AARC Draft Blueprint Architecture

Christos Kanellopoulos
Architecture (JRA1) WP Leader, GRNET

Internet2 2016 Global Summit
May 15 – 18, Chicago
The starting point

• The scenario:
  • There is a technical architect of a research community
  • Her community is distributed internationally
  • Increasing number of services need authentication and authorization
  • Her job is to find a solution
  • She wants to focus on research and not reinvent the wheel
  • She starts googling

• So, there are some solutions available, but...
The goals

1. Users should be able to access the all services using the **credentials from their Home Organization**

2. Users should have one **persistent non-reassignable non-targeted unique identifier**.

3. Attempt to **retrieve user attributes** from the user’s Home Organization. If this is not possible, then an alternate process should exist.

4. Distinguish **(LOA)** between self-asserted attributes and the attributes provided by the Home Organization/VO

5. **Access** to the various services should be granted **based on the role(s)** the users have within the collaboration

6. Services should not have to deal with the complexity of multiple IdPs/Federations/Attribute Authorities/technologies.
**AARC: Analysis of User Communities and e-Infrastructure Providers**

<table>
<thead>
<tr>
<th>Attribute Release</th>
<th>Attribute Aggregation</th>
<th>User Friendliness</th>
<th>SP Friendliness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential translation</td>
<td>Persistent Unique Id</td>
<td>User Managed Information</td>
<td>Credential Delegation</td>
</tr>
<tr>
<td>Levels of Assurance</td>
<td>Guest users</td>
<td>Step-up AuthN</td>
<td>Best Practices</td>
</tr>
<tr>
<td>Community based AuthZ</td>
<td>Non-web-browser</td>
<td>Social &amp; e-Gov IDs</td>
<td>Incident Response</td>
</tr>
</tbody>
</table>
The functional Components

User Community Requirements

https://goo.gl/kSxENp
Why the proxy model?

• All internal Services can have one statically configured IdP

• No need to run an IdP Discovery Service on each Service

• Connected SPs get consistent/harmonised user identifiers and accompanying attribute sets from one or more AAs that can be interpreted in a uniform way for authZ purposes

• External IdPs only deal with a single SP proxy
The Functional Components and available AAI tools

Available AAI Components

IdPs

Attribute Authorities

Proxies

Token Translation

Service Provider

Analysis of User Communities

And Infrastructure Providers

https://aarc-project.eu
eduGAIN & AARC

eduGAIN and the Identity Federations

A solid foundation for federated access in R&E

Authentication and Authorization Architecture for Research Collaboration

A set of building blocks on top of eduGAIN for International Research Collaboration
A real life implementation...
A real life implementation...

- IdP Discovery
- User Enrolment
- User Consent
- Support for LoA
- Attribute Aggregation
  - SAML2.0 Attribute Query, REST, LDAP
- Attribute mapping
- Support for OIDC/OAuth2
  - Google, Facebook, LinkedIn, ORCID
- Support for eGov IDs
Pilots

Requirements
User Community

Overview Available
AAI Components

Draft Blue-Print
Architecture

With Communities

Plan

Develop

Test

Input for training

Include Feedback

Pilots

Package/release

https://goo.gl/kSxENp

https://goo.gl/NzQA2U

https://goo.gl/7dZZF4

aarc-project.eu

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

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

The perspective for user authentication is demonstrated. First, the user authentication component needs to be authenticated (i.e., via OAuth, SAML, or another method). After authentication, the user can access the services (e.g., APIs or dashboards). The authentication process is typically a two-factor authentication, where the user needs to enter a username and password. Then, the authentication process can be completed. Further, the authentication process can be verified through the user's biometric data (e.g., fingerprint, face recognition). The authentication process can be verified through the user's biometric data (e.g., fingerprint, face recognition). The authentication process can be verified through the user's biometric data (e.g., fingerprint, face recognition).
Thank you
Any Questions?

Christos Kanellopoulos
skanct@admin.grnet.gr

https://aarc-project.eu

© GÉANT on behalf of the AARC project.
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).