15-12-2016

Deliverable DSA1.2:
First report on the pilots deployed by SA1

Deliverable DSA1.2

Contractual Date:	31-07-2016
Actual Date:	15-12-2016
Grant Agreement No.:	653965
Work Package:	SA1
Task Item:	T2
Lead Partner:	SURFnet
Document Code:	DSA1.2
Authors:	P. van Dijk (SURFnet)

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

Abstract

This document provides an overview of the pilots undertaken in Year 1 by AARC Service Activity 1. It summarises the overall pilot approach, outlines the technical platform and support infrastructure established, and gives a structured description of the pilots running within each Task, including the use case, requirements, components being used, results and plans for Year 2.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This document provides an overview of the pilots undertaken in Year 1 within AARC Service Activity 1 Pilots (SA1).

The first cycle of pilots has taken as input the results from key deliverables and milestones produced by other Activities, including the user and service provider requirements and AARC blueprint architecture (from Joint Research Activity 1 Architectures (JRA1)) and the preliminary results from Networking Activity 3 Policy Harmonisation (NA3).

After the first year of AARC, more than eight pilots are running. The work has been organised according to the thematic Tasks in SA1:

- Task 0 – Work Package Leadership.
- Task 1 – Guest Access.
- Task 2 – Attribute Management.
- Task 3 – Access to Resources.

Some of the pilots, such as SAML/IP Bridge, Walk-by Users and IdP/SP Proxy for Library Consortia within Task 1, are close to finalisation, and one, CILogon, within Task 3, has already been handed over to NA3 for sustainability and operational models to be developed for the service.

Based on the pilots, SA1 has identified interesting ideas for solutions, and also a number of challenges. Plans are in place to extend and build on the pilots in Year 2, including joint Task work on solutions for bridging towards social and e-governmental identities, and further token translation and ORCID solutions.

The deliverable provides a general overview of the SA1 Year 1 pilots. Each section covers one Task and follows a similar structure, providing a brief description of the use case, the components being used, and pilot results. A more in-depth description of the AARC pilots is available in the AARC public Wiki [AARCWiki].

1 Introduction

Service Activity 1 Pilots (SA1) aims to facilitate research by providing access management tools and a framework to support collaboration in a distributed environment. To this end, the Activity demonstrates through (pre-)production pilots that:

- Existing authentication and authorisation infrastructures (AAIs) and authentication sources can be leveraged to enable (single sign-on (SSO)) access, with appropriate level of assurance, for any natural person (both within and outside academia), to shared resources offered by different e-infrastructure providers and communities.
- Authoritative decisions and user/group context can be based on distributed group managers and attribute providers.
- Access to non-web and commercial services can be enabled. This requires the bridging of security assertion markup language (SAML)-based infrastructures (the national research and education network (NREN) world) and token/certificate-based services as commonly delivered by e-infrastructure providers.

1.1 Pilot Approach

The AARC pilots are driven by two main use cases:

- Research communities that require access to services offered by different research or e-infrastructures and wish to use their existing credentials.
- Research and/or e-infrastructures that want to build an AAI and are looking for recommendations and best practices to do that in the most effective and interoperable way.

The approach followed by the AARC pilots is to deploy existing technical components as identified within Joint Research Activity 1 Architectures (JRA1), and to integrate a selection of these components in line with the use cases and according to a common blueprint architecture proposed by AARC. As part of the pilots, policy aspects elaborated in Networking Activity 3 Policy Harmonisation (NA3) are also tested.

To this purpose, SA1 established a stable pilot environment with solutions to be assessed by the stakeholders (e.g. research library communities, ELIXIR, BBMRI and EGI) of research communities. A more detailed description of the aims and approach of the pilot activity is available in *Milestone MSA1.1: Specify the work to be undertaken in collaboration with JRA1 and NA3* [MSA1.1].

As soon as the research community requirements became available (August 2015) and as soon as other documents concerning the blueprint architecture and the policy harmonisation work were produced, the

AARC pilot team started to scope the pilots and to define the platform to execute them. The most influential documents for the pilots are listed below:

- *Milestone MSA1.1: Specify the work to be undertaken in collaboration with JRA1 and NA3* [MSA1.1].
- *Deliverable DJRA1.1: Analysis of user community and service provider requirements* [DJRA1.1].
- *Milestone MJRA1.1: Existing AAI and available technologies for federated access* [MJRA1.1].
- *Milestone MJRA1.2: Design for Deploying Solutions for "Guest Identities"* [MJRA1.2].
- *Milestone MJRA1.3: Design for the integration of an Attribute Management Tool* [MJRA1.3].
- *Milestone MJRA1.4: First Draft of the Blueprint Architecture* [MJRA1.4].

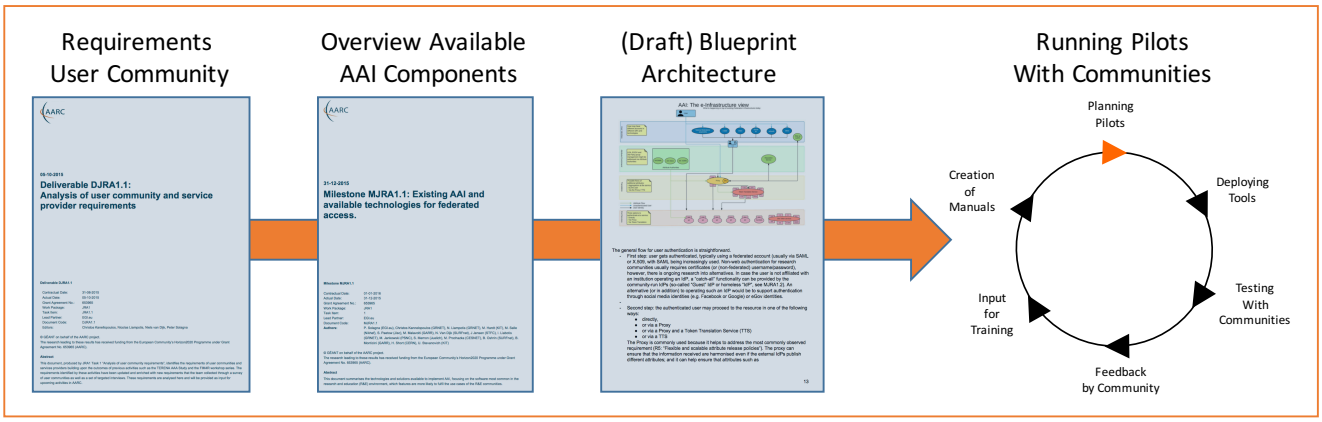

Figure 1.1: Examples of AARC deliverables and milestones guiding pilots with communities

With the feedback from members of the community, lessons learned and the creation of manuals, SA1 closes a pilot cycle and hands over the results of successful pilots to NA3 to work on sustainability aspects [NA3-WIKI-SOM]. NA3 has a Task dedicated to providing recommendations for adoption by operational infrastructures, and guidance as to which model is applicable given the operating model of a community. Its findings are being documented in *Deliverable DNA3.3: Recommendation for service operational models for enabling cross-domain sustainable services*, due in M21. With those recommendations at hand, the NA3 and the SA1 teams will provide suggestions for operational models for the piloted solutions.

1.2 In this Document

This document provides an overview of the pilots undertaken by SA1 in Year 1. It is structured by Task, in each case (except Task 0 Activity Leadership) covering:

- Use case focused on.
- Requirements to be met.
- For each pilot, a table summarising and/or providing links to:
  - Focus.
  - Approach/AARC identified solution.
  - Components piloted.

    - Gain for end users/administrators.
    - Demo/video.
    - Detailed technical description.
    - Documentation of components.
    - Software sources.
    - Lead.
    - Community partners.
    - Status.
- Observations.

The document ends with a brief Conclusions section, summarising and evaluating the progress made to date.

A more in-depth description of the AARC pilots is available in the AARC public wiki [AARCWiki].

2 Year 1 Results from Task 0 – Activity Leadership

2.1 Focus in Task 0

To fully support all pilot activities and to provide a jump start for each pilot sub-task, SA1 has created a pilot platform. This platform is a staging area and can be used to test and deploy services and to pilot services with the communities. It is not considered as a production facility. Nevertheless, ample attention has still been paid to operational aspects, including security, updates and deployability of software components.

2.2 The Pilot Platform

A technical platform has been delivered by ~okeanos [~okeanos], the GRNET Infrastructure as a Service (IaaS) platform. For AARC, 30 virtual machines (VMs) are available with appropriate specifications to run the pilots. The platform has been designed in line with AARC's blueprint architecture [MJRA1.4]. It combines the open source software OpenConext [OpenConext] and the collaboration management platform COmanage [COmanage] to leverage a service provider (SP) proxy scenario that can serve AARC itself. COmanage is used to centrally manage specific virtual organisation (VO) groups and attributes, including secure shell (SSH) and virtual private network (VPN) provisioning; OpenConext takes care of the SP proxy. Attribute aggregation from COmanage and other sources (e.g. ORCID [ORCID]) and OpenConext authorisation are used to test authorisation scenarios on behalf of the services of the VO. This approach has been demonstrated at several occasions e.g. in meetings with research community representatives. The team delivered a screen-capture video [PilotPlatformVideo] and documentation for the OpenConext and COmanage components being used.

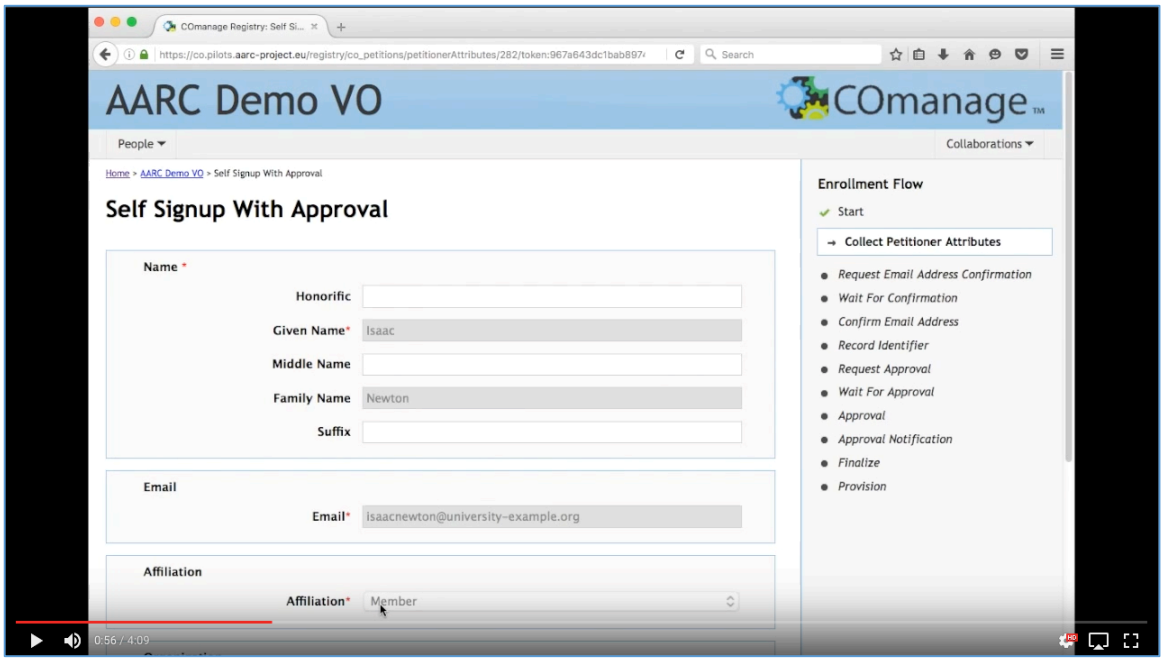

Figure 2.1: Still from screen-capture video on using COmanage to provide self-service access to a Linux server

One year on from the start of the AARC project, 27 out of the 30 VMs are in use for 11 different pilots. To ensure secure access to these VMs, the pilot platform was equipped with ZeroTier VPN [ZeroTier]. Only registered clients will obtain access to the virtual pilot LAN.

2.3 Additional Features and Resources

A top-level domain has been created for the pilot projects: *.pilots.aarc-project.eu, to ensure that the targeted AARC communities can easily find and access AARC pilot setups and demonstrators.

To facilitate any testing by communities, a SimpleSAMLphp DIY test identity provider has been included in this environment. This identity provider is named “DIY IdP” and is available as a test IdP for AARC pilot projects. It allows the testing of various login and attribute scenarios that are common when dealing with SAML identity providers.

Code, configuration data, results and documentation for the pilot projects can be stored in the central AARC pilot Git repository [AARCGit]. For more sensitive data, such as specific configuration data, keys and certificates, a private GitLab repository is available [AARCPrivate].

First-line support for using the pilot infrastructure, e.g. to join the ZeroTier network, is provided by SURFnet staff. Further details on the pilot infrastructure are available in the AARC public Wiki [AARCWiki].

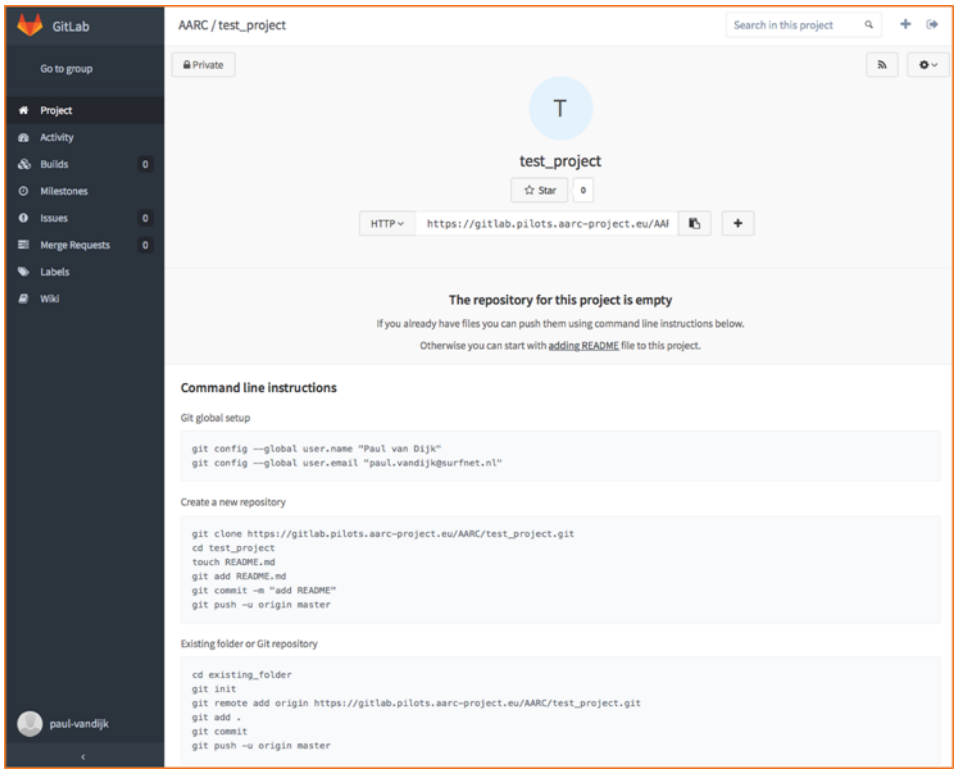

Figure 2.2: Screenshot of the AARC pilot GitLab staging area

2.4 Pilots Started

Based on information from the deliverables and milestones from the AARC Architectures (JRA1) and Policy Harmonisation (NA3) Activities, SA1 commenced the first cycle of pilots as follows:

- In **Task 1 Guest Access**, a pilot has started that involves libraries in the identification and hands-on implementation of relevant solutions to support their migration from IP address-based authentication against publishers' online resources to a SAML-/federated-based approach. This work focuses on embracing:
    1. All possible users who need access to library resources, including so-called walk-by users, who may be citizen scientists.
    2. All relevant service providers, including those who only support IP-address based access control.

  The aim of this pilot is to show that it is possible to apply the principle of inclusiveness and at the same hide complexity for users and librarians.
- In **Task 2 Attribute Management**, a pilot has started that tests the use of SAML-based attribute authorities to provide authoritative information to be consumed by cloud services offered by e-infrastructures and other providers (e.g. at EGI). Attribute authority components tested so far are Perun [Perun] and COmanage [COmanage]. Attribute aggregation components used are OpenConext [OpenConext] and SimpleSAMLphp [SimpleSAMLphp]. In a later phase the Task aims to address and pilot scenarios where attributes from multiple attribute authorities (and probably multiple VOs) flow

into services; for example, a cloud provider that serves several virtual organisations, managed by different virtual organisation manager entities.

- In **Task 3 Access to Resources**, token translation services have been established and piloted. Two pilots are running as part of this Task:
    1. One pilot focuses on developing a CILogon pilot service for Europe [CILogon] based on the components developed by the CILogon service in the US. Several extensions have been added to the code and a certification authority (and the relevant policies) have also been created as part of the pilot. The CILogon pilot works as a token translation service to bridge the gap between SAML-based authentication (NRENs) and certificate-based authentication (e-science and e-infrastructure providers).
    2. A second pilot, on access to resources, assesses the feasibility of enabling non-web single sign-on based on LDAP-Facade [LDAPFacade], a tool developed by the Karlsruhe Institute of Technology (KIT), which is participating in AARC.

    A pilot to test a third solution, Unity-IdM [Unity-IdM], is in preparation.

    A fourth pilot, using ORCID [ORCID] to showcase federated access to third-party services, is also underway.

A general overview of the AARC pilots is given in the following sections. Each section covers one Task and follows a similar structure, providing a brief description of the use case, the components being used, and pilot results. A more in-depth description of the AARC pilots is available in the AARC public Wiki [AARCWiki].

3 Year 1 Results from Task 1 Guest Access

3.1 Focus in Task 1

This Task deals with the pilot work to be set up for AARC in the domain of guest identities. It liaises with the AARC Architectures (JRA1) and Policy Harmonisation (NA3) Activities in order to effectively demonstrate the validity of the components selected and architecture designed, and the best practices and recommendations identified.

The Task consists of several sub-tasks with different focus areas:

- Long Tail of Science – This work area deals with bridging the NREN world towards social and governmental IDs, using level of assurance (LoA)-enhancing mechanisms to enable them to make use of federated services (SPs).
- Catch-all Federation and Guest IdP / Cloud IdP – This work area deals with the enrolment of new IDs in a federated model, creating a catch-all federation for IdPs without a reference federation, and providing a new IdP through the cloud.
- Libraries – This work area deals with piloting solutions to lower the threshold for inclusion of library tools, including those handling access based on IP addresses, and a workflow into a federated model for identity management, with support for library walk-by users (e.g. citizen scientists) who are not registered in the campus identity management systems.

During the first 12 months of the AARC project the main focus of the SA1 Task 1 team has been on pilots for library use cases. The results presented in this section therefore mainly concern pilot solutions for libraries. Another deliverable, *DSA1.1 Pilots to support guest users solutions*, that is due to be released at the same time as this one, provides a more extensive and in-depth description of the results achieved in SA1 Task 1 so far.

3.2 Research Library Requirements

One of the goals of AARC is to improve access to digital resources offered by libraries. This work takes place in collaboration with AARC partners Ligue des Bibliothèques Européennes de Recherche – Association of European Research Libraries (LIBER), the Moravian Library (MZK) and several other national bodies representing research libraries in Greece, Italy and The Netherlands. Several pilots have been started to address the needs and problems faced by libraries and library consortia.

The Task identified three different but related issues that hamper the adoption of federated access and access control in the world of research libraries:

- First, to date, many library resources, such as journals and tools, are not accessible with an institutional account. To restrict access to such resources, libraries still rely on IP address-based access control. Although this method of access control is in use at many libraries worldwide, library ICT staff members need to maintain the correct IP address ranges and regard this approach as too labour intensive and inaccurate.
- Second, many librarians are broadening access to their own and remote resources to the general public, in line with their aim to share knowledge with a wide community. This includes, for example, citizen scientists who are not affiliated with an institution and lack a verified institutional account to obtain access to restricted library sources. Up until now, most libraries offer access for any user visiting the library. This type of user is called a "walk-by user". For access to content based on IP address ranges, this is not a problem, but as soon as federated access-based solutions are introduced as a replacement for IP address-based access, non-academic users are no longer able to access restricted resources. Therefore, for providers supporting SAML-based access only, a solution to serve walk-by users is needed.
- A third observation that emerged was that in some countries libraries maintain a mesh-based SAML federation parallel to national identity federations. This approach introduces a lot of complexity, for example in terms of the number of interactions between IdPs and SPs that need to be maintained. By introducing a proxy component, librarians and library consortia can drastically reduce the number of end-point interactions. At the same time, tools and facilities become available to brand and arrange the authentication flow in a consistent and trustworthy way.

As a result of the above-mentioned issues, users are currently confronted with inconsistent and confusing ("if this then that") user interfaces depending on who they are (academic/non-academic), the resource they want to access and the location at which they reside (at home or on campus).

The Task translated these issues into requirements, which have been described in detail in *Deliverable DJRA1.1: Analysis of user community and service provider requirements* [DJRA1.1]. That document provides a dedicated description of the issues research communities (including librarians) currently face with regard to federated identity management. Requirements R1, R2, R7 and R_P_6, summarised in Table 3.1 below, are applicable to libraries and have been guiding the work in this pilot. ("R" denotes architectural and technical requirements; "R_P" denotes policy and best practice requirements.)

ID	Title	Description
R1	User friendliness	The Federated AAI framework should provide simple and intuitive tools that are able to address the needs of users with different levels of ICT literacy
R2	Homeless users	The Federated AAI framework should support users without a federated institutional IdP, such as citizen scientists and researchers without formal association to research laboratories or universities
R7	Federation solutions based on open and standards-based technologies	Open and standards-based AAI technologies should be used by the different communities to allow for interoperability by means of suitable translation services

ID	Title	Description
R_P_6	Simplified process for joining identity federations	The bureaucracy involved in joining identity federations should be reduced

Table 3.1: Functional requirements for library pilots

3.3 Piloted Library Solutions

Three library solutions have been piloted:

- SAML/IP bridge.
- Walk-by users.
- IdP/SP proxy for library consortia.

Each of these is described below.

3.3.1.1 *Pilot 1 – SAML/IP Bridge*

Task 1 established a pilot proxy to be used by libraries to give access to restricted content no matter whether the (content) provider supports SAML or not. This approach is not new and in fact an existing solution called EZproxy [EZproxy] offers functionality to bridge SAML to IP. EZproxy is a comprehensive product provided by the Online Computer Library Centre (OCLC) [OCLC], a fully fledged rewriting proxy capable of managing both SAML- and IP-based authentication for users against online SPs. It also foresees the option to provide the product in a hosted fashion, if needed. It allows the proxy administrators to configure resources that need to be accessed in a federated fashion – provided a user is authenticated on a local IdP – and those that will be accessed in an IP-proxy fashion, based on the source IP of the EZproxy tool itself. A summary, with links to more details, is given in Table 3.2 below.

Task 1, Pilot 1	SAML/IP Bridge
Focus	Support access to federated and non-federated library resources – bridging SAML- and IP address-based access methods (SAML to SAML + SAML to IP)
Approach/AARC identified solution	Establish a proxy to bridge SAML and IP address access methods, a so-called access mode switch
Components piloted	EZproxy for SAML-IP bridge
Gain for end users/administrators	• Same entry point for users regardless of the type of authentication technology required by the service provider • A better user experience • An easy way for technical administrators at the libraries to introduce federated access without disrupting access to services that only support IP-based authentication

Task 1, Pilot 1	SAML/IP Bridge
Demo/video	• Demo • Flow • Video
Detailed technical description	AARC Wiki
Documentation of components	Documentation for EZproxy access mode switch
Software source(s)	EZproxy
Lead	GARR
Community partners	IT: GARR, Library NL: UKB library consortium
Status	Close to finalisation. Awaiting final phase of feedback from communities.

Table 3.2: Task 1, Pilot 1 – SAML/IP Bridge

3.3.1.2 *Pilot 2 – Walk-by Users*

To address the need to maintain the current practice of opening up resources to anyone who needs scientific information, including citizen scientists not affiliated with an institution ("walk-by users"), the Task added a component that is able to handle access requests from walk-by users (e.g. citizen scientists). The IP-based authentication plugin of Shibboleth IdP v3 [Shibboleth] can be used to authenticate local walk-by users based on the IP address of the terminal used at the library. The user chooses the library walk-by Shibboleth IdP and, in case the terminal resides within a valid IP address range, the IdP provides an attribute with the entitlement "walk-by user". Based on this attribute, a service provider can authorise the user to access restricted resources. More details about this pilot are available in Table 3.3 below.

Task 1, Pilot 2	Walk-by Users
Focus	Support authorised access for citizen scientists to library resources (SAML+IP to SAML with AuthZ)
Approach/AARC identified solution	Establish a guest SAML IdP that adds attributes to authorise non-institutional users. In addition, explore exploitation models: per library or per national library consortium deployment.
Components piloted	Shibboleth v3 for IdP with IP-based AuthZ attribute
Gain for end users/administrators	• More consistent interface no matter which resource is being approached • Ability to use this access method and at the same time maintain full privacy • Admin interface for librarians to scope/configure valid IP ranges
Demo/video	• Flow • Demo admin portal

Task 1, Pilot 2	Walk-by Users
	• Demo user portal
Detailed technical description	AARC Wiki
Documentation of components	Documentation for walk-by user access component, access control Wiki
Software source(s)	Shibboleth v3 for walk-by user access
Lead	GARR/DAASI
Community partners	IT: GARR, Library NL: UKB library consortium
Status	Close to finalisation. Awaiting final phase of feedback from communities.

Table 3.3: Task 1, Pilot 2 – Walk-by users

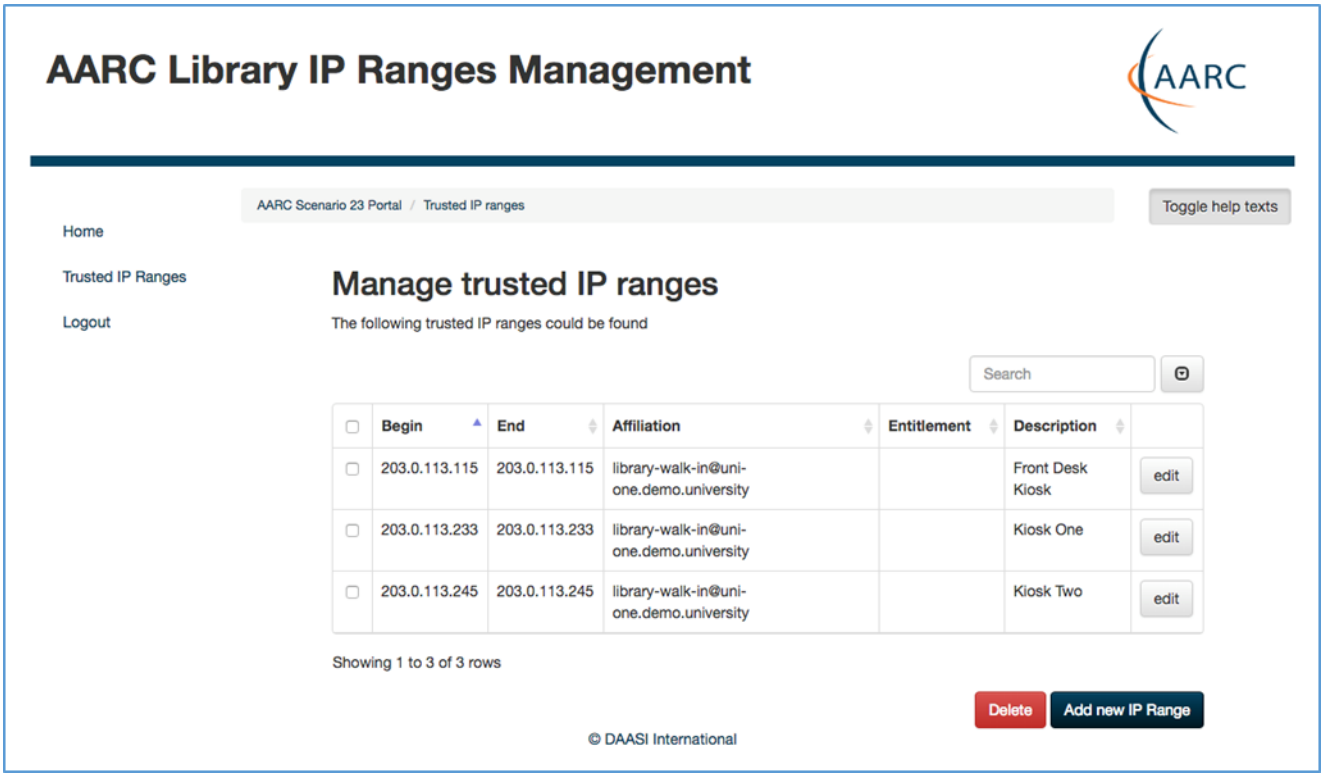

Figure 3.1: Screenshot of the library walk-by users admin portal

3.3.1.3 *Pilot 3 – IdP/SP Proxy for Library Consortia*

To address the many-to-many SAML interactions topic that some library consortia are dealing with, the Task piloted the suitability of an IdP/SP proxy solution. More detailed descriptions and links are given in Table 3.4 below.

Task 1, Pilot 3	IdP/SP Proxy for Library Consortia
Focus	Showcase a model for library consortia to reduce the number of interactions between IdPs and SPs from a technical and trust point of view while preserving the privacy of users
Approach/AARC identified solution	Establish a proxy as a single point for interaction between IdPs and SPs, branded as a HEAL-Link initiative
Components piloted	SimpleSAMLphp as IdP/SP proxy
Gain for end users/administrators	• More consistent interface no matter which resource is being approached • Better service to end users, standardised access method • Less effort to maintain and administer access for library administrators • Allows publisher contracts to be managed centrally by the consortium • Easier to implement and manage trust relationships among IdPs and SPs • Library consortium will retain control on branding and policies • More precise and easier to produce statistics
Demo/video	• Flow • Demo
Detailed technical description	AARC Wiki
Documentation of components	Documentation for the HEAL-Link proxy
Software source(s)	SimpleSAMLphp for the IdP/SP proxy Memcached Shibboleth
Lead	GARR/GRNET
Community partners	GR: HEAL-Link consortium GR: Aristotle University of Thessaloniki (identity provider) US: Wiley Online Library (service provider)
Status	The IdP/SP proxy has joined the GRNET federation and the login workflow has been tested using the production IdP of one of the participating academic organisations, namely the Aristotle University of Thessaloniki. The interconnection of the proxy with the (pre-production) SP of Wiley Online Library (partners with HEAL-Link) is close to finalisation.

Table 3.4: Task 1, Pilot 3 – IdP/SP proxy for library consortia

Figure 3.2: Screenshot of the demo library service provider portal

3.3.1.4 *Observations*

Overall, with the approaches and solutions provided above, users of library resources will have a smoother experience while accessing resources, irrespective of the authentication method that is supported. At the same time, these solutions offer opportunities to reduce the administrative burden of library staff in relation to managing SAML connections and maintaining access to restricted library resources.

3.4 New Pilots Started in Task 1

At the time of writing, several pilots in the category “guest access” have been started and are still ongoing. These include:

- Piloting solutions for bridging towards social and e-governmental identities. The social identities pilot is being carried out in collaboration with Task 2. Its goals are to demonstrate the actual inclusion of guest identities (e.g. Google ID, Facebook ID, etc.) in the provisioning and consumption of federated services and to provide pragmatic suggestions for vetting the identity of users authenticating with social IDs. Such a setup can be achieved by establishing an IdP/SP proxy bridging OAuth2 [OAuth2] / OIDC [OIDC] and SAML, an attribute authority (based on the COmanage component), providing additional attributes to the ID.
- In parallel, a second social ID pilot has started. In this pilot the focus is on establishing a transparent external identity proxy (TEIP) based on the work of the GN4-1 SA5 Virtual Organisation Platform as a Service (VOPaaS) project [VOPaaS]. With this pilot the Task hopes to show that the VOPaaS TEIP approach provides useful possibilities for handling social IDs in a generic and consistent way. For example, it features functionalities to feed in many different IDs (eduID, Feide.id, Google ID, etc.), it assesses and applies level of assurance (LoA) according to the eIDAS EU Regulation [eIDAS] and it provides a single unique identifier.
- Some first steps have been taken to pilot with e-governmental IDs as well. For cross-border authentication using eIDs, the eIDAS EU regulation is being followed. eIDAS developed the “eIDAS Interoperability Framework”, which foresees an infrastructure based on national gateways

implemented at the EU member states. The eIDAS framework is intended to provide a means for member states to recognise each other's eIDs to access public services.

AARC is working with eIDAS representatives in order to establish a pilot activity that will assess the interoperability of the technical implementations and policy framework and that will investigate the use of eIDAS as one of the potential solutions for guest identities and for step-up authentication.

4 Year 1 Results from Task 2 – Attribute Management

4.1 Focus in Task 2

This Task deals with the deployment of pilots to establish an attribute management framework for collaborative single sign-on (SSO) scenarios. Based on the tools, methodology and blueprint architecture identified by JRA1, the Task started to pilot and test a number of solutions that facilitate and enable:

- **Attribute management**. 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 are being selected for a pilot. The tools 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 aims to 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 is investigating feasibility, security and privacy implications of at least two protocols.
- **Attribute-based authorisation**. Service providers will base authorisation on a combination of identity provider (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, level of assurance (LoA) requirements with regard to authorisation attributes are being considered and tested.

4.2 Attribute Management Requirements

Based on questionnaire responses and interviews with representatives of research communities and e-infrastructure providers, the Task identified several key requirements regarding attribute management that need to be met. The requirements have been described in detail in *Deliverable DJRA1.1: Analysis of user-community and service provider requirements* [DJRA1.1], and are summarised in Table 4.1 below. ("R" denotes architectural and technical requirements; "R_P" denotes policy and best practice requirements.)

ID	Title	Description
R1	User friendliness	The Federated AAI framework should provide simple and intuitive tools that are able to address the needs of users with different levels of ICT literacy
R3	Different Levels of Assurance	Credentials issued under different policies and procedures should

ID	Title	Description
		include the provenance of the level under which they were issued
R5	Flexible and scalable attribute release policies	Flexible negotiation mechanisms are required to govern the release of identity attributes
R7	Federation solutions based on open and standards-based technologies	Open and standards-based AAI technologies should be used by the different communities to allow for interoperability by means of suitable translation services
R8	Persistent user identifiers	The Federated AAI framework should reference the digital identities of users through long-lasting identifiers
R9	Unique user identities	Each user should have a single digital identity to allow SPs to uniquely identify their users
R_P_3	Sufficient attribute release	The set of attributes released to SPs should be extended, primarily, to allow consuming services to operate and, also, to allow for more advanced features, such as personalisation of services

Table 4.1: Functional requirements for attribute management pilots

4.3 Ongoing Pilots in Task 2

Currently, two attribute management pilots are running, to test components in the context of:

- EGI e-infrastructure.
- BBMRI-ERIC.

Each of these is described below.

4.3.1 Pilot 1 – EGI e-Infrastructure

The first pilot is to test components for attribute management in the context of the EGI e-infrastructure and its community.

Principles applied in this context are:

- Access to the various services should be granted based on the virtual organisation (VO) roles users have.
- Roles should be expressed in attributes.
- Back-end services should not have to deal with the complexity of multiple IdPs/federations/attribute authorities/technologies. Therefore, an attribute aggregation scenario is preferred.

Table 4.2 below provides further information and links to detailed resources on this pilot.

Task 2, Pilot 1	Attribute Management in the Context of the EGI Community
Focus	Investigate and pilot the usability of SAML-based AAI components to use externally managed attributes to provide and restrict access to cloud services
Approach/AARC identified solution	Establish an AAI infrastructure of IdPs and external attribute authorities; aggregate attributes from these sources to feed them to cloud service providers
Components piloted	Perun AA and SimpleSAMLphp as attribute aggregator component. At a later stage the components OpenConext, COmanage and CILogon will be added to this pilot setup
Gain for end users/administrators	• Consistent access procedures when accessing (shared) cloud services • Ability to control access to shared resources on a research community level • Ability to externalise and delegate the management of attributes to different partners and sources • Ability to mix, match and use different resources side by side (IdPs, AAs and SPs) • Ability to utilise level of assurance provided by IdPs
Demo/video	Not available yet
Detailed technical description	AARC Wiki
Documentation of components	Perun SimpleSAMLphp Integration of both components in the EGI infrastructure is expected soon
Software source(s)	Perun SimpleSAMLphp
Lead	EGI
Community partners	EGI
Status	Deployment of the EGI attribute management framework is in progress. Attribute authorities have been set up (Perun, GOCDB) and SimpleSAMLphp is in place to manage aggregation. COmanage will be added as a 3rd attribute source and OpenConext will be deployed to handle attribute aggregation. In addition, the CILogon setup described in Section 5.3.1 is in place and will be used in this context as well.

Table 4.2: Task 2, Pilot 1 – Attribute management in the context of the EGI community

4.3.2 Pilot 2 – BBMRI ERIC

In the second pilot the Task has started to test components for attribute management in the context of the biomedical Biobanking and BioMolecular resources Research Infrastructure – European Research

Infrastructure Consortium (BBMRI-ERIC). Here the aim is to establish a fully fledged standardised AAI for the BBMRI-ERIC community to enable access and authorisation to shared biomedical resources with appropriate level(s) of assurance. Links and further descriptions are given in Table 4.3 below.

Task 2, Pilot 2	Attribute Management in the Context of the BBMRI-ERIC
Focus	Establish a fully fledged standardised AAI for the BBMRI-ERIC community to enable access and authorisation to shared biomedical resources with appropriate level(s) of assurance
Approach/AARC identified solution	Based on existing infrastructures (eduGAIN, NREN federations) and components an entire AAI architecture will be piloted
Components piloted	Perun TEIP components
Gain for end users/administrators	• Consistent access and authorisation flows when accessing (shared) biomedical resources • A single standardised AAI with sufficient levels of assurance and ways to on-board all relevant members of the communities
Demo/video	Not available yet
Detailed technical description	Not available yet
Documentation of components	In progress
Software source(s)	In progress
Lead	CESNET/BBMRI-ERIC
Community partners	BBMRI-ERIC
Status	A pilot infrastructure has been established, Perun has been deployed (https://perun.bbmri-eric.eu) and registration processes have been defined. Selected applications from the BBMRI-ERIC community are in process of on-boarding to the piloted AAI. Preparations are currently underway to pilot with authentication and authorisation level of assurance and persistent identification approaches across e-infrastructures.

Table 4.3: Task 2, Pilot 2 – Attribute management in the context of BBMRI-ERIC

4.3.3 Observations

In both pilots the IdP/SP proxy approach has been adopted to handle all complexity. The Task recognises that the two pilots share many requirements and components. The teams share ideas and interact often to make sure that a common and generic approach results from their work and that duplication of effort is prevented.

In the second year of AARC the work of these pilots will be extended by adding components from Task 1 (guest access), e.g. to enable access for users with a social or e-governmental ID, and Task 3, to include solutions for non-web-based access, e.g. secure shell (SSH) and X.509 access.

5 Year 1 Results from Task 3 – Access to Resources

5.1 Focus in Task 3

This Task aims to improve access to relevant non-web resources located outside the home organisation of the user. The main improvement is to make use of existing AAIs that provide verified institutional user credentials and (external) authorisation attributes instead of local user management. While many successful implementations exist already for web portals, the technology for non-web scenarios (e.g. secure shell (SSH) or X.509 access) is still immature. As a result, the use of institutional credentials for research infrastructures and research services is still lacking. The focus of this Task is therefore on suitable approaches and services for token translation to bridge both worlds.

Another focus in Task 3 is that of access to (commercial) third-party services. Section 5.3.4 below summarises the work that has been done so far.

5.2 Access to Non-Web Resources Requirements

The requirements relevant to accessing non-web resources are described in detail in *Deliverable DJRA1.1: Analysis of user community and service provider requirements* [DJRA1.1] and summarised in Table 5.1 below. ("R" denotes architectural and technical requirements.)

ID	Title	Description
R1	User friendliness	The Federated AAI framework should provide simple and intuitive tools that are able to address the needs of users with different levels of ICT literacy. There should be no need to install additional software on the user side. There should be no need to maintain local accounts on each resource manually.
R4	Community-based authorisation	The Federated AAI framework should enable communities to manage the assignment of attributes to their members for authorisation purposes
R11	Up-to-date identity information	The up-to-dateness of identity attributes should be guaranteed through an on-demand and/or recurring verification process
R12	User groups and roles	The Federated AAI framework should support the assignment of groups to users, as well as the assignment of roles to users within their groups. This also applies to non-web scenarios.

ID	Title	Description
R14	Browser- & non-browser-based federated access	The Federated AAI framework should provide federated access to both web-based and non-web-based services/applications

Table 5.1: Functional requirements for access to non-web resources

5.3 Ongoing Pilots in Task 3

To address the token translation topic, the Task started two pilots: the CILogon pilot and the LDAP-Facade pilot. For both, preliminary results are available already. Preparation for a third pilot, with the Unity-IdM component, has started recently; first results will be available at a later stage. A fourth pilot, that aims to improve and showcase federated access to third-party services, is also underway. Each of these pilots is described below.

5.3.1 Pilot 1 – CILogon

The CILogon pilot aims to test the feasibility of providing a more advanced online service for producing certificates based on an institutional login and delegating a proxy certificate to a non-web back-end service, without troubling the user with certificate-related complexity. Public key infrastructures (PKIs) work very well for experts who are used to handling certificates and private keys, but are considered to be very difficult by most end users. For automated systems, certificate-based authentication is, however, fast, reliable, well supported, well understood from a security point of view, etc.

The pilot setup roughly falls into three separate parts:

- A central online certification authority (CA) with a web front end.
- A caching and credential-handling master portal.
- Science gateways run by virtual organisations (VOs) (VO portals).

The end user interacts almost exclusively with the science gateway. As a result of this pilot and the components tested, the team established a white-label Research and Collaboration Authentication CA Service for Europe (RCauth.eu) [RCauth]. This online CA service hides complexity for users, is Interoperable Global Trust Federation (IGTF) [IGTF] accredited, and complies with Security Incident Response Trust Framework for Federated Identity (Sirtfi) [Sirtfi], the REFEDS Research and Scholarship specifications [REFEDS-R&S] and the eduGAIN 2.0 declaration [eduGAIN]. Because of those features it is already recognised as an attractive solution for research collaborations and e-infrastructures to share their resources with their communities.

A summary of the pilot and links to further detail are provided in Table 5.2 below.

Task 3, Pilot 1	Access to Non-web Resources – CILogon
Focus	Pilot a combination of solutions (workaround) to enable access to non-web, X.509-based resources that are common in the GRID world with SAML-based credentials in an end-user-friendly way
Approach/AARC identified solution	CILogon is the central component in this pilot, which provides X.509 certificates using OpenID Connect and a SAML-based federated identity. End users interact with web portals (science gateways), which are represented in the pilot in the form of a demonstrator "VO Portal". Additional components, such as a separate "Master Portal", have been introduced to hide complexity for the users and science gateways and to provide sufficient scalability. At the same time, interfacing with the Virtual Organisation Membership Service (VOMS) [VOMS] as an attribute provider is being investigated and piloted.
Components piloted	CILogon software (including OA4MP, Shibboleth, MyProxy, Simple CA), VOportal + Master Portal, VOMS (interface with)
Gain for end users/administrators	• Providing X.509-based access capabilities to the end user without the need for them to maintain or understand PKI • No need to help end users with difficult-to-manage certificate credentials • A single entry point can provide access to a wide range of resources, both web- and non-web-based
Demo/video	• A clear explanation of this effort is provided as a blog with the title "Digital certificates behind the scenes: the AARC CILogon pilot" on the AARC project website here. • Demo
Detailed technical description	• FOM-NIKHEF AARC pilot Wiki • RCauth.eu presentation
Documentation of components	See FOM-NIKHEF AARC pilot Wiki
Software source(s)	See www.rcauth.eu and.RCauth.eu github
Lead	FOM-NIKHEF
Community partners	ELIXIR, EGI, CESNET, CSC
Status	After successful pilots with the ELIXIR and EGI community, a white-label CA pilot service has been created: RCauth.eu. In a next step, command line access to proxy credentials using SSH keys will be piloted.

Table 5.2: Task 3, Pilot 1 – Access to non-web resources – CILogon

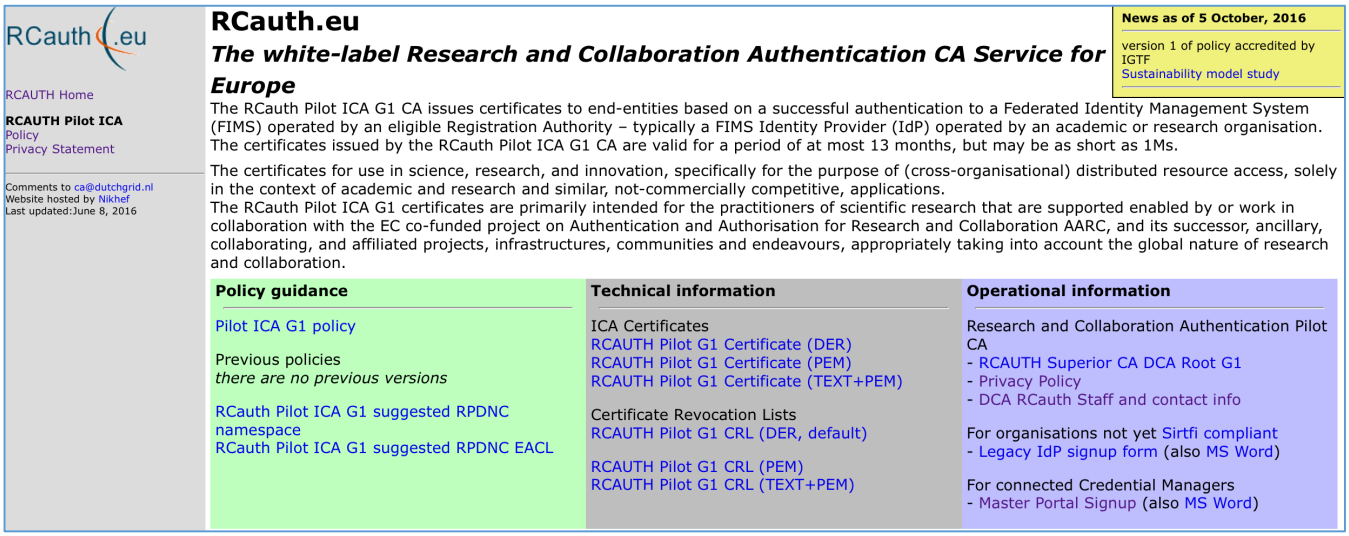

Figure 5.1: Screenshot of the RCauth.eu white-label CA service for Europe

With regard to AARC's aim to develop sustainability and operating models for emerging (AARC pilot) services, the CILogon pilot was a firstling. As part of the NA3 Policy Harmonisation Activity, the Service Operational Models Task (Task 3) has started to describe models and scenarios for this pilot. See *Sustainability models for the AARC CILogon-like TTS Pilot and RCauth.eu* [CILogon-Models] for more information.

5.3.2 Pilot 2 – LDAP-Facade

The second token translation pilot, based on the LDAP-Facade component, aims to provide access to non-web resources (e.g. SFTP, SSH console) for non-grid users by exploiting the existing AAIs, without the need to obtain user certificates. A summary of the pilot and links to further detail are provided in Table 5.3 below.

Task 3, Pilot 2	Access to Non-web Resources – LDAP-Facade
Focus	The pilot aims to provide access to non-web resources (e.g. SFTP, SSH console) to non-grid users using existing AAIs, without needing to obtain user certificates
Approach/AARC identified solution	LDAP-Facade is a single software component, which needs to be installed at the SP. It makes use of the local accounts prepared during the registration step. The software is able to replace the traditional LDAP server, as it provides the same interface. As a result, LDAP-Facade can be used as a local user manager, as well as an authentication and authorisation component, without any modification to servers (not only is core code unchanged, even implementing a specialised plugin is not necessary). On the other side (collaboration with external IdP), the deployment is the same as for any other SAML-based SP.
Components piloted	LDAP-Facade

Task 3, Pilot 2	Access to Non-web Resources – LDAP-Facade
Gain for end users/administrators	• No need to install additional software on user side • Limited use of user groups (depends on available attributes) • Federated access to non-web services • No need to manually maintain local accounts on each resource • No modification to server software • Up-to-date identity information (requires EPC or AQ SAML profiles support by the IdP. Workarounds have been proposed but are not yet implemented)
Demo/video	Demo (see flow description and instructions here)
Detailed technical description	AARC Wiki
Documentation of components	LDAP-Facade Wiki at KIT
Software source(s)	Git at KIT
Lead	PSNC, KIT
Community partners	PSNC, KIT
Status	Finalised. The LDAP-Facade portal is working. It is possible to log in there using eduGAIN credentials and register to a test service. The user is then able to log in to the resource using a local password. Limitation: the user's credentials are not checked against his/her IdP while logging in to the resource.

Table 5.3: Task 3, Pilot 2 – Access to non-web resources – LDAP-Facade

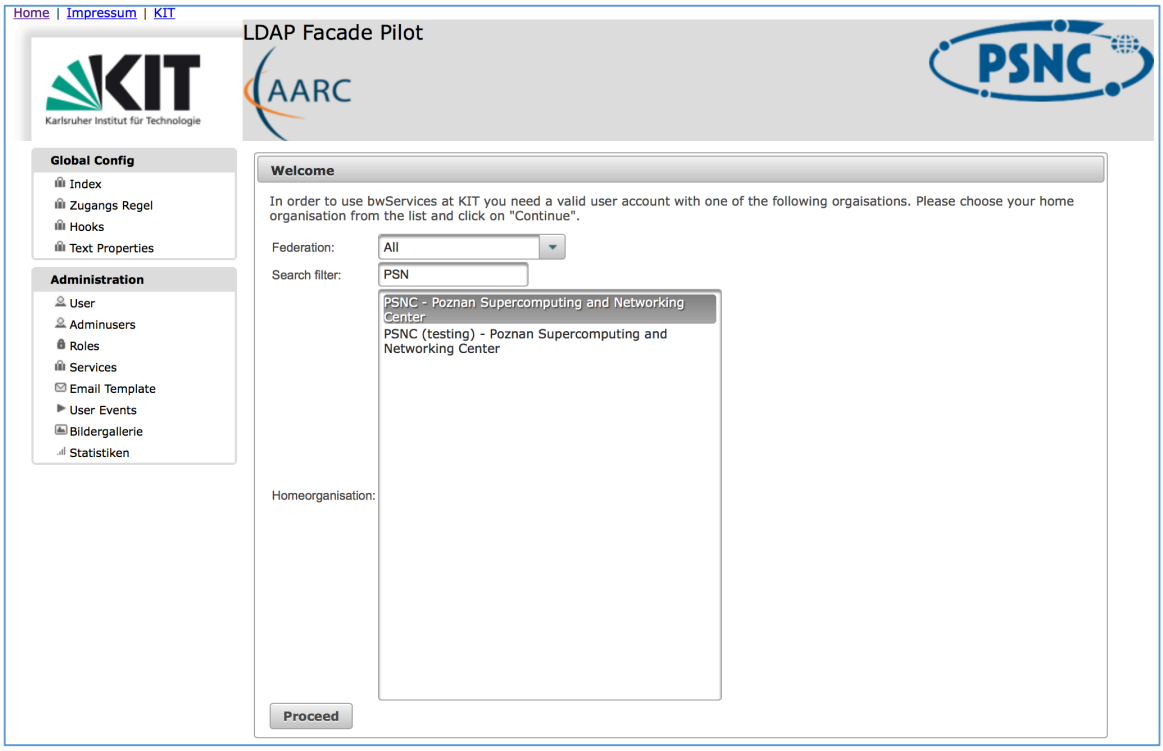

Figure 5.2: Screenshot of the LDAP-Facade pilot service

5.3.3 Pilot 3 – Unity-IdM

Unity-IdM [Unity-IdM] is a third potential solution for bridging SAML-based identities and attributes to non-web resources, which the Task aims to assess in the second year of the AARC project. It is currently used at EUDAT as the core component for their B2ACCESS service [EUDAT-B2ACCESS]. At the same time, EUDAT, as well as PRACE and EGI, are interested in applying the RCauth.eu services. The Task therefore aims to initiate a collaborative pilot with EUDAT AAI, PRACE and EGI. This effort is currently in preparation.

5.3.4 Pilot 4 – ORCID

Task 3 also has a focus on improving and showcasing federated access to third-party services. The ORCID pilot is one example of a third-party service that has been tested in the context of AARC. The pilot consists of three steps:

1. ORCID as a service provider (SP).
2. ORCID as an identity provider (IdP) (in progress).
3. ORCID as an attribute authority (OAuth2-based setup, as part of Task 2).

The first step has been piloted and finalised. Federated access to ORCID is now in production and widely available to the community. Preparations to pilot the use of ORCID as an authentication and/or attribute authority provider have started and results are expected soon.

A summary of the pilot and links to further detail are provided in Table 5.4 below.

Task 3, Pilot 4	Access to Non-web Resources – ORCID
Focus	This pilot showcases the integration between federated identity and ORCID.org to obtain a persistent life-long identifier and use that identifier as part of the federated identity
Approach/AARC identified solution	To be able to use the ORCID API, some customisation of AARC's AAI solutions is needed. In a first step ORCID has become available as an eduGAIN SP.
Components piloted	In the **basic** setup a linking service will be introduced (developed in the VOPaaS project) and tested. In the **advanced** setup an SP proxy to aggregate attributes from institutions, ORCID and other sources will be introduced and tested.
Gain for end users/administrators	• Ability to reuse a single persistent identifier and link multiple accounts to this single identifier • Ability to identify a single/unique user no matter whether this user authenticates with account A or account B
Demo/video	• Demo production service (at ORCID.org) • Blog with further description
Detailed technical description	AARC Wiki
Documentation of components	See the SURFnet ORCID Wiki
Software source(s)	See the SURFnet ORCID Wiki
Lead	SURFnet
Community partners	NL and IT libraries and research communities
Status	In the first step the Task established a setup with ORCID as an SP. In a second step, ORCID will act as an attribute authority. For this (second) purpose, a user's institutional account needs to be linked to an ORCID account. An initial pilot setup was created and tested with the Dutch federation SURFconext. The work will continue by showcasing integrated ORCID attribute aggregation flows into VO attribute management platforms. This will take place during the second year of AARC.

Table 5.4: Task 3, Pilot 4 – Access to resources – ORCID

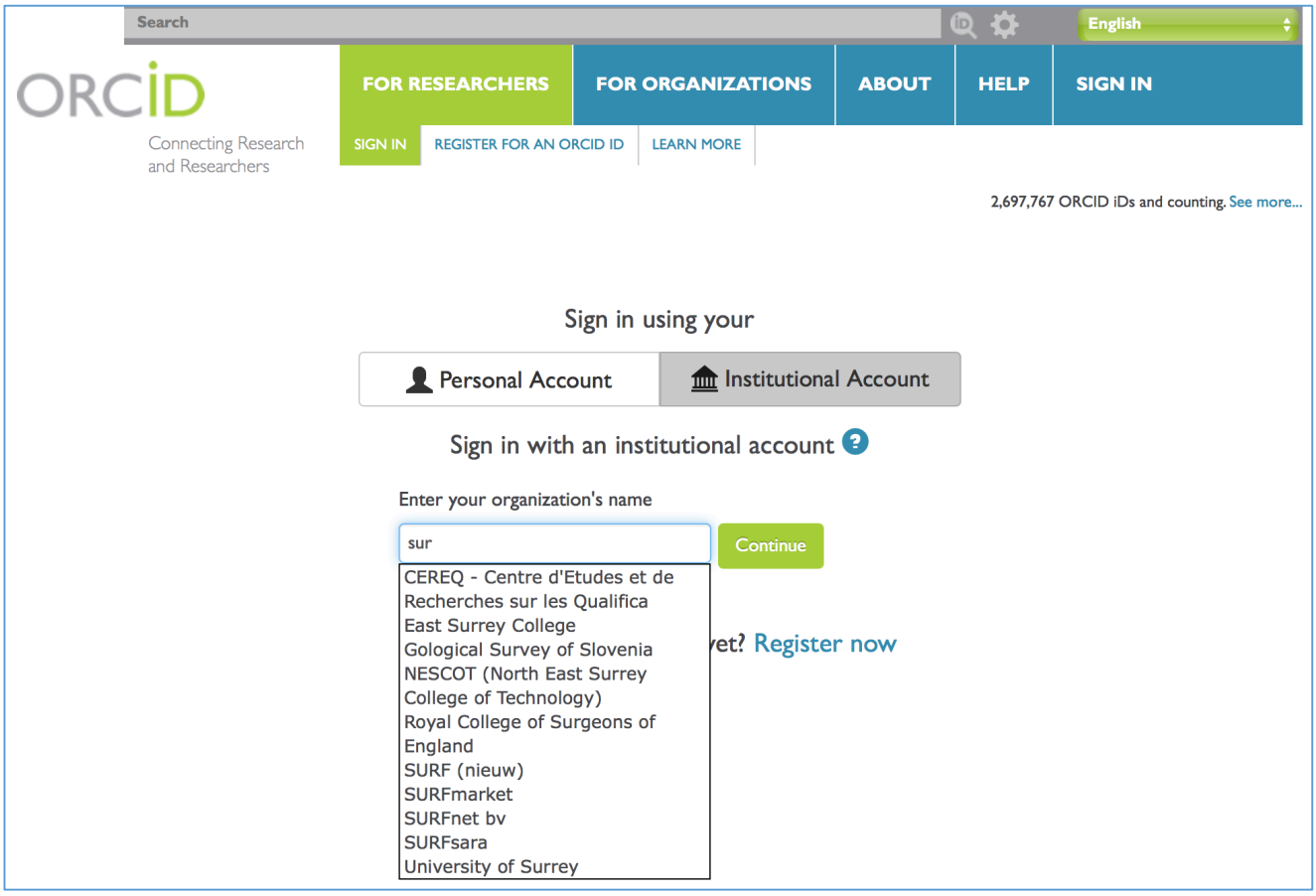

Figure 5.3: Screenshot of the ORCID SAML connection

5.3.5 Observations

Task 3 activities in the second year of AARC will focus on a comparison of different token translation services, testing of proposed setups with communities and adoption by communities.

6 Conclusions

Through its pilots, SA1 aims to demonstrate that:

- Existing authentication and authorisation infrastructures (AAIs) and authentication sources can be leveraged to enable (single sign-on (SSO)) access, with appropriate level of assurance, for any user, to shared resources offered by different e-infrastructure providers and communities.
- Authoritative decisions and user/group context can be based on distributed group managers and attribute providers.
- Access to non-web and commercial services can be enabled.

Having first set up a technical platform, top-level domain, DIY test identity provider, central repository and first-line support to facilitate the testing, deployment and piloting of services, SA1 has started – and, in certain cases, finalised – a number of pilots that, at the end of Year 1, mean the Activity is well on the way to achieving those aims.

Task 1 Guest Access has piloted three solutions for library use cases, all of which are close to finalisation:

- SAML/IP bridge, to allow access to restricted library resources whether or not the provider supports SAML.
- Walk-by users, to support authorised access to library resources for anyone who needs scientific information, including citizen scientists not affiliated with an institution.
- IdP/SP proxy for library consortia, to reduce the number of interactions between IdPs and SPs from a technical and trust point of view while preserving the privacy of users.

Together, these solutions will give users of library resources a smoother experience while accessing resources, irrespective of the authentication method that is supported. They also offer opportunities to reduce the administrative burden of library staff in relation to managing SAML connections and maintaining access to restricted library resources.

Task 2 Attribute Management focuses on establishing a framework for collaborative SSO scenarios, piloting solutions to facilitate and enable attribute management, attribute aggregation and attribute-based authorisation. Pilots are in progress testing components in the context of two infrastructures and communities:

- EGI e-infrastructure, investigating and piloting the usability of SAML-based AAI components to use externally managed attributes to provide and restrict access to cloud services.
- BBMRI-ERIC, establishing a fully fledged standardised AAI to enable access and authorisation to shared biomedical resources with appropriate level(s) of assurance.

In both pilots the IdP/SP proxy approach has been adopted to handle all complexity. The teams share ideas and interact often to make sure that a common and generic approach results from their work and that duplication of effort is prevented.

Task 3 Access to Resources focuses on improving access to non-web resources through token translation solutions, and on accessing third-party services. Four pilots are in progress, with preliminary results already available for three of them:

- CILogon, to test a combination of solutions to enable access to non-web, X.509-based resources with SAML-based credentials in an end-user-friendly way. NA3 has already started to develop sustainability and operation models for this service.
- LDAP-Façade, to provide access to non-web resources to non-grid users using existing AAIs, without needing to obtain user certificates. Finalised.
- Unity-IdM, to test a third potential solution for bridging SAML-based identities and attributes to non-web resources. This pilot is at the preparation stage.
- ORCID, to showcase the integration between federated identity and ORCID.org to obtain a persistent life-long identifier and use that identifier as part of the federated identity.

Through this work SA1 has identified interesting ideas for solutions, and also a number of challenges that need to be solved to be able to increase user friendliness and to bridge different research infrastructures and communities. Plans are in place to extend and build on the pilots in Year 2, including joint Task work on solutions for bridging towards social and e-governmental identities, additional token translation solutions and further integration with ORCID.

References

[~okeanos] https://okeanos.grnet.gr/home/

[AARCGit] https://github.com/AARCProject

[AARCPrivate] https://gitlab.pilots.aarc-project.eu

[AARCWiki] https://wiki.geant.org/display/AARC/AARC+Pilots

[BBMRI] http://www.bbmri-eric.eu/

[CILogon] https://cilogon.org

[CILogon-Models] *Sustainability models for the AARC CILogon-like TTS Pilot and RCauth.eu* https://wiki.geant.org/download/attachments/56918657/AARC-sustainability-models-for-RCauth-20160506.pdf?version=1&modificationDate=1462630136894&api=v2

[COmanage] http://www.internet2.edu/comanage

[DJRA1.1] *Deliverable DJRA1.1: Analysis of user community and service provider requirements* https://aarc-project.eu/wp-content/uploads/2015/10/AARC-DJRA1.1.pdf

[eduGAIN] http://www.edugain.org/

[eIDAS] http://www.mizs.gov.si/fileadmin/mizs.gov.si/pageuploads/Informacijska_druzba/eIDAS/DrugiDok/LOA_Guidance_vFinal.pdf

[ELIXIR] http://www.elixir-europe.org/

[EUDAT-B2ACCESS] https://www.eudat.eu/services/b2access

[EZproxy] https://www.oclc.org/ezproxy.en.html

[IGTF] https://www.igtf.net

[LDAPFacade] http://wiki.data.kit.edu/index.php/LDAP-Facade

[MJRA1.1] *Milestone MJRA1.1: Existing AAI and available technologies for federated access* https://aarc-project.eu/wp-content/uploads/2016/01/MJRA1.1-Existing-AAI-and-available-technologies.pdf

[MJRA1.2] *Milestone MJRA1.2: Design for Deploying Solutions for "Guest Identities"* https://aarc-project.eu/wp-content/uploads/2016/06/MJRA1.2-Design-for-Deploying-Solutions-for-Guest-Identities.pdf

[MJRA1.3] *Milestone MJRA1.3: Design for the integration of an Attribute Management Tool* https://aarc-project.eu/wp-content/uploads/2016/06/MJRA1.3-Design-for-the-integration-of-an-Attribute-Management-Tool.pdf

[MJRA1.4] *Milestone MJRA1.4: First Draft of the Blueprint Architecture* https://aarc-project.eu/wp-content/uploads/2016/08/MJRA1.4-First-Draft-of-the-Blueprint-Architecture.pdf

[MSA1.1] *Milestone MSA1.1: Specify the work to be undertaken in collaboration with JRA1 and NA3* https://aarc-project.eu/wp-content/uploads/2015/10/MSA1.1-v8FINAL.pdf

[NA3-WIKI-SOM] https://wiki.geant.org/x/5oc0Aw

[OAuth2] https://oauth.net/2/

[OCLC] http://www.oclc.org/

[OIDC]	http://openid.net/connect/
[OpenConext]	http://www.openconext.org
[ORCID]	http://orcid.org/
[Perun]	http://perun.cesnet.cz
[PilotPlatformVideo]	https://aarc-project.eu/aarc-pilot-platform-approaching-take-off/
[RCauth]	http://rcauth.eu
[REFEDS-R&S]	https://refeds.org/category/research-and-scholarship
[Shibboleth]	https://wiki.shibboleth.net/confluence/x/i4EEAQ
[SimpleSAMLphp]	https://simplesamlphp.org
[Sirtfi]	https://refeds.org/sirtfi
[Unity-IdM]	http://unity-idm.eu
[VOMS]	https://italiangrid.github.io/voms/
[VOPaaS]	https://wiki.geant.org/display/gn41sa5/Task+4+-+FaaS
[ZeroTier]	https://www.zerotier.com/index.shtml

Glossary

AA	Attribute Authority
AAI	Authentication and Authorisation Infrastructure
AARC	Authentication and Authorisation for Research and Collaboration
API	Application Programming Interface
AQ	Attribute Query
AuthZ	Authorisation
BBMRI	Biobanking and BioMolecular resources Research Infrastructure
BBMRI-ERIC	Biobanking and BioMolecular resources Research Infrastructure – European Research Infrastructure Consortium
CA	Certification Authority
CILogon	CILogon enables users to authenticate with their home organisation and obtain a certificate for secure access to Cyber Infrastructure (CI)
DIY	Do-It-Yourself
eduGAIN	International interfederation service interconnecting research and education identity federations
EGI	European Grid Infrastructure
eID	Electronic Identification
eIDAS	EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the European internal market
EPC	End Point Criterion
Git	A free and open source distributed version control system
GOCDB	Grid Operations Configuration Database, an EGI service
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IdP	Identity Provider in the context of SSO scenarios, such as supported by Shibboleth
IGTF	Interoperable Global Trust Federation – 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
IP	Internet Protocol
JRA1	Joint Research Activity 1 Architectures
KIT	Karlsruhe Institute of Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LIBER	Ligue des Bibliothèques Européennes de Recherche – Association of European Research Libraries
LoA	Level of Assurance – degree of certainty that the user has presented a credential that refers to that user's identity
M	Project Month
MZK	Moravská zemská knihovna v Brně – Moravian Library

NA3	Networking Activity 3 Policy Harmonisation
NREN	National Research and Education Network
OA4MP	OAuth for MyProxy provides an OAuth-compliant REST web interface to the MyProxy service for providing user certificates to science gateways
OAuth	OAuth is an open standard for authorisation
OCLC	Online Computer Library Centre
OIDC	OpenID Connect
ORCID	A not-for-profit organisation that provides a unique identifier for individuals to use with their name as they engage in research, scholarship, and innovation activities across disciplines, borders and time
Perun	A wide system providing user management and user-connected services to various types of facilities in various infrastructure sizes
PKI	Public Key Infrastructure
R&E	Research and Education
RCauth.eu	The white-label Research and Collaboration Authentication CA Service for Europe
REST	Representational State Transfer
SAML	Security Assertion Markup Language is an XML-based, open-standard data format for exchanging authentication and authorisation data between parties, in particular, between an identity provider and a service provider
SA1	Service Activity 1 Pilots
SFTP	SSH File Transfer Protocol
Sirtfi	Security Incident Response Trust Framework for Federated Identity
SP	Service Provider in the context of SSO scenarios, such as supported by Shibboleth
SSH	Secure Shell
SSO	Single Sign-On
TEIP	Transparent External Identity Proxy
TTS	Token Translation Service. RCauth.eu is a Token Translation Service that translates SAML to X509
VM	Virtual Machine
VO	Virtual Organisation – a dynamic set of individuals or institutions defined around a set of resource-sharing rules. Resource sharing is, necessarily, highly controlled, with resource providers and consumers defining clearly and carefully exactly what is shared, who is allowed to share, and the conditions under which sharing occurs
VOMS	Virtual Organisation Membership Service
VOPaaS	Virtual Organisation Platform as a Service
VPN	Virtual Private Network
X.509	Standard for a public key infrastructure to manage digital certificates
XML	Extensible Markup Language