work together with eduGAIN/GÉANT4 to ensure a sustainable service delivery model.

Deliverables
DSA1.1 Pilots to support guest users solutions, M14
DSA1.2 First results on the initial pilots, M15
DSA1.3 Pilot on attribute provider framework, M20
DSA1.4 Pilot to improve access s to R&E relevant resources, M23

Table 3.1b: List of work packages

Work package No	Work Package Title	Lead Participant No	Lead Participant Short Name	Person-Months	Start Month	End month
NA1	Project Management	1	TERENA	14	M1	M24
NA2	Training and Outreach	1	TERENA	75	M1	M24
JRA1	Architectures for an integrated and interoperable AAI	5	GRNET	75	M1	M24
NA3	Policy and Best Practices Harmonisation	15	FOM-NIKHEF	66	M1	M24
SA1	Proof of concepts on cross sector SSO and attribute management	19	SURFnet	96	M1	M24
			Total PM	**326**		

Table 3.1 c: List of deliverables

Deliverable Number	Deliverable Name	WP no.	Short name of lead participants	Type	Dissemination Level	Delivery Date
DNA1.1 and **DNA1.2**	Annual Reports	NA1	TERENA	R	PU	PM12, PM24
DNA1.3	Summary of main dissemination activities, main achievements of AARC for and Exploitation Report	NA1	TERENA	R	PU	PM23
DNA2.1	Report on the identified target groups for training and their requirements	NA2	TERENA	R	PU	PM3
DNA2.2	Training material on main technical and policy concepts of federated access	NA2	TERENA	DEC	PU	PM5
DNA2.3	Training material targeted to Resource and Service Providers	NA2	CSC	DEC	PU	PM9
DNA2.4	Training material targeted to Identity providers	NA2	GARR	DEC	PU	PM14
DNA3.1	Differentiated LoA recommendations for policy and practices of identity and attribute providers	NA3	CSC	R	PU	M23
DNA3.2	Generic security incident response procedure for federations	NA3	CERN	R	PU	M20
DNA3.3	Recommendation for service operational models for enabling cross-domain sustainable services	NA3	DAASI	R	PU	M21
DNA3.4	Recommendations on the grouping of entities and their deployment	NA3	STFC	R	PU	M24

	mechanisms in scalable policy negotiation					
DNA3.5	Recommendations and template policies for the processing of personal data by participants in the pan-European AAI	NA3	KIT	R	PU	M18
DJRA1.1	Analysis of user-community requirements	JRA1	EGI	R	PU	M4
DJRA1.2	Blueprint architectures	JRA1	KIT	R	PU	M24
DSA1.1	Pilots to support guest users solutions	SA1	GARR	DEM	PU	PM15
DSA1.2	First report on the Pilots deployed by SA1	SA1	SURFnet	R	PU	PM15
DSA1.3	Final pilot on attribute provider framework	SA1	EGI	DEM	PU	PM20
DSA1.4	Pilot to improve access to R&E relevant resources	SA1	PSNC	DEM	PU	PM23

Appendix – Glossary

Attribute Authorities	The AA is a component of the Identity Provider. It issues attributes on behalf of an organisation.
Code of Conduct [CoC]	The CoC, also called Data Protection CoC or CoC for Service Providers describes an approach to meet the requirements of the EU Data Protection Directive in federated identity management. It defines behavioural rules for Service Providers [SP] which want to receive user attributes from the Identity Provider. https://refeds.terena.org/index.php/Data_protection_coc
DARIAH	The Digital Research Infrastructure for the Arts and Humanities project was set up with the mission to enhance and support digitally-enabled research across the humanities and arts. In August 2014, DARIAH became a legal entity. https://www.dariah.eu/
e-Infrastructures	In the context of the AARC project, e-Infrastructures are the entities that offer network, data, storage and computational facilities for research and education. The e-Infrastructures that are considered are GÉANT (the pan-European research and education network), EUDAT (the pan-European research and education data infrastructure), EGI (the pan-European high throughput and cloud data analysis infrastructure for researchers), PRACE (high performance computing infrastructure) and the ESFRI cluster projects .
ELIXIR	ELIXIR's goal is to orchestrate the collection, quality control and archiving of large amounts of biological data produced by life science experiments. http://www.elixir-europe.org/
eduroam	eduroam is the European born global infrastructures to enable for federated access to the network. To date 54 countries participate in eduroam. http://www.eduroam.org
eduGAIN	eduGAIN provides legal and technical frameworks to make Identity Federations [IDF] interoperate. As of April 2014 24 identity federations world-wide participate in eduGAIN. http://www.edugain.org
ESFRI Cluster Projects	ESFRI, the European Strategy Forum on Research Infrastructures, is a European multilateral initiative - namely a forum - supported by the EC and associated member states, aimed at enabling the establishment and the consolidation of research infrastructure in Europe. Since December 2012 the main task of ESFRI is to help the projects on the roadmap (to move towards implementation. Until now ESFRI working areas are: 1. Social Sciences and Humanities

	2. Environmental Sciences 3. Energy 4. Biological and Medical Sciences 5. Engineering, Physical Sciences, 6. Materials and analytical Facilities 7. e-Infrastructures ESFRI roadmap: http://ec.europa.eu/research/infrastructures/pdf/esfri-strategy_report_and_roadmap.pdf
EU Data Protection Laws	To date the data protection laws are regulated by the Data Protection Directive: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT
FIM4R	In summer 2011 a group of large research projects started to investigate Federated Identity Management (FIM) for research collaborations. This group is now known as FIM4R. Through a number of workshops, the research communities have converged on a common vision for FIM, enumerated a set of requirements and proposed a number of recommendations for ensuring a roadmap for the uptake of FIM is achieved. These points have been documented in a paper: https://cdsweb.cern.ch/record/1442597
Federated Identity Management (FIM)	Federated Access, or Federated Access Management, or Federated Identity Management (FIM) or simply Identity Federation (IDF) is a mix of technology and policies to allow a user authenticated by an institution (identity provider) to access resources and services offered by different providers (service providers) in different administrative domains that are part of the same federation. This approach enables Single-Sign-On (SSO), in which a user's single authentication token is trusted across multiple systems or organisations. The benefits of federated access are for institutions to offer a richer portfolio of services in a more cost-effective manner and for the users to deal with less credentials.
Identity Provider	In federated access, and Identity provider is the institution that issues the user's credentials that are trusted by the resources and services available in the federation.
IGTF	The Interoperable Grid Trust Federation (IGTF) is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers, and other qualified relying parties. https://www.igtf.net/

Kantara Initiative	The Kantara Initiative is Kantara Initiative is a non-profit membership organisation that connects businesses, consumers, governments, and citizens through innovations and programs that support more natively trust worthy on-line experiences. https://kantarainitiative.org/about/
LHC	Large Hadron Collider, the world's largest and most powerful particle accelerator.
NREN	An National Research and Education Network is responsible for offering the network connectivity within a country. NRENs typically operate (directly or via sub-contractors) the R&E identity federation as well.
RDA	The Research Data Alliance**,** RDA, aims to enable researchers and innovators to openly share data across technologies, disciplines, and countries to address the grand challenges of society. https://rd-alliance.org/
REFEDS	The Research and Education FEDerationS group is the international body led by TERENA to coordinate Identity Federation processes, practices and policies in the Higher R&E sector and to discuss ways to manage inter-federation work. https://refeds.org/
SAML	The Security Assertion Markup Language - is an XML framework for exchanging authentication and authorization information. SAML is a standard of OASIS.
Service Provider	In FIM, a service provider, is a component that evaluates the authentication information received from an IdP and uses them for controlling access to protected services.
WLCG	The Worldwide LHC Computing Grid is a global collaboration of more than 170 computing centres in 40 countries, linking up national and international grid infrastructures. The aim of WLCG is to provide global computing resources to store, distribute and analyse the ~30 Petabytes (30 million Gigabytes) of data annually generated by the Large Hadron Collider at CERN. http://wlcg.web.cern.ch/
X.509	X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm**.**