Federated Identity Management for Research

CHEP, 10th July 2018, Sofia
Presenter: Hannah Short (CERN)

** Not all contributors’ logos represented

With thanks to the FIM4R Authors and Contributors for their collaboration on the whitepaper and the following slides.
“Every researcher is entitled to focus on their work and not be impeded by needless obstacles nor required to understand anything about the FIM infrastructure enabling their access to research services.”  FIM4R version 2
Motivation

• Research Communities provide complex use cases where federated identity can be leveraged to great effect
  – Distributed users
  – Distributed services
• The specific way of working brings challenges that go beyond the functionality typically offered by federations and interfederation
• Many communities around HEP are facing similar challenges in authenticating and authorising their users

FIM4R provides a forum for Research Community representatives to exchange experiences of implementing AAI and by combining our voices we hope to influence the future direction of FIM in a way that meets the needs of our Users
FIM4R Whitepaper

• A second version of a 2012 whitepaper
• Representatives of more than 20 research communities provided input
• Five face to face meetings in Europe and North America
  – Vienna (TIIME) x 2
  – Montreal (RDA)
  – Barcelona (RDA)
  – San Francisco (Internet2 TechEx)
• Produced a new distillation of specific requirements and a set of recommendations

[DOI Link] https://doi.org/10.5281/zenodo.1296031
Who is represented?

Research Fields (14)

- Arts and Humanities
- Climate Science
- Earth Observation
- European Neutron and Photon Facilities
- Gamma-Ray Astronomy
- Gravitational Wave Astronomy
- High Energy Physics
- Ionospheric and Atmospheric Science
- Infectious Disease Research
- Life Sciences
- Linguistics
- Nuclear Physics
- Radio Astronomy
- Virtual Atomic and Molecular Data Centre

Others

Research Driven Services
- HNSciCloud
- ORCID

Identity Federation Projects/Communities
- AARC(2)
- GÉANT-GN4
- InCommon/Internet2
- REFEDS
Progress since 2012
What are the successes since 2012?

Much has changed since 2012. The FIM4R paper was taken seriously and AAI is now more mature with many successes

- European Commission funding (H2020) for the AARC/AARC2 projects
- Federations and interfederation have found their role as an Authentication infrastructure; Authorisation managed by Communities
- eduGAIN’s operational support capability is now in place and maturing
- e-Infrastructures are deploying shared AAI services (EGI, EUDAT, GÉANT, EOSC-hub, …)

- Specific successes include the Sirtfi and Snctfi trust frameworks
- Standardisation and best practices for the emerging trend of “proxy” architecture (The AARC Blue Print Architecture)
The Proxy Architecture allows Research Communities to satisfy many FIM4Rv1 requirements themselves, but comes with a large overhead.

https://aarc-project.eu/architecture/
Outstanding Challenges (1)

• Usability & User Experience
  – Considerable time spent in bilateral debugging
  – Discovery services unintuitive

• Data Privacy and EU GDPR
  – Better data access and privacy expectations need to be balanced, E.g. ELIXIR Human Data resources are potentially liable for breaches
  – Attribute release by risk averse IdPs is already problematic, this may be aggravated

• Level of Assurance
  – Frameworks defined but not well adopted or propagated
Outstanding Challenges (2)

- Interfederation and many federations do not offer an adequate level of operational support and security for Research use cases
  - eduGAIN has become recognised as a brand and those wishing to “join” experience a steep learning curve and inconsistent federation practices
- Although several generic AAI infrastructures are evolving, their respective advantages and availability are unclear
Research Community Use Case Highlights
gw-astronomy.org (e.g. LIGO, KAGRA, VIRGO)

• Collaboration hub for gravitational-wave and multi-messenger astronomy (MMA)
• Federated identity collaboration registry (COmanage), wiki, and email list server
• Used to manage collaboration around the August 17, 2017 kilonova event (binary neutron star inspiral with gravitational-wave and electromagnetic counterpart)
• **Mesh configuration but beginning transition to proxy architecture**
  – Both SAML (SATOSA) and OIDC (CILogon)
World-wide LHC Computing Grid Project (WLCG)

• 13K physicists, analyse Large Hadron Collider (LHC) data
• Long history of federated X.509 through IGTF
• Non-X.509 increasingly interesting including eduGAIN and ORCID
• "The definition and adoption of Trust Frameworks, including Sirtfi, has built confidence in the potential for such identities to demonstrate an acceptable level of assurance"
• WLCG Authorisation Working group has been established to
  – Define a schema for JWT Tokens for use within WLCG (OAuth and OIDC)
  – Define requirements for a pilot for non-web access and work towards deployment

Come along to the WLCG Authorisation Working Group pre-GDB next Tuesday!
Helix Nebula Science Cloud Pre-Procurement Project

- €5.3 million Pre-Commercial Procurement tender for EU hybrid cloud platform
  - support deployment of HPC and big-data capabilities for scientific research
- Challenged to enable access via SAML/eduGAIN and become SP in ELIXIR AAI
- WLCG is key use case, represented by CERN, CNRS, DESY, IFAE, INFN, KIT, STFC and SURFSARA as procurers
- Issues:
  - R&S bundle use not clear
  - Lack of central automated testing for SPs against IdPs
  - Lack of central point of contact for operational support
  - Lack of structured documentation for SP onboarding, service best practices
  - No native command-line option, need to be connected to complex AAI that follows the AARC blueprint, but is not suitable or feasible for some use cases
Common Requirements
Common Requirements

- Identity Lifecycle & Linking
- Discovery & Usability
- Authorization & De/provisioning
- Attribute Release
- Security Incident Response
- Research e-Infrastructure Proxies
- Assurance & MFA
- Consistent Operations
- Non-Web
- Onboarding & Support
- Sustaining Critical Infrastructure
Recommendations

- Governance & Sustainability
  - Research representation, funding for sustainable operation, ongoing coordination

- Baseline of User Experience
  - Attribute release, remove interoperability barriers, non-legal status, user mobility

- Security Incident Response Readiness
  - For federations, interfederation and organisations

- Harmonisation of Proxy Operations & Practices
  - Reuse generic services, follow best practices for interoperability

- Sensitive Research User Experience
  - Support multifactor authentication and publish Assurance Profiles
Recommendations

- FIM landscape changes, as do those providing a service
- Recommendations mapped to current stakeholders for ease

<table>
<thead>
<tr>
<th>Groups</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>GÉANT, Internet2, and R&amp;E federations</td>
<td>Increase research representation in FIM governance</td>
</tr>
<tr>
<td></td>
<td>Sustain operation of critical FIM services</td>
</tr>
<tr>
<td></td>
<td>Provide venues for ongoing coordination</td>
</tr>
<tr>
<td>Research funding bodies</td>
<td>Sustain operation of critical FIM services</td>
</tr>
<tr>
<td></td>
<td>Provide venues for ongoing coordination</td>
</tr>
<tr>
<td>Home organisations</td>
<td>Release Research &amp; Scholarship attributes</td>
</tr>
<tr>
<td></td>
<td>Provide usability essentials</td>
</tr>
<tr>
<td></td>
<td>Security Incident Response Readiness</td>
</tr>
<tr>
<td></td>
<td>Sensitive Research User Experience</td>
</tr>
<tr>
<td>R&amp;E federations</td>
<td>Release Research &amp; Scholarship attributes</td>
</tr>
<tr>
<td></td>
<td>Provide usability essentials</td>
</tr>
<tr>
<td></td>
<td>Remove interoperability barriers in eduGain metadata processes</td>
</tr>
<tr>
<td></td>
<td>Admit research organisations to federation</td>
</tr>
<tr>
<td></td>
<td>Security Incident Response Readiness</td>
</tr>
<tr>
<td>eduGain operator</td>
<td>Remove interoperability barriers in eduGain metadata processes</td>
</tr>
<tr>
<td></td>
<td>Security Incident Response Readiness</td>
</tr>
<tr>
<td>Research community proxies</td>
<td>Enable researcher mobility</td>
</tr>
<tr>
<td></td>
<td>Security Incident Response Readiness</td>
</tr>
<tr>
<td></td>
<td>Follow the proxy model and related AARC guidelines</td>
</tr>
<tr>
<td></td>
<td>Re-use shared AAI and related services</td>
</tr>
<tr>
<td></td>
<td>Sensitive Research User Experience</td>
</tr>
<tr>
<td>Research communities</td>
<td>Re-use shared AAI and related services</td>
</tr>
</tbody>
</table>
Read the paper at fim4r.org
Questions?