The AARC Blueprint Architecture

Christos Kanellopoulos - GÉANT
International Research Collaborations

1. Users should be able to access the all services using the credentials from their Home Organizations when available.

2. Secure integration of guest identity solutions and support for stronger authentication mechanisms when needed.

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

4. Users should have one persistent identity across all community services when needed.

5. Ease of use for users and service providers. The complexity of multiple IdPs/Federations/Attribute Authorities/technologies should be hidden.
Identity & Access Management for International Research Collaborations

A Blueprint Architecture for authentication and authorization

A set of architectural building blocks on top of eduGAIN

eduGAIN and the Identity Federations

A solid foundation for federated access in Research & Education
Identity & Access Management for International Research Collaborations

A Blueprint Architecture for authentication and authorization

A set of architectural building blocks on top of eduGAIN

eduGAIN and the Identity Federations

A solid foundation for federated access in Research & Education
AARC Blueprint Architecture

User Community Requirements

https://goo.gl/kSxENp

https://aarc-project.eu/roadmap/blueprint-architecture/
Guidelines and support documents

- Best practices for managing authorisation
- Expressing group membership and role information
- Scalable attribute aggregation
- Implementation of token TTS
- Credential delegation
- Non-web access
- Social media IdPs
- Use cases for account linking
- Use cases for LoA elevation via step-up authentication

https://aarc-project.eu/blueprint-architecture/
Policy recommendations & frameworks

- Security Incident Response Trust Framework for Federated Identity – Sirtfi
- Scalable Negotiator for a Community Trust Framework in Federated Infrastructures – Snctfi
- Recommendations on Minimal Assurance Level Relevant for Low-risk Research Use Cases
- Differentiated LoA recommendations for policy and practices of identity and attribute providers
- Recommendations and template policies for the processing of personal data by participants in the pan-European AAI
<table>
<thead>
<tr>
<th>Attribute Release</th>
<th>Attribute Aggregation</th>
<th>User Friendliness</th>
<th>SP Friendliness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistent Unique Id</td>
<td>Credential translation</td>
<td>Credential Delegation</td>
<td>User Managed Information</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>
Thank you

Any Questions?