Author: L. Florio (GÉANT)
Date: 8 Dec 2016-12-15
Version: 1.0

AARC Strategy

Why AARC?

Federated access has become a secure and user-friendly approach to access resources. Via the eduGAIN inter-federation infrastructure this approach scales at global level, making it possible for users to collaborate and access services and resources globally, using the same credentials that they use at their local institutions. However, there is a need to expand the basic authentication and authorisation (AA) offering in order to better support international research collaborations that span across multiple countries and national identity federations. Their requirements pose challenges to eduGAIN, and in general to federated access.

The AARC project started in May 2015 with the aims of tackling these challenges and championing federated access among research collaborations, libraries and e-infrastructures. For two years, AARC is bringing together 20 partners from among these communities to jointly design, test and promote technical and policy solutions to:

- address the requirements that characterise international research collaborations and go beyond present-day federated access capabilities;
- deliver production-ready architectural building blocks and best practices to enable research collaborations and e-infrastructures to build interoperable authentication and authorisation infrastructures (AAIs) and integrate them into their production environment.

This document highlights factors crucial to enabling broad access to services that are relevant for the research and education community, and presents the AARC strategy to address them.

Challenges AARC wants to address

The list below shows what AARC sees as the main challenges for federated access:

1. **Coverage of federated access** - Although the global coverage of national academic identity federations is high, the number of institutions connected to academic federations varies from country to country. Even in countries that have very high penetration rates for federated identities (i.e. in the US and Europe), there are still users in the R&E space who do not have access to a federated identity. This makes their participation in international research projects more challenging and requires solutions to enable their participation.

2. **Global policies for eScience collaboration** – Enabling access to resources on a global scale requires an environment of trust among different parties and the exchange of user identity information across organisational and jurisdictional boundaries. The complexity and disambiguation of national and international data privacy laws, along with the distance between resources/services and identity providers, the diversity of security requirements among resources/services, and the need to deal with security incidents on a global scale, create a very challenging environment that requires globally accepted policy frameworks.

3. **Support for eScience requirements** - The prevailing technology in most of the national academic identity federations is Security Assertion Markup Language. SAML is a battle-tested security protocol, in use for a long time, which is complex to implement properly and focuses mostly on HTTP-based services accessed via web browsers. Within eScience research collaborations, there are strong requirements for accessing non-web based services (i.e. via terminals or APIs), for having agents

running unattended for long periods of time without any interaction from the user, and for requiring stronger identity vetting for accessing some data. The fact that global collaboration is not aligned with national identity federations' boundaries increases the complexity.

4. **Sustainability aspects** - Even with identity vetting and user management being 'outsourced' to the users' home organisations, there is the need for research collaborations and infrastructures to manage controlled access to their services. This comes with related costs. Operating services at an international scale requires resources and long-term planning. Historically, large, organised research communities have been able to set up their own authentication and authorisation solutions, which have served them for many years. But, as research increasingly crosses disciplinary boundaries and grows globally, maintaining such AA solutions becomes challenging. Solutions with sustainable cost models that can meet today's and tomorrow's research requirements are needed.

AARC's strategy to address these challenges

There is consensus that most of the necessary technical components have already been developed and, to a certain extent, tested. AARC has taken the view to focus on verifying whether eScience requirements can be addressed with the available components and whether their integration in the existing workflows is possible and cost-effective. Any development done in AARC is meant to address the gaps.
As significant work has already been invested by national identity federations and research collaborations to integrate with eduGAIN, eduGAIN is considered the corner stone AAI framework for future developments.

More specifically AARC proposes a number of steps to address the above challenges.

1. **Increase the user-base of federated access** – AARC is taking a two-fold approach to address this aspect:

    - AARC uses the close relationship of project partners to eScience communities, libraries and scientific service and resource providers as a route to promote the value proposition of federated access to them.
    - AARC works also to support the so called long 'long tail of science', by investigating the usage of social identities and eGOV IDs (when they become widely available) and the related trustworthiness of those credentials to access scientific resources.

2. **Support global policies for federated access for eScience** - AARC sponsors work on the development and promotion of key policy frameworks that aim to add additional 'flavours' to the existing identity federations and eduGAIN. This will address specific global research collaborations' requirements to use eduGAIN and to make it the backbone identity layer within the research collaborations. Work in this area focuses on incident handling in federated research infrastructures, data protection aspects relevant to offer services internationally and assurance. To make results effective work in this area is carried out in collaboration with relevant international groups.

3. **Design a layered approach to address eScience requirements** - In collaboration with research and e-infrastructure providers and implementers of identity management and AA solutions, AARC has designed a technical Blueprint Architecture. This builds on top of the eduGAIN inter-federation service and adds the missing components that are required to implement secure and interoperable AA solutions that meet the requirements of international research collaborations.

4. **Pilot results in a production environment** - AARC is working with research communities and e-infrastructure on the implementation of pilots, with the aim to showcase how the proposed

approaches and the blueprint architecture addresses the identified use-cases and to test their integration in production-ready environments.

5. **Make AARC results sustainable** - AARC by design will not run any service; this is a strategic choice, based on the consideration that existing e-Infrastructures and research infrastructures are better positioned to operate services and to adopt to date best practices. Instead AARC offers blueprints, guidelines and policy frameworks as well as operational models to help research communities and e-infrastructure operators decide on the best way to deploy AARC results. Examples are the operational models for the pilots on credentials translation and for the operation/use of guest identity providers.

6. **Provide targeted training and outreach** – Based on the project participants' close ties with target communities, AARC is engaging with those communities to understand their needs, get their inputs on project activities at key stages, and to deliver appropriate solutions. AARC is building a differentiated set information and training modules with the aim to promote the adoption of federated access among research communities, e-infrastructures and libraries, promote the usage of best practices and standard AAI technologies and provide how-to modules to promote AARC results.