Milestone MSA1.1 : Specify the work to be undertaken in collaboration with JRA1 and NA3

Milestone MSA1.1

Contractual Date:	31-08-2015
Actual Date:	**Error! Reference source not found.**2015
Grant Agreement No.:	653965
Work Package:	SA1
Task Item:	SA1.0
Lead Partner:	SURFnet.nl
Document Code:	MSA1.1
Authors:	Mario Reale (GARR), Peter Solagna (EGI), Maciej Brzeźniak (PSNC), Michał Jankowski (PSNC), Niels van Dijk (SURFnet), Paul 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, produced by the Pilot Work Package (SA1) Task 0 "Specify the work to be undertaken in collaboration with JRA1 and NA3", describes the dependencies of the AARC pilots with the "Architectures for an integrated and interoperable AAI" (JRA1) and the "Policy and Best Practices Harmonisation" (SA1) work packages. The plans presented in this document build on the results of first discussions with all stakeholders within AARC and upon the outcomes of previous activities such as the TERENA AAA Study [AAA Study] and the FIM4R workshop series {FIM4R]. Based on these plans a test-bed was created, a workflow for the running of pilots with research communities was drawn and components for pre-pilots have been identified.

Table of Contents

Table of Figures

Executive Summary

This document provides an overview of the first steps and ideas to define and execute AAI pilots together with representatives of several research communities (some of which are represented by the AARC partners).

Chapter two provides a brief description of the dependencies between the pilot work and the outcomes of JRA1 and NA3. Chapter 3 gives a description of preparatory work performed to kick-start the pilots process. This work includes the creation of a test-bed and the laying out of a workflow for running pilots with research communities. Chapter 4 presents topics and challenges to be addressed in the three tasks: TSA1.1 guest access, TSA1.2 attribute management and access to resources TSA1.3. In chapter 5 we further defined the KPIs of this activity.

1 Introduction

This activity aims at facilitating researchers by providing the access management tools and framework to support collaborative research in a distributed environment. To this end, in SA1 we will demonstrate through (pre-) production pilots that:

- Existing AAIs and authentication sources can be leveraged to enable (SSO) access with appropriate level of assurance for researchers (in academia and non-academia) to access shared resources offered by different e-Infrastructure providers and communities. (task TSA1.1)
- Authoritative decisions can be based on attributes from external attribute authorities. (TSA1.2)
- Access to non-web and commercial e-infrastructure services can be enabled. This requires the bridging of SAML NREN world and token/certificate based e-infrastructure provider/communities world. (TSA1.3)

The approach consists of selecting existing components of production AAI as identified by JRA1 and to integrate these components according to a common architecture that will be drafted in JRA1 as well. To this purpose we will establish a stable pilot environment where the proposed approach defined in JRA1 and NA3 will be tried and assessed by representatives of the research communities affiliated with the project (and beyond).

2 Dependencies of SA1 and NA3

The pilot work in SA1 will be guided by the requirements analysis [DJRA1.1 Analysis of user-community requirements] and the blue print architecture drafted in JRA1 (the first internal draft is expected in early November 2015), and by best practices and recommendations identified in NA3. This clearly creates significant dependencies on the first outcomes of JRA1 and NA3, which is clearly a risk for this work package. To mitigate this risk, and inline with the AARC technical annex to involve the user communities to scope the pilots, SA1 has taken the following approach:

1) Start by creating a test-bed environment for the pilots;
2) draft the initial user-community driven use cases representing the broad spectrum of requirements;
3) make a provisional selection of tools that will likely be included in the pilots immediately after the kick-off of the project and start to pilot them;
4) Feed the initial results of these pilots back to JRA1 and NA3;
5) Implement the first outputs of JRA1 and NA3 as soon as they become available

By creating a feedback loop to the other activities in AARC, we can provide useful input based on our preliminary hands-on experience with the selected tools.
Efficient communication is one of the key success factors within this project. The team has therefore identified ways to establish consensus and to create a pilot environment that reflects the needs of the intended users. The figure below shows the flow for the identification of user requirements and the interaction with research communities. This work package will actively interact with the AARC target communities, by sending out questionnaires, reviewing existing reports and sharing information and outputs to verify that the community needs are met.

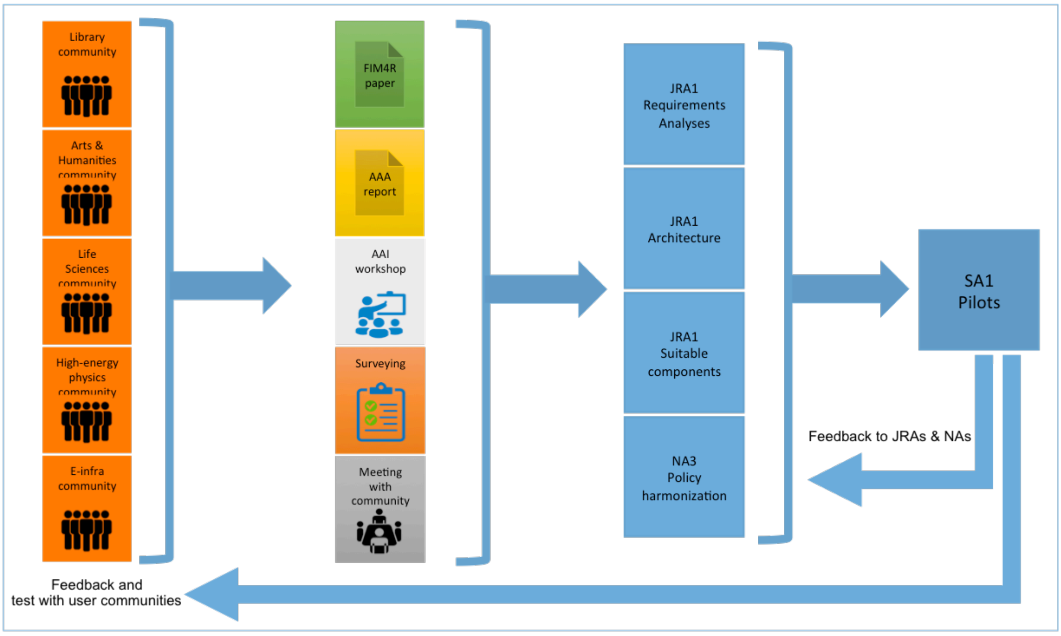

Figure 1: From community requirements to pilots

3 Preparatory work

To test the proposed solutions and architecture we need a test-bed that reflects a real life deployment scenario and that is stable enough to give a good impression of how the different components can be used in connection with each other.

We propose to create two environments:

- An environment for development and experimentation including code to glue components together. For this purpose, everyone can use self-owned or hosted environments on GRNET’s ~okeanos “preview” environment, which is available via eduGAIN.
- A formal and stable environment(s) for the pilots with our target audience. This virtual environment is based on the ~okeanos production environment. Instantiation and distribution of accounts will be handled by the ask leads.

For the adoption of AAI tools by research communities, a simple and straightforward software deployment and integration approach is regarded as an essential and key success factor. To make sure the products are maintainable and secure, we will define requirements on how the tools are installed, maintained, monitored and how issues with the software are handled.
We will perform peer reviews, create manuals, standard procedures and use solutions like Jenkins, Puppet, Chef or Ansible to support easy deployment of the proposed components. As soon as the user communities have confirmed that the proposed setup fulfils their functional requirements, the overall security of the connected components needs to be assessed.

Although the selection of components and the drafting of the blueprint architecture is defined as an activity of JRA1, we will start exploring a number of “want-to-have” solutions to enable guest access, attribute management and non-web single sign-on. This pre-selection of solutions will be done in close collaboration with the JRA1 team. In addition, we will need components like test Identity Providers (IdPs), an attribute aggregation hub and test Service Providers (SPs) to be able to create a realistic pilot environment as soon as possible.

To put the pilots with our target communities on the right lines, pilots are being coordinated according to a standard workflow and a formal pilot enrolment form (see appendix 3). The pilot enrolment form ensures that both AARC partners and communities follow the same approach, define clear goals and commitment and a pre-defined definition of done (DoD). The execution of the pilots with representatives of the research communities will consist of the steps depicted in the figure below.

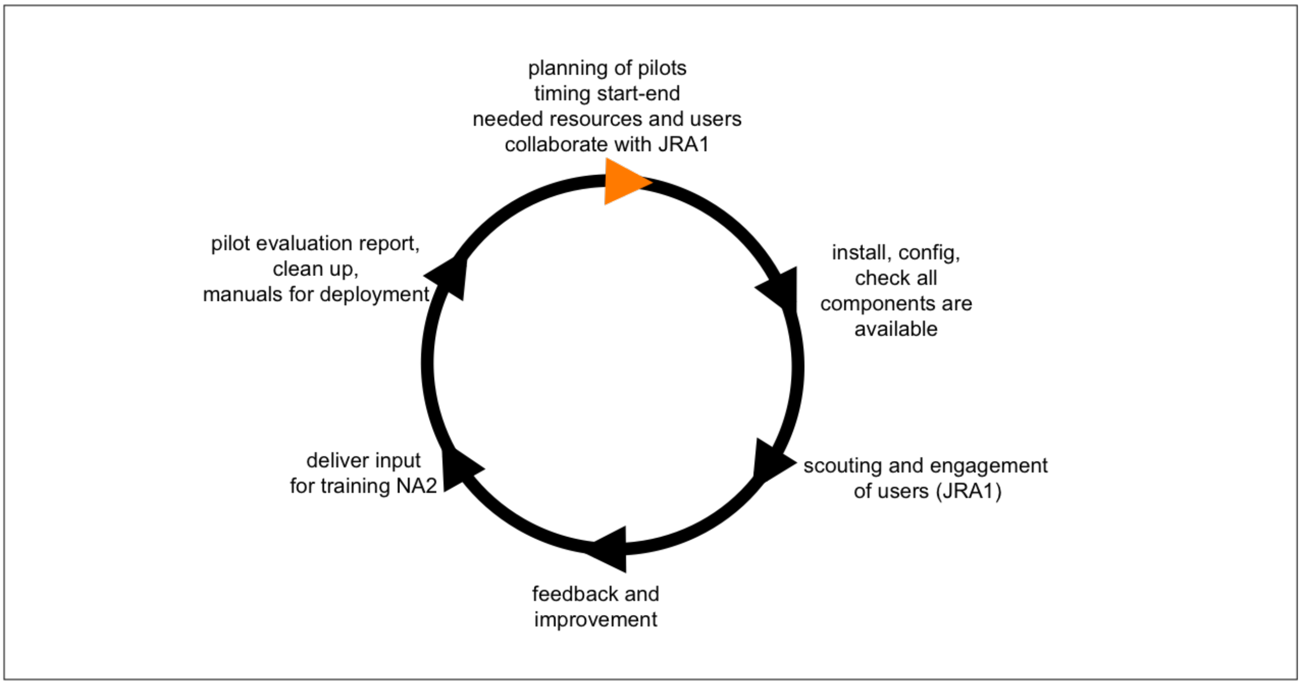

Figure 2: Pilots workflow

Given the many dependencies of other AARC activities, the aim to run several pilots per task (e.g. guest access solutions) and inter related tasks (providing guest access, manage authoritative attributes and provide access to non-web resources to proof the integration) a well-tuned timing for the initiation of pilots and the delivery or results is of major importance. The delivery of pilot tasks deliverables and milestones in SA1 are indicated in figure 3.

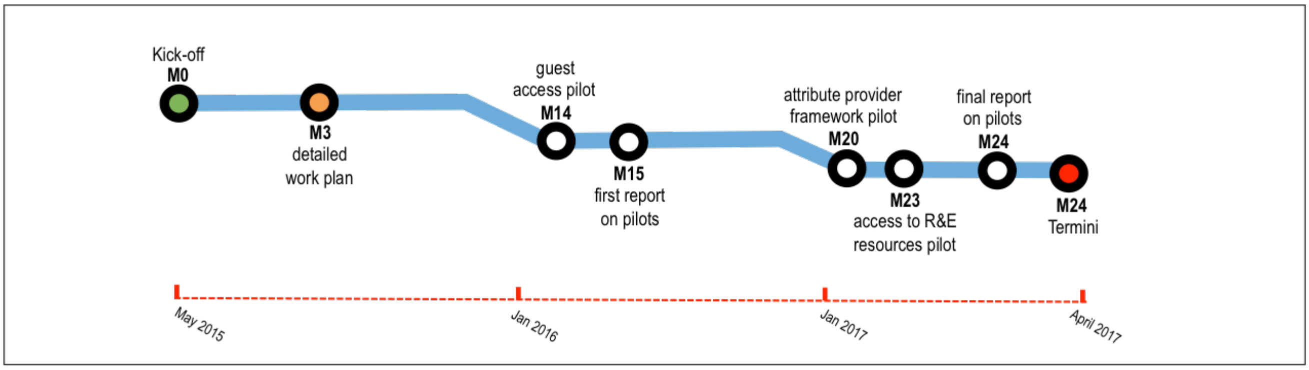

Figure 3: Planning of milestones and deliverables in SA1

4 Task specific activities

4.1 Guest Access (TSA1.1)

This task deals with the pilot activities to be set up for AARC in the domain of guest Identities. It will mostly liaise with JRA1 and NA3 work packaged in order to effectively demonstrate the validity of the selected solutions and architecture as designed in JRA1 and the best practices and recommendations identified in NA3.

The main idea behind the work plan for this task is to demonstrate with actual use cases, involving end users from several communities, the components that are available to enrol guest users that need to be able to participate in research collaborations as first class citizens. Dealing with Guest Identities is a challenge in the world of identity federations (particularly for resource providers) in what concerns the trustworthiness of the procedures follow to validate an identity (Level of Assurance, known as LoA). While dealing with guest identities, components and procedures needed are for example: LoA enhancement mechanisms for non federated IDs, Guest IdPs, Cloud based IdPs, eGov IDs, Social to SAML bridges and SAML to SAML bridges.

Task TSA1.1 identified 3 main pillars for its activities, which are being coordinated and agreed upon with JRA1, NA3 and the AARC project overall. These 3 pillars are:

- Designing and pilot a strategy to include new non academic IDs among the potential beneficiaries of services, bridging federations towards social and governmental IDs and other identity sources

- Increase the size of the set of academic federated identities by extending federations (e.g. new IdPs, Catch-all Federation, Cloud IdP approaches)

- Modify access to library services by migrating from IP-address based authentication, which is currently common practice, to federated authentication

4.2 Attribute Management (TSA1.2)

This task deals with the piloting of solutions to manage attributes on a central and cross application level. An integrated framework of identity providers, attribute and group providers, attribute aggregation platforms and shared e-infrastructure services that are able to consume attributes will be demonstrated and tested.

Based on the feedback from the requirement gathering process in JRA1 we already identified some of the use cases for the attribute management:

- The need for community managed authorization mechanisms in shared research services
- The integration and aggregation of attributes provided by the IdP with community managed attributes

- The need to attach information about the authentication vetting of users

As requirements gathering activities are currently progressing and the definition of the blueprint has started, more use cases will be defined and may possibly extend the pilots with new capabilities.

The work plan for the first year consists of the deployment of an initial attribute aggregation platform and one or more community-based attribute authorities.

4.3 Access to resources (TSA1.3)

This task aims at improving access to relevant research and education non-web resources located outside the home organization of the user. The main improvement is making use of existing AAI that provide user credentials and authorisation attributes instead of local user management. While many implementations exist already for web portals, the technology for non-web scenarios is still immature.

A number of pilots are going to be setup in order to investigate emerging non-web SSO solutions and workarounds. The selection of software to be piloted is going to be discussed with JRA1 in order to focus on tools that fit with the requirements of the research community and the blueprint architecture (JRA1.3 and JRA1.4). Also the requirements gathered by JRA1.1 will be used as input material for the assessment of technologies used in the pilots. Finally, the experience gathered with the deployment, integration and application of the available solutions by stakeholders in the community will be used as feedback for the final shaping of the blueprint architecture in JRA1 and best practices recommendations in NA3.

Compatibility between the technologies piloted within this task and technologies used for collecting attributes within task SA1.2 will be checked. Attribute requirements for non-web SSO, authorisation and provisioning will be investigated and defined. Usage of user credentials and attributes coming from different AAIs, including guest IdPs proposed by SA1.1 will be analysed as well.

In the three SA1 tasks described above we carefully started some pre-pilot experimentation with components that will likely be included in the final architecture. With this approach we avoid the loss of time during the initial phase of the project while at the same time gain some useful first insights and experience with potentially eligible solutions.

5 Key performance indicators for SA1

For the definition of KPIs in SA1 we roughly applied the following division:

- In year 1 we focus on “proof of technologies”. This means that single solutions will be deployed and tested one by one to assess their suitability from a functional point of view, their maturity and their ability to integrate in the blue print architecture.
- In year 2 we will gradually shift the focus to the “proof of integration” of components assessed in the first year.

The main KPIs of activities in SA1 are summarised below:

- A research service is available for users from at least three different research communities (year 2).
- One pilot to test the feasibility to authenticate with a social ID and/or eGov ID and to bridge this authentication method with a SAML based service provider (year 2).
- Authorisation can be managed in a centralized cross community way. At least 2 different attribute authority sources and 1 attribute aggregation platform will be assessed and piloted (year 1 and year 2).
- SAML based authentication can be applied successfully in 2 different non-web based services. At least 2 different token translation services will be assessed and piloted (year 1 and year 2).
- At least one service provider by a commercial provider was successfully added to the pilot AARC platform and able to consume SAML based attributes for authentication and authorization (year2).

6 Conclusions

This document describes the approached to the AARC pilots. Although the work in SA1 will be guided by the outcomes of other AARC activities, which were not yet available at the fifth month of the AARC project yet, a number of preparatory steps could be undertaken to enable a quick start for this activity. All partners in SA1 now have a clear overview of the goals to be achieved and the kind of components that need to be assessed and tested, both on itself and in connection to each other.
In the months to come, more detailed requirements and a blue print architecture will become available from the JRA1 activity as well as guidelines for the harmonisation of policies from the NA3 activity. This detailed input will further guide the activities for SA1 which may require some adjustment based on these outcomes.

7 Appendix 1: Resources available

Available resources include:

Task name	Partners (PMs)
SA1.0 Work package leadership Lead: SURFnet	SURFnet (5)
SA1.1 Guest identities Lead: GARR	GARR(6), SURFnet(6), GRNET(3), DAASI(2), MZK(1), KIT(2), NIKHEF(4), STFC(0)
SA1.2 Attribute Management Lead: EGI	EGI(7), SURFnet(6), NIKHEF(4), CESNET(4), DAASI(3), GRNET(3)
SA1.3 Access to resources Lead: PSNC	PSNC(12), NIKHEF(2), SURFnet (6), CESNET(4), KIT(4), EGI (4), CSC(4), DAASI (2)

8 Appendix 2: List of deliverables and milestones for SA1

8.1 List of deliverables

Deliverable number + name	Lead participant	Type	Dissemination level	Delivery date
DSA1.1 Pilots to support guest users solutions	GARR	DEM	PU	PM15
DSA1.2 First report on the Pilots deployed by SA1	SURFnet	R	PU	PM15
DSA1.3 Final pilot on attribute provider framework	EGI	DEM	PU	PM20
DSA1.4 Pilot to improve access to R&E relevant resources	PSNC	DEM	PU	PM23

DEM=Demo, R=Report, PU=Public

8.2 List of milestones

Milestone number + name	Description	Delivery date	Means of verification
MSA1.1 Specify the work to be undertaken in collaboration with JRA1 and NA3	Detailed workplan	M3	Online document
MSA1.2 Report on the user testing and future recommendations	Brief report about the tests done on the pilots	PM24	Online document

9 Appendix 3: Pilot enrolment template

Contact data of AARC participants involved

Please provide contact details for AARC participants involved in this pilot

	Name(s)
AARC SA1 Pilot name:	
AARC SA1 Pilot subtask:	
Technical contact(s) in AARC:	

Contact data of Parties involved

Please provide contact details for additional organisations involved in this pilot

Organisation Name	Person names	Role in pilot

Pilot description

- Please describe high-level goal of pilot, provide overview of activities and participants. Please describe how commitment from various partners is warranted.

Pilot goals

- Please describe goals of pilot, including activities and participants. Describe when the pilot is done and how to measure the success of it, in a SMART way.

Pilot resources

- Please describe required resources for the pilot, including VMs, DNS and certificates

Contact data

Date	Activity	Owner	Minuits
January 1, 2015	Kickoff meeting		

Documents:

(attach documents to this page to get them listed)

10 References

[DJRA1.1 Analysis of user- community requirements] Kanellopoulos C., Liampotis N., van Dijk N., Solagna P. https://aarc-project.eu/documents/deliverables/

11 Glossary

AAI	Authentication and Authorisation Infrastructure
DoD	Definition of Done
eduGAIN	International interfederation service interconnecting research and education identity federations
IdP	Identity Provider
LoA	Level of Assurance – degree of certainty that the user has presented a credential that refers to that user's identity
SAML	Security Assertion Markup Language
SP	Service Provider