Authentication and Authorisation for Research and Collaboration

Authentication and Authorisation for Research and Collaboration

Where are we at.

Alessandra Scicchitano
NA2 WP Leader, GEANT

Taipei Taiwan
3 March 2016

AARC – Authentication and Authorisation for Research and Collaboration

- Started on 1 May, 2015
- Two-year EC-funded project
- 20 partners
  - NRENs, e-Infrastructure providers and Libraries as equal partners
- About 3M euro budget
- https://aarc-project.eu/

- Working now on the proposal for AARC2

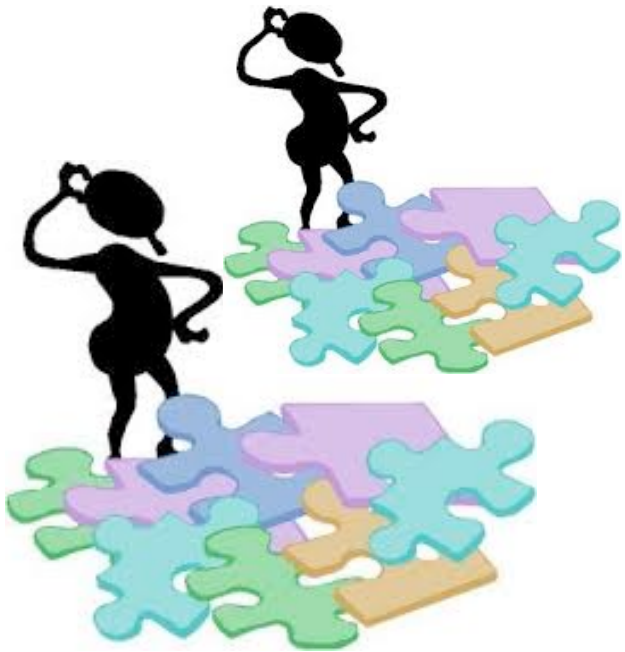
And where is this coming from????

- The growth of demand for federated access
- Many use cases for ID Feds
- Various existing AAIs

Nice! BUT…

It would be nicer if there was also compatibility & interoperability

Common challenges



- Attribute aggregation
- User friendliness
- Credential translation
- Attribute release
- Levels of Assurance
- Homeless users
- Bridging Communities
- Non-web-browser

AARC addresses these challenges of interoperability and functional gaps.

AARC - Objectives

Improve adoption of federated access

Pilot components to integrate existing AAIs

Making identities 'consumable' by different e-Infrastructures to access different services

Define policy frameworks and pilot them

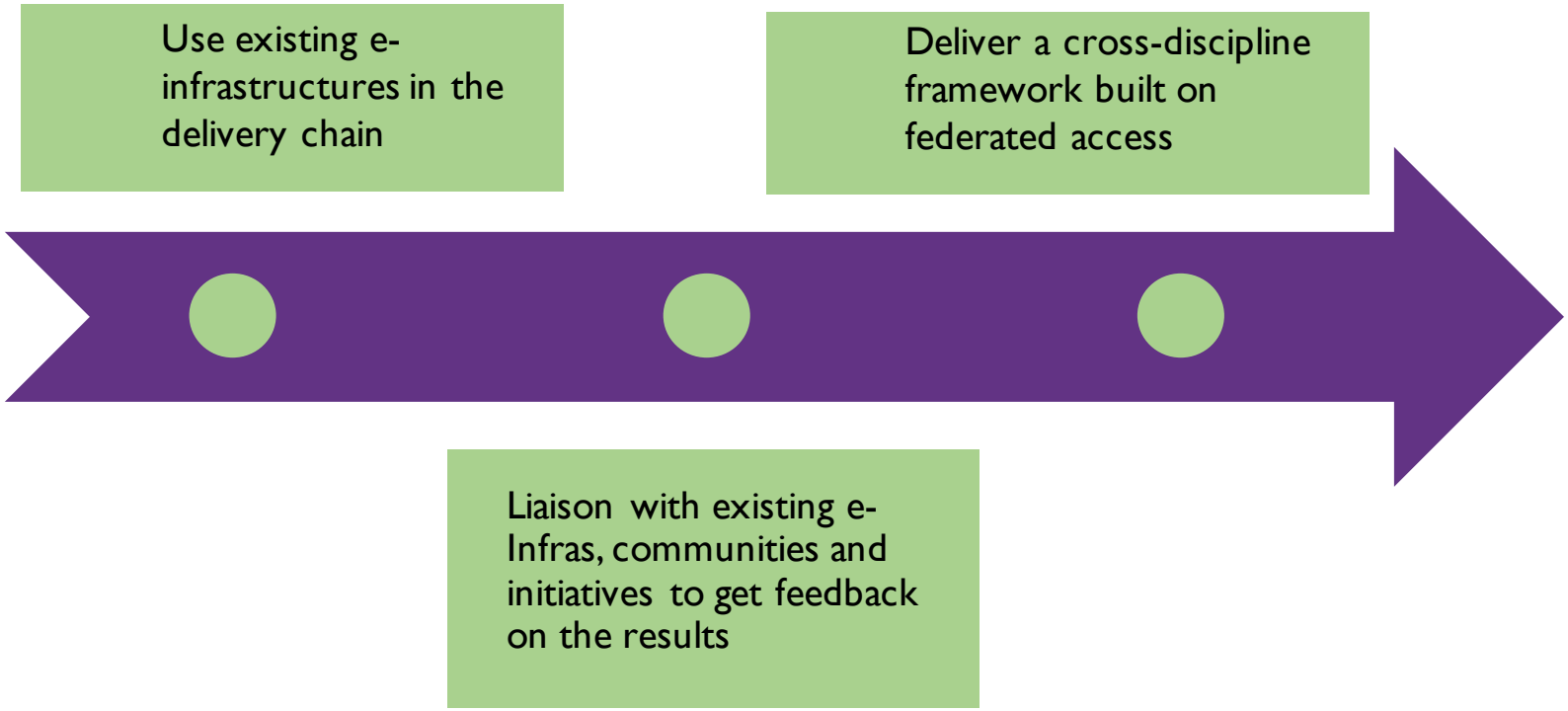
Develop Training packages

AARC - Workplan

- OUTREACH and TRAINING
  - To lower entry barriers for organisations to join national federations
  - To improve penetration of federated access

- TECHNICAL and POLICY Work
  - To develop an integrated AAI built on production services (i.e. eduGAIN)
  - To define an incident response framework to work in a federated context
  - To agree on a LoA baseline for the R&E community
  - To pilot new components and best practices guidelines in existing production services

Approach


Use existing e-infrastructures in the delivery chain
Deliver a cross-discipline framework built on federated access
Liaison with existing e-Infras, communities and initiatives to get feedback on the results

Almost a year has passed…

…and here is where we stand now.

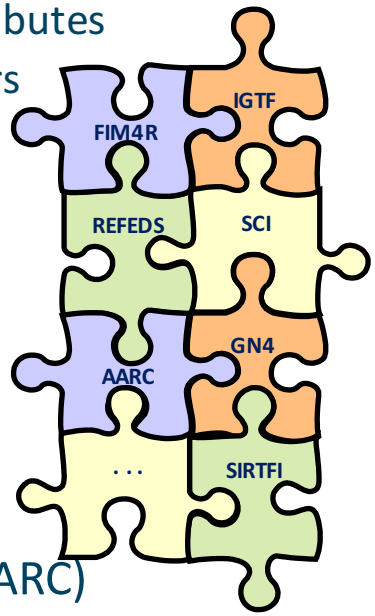
Training and Outreach

Training and Outreach

- Document describing the approach to the training - MNA2.1 Guideline document for AARC training materials
  - https://aarc-project.eu/documents/milestones/
- Report on the identified target groups for training and their requirements
  - https://aarc-project.eu/wp-content/uploads/2015/04/AARC-DNA2.1.pdf
- First two online modules: Federation101 and SP training material
  - https://aarc-project.eu/documents/training-modules/
- First two trainings based on the modules about to be delivered

Policy and Best Practices Harmonisation

- The Policy Puzzle: Many groups and (proposed) policies, but leaving many open issues
- AARC is tackling a sub-set of these
  - "Levels of Assurance" – a minimally-useful level and a differentiated set, for ID and attributes
  - "Incident Response" – encouraging 'expression' of engagement by (federation) partners and a common understanding https://wiki.refeds.org/display/GROUPS/SIRTFI
  - "Sustainability models and Guest IdPs"– how can a service be offered in the long run?
  - "Scalable policy negotiation" – beyond bilateral discussion (and more IGTF style ?)
  - "Protection of (accounting) data privacy" – aggregation of PI-like data in collaborative infrastructures



- Strategy is to support and extend established and emergent groups so as to leverage their support base (and 'multiply' the effect of policy investments from AARC)

Key results that have already been adopted and completed

- consensus '**baseline authentication assurance profile**' for many low-risk research cases* based on depth-interviews with the major research communities and e-Infra's in Europe ...
  - Accounts belong to a known individual (i.e. no shared accounts)
  - Persistent identifiers (i.e. are not re-assigned)
  - Documented identity vetting (not necessarily F2F)
  - Password authN (with some good practices)
  - Departing user's account closes/ePA changes promptly
  - Self-assessment (supported with specific guidelines)

  pushed to a REFEDS task force to evolve into **globally implementable guidelines**
- **Sirtfi** – security incident response trust framework for federated identity
  - defines **basic security incident response** capabilities to which organizations can **self-assert compliance**
  - based on SCI grouping of capabilities

  endorsed by REFEDS to stimulate adoption – but framework is general for SPs and communities
- Data protection in exchange of (accounting) data between infrastructures: **regulation survey** done

** AARC MNA3.1 (Mikael Linden et al.), see http://www.aarc-project.eu/*

But there are lots of challenges still open!

- 'baseline assurance' covers only simple use cases – we need *differentiated assurance* and that even with considering access controls to medical patient research data

- expression of trust marks in federations is only slowly adopted:
  which operational practices and policies are in the way of wider adoption?
  how can we prevent 1-on-1 negotiation between all federation participants?

- Many technical solutions require the operation of 'bridge' services: how can these be best sustained in the federated world? Who can most effectively run these in production?

- What policies need to be in place for research communities and e-Infrastructures to gain insight in usage data across federated services – without violating privacy principles?

  … let alone what to do with the composite architectures that come out of the AARC blueprint – that's for the future to tackle, alongside the new EU General Data Protection Regulation, and policy management of community attribute stores and services!

Architectures for an integrated and interoperable AAI

- Finalising the first draft of the Blueprint Architecture for interoperable AAIs for Research Infrastructures and e-Infrastructures.

- This draft presents a high level architectural pattern that includes all the necessary functional components in order to build integrated and interoperable AAI solutions on top of the eduGAIN.

- It is in its final stages and will be made available to the AARC stakeholders any day now.

Architectures for an integrated and interoperable AAI

Furthermore working:

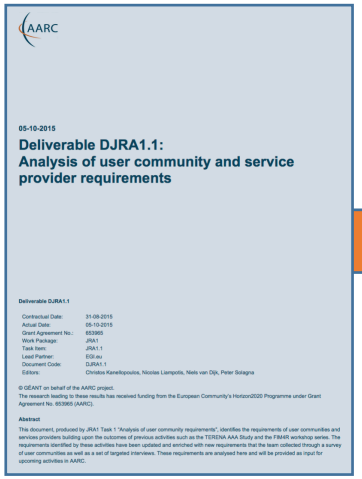
- on the problem of Guest Identities and how it can be addressed. Looking to Identity Providers of "last resort", but also at the integration of social network and e-Gov IDs as a mean to cover the users in the long tail of science, who in many cases do not have institutional IDs.

- on the topics of Attribute Management, Release and Aggregation and how these can be addressed from the point of view of the Attribute Authorities, the RIs and the e-Infrastructures

- on the topics of non-web access and credential delegation. Although these topics often go together, this is not always the case. At the moment the WP is analysing existing solutions and architectural pattern for both topics.

Pilots

Requirements User Community



05-10-2015

Deliverable DJRA1.1: Analysis of user community and service provider requirements

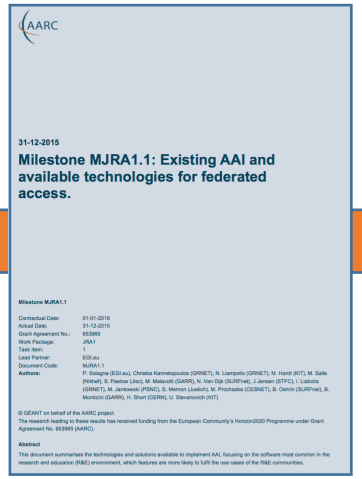
Deliverable DJRA1.1

Contractual Date: 31-08-2015
Actual Date: 05-10-2015
Grant Agreement No.: 653965
Work Package: JRA1
Task Item: JRA1.1
Lead Partner: EGI.eu
Document Code: DJRA1.1
Editors: Christos Kanellopoulos, Nicolas Liampotis, Niels van Dijk, Peter Solagna

Abstract

This document, produced by JRA1 Task 1 "Analysis of user community requirements", identifies the requirements of user communities and services providers building upon the outcomes of previous activities such as the TERENA AAA Study and the FIM4R workshop series. The requirements identified by these activities have been updated and enriched with new requirements that the team collected through a survey of user communities as well as a set of targeted interviews. These requirements are analysed here and will be provided as input for upcoming activities in AARC.

Overview Available AAI Components



31-12-2015

Milestone MJRA1.1: Existing AAI and available technologies for federated access.

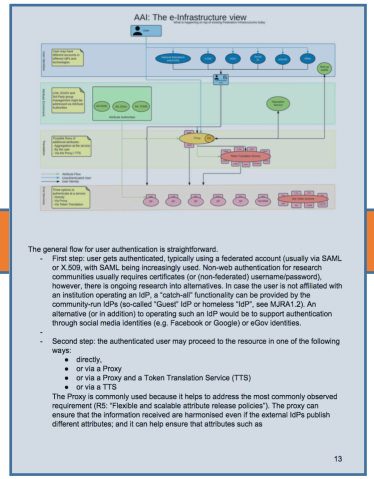
Milestone MJRA1.1

Contractual Date: 01-01-2016
Actual Date: 31-12-2015
Grant Agreement No.: 653965
Work Package: JRA1
Task Item: 1
Lead Partner: EGI.eu
Document Code: MJRA1.1
Authors: P. Solagna (EGI.eu), Christos Kanellopoulos (GRNET), N. Liampotis (GRNET), M. Hardt (KIT), M. Salle (Nikhef), S. Paetow (Jisc), M. Malavolti (GARR), N. Van Dijk (SURFnet), J Jensen (STFC), I. Liabotis (GRNET), M. Jankowski (PSNC), S. Memon (Juelich), M. Prochazka (CESNET), B. Oehm (SURFnet), B. Monticini (GARR), H. Short (CERN), U. Stevanovich (KIT)

Abstract

This document summarises the technologies and solutions available to implement AAI, focusing on the software most common in the research and education (R&E) environment, which features are more likely to fulfil the use cases of the R&E communities.

Draft Blue-Print Architecture



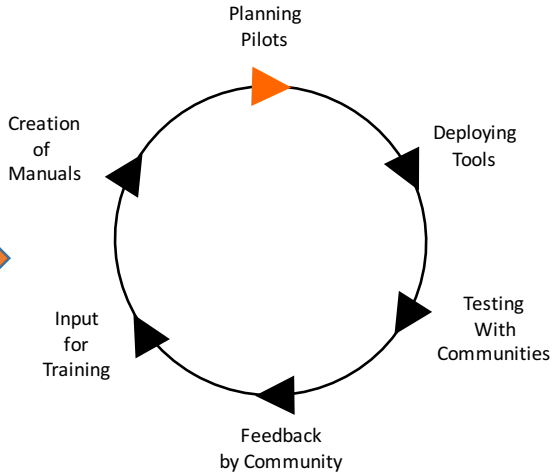
The general flow for user authentication is straightforward.

- First step: user gets authenticated, typically using a federated account (usually via SAML or X.509, with SAML being increasingly used. Non-web authentication for research communities usually requires certificates (or (non-federated) username/password), however, there is ongoing research into alternatives. In case the user is not affiliated with an institution operating an IdP, a "catch-all" functionality can be provided by the community-run IdPs (so-called "Guest" IdP or homeless "IdP", see MJRA1.2). An alternative (or in addition) to operating such an IdP would be to support authentication through social media identities (e.g. Facebook or Google) or eGov identities.
-
- Second step: the authenticated user may proceed to the resource in one of the following ways:
  - directly,
  - or via a Proxy
  - or via a Proxy and a Token Translation Service (TTS)
  - or via a TTS

The Proxy is commonly used because it helps to address the most commonly observed requirement (R5: "Flexible and scalable attribute release policies"). The proxy can ensure that the information received are harmonised even if the external IdPs publish different attributes; and it can help ensure that attributes such as

13

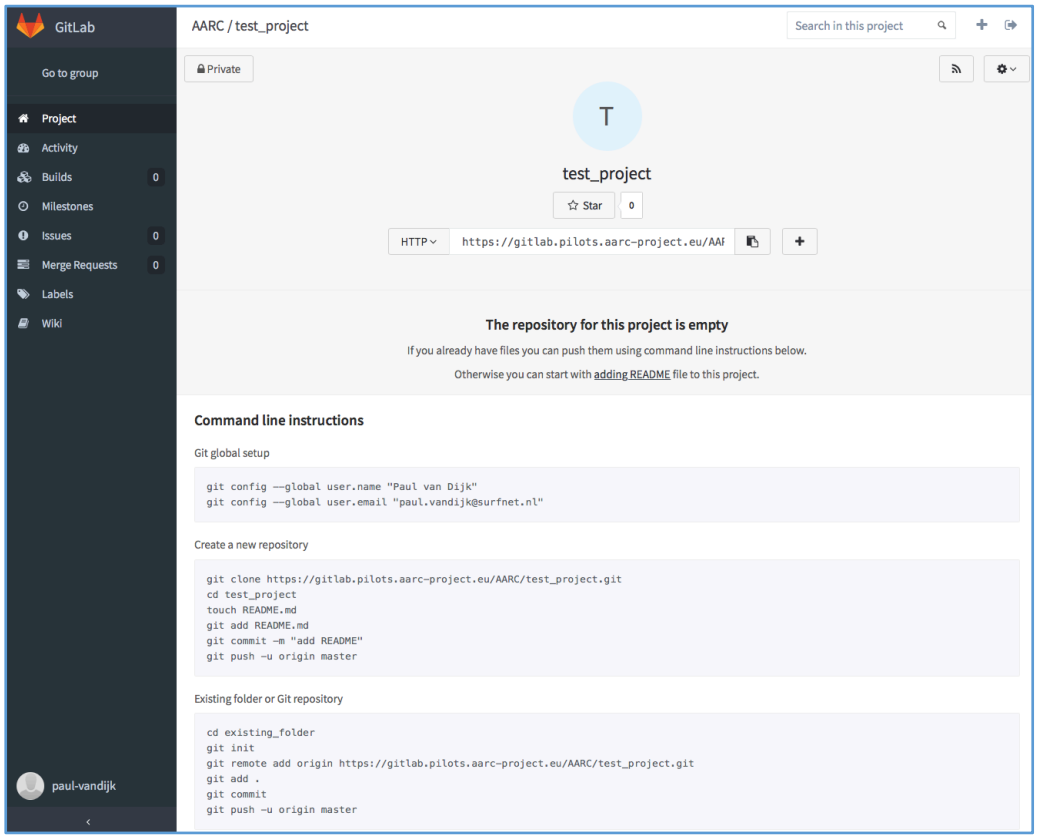
Running Pilots With Communities



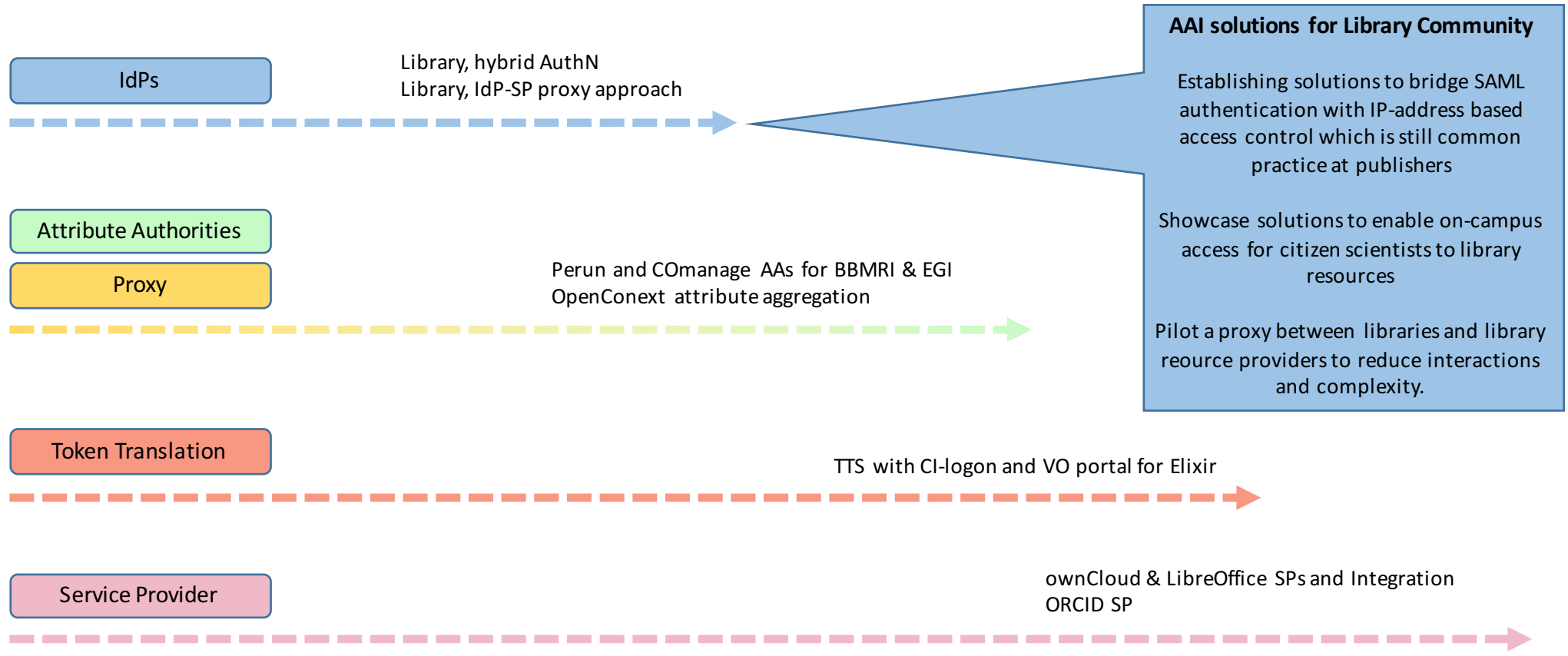
aarc-project.eu

Established a pilot platform *.pilots.aarc-project.eu

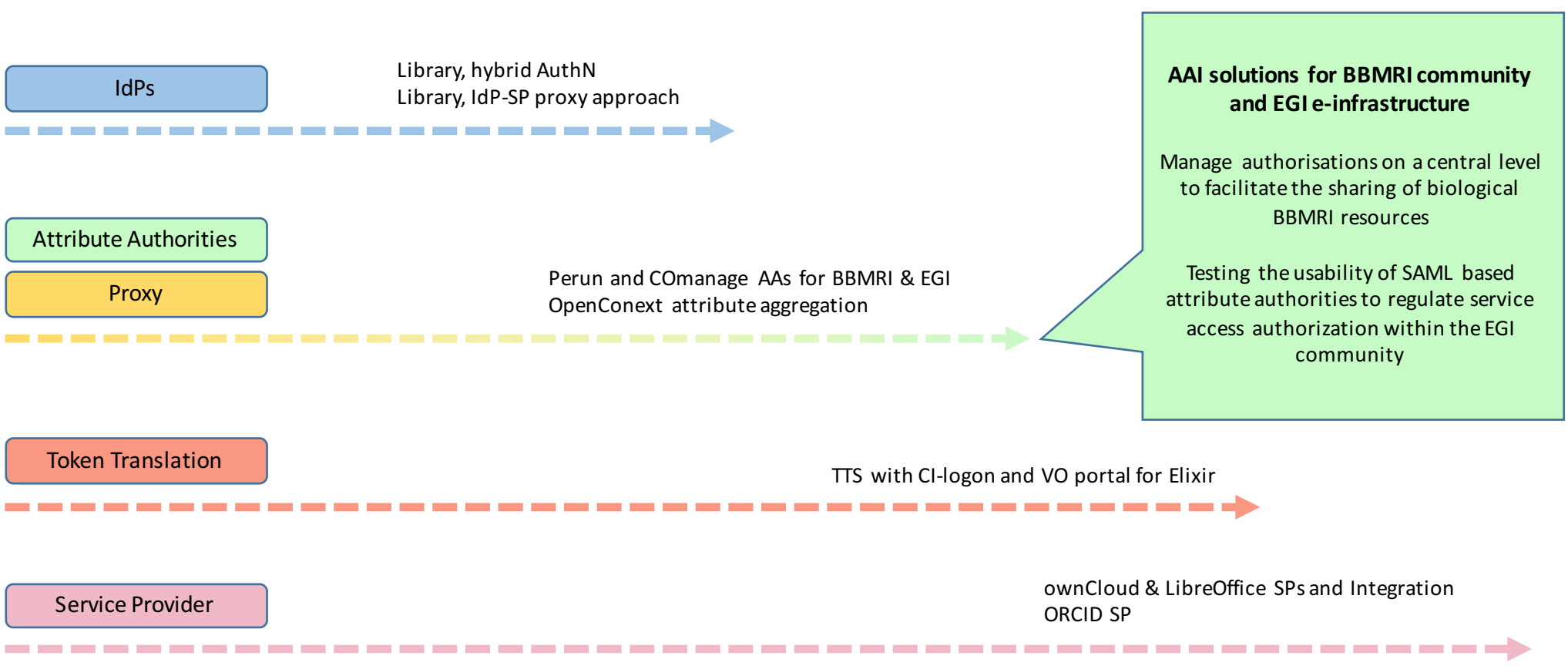
- A staging area for our services
- Technical platform delivered by okeanos
- >20 VMs instantiated
- Using Ansible scripts for deployment
- SimpleSAMLphp DIY IdP available
- Gitlab for collaborative coding, deployment and testing: gitlab.pilots.aarc-project.eu
- Online support by SURFnet staff



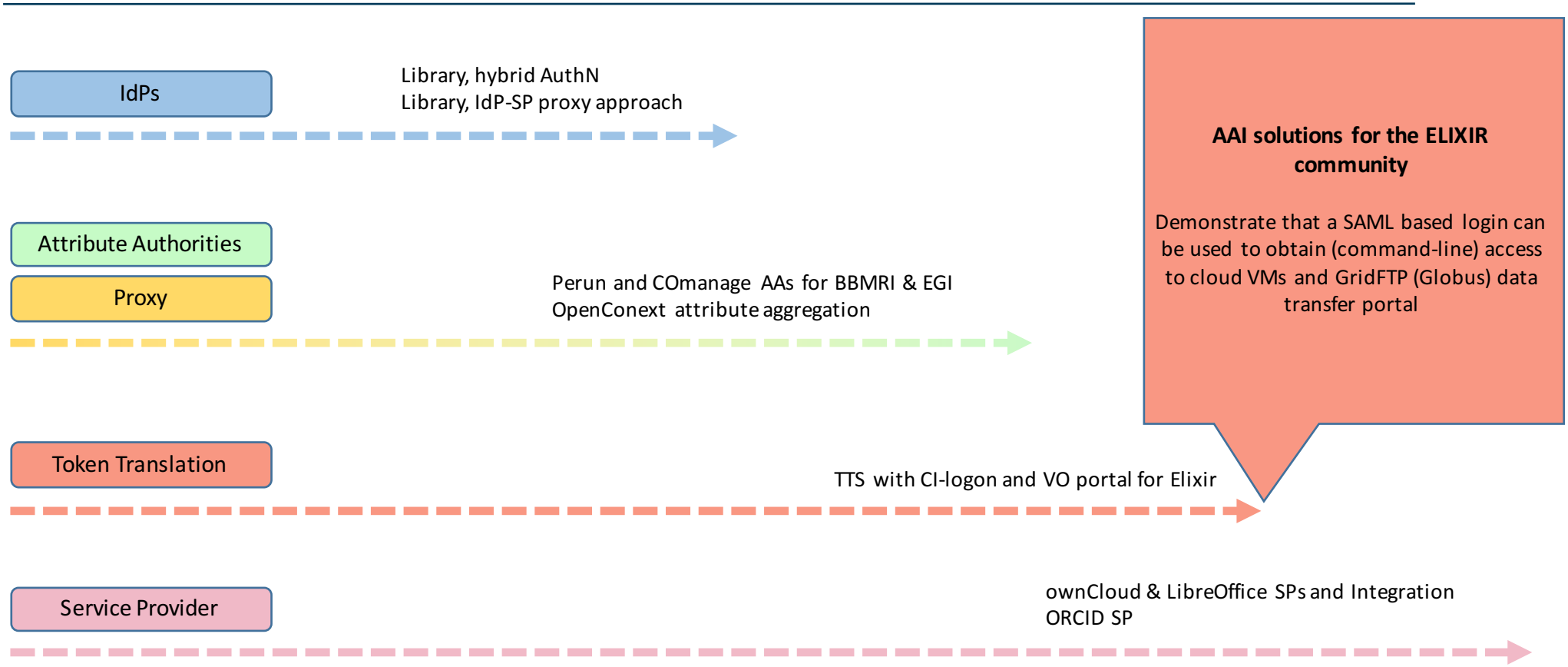
AAI building blocks and pilots commenced
First results expected at Q1 2016



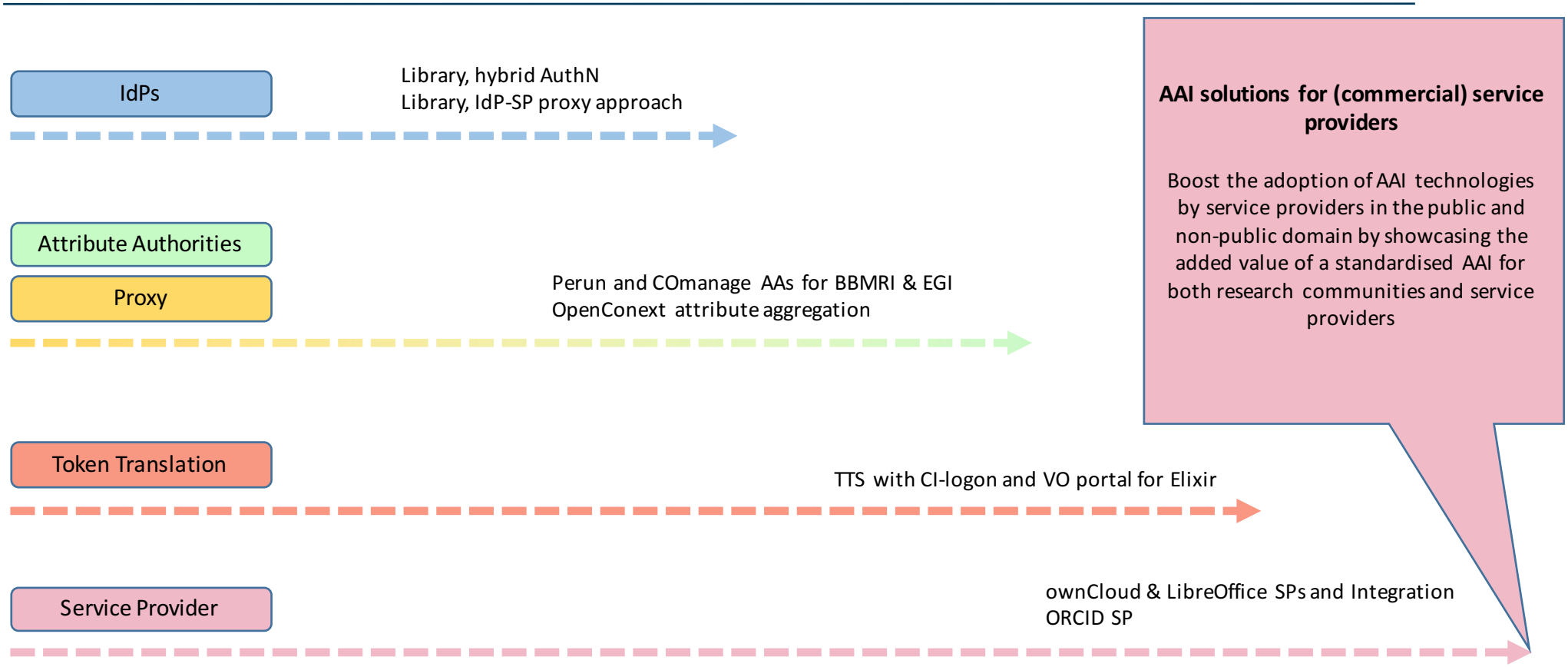
AAI building blocks and pilots commenced
First results expected at Q1 2016



AAI building blocks and pilots commenced
First results expected at Q1 2016



AAI building blocks and pilots commenced
First results expected at Q1 2016



AARC 2

We are preparing the follow-up of AARC!

AARC 2

- Support User-Driven Innovation of Trust and Identity
  Enable federated access for use-cases that meet data intensive and cross e-Infrastructure requirements

- Deploy AARC/AARC2 Results
  Support e-Infrastructures and research infrastructures to deploy AARC/AARC2 results to enable seamless service delivery to the users.

- Training and outreach
  Offer different level of training and reach out to different communities to promote AAI adoption when building new services.

Thank you

Any Questions?

Alessandra.Scicchitano@geant.org

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).