Minutes AARC Kick-Off Meeting
2-3 June 2015, Amsterdam

Table of Contents

1. Welcome from the EC

AARC participants gathered for a two-days meeting in Amsterdam to plan the work for AARC. All work package leaders presented the respective objectives and brainstormed on how their plans and on how to achieve the objectives.

Participants were welcomed by **Jean-Luc Dorrel (EC)** who provided a overview on the evolution of federated access and how AARC fits in the landscape. Jean-Luc acknowledged that federated access and eduroam have gronw a lot. Iit would be desirable if in the near future eduroam were available at the EC premises for instance and if EC portals were federated and available via eduGAIN. This however brings new challenges concerning the business model and the availability of these services outside the R&E community.

There is a lot of interest in AARC for different reasons. AARC represents different communities, is representing all sites of the identity ecosystem (e-Science, supercomputers, Librarians, e-infrastructures and networking communities) and as such can play an important role in addressing the research community requirements as well as the libraries and to look at scalable policy models to share services.

Jean-Luc noted, looking at the methodology, that AARC should include clear KPIs (Key performance indicators), quantify them and add targets for each year of the project. There is a lot of expectation on AARC, but on the other hand it is only a two-year project, therefore it is even more important for this project to demonstrate its achievements.

ACTION: Define targets for the first year and review the KPIs (some of them were already indicated in the technical annex).

2. Overview on the AARC Project and its Management

Licia Florio, the project coordinator (NA1), gave an introduction on AARC, its objectives and how AARC positions itself with regards to other AAI funded initiatives. She noted that the main goal of AARC is to deliver an integrated AAI built on federated access, delivered by gluing existing components.

AARC has an extensive training and outreach package which will leverage on existing and national efforts. AARC will take advantage of the consortium to address wide scale use-cases and training that are very common in the research collaboration.

Licia also noted that AARC is a temporary project as such there is no aspiration to become yet another e-infrastructure. All AARC results should be moved into productions and operated by existing e-Infrastructures; eduGAIN being one of the most obvious candidate.

Licia also reported on some administrative matters, namely:

- Website: https://aarc-project.eu / Blog. NA1 will manage this; WP leaders can manage their own space. The idea however is to use the website a the place to store finalized documents. The day-to-day work should take place on the wiki.
- Wikis, there is a private space and a public space
    - https://wiki.geant.org/display/AARC/AARC+Private+Space
    - Public Wiki: https://wiki.geant.org/display/AARC+Home

Currently the mailing lists are operated under the former TERENA domain, but a migration to a better system and to the new domain (geant.org) is expected by the end of 2015. More information will be provided at due time.

Licia also covered some internal procedures, such as the quarterly reports, to be compiled by the WP leaders on the wiki to keep an overview on the progresses. For more information please refer to the slides on line (https://aarc-project.eu/aarc-kick-off/).

There was a request for a shared calendar to show when each team meet.
ACTION: Licia to investigate a way to support this.

3. Training and Outreach (NA2), Alessandra Scicchitano

Alessandra gave an overview on NA2 and its goals. Its primary goal is to promote federated access, lower entry barriers for organisations to participate in Identity-Federations. NA2 should define the communities to targets, define their requirements, and address them.

In the initial phase NA2 will focus on revisiting the requirements for training and in developing general purpose material to promote federated access (most of this work consists in re-packaging and updating existing material). Further work will include documenting and disseminating best practices in enabling SAML support in applications, developing a training package for targeted services as well as in promoting tools to facilitate the creation of IdPs in small institutions with limited manpower or limited know-how.

This WP has been broken down in 4 tasks:
- T0 management
- T1 – learning analysis
- T2 – Outreach and dissemination
- T3 – Training for Resource and Service Providers
- T4 – Training for ID-Providers

During the break out session it was agreed to focus on the following aspects:
- Reduce the usage of IP-based authN (in the libraries) or at least understand what are the show-stoppers in this area
- Produce a value proposition for federated access for decision makers

3

- Define a package to motive institutions and research collaboration to operate an IdPs
- Enable federated access for targeted SPs

Q1: What are your selection criteria to select communities
A: two-dimensional: we will look at the existing requirements, although not all of them have been spelled out. We will start by addressing the communities in AARC, i.e. libraries and other ESFRI projects.

Q2: Scaling up the training to EU-dimension will be fundamental, you are creating good mechanisms to for this?
A: The plan is to tailor and test the training within an initial group and to make that training available for others. Most of the training should be available on line.

Q3: for many SPs there is a business issue and accountability. Have you considered not only addressing the technical aspect but to also look at a clear business case or value proposition?
A: we will consider this.

4. Policy and Best Practices (NA3), David Groep

David gave an overview about NA3. The goal of this activity is to 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.
There are four main output expected by this activity:

- T1: 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). This work should link with results coming from other AARC WPs as well as to look at external player, such as eIDAS (the EU reregulation approved last year to offer a legal framework for cross national ID in Public Administration), STORK, REFEDS, IGTF etc.
  This work will be led by e-Infrastructure needs and use-cases. My M7 this task will have a collection of existing requirements (M7) which will be shared with the rest of the project and the relevant communities.
  The full framework based on engagement through existing forae and links (by M23
- T2: identify a distributed approach to handling security incidents in a federated environment. Some of work has already started with Sirfi. We will continue to use sirtifi as the main discussion forum and use AARC funding to support the work of some key people.
- T3: specify scalable policy negotiation mechanisms between identity providers, attribute providers and service providers to facilitate resource providers;
- T4: investigate terms of usage for delivering commercial services. This will result in a legally sounded workflow for processing data.

During the break out session that followed it was agreed that eIDAS is certainly something to monitor but that there are many challenges with this frameworks; one of the biggest being the

heterogeneous uptake among member states. The usefulness of eIDAS for guest user appears at this point very limited.

A further aspect to look relates to the usage of persistent identifiers. It is envisaged that there will be different sources of Identifiers and that every SP/community will have to manage local identifiers, so ways to link them are needed. Due to the duration of AARC and the type of use-cases this may not be in scope.

5. Architecture Goals and Plans - Christos Kanellopoulos

Christos presented the goal of this WP, that is to research on technologies and deliver the design for the global interoperable AAI. Christos noted that eduGAIN and the federations are the starting point. The WPL will also at ongoing work such as Elixir AAI Task Force, EUDAT work on AAI, STORK and

The main areas of work are:

- Task 1: Requirements analysis. The requirements will be derived from the existing FIM4R document, REFEDS, ESFRI project and AAA Study coordinated by TERENA.
- Task 2: Blueprint architectures, Christos noted that based on a preliminary discussion with the team they agreed to push back the first draft version of the architecture at M5 .This should facilitate feedback from the community and should allow some work in the pilots to start sooner.
- Task 3: Models for supporting guest Identities and alternative methods of Identification (Jens).
- Task 4: Models for implementing attribute providers and token translation services (Andrea). Some aspect to look at relate to: confidentiality, privacy and discovery in eduGAIN which may have in impact on security and user experience.
    - Q: What is the plan concerning token translation services?
      A: token translation normally happens close to a service that implement them. This was a clear requirement in the call for proposals; we are not looking at creating a new token translation services, we should be looking at a model to implement when we want to translate credential between SAML and other technologies. A lot has been already done in this area; we should start by assessing what we have.

The trend seems to be that each community is now creating a platform , or better SP proxies, to get Identities from different sources, add support for group management and for unique identifier. There should a be a way to link identities from of these proxies to another.

One of the use-case to look at is how to enable a service in an e-infrastructure to access and consume additional information/attributes a user has from being a member of any VO (that being ELIXIR, EUDAT etc). Jens noted that EUDAT has designed an architecture for this.
There was a lot of discussion around this and how
ACTION: Look at the work EUDAT has done to consume VO membership info.

A second use-case mentioned was how to enrich social media identities and how to transfer 'reputation' among SPs in different e-infrastructures. This will be worked out in the task 3.

ACTION: Jens to share a previous deliverable on building level of trust.

6. Pilots (SA1) – Paul van Dijk

Paul provided an overview on the Pilots WP. The pilots are intended to demonstrate that the solutions identified and proposed by JRA1 and NA3 are (i) effectively addressing the requirements of the communities and (ii) that they can be deployed.

The WP foresees the following pilots:

- T1: Pilot solutions for guest users – the aim is to support those use-cases already identified in the FIM4R paper, the AAA Study and the libraries where walk-in users (without federated credentials) are an important factor. The pilots will showcase viable solution whether commercially available or NRENs-built. Clearly the LoA aspect for credentials managed via these IdPs is an important aspect and will be considered.

- T2: Pilots of an attribute management framework - There consensus that communities should manage their own attributes rather than asking IdPs to manage and release them. A lot of work has been done in this area; this led to different tools:
  - VOMS
  - HEXAA
  - UNITY
  - PERUN
  - REMS
  - COmanage

  A comparison among these tool was done as part the Hn3plus research activity on Identity and Trust; the summary is available online:

  https://docs.google.com/spreadsheets/d/1SZGw3Nl9OOTToiuHibv3b0zKteU-xlaMj1QNm225J78/edit#gid=0

  EGI, as leading partner for this task has done some preliminary work:
  https://wiki.egi.eu/wiki/AAI_pilot

- T3: Pilot AAI for accessing non-web resources – The use-case are known, namely access to sync & Share cloud services (e.g. based on Seafile, OwnCloud..), access to storage services through SSH, access to Virtual Machines, etc. Some tools already developed by AARC partners were presented: such as:
  - the LDAP-Façade (developed by KIT) Deployable like any other SAML-based service provider;
  - CILogon ECP (developed by CTSC) Easily integrated with portals, see for instance Globus. David Groep noted that the CA used by the new TCS service would allow to build a service similar to CILogon.
  - Moonshot some of the deployment taking place in the GN4 project.

6

In response to the questions on where the business model with services should be tested, Paul answered that the masterplan about the sustainability models should be in the NA3.

This WP will liaise also with the VO-PaaS work that is being carried out in the GN4 project by Niels Van Dijk, who gave an overview on this work. The VO-PaaS team gathered requirements from many VOs: FIM4R paper, UMBRELLA, CLASSe, DARIAH, CERN, CLARIN, Virtual Campus Hub, GEANT AuthZ Management System ,ELIXIR. Some of the services they intent to offer are Vo-specific attribute management, Vo specific group management and A proxy for aggregating data from core services. Niels noted that it would be important for the VO-PaaS and the AARC Pilots team to closely collaborate.

7. Summary of the meeting and actions

The main actions are reported below:

Action	Assigned to	Description	Status	Comments
06-2015-01	NA1(LF)	To finalise the process to appoint members for the AARC board	CLOSED	Board was appointed on 12-07-2015
06-2015-02	WP leaders	To update their WP wiki page	ONGOING	
06-2015-03	NA1 Licia	To work with WP leaders to review AARC KPIs (Sept)	ONGOING	
06-2015-04	NA1 Licia	To work with WP leaders to define AARC goals for Y1 (Sept)	ONGOING	
06-2015-05	NA1 Licia	To provide a calendar to show meetings of the various tasks	Not Started	
06-2015-06	NA1 Licia	To agree on a date and venue for an AARC meeting in the fall	Started	The original proposal to co-locate the meeting with the EGI User conference will not be pursued.
06-2015-07	JRA1 – Christos	To gather clear use-cases, and prioritize them. Being pragmatic is key for being successful	Started	
06-2015-08	JRA1	To look at the work EUDAT has done to consume VO membership info.		

06-2015-09	Jens	To share a previous deliverable on building level of trust		
06-2015-10	Niels Van Dijk	To share deliverable to the WOT4LoA		
06-2015-11	NA3 - David Groep	To look into sustainable models for guest IdPs (i.e. one per project/VO/per e-infra?)		