Authentication and Authorisation for Research and Collaboration

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 AAI\s

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

Liaison with existing e-Infras, communities and initiatives to get feedback on the results

Deliver a cross-discipline framework built on federated access
Almost a year has passed...

...and here is where we stand now.
Training and Outreach

Requirements & existing material

Repackage and add what is missing

- Value proposition
- Federation 101
- Training for SPs
- Training for IdPs
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

- 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
Architectures for an integrated and interoperable AAI

• Finalising the first draft of the Blueprint Architecture for interoperable AAI 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.
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.
Established a pilot platform pilots.aarc-project.eu

- A staging area for our services
- Technical platform delivered by kkeanos
- >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

IdPs

Attribute Authorities

Proxy

Token Translation

Service Provider

Library, hybrid AuthN Library, IdP-SP proxy approach

Perun and COmanage AAs for BBMRI & EGI OpenConext attribute aggregation

TTS with CI-logon and VO portal for Elixir

ownCloud & LibreOffice SPs and Integration ORCID SP

AAI solutions for Library Community

Establishing solutions to bridge SAML authentication with IP-address based access control which is still common practice at publishers

Showcase solutions to enable on-campus access for citizen scientists to library resources

Pilot a proxy between libraries and library resource providers to reduce interactions and complexity.
AAI building blocks and pilots commenced
First results expected at Q1 2016

IdPs
Library, hybrid AuthN
Library, IdP-SP proxy approach

Attribute Authorities
Perun and COmanage AAs for BBMRI & EGI
OpenConext attribute aggregation

Proxy

Token Translation

Service Provider

AAI solutions for BBMRI community and EGI e-infrastructure
Manage authorisations on a central level to facilitate the sharing of biological BBMRI resources
Testing the usability of SAML based attribute authorities to regulate service access authorization within the EGI community

TTS with CI-logon and VO portal for Elixir

ownCloud & LibreOffice SPs and Integration ORCID SP
AAI building blocks and pilots commenced
First results expected at Q1 2016

Library, hybrid AuthN
Library, IdP-SP proxy approach

Perun and COmanage AAs for BBMRI & EGI
OpenConext attribute aggregation

TTS with Cl-logon and VO portal for Elixir

ownCloud & LibreOffice SPs and Integration
ORCID SP

AAI solutions for the ELIXIR community
Demonstrate that a SAML based login can be used to obtain (command-line) access to cloud VMs and GridFTP (Globus) data transfer portal
AAI building blocks and pilots commenced
First results expected at Q1 2016

- **IdPs**
  - Library, hybrid AuthN
  - Library, IdP-SP proxy approach

- **Attribute Authorities**
  - Perun and COmanage AAs for BBMRI & EGI
  - OpenConext attribute aggregation

- **Proxy**

- **Token Translation**

- **Service Provider**
  - TTS with CI-logon and VO portal for Elixir
  - ownCloud & LibreOffice SPs and Integration
    - ORCID SP

**AAI solutions for (commercial) service providers**

Boost the adoption of AAI technologies by service providers in the public and non-public domain by showcasing the added value of a standardised AAI for both research communities and service providers.
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