LS AAI

2 Feb 2018
Background

- Develop a customized AAI that meets LS community requirements:
  - Uniquely authenticate users and assign them an unique ID (LifeScienceID)
  - Support management of accounts and attributes
  - Enable users to access both LS services as well as generic services
  - Support federated access to different type of services (SAML, OIDC, X.509)
- Entrust the operation of this AAI in the hands of e-infrastructure
- A pilot started end of Nov 2017 to implement the AAI in the EUDAT, EGI and GÉANT proposal. Three phases are foreseen:
  - **Phase 1: end Nov 2017 - end of Jan 2018**
  - Phase 2: 1 Feb 2018 - end of May 2018
  - Phase 3: will be delivered later
Key aspects

• Implements AARC Blueprint Architecture, in a multi-domain scenario
• AAI components operated by 3 different e-infrastructures
• Supports for multiple protocols
• Collaboration across infrastructures to offer a joint service
• The work is carried out in the context of the AARC project
A view behind the scenes: Architecture
A view behind the scenes: Architecture

Pilot Infra

“Production” infra
Phase 1 includes

- User, Group & Attribute Management via Perun
  - LifeScienceID
- LS AAI Proxy
  - IdP facing Proxy (eduTEAMS IdHub Proxy)
  - Service facing SAML Proxy (CheckIn)
  - Service facing OIDC Proxy (B2ACCESS)
- Token translation service (Watts)
- Connect 3 service providers
  - Virtual Coffee Room (SAML)
  - EuroBioImaging Web access (SAML)
  - Perun (SAML)
  - Watts (OIDC)
Phase 2 includes (Prioritised according to the latest input from LS)

High Priority
• 3.5. Account linking for Life Science service IDs
• 4.2 User Research Infrastructure Attribute
• 4.4 Groups
• 5.3 User Synchronisation
• 5.4 Provisioning
• 5.1 Federated Login and attribute release
• 6 Logging, Statistics and Data retention

Low Priority
• 4.3 Researchers qualifications
• 4.6 Other attributes
• 4.7 active role selection
Comments? Questions?

• Did I miss something?
Today’s Demo

Will focus on showing:

- How the architecture has been bootstrapped
- How a Life Science user can access services that are operated by different infrastructure in a federated fashion
Connection to the IdPS

Protocol

Remarks

SAML2

Presents a SAML2 SP, conformant with eduGAIN, SAML2INT, R&S

Required attributes:

- R&S bundle
  (https://refeds.org/category/research-and-scholarship)
- eduPersonScopedAffiliation (optional)
- eduPersonORCID (optional)

or

- eduPersonTargetedID (required)
- givenName (required)
- sn (required)
- email (required)
- cn (optional)
- displayName (optional)
- eduPersonScopedAffiliation (optional)
- eduPersonORCID (optional)
Protocol | Remarks
---|---
OIDC, OAuth2 | Presents an OIDC, Oauth2 endpoint for external authentication providers
This interface connects to specific authentication through OIDC or proprietary interfaces.

In the pilot the following authentication providers are included:

- Github (p1)
- Linkedin (p1)
- Google (p2)
- Facebook (p2)
- ORCID (p2)
Internal Proxy Connections

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| SAML2    | Identifier:  
|          | ● schacPersonalUniqueCode |
Internal Proxy Connections: Perun

**Protocol**
- SAML2

**Remarks**
- **Identifier:**
  - schacPersonalUniqueCode

- **Attributes:**
  - eduPersonTargetedID (if provided)
  - eduPersonPrincipleName (if provided)
  - givenName
  - sn
  - email
  - displayName
  - eduPersonScopedAffiliation (optional)
  - eduPersonORCID (optional)