AARC blueprint guidelines
Authentication and Authorisation for Research and Collaboration

Nicolas Liampotis
JRA1: Integrated AAI Developments, AARC2
GRNET

Digital Infrastructures for Research 2017, Brussels
30 November 2017
AARC recommendations & best practices

Overview

- [AARC-JRA1.4A] Guidelines on expressing group membership and role information
- [AARC-JRA1.4B] Guidelines on attribute aggregation
- [AARC-JRA1.4C] Guidelines on token translation services
- [AARC-JRA1.4D] Guidelines on credential delegation
- [AARC-JRA1.4E] Best practices for managing authorisation
- [AARC-JRA1.4F] Guidelines on non-browser access
- [AARC-JRA1.4G] Guidelines for implementing SAML authentication proxies for social media identity providers
- [AARC-JRA1.4H] Account linking and LoA elevation use cases and common practices for international research collaboration
- [AARC-JRA1.4I] Best practices and recommendations for attribute translation from federated authentication to X.509 credentials
Guidelines on expressing group membership and role information
AARC-JRA1.4A

- Standardising the way group membership information is expressed for cross-infrastructure exchange
- Indicating the entity that is authoritative for each piece of group membership information
- Expressing VO membership and role information
- Supporting group hierarchies in group membership information
- Revision (201710) signed off by AEGIS

```
<NAMESPACE>:group:<GROUP>[:<SUBGROUP>]*[:role=<ROLE>]#<GROUP-AUTHORITY>
```
Guidelines on attribute aggregation
AARC-JRA1.4B

- Models for Attribute Aggregation ("pull" vs "push" vs "preprovision")
- Persistent, unique identifiers for linking records
- Explicit consent for data sharing
- Centralising aggregation “Business Logic” away from the SP
- Scoping attribute values
- Filtering attributes according to source
- Harmonising attribute vocabularies
Guidelines on token translation services
AARC-JRA1.4C

• Operation modes for TTS services ("embedded" vs "standalone")
• Consistency of user information
• Deployment considerations
• Security considerations
• Transparency, data protection and data minimisation
Guidelines on credential delegation

AARC-JRA1.4D

- Types of delegation ("rights" vs "access" vs "credential")
- Example flows:
  - OAuth2/OIDC
  - SAML authentication
  - OAuth2 token exchange
  - GSI proxies
  - Combined use of X.509 and OIDC
- Implementation guidelines
- Risks associated with delegations
Best practices for managing authorisation

AARC-JRA1.4E

- Authorization information sources
  - IdPs
  - AAs
- Authorisation attributes
  - Affiliation
  - Entitlement
  - Assurance
- Trust relationships
Guidelines on non-browser access
AARC-JRA1.4F

- CLI: SSH/SFTP
  - GSI enabled SSH
  - SSH key provisioning with web portal
- Accessing HTTP APIs using:
  - OIDC/OAuth2
  - X.509 certificates
  - service specific API tokens
Guidelines for implementing SAML authentication proxies for social media identity providers
AARC-JRA1.4G

• Generating SAML eduPersonUniquesIds based on social media profile identifiers
• Mapping social identity profile fields to SAML attributes:
  • Google / OpenID Connect
  • Facebook
  • LinkedIn

<table>
<thead>
<tr>
<th>SAML</th>
<th>Google / OIDC</th>
<th>Facebook</th>
<th>LinkedIn</th>
</tr>
</thead>
<tbody>
<tr>
<td>eP UID</td>
<td>sub</td>
<td></td>
<td>issuer</td>
</tr>
<tr>
<td>displayName</td>
<td>name(1)</td>
<td>name</td>
<td>formatted-name(4)</td>
</tr>
<tr>
<td>givenName</td>
<td>given_name</td>
<td>fist_name</td>
<td>first-name(4)</td>
</tr>
<tr>
<td>sn</td>
<td>family_name</td>
<td>last_name</td>
<td>last-name(4)</td>
</tr>
<tr>
<td>mail</td>
<td>email(2)</td>
<td>email</td>
<td>email-address(5)</td>
</tr>
</tbody>
</table>
Account linking and LoA elevation use cases and common practices for international research collaboration

AARC-JRA1.4H

- Account linking use cases
  - Consistent user identification/representation
  - Accounting of resource usage
  - Traceability and security incident response
- Account linking process ("Explicit" vs "Automatic")
- Reconciling identity information
- LoA elevation
  - Linking High-LoA Identity
  - Step-Up Authentication
  - Attribute origin Information
Best practices and recommendations for attribute translation from federated authentication to X.509 credentials

**AARC-JRA1.4I**

- Translating SAML attributes into a subject DN
- Defining the user Common Name (CN) component from IdP attributes
- Defining the Organisation (O) component from IdP attributes
- Translating group information using VOMS Attribute Certificates (ACs)
AARC2 recommendations & best practices

Overview

• [AARC2-JRA1.1x] Guidelines for interoperable exchange of user and community information between AAIs

• [AARC2-JRA1.2C] Guidelines for step-up authentication via Two-Factor Authentication

• [AARC2-JRA1.3A] Guidelines for evaluating the combined assurance of linked identities

• [AARC2-JRA1.4A] Roles, responsibilities and security considerations for VOs
Interoperable exchange of user and community information across infrastructures

AARC2-JRA1.1x

• AARC2-JRA1.1A: Guidelines for interoperable exchange of user and community information between AAIIs: Assurance information – Final draft

• AARC2-JRA1.1F: Guidelines for uniquely identifying users across infrastructures (ePUID + subject ID) – Final draft

• AARC2-JRA1.1X: Guidelines for exchanging home organisation and affiliation information between infrastructures – NEW
Step-up authentication via Multi-Factor Authentication

AARC2-JRA1.2C

- Identified current use cases and example implementations (e.g. HAKA, SURFnet)
- Many discussions around the various assurance-related concepts and terms: components, profiles, etc.
- Input for the upcoming GÉANT two-factor authentication solution for research communities
Guidelines for evaluating the combined assurance of linked identities
AARC2-JRA1.3A

- Initial version of the evaluation model already in place
- Identified main use cases
- Identity linking risks

<table>
<thead>
<tr>
<th>Linked Identity B</th>
<th>Identity proofing and credential issuance, renewal and replacement</th>
<th>Attribute Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity linking risks</td>
<td>$\text{PREFIX}/IAP/assumed</td>
<td>$\text{PREFIX}/IAP/verified</td>
</tr>
<tr>
<td>N/A</td>
<td>$\text{PREFIX}/IAP/assumed</td>
<td>$\text{PREFIX}/IAP/verified</td>
</tr>
<tr>
<td>N/A</td>
<td>$\text{PREFIX}/IAP/assumed</td>
<td>$\text{PREFIX}/IAP/verified</td>
</tr>
<tr>
<td>N/A</td>
<td>$\text{PREFIX}/IAP/assumed</td>
<td>$\text{PREFIX}/IAP/verified</td>
</tr>
<tr>
<td>N/A</td>
<td>$\text{PREFIX}/IAP/assumed</td>
<td>$\text{PREFIX}/IAP/verified</td>
</tr>
</tbody>
</table>

https://aarc-project.eu
• Technical requirements to:
  • support policies (e.g., involving VO security contacts in incidents relating to their VO)
  • improve operations (e.g. delegating rights and responsibilities to deputies when the primary person in the role is not available) in a scalable manner

<table>
<thead>
<tr>
<th>Role</th>
<th>Source</th>
<th>Comment/responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td></td>
<td>Accept and abide to the VO AUP, use the resources only for the purposes described by the VO. Must be contactable (by email)</td>
</tr>
<tr>
<td>PI</td>
<td></td>
<td>Define scope of VO, and the VO AuP. Ensuring that the VO AuP is aligned with the requirements of the Infrastructures.</td>
</tr>
<tr>
<td>Security contact(s)</td>
<td>EGI, SIRTFI</td>
<td>Collaborate with infrastructure in case of an incident</td>
</tr>
<tr>
<td>User membership mgmt</td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>
Thank you

Any Questions?

nliam@grnet.gr

https://aarc-project.eu