EOSC AAI Implementation

Christos Kanellopoulos - GEANT
Slavek Licehammer - MUNI
Nicolas Liampotis - GRNET
The evolution of the EOSC AAI architecture
EOSC AAI Baseline Architecture

Based on the AARC Blueprint Architecture

The purpose of the Community AAI is to streamline researchers’ access to services, both those provided by their own infrastructure as well as the services provided by infrastructures that are shared with other communities.

Infrastructure Proxy

The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single integration point, where the Infrastructure can maintain centrally all the relevant policies and business logic for making available these resources to multiple communities.
Community AAI

The purpose of the Community AAI is to streamline researchers’ access to services, both those provided by their own infrastructure as well as the services provided by infrastructures that are shared with other communities.

Infrastructure Proxy

The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single integration point, where the Infrastructure can maintain centrally all the relevant policies and business logic for making available these resources to multiple communities.
Based on the AARC Interoperability Guidelines

AARC Interoperability Guidelines Approved by AEGIS

Created by Christos Kanellopoulos, last modified by Nicolas Liampitsis on Jan 14, 2022

<table>
<thead>
<tr>
<th>#</th>
<th>Document</th>
<th>AARC Identifier</th>
<th>Date presented</th>
<th>Date approved</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Guidelines on expressing group membership and role information</td>
<td>AARC-G002</td>
<td>2017-11-13</td>
<td>2017-11-15</td>
<td>Current</td>
</tr>
<tr>
<td>2</td>
<td>Exchange of specific assurance information between Infrastructure</td>
<td>AARC-G021</td>
<td>2018-03-12</td>
<td>2018-03-12</td>
<td>Current</td>
</tr>
<tr>
<td>3</td>
<td>Guidelines for evaluating the combined assurance of linked identities</td>
<td>AARC-G031</td>
<td>2018-05-14</td>
<td>2018-07-09</td>
<td>Current</td>
</tr>
<tr>
<td>4</td>
<td>Specification for expressing resource capabilities</td>
<td>AARC-G027</td>
<td>2018-12-10</td>
<td>2019-12-10</td>
<td>Current</td>
</tr>
<tr>
<td>5</td>
<td>Implementing scalable and consistent authorisation across multi-SP</td>
<td>AARC-G047</td>
<td>2019-03-11</td>
<td>2019-03-11</td>
<td>Current</td>
</tr>
<tr>
<td>6</td>
<td>A specification for IdP hinting</td>
<td>AARC-G049</td>
<td>2019-03-11</td>
<td>2019-04-08</td>
<td>Superseded by AARC-G061</td>
</tr>
<tr>
<td>7</td>
<td>Guidelines for expressing affiliation information</td>
<td>AARC-G028</td>
<td>2019-03-11</td>
<td>2019-10-14</td>
<td>Current</td>
</tr>
<tr>
<td>8</td>
<td>AARC Blueprint Architecture 2019</td>
<td>AARC-G045</td>
<td>2019-11-11</td>
<td>2020-02-10</td>
<td>Current</td>
</tr>
<tr>
<td>9</td>
<td>Inferring and constructing voPersonExternalAffiliation</td>
<td>AARC-G057</td>
<td>2020-07-13</td>
<td>2021-02-08</td>
<td>Current</td>
</tr>
<tr>
<td>10</td>
<td>A specification for IdP hinting</td>
<td>AARC-G061</td>
<td>2020-06-11</td>
<td>2021-02-08</td>
<td>Current</td>
</tr>
<tr>
<td>11</td>
<td>Guidelines for expressing community user identifiers</td>
<td>AARC-G026</td>
<td>2019-09-09</td>
<td>2021-06-14</td>
<td>Current</td>
</tr>
<tr>
<td>12</td>
<td>Specification for hinting an IdP which discovery service to use</td>
<td>AARC-G062</td>
<td>2021-09-13</td>
<td>2021-10-11</td>
<td>Current</td>
</tr>
</tbody>
</table>
EOSC AAI Architecture 2022

● Consistent user experience and interfaces for service providers
● Multi-infrastructure workflows
● Scaling trust
● Growth of EOSC beyond the research and education community
● Community attributes and authorisation
EOSC AAI Architecture 2022

- Consistent user experience and interfaces for service providers
- Multi-infrastructures workflows
- Scaling trust
- Growth of EOSC beyond the research and education community
- Community attributes and authorisation
EOSC AAI Architecture 2022 Working Areas: Consistent user experience and interfaces

- Users need to go through multiple Identity Provider discovery steps
  - Example: First select Community AAI then select the Identity Provider of their Home Organisation
- Users don’t need to re-enter their login credentials **but** the IdP selection can be frustrating
- Adoption of AARC “hinting” documents
  - IdP selection hints ⇒ AARC-G061
  - Discovery Service selection hints ⇒ AARC-G062
  - Service hints ⇒ AARC-G063
Adoption of AARC Community-based Access Entity Category (AARC-G079) can be used to:

- Distinguish Community AAIs from authenticating IdPs during discovery
- Services that control access based on community identity attributes (e.g. community-managed groups and roles) ⇒ Filter out IdPs that don’t assert the Community Entity Category Support attribute
- Services that don’t rely on community identity attributes ⇒ Include only authenticating IdPs during discovery
- Facilitate IdP decisions to release a defined set of attributes to services.
EOSC AAI Architecture 2022

- Consistent user experience and interfaces for service providers
- **Multi-infrastructure workflows**
- Scaling trust
- Growth of EOSC beyond the research and education community
- Community attributes and authorisation
EOSC AAI Architecture 2022 Working Areas: Multi-infrastructure workflows

- Current EOSC AAI architecture works when the user is consuming services directly.
- However, some use cases require a service agent to be able to act autonomously—on behalf of the user—to consume services and resources.
- If the services consumed by the agent are behind the same proxy, the current architecture works.
- But what happens if an agent running on Service A needs to access resources on Service B connected by a different infrastructure?
EOSC AAI Architecture 2022 Working Areas: Multi-infrastructure workflows (Contd.)

- OAuth 2.0 token validation: Existing standards rely on direct trust relationship between the protected resources and the Authorisation servers issuing OAuth 2.0 tokens
- Example: Community service (infrastructure A) accessing e-Infra service (infrastructure B) on behalf of user
EOSC AAI Architecture 2022 Working Areas: Multi-infrastructure workflows (Contd.)

- Resource servers need to directly trust multiple Authorisation Servers across infrastructures instead of relying on a single Proxy

- **BUT**
  - Requires additional integration effort from services
  - Cannot scale
● OpenID Connect Federation specification v1.0 (draft) ⇒ Long-term solution for dynamically establishing trust in a distributed environment

● OAuth 2.0 Token Proxyed Introspection specification (AARC-G052) ⇒ Interim solution until the OIDC Federation Specification is finalised & becomes widely available.
EOSC AAI Architecture 2022

- Consistent user experience and interfaces for service providers
- Multi-infrastructure workflows
- Scaling trust
- Growth of EOSC beyond the research and education community
- Community attributes and authorisation
EOSC AAI Architecture 2022 Working Areas: Scaling trust

- Trust between Community AAI and Infrastructure Proxy services needs to be established via exchange of metadata
- Growing number of Community AAI and Infrastructure Proxy services that need to be interconnected for enabling access to resources across infrastructures within the wider EOSC environment
- Establishment of M:N relationships → *scalability* issues
EOSC AAI Architecture 2022 Working Areas: Scaling trust (Contd.)

Solution: EOSC AAI Federation

- Community AAIs and Infrastructure Proxies connect once with the EOSC AAI Federation (register metadata, URN namespaces, policies etc)
- Community AAIs and Infrastructure Proxies discover and establish trust with the rest of the Community AAIs and Infrastructure Proxies through the EOSC AAI Federation
- No need to register entities that are already registered in a Peer Federation (e.g. eduGAIN)
EOSC AAI Architecture 2022

- Consistent user experience and interfaces for service providers
- Multi-infrastructure workflows
- Scaling trust
- **Growth of EOSC beyond the research and education community**
- Community attributes and authorisation
EOSC AAI Architecture 2022 Working Areas: Beyond the research and education community

- Enables access to users from 5100+ identity providers from R&E community but needs to support citizen scientists, public sector organisations, and industry users

- Extending access:
  - Social media identities
  - eIDAS (national identification scheme) identities
  - Organisations beyond R&E:
    - Organisation can join National Federation to register the authenticating entity; or
    - EOSC AAI Federation Operator can import the authenticating entity of that organisation into the federation
EOSC AAI Architecture 2022

- Scalability
- Multi-infrastructure workflows
- Consistent user experience and interfaces for service providers
- Growth of EOSC beyond the research and education community
- Community attributes and authorisation
EOSC AAI Architecture 2022 Working Areas: Community attributes & authZ

- Attribute Providers (AtP) can be independent from authenticating/Community IdPs
- Need to consider different –not only community-controlled– attribute/access management services
Next steps:

-Specify scalable mechanism for establishing trust between OAuth 2.0 Authorization Servers within the EOSC AAI Federation

-More streamlined discovery process (e.g. “EOSC Login” button)?

-Introduce minimum assurance requirements?
THANK YOU