Authentication and Authorisation for Research and Collaboration

FIM4R - Requirements

Federated Identity Management for Research

David Kelsey
AARC2 Community Engagement/Policy and Best Practice Harmonisation
STFC – UK Research and Innovation

https://fim4r.org

Modified and shown at GridPP41 workshop 29 Aug 2018

Internet2 Global Summit, San Diego
9 May 2018

What is FIM4R? & the AARC Community Engagement Forum?

- Founded in 2011, FIM4R (Federated Identity Management for Research) is a collection of research communities (and some infrastructures)
- FIM4R collects requirements both on technical architecture, functionality and on operational policies
- These requirements may apply to R&E Federations or to the Research/e-Infrastructures
- The **Community Engagement Forum** helps AARC to best support the authentication and authorisation needs of research communities
- Research communities that participate in the Community Engagement Forum meet within the FIM4R (Federated Identity Management For Research) group

“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**

Who is represented? (open to all)

Research Fields

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

Experiences from Research Driven Services

- HNSciCloud
- ORCID

Identity Federation Projects/Communities

- AARC2
- GÉANT-GN4
- InCommon/Internet2
- REFEDS

FIM4R – Version 1 white paper

FIM4R

- Published a whitepaper in 2012 that guided the direction of identity federation for research *https://fim4r.org/documents/*
- Specified a common vision together with common requirements and recommendations
- Revised (just to specify priorities) in 2013

Federated Identity Management for Research Collaborations

Paper Type: Research paper

Date of this version: 28 August 2013

Abstract

Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

A number of laboratories including national and regional research organizations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries.

Driven by these needs, representatives from a variety of research communities, including photon/neutron facilities, social science & humanities, high-energy physics, atmospheric science, bioinformatics and fusion energy, have come together to discuss how to address these issues with the objective to define a common policy and trust framework for Identity Management based on existing structures, federations and technologies.

This paper will describe the needs of the research communities, the status of the activities in the FIM domain and highlight specific use cases. The common vision for FIM across these communities will be presented as well the key stages of the roadmap and a set of recommendations intended to ensure its implementation.

Keywords
federated identity management, security, authentication, authorization, collaboration, community

CERN-OPEN-2012-006
28/08/2013

Introduction

Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

A number of laboratories including national and regional research organisations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries. Many of the users have accounts at several research organisations and will need to use services provided by yet more organisations involved in research collaborations. All these identities and services need to be able work together without the users' being obliged to remember a growing number of accounts and passwords. As the user communities served by these organizations are growing they are also becoming younger and this younger generation has little tolerance for artificial barriers, many being the relics of technology and policies that could, if reasoned, also evolve. This "Facebook" generation [1] has triggered a change in the attitude towards IT tools. One expects to be able to share data, software, results, thoughts and emotions with whom they choose, when they choose. The boundaries between work and social life are less sharp, and it is expected that tools blend into this environment seamlessly. The interaction with commercial services such as the social networks must not imply that the users and research communities relinquish control over access to resources and security policies. The frequency of use will vary between the different users. Some will use these new tools continuously each day while others will log in a few times per year. This implies that operation has to be very intuitive, preferentially in a style known from common commercial devices and applications (PCs, smart phones, tablets etc).

FIM4R Version 2 - Aims & Methods

- In early 2017 FIM4R decided to start work on a Version 2 paper
- 5 years on, much had changed & time to review progress
- Representatives of more than 20 research communities have provided input
- Four face to face meetings in Europe and North America
- An final distillation of specific requirements is the result of this process

- **FIM4R – recent meetings** - *https://fim4r.org/events/*

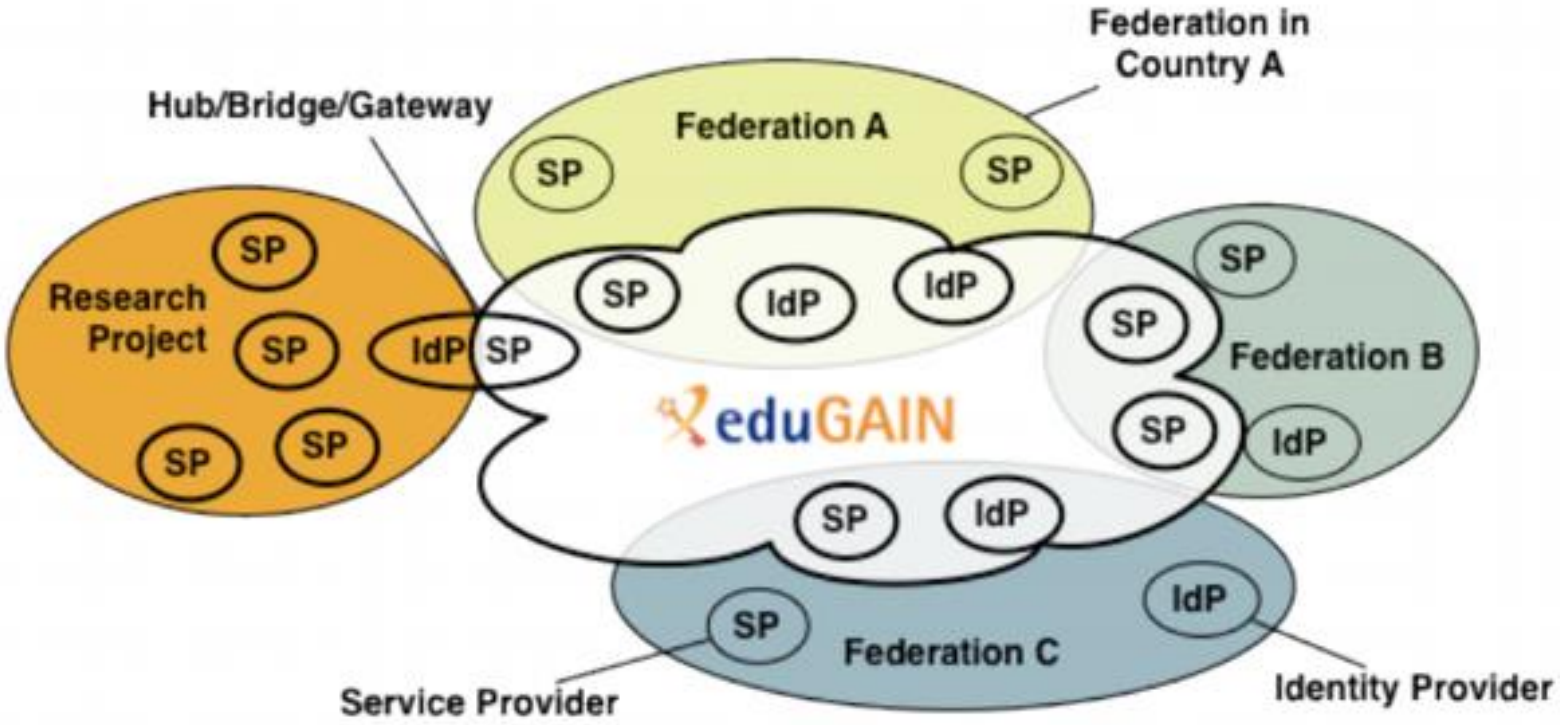
Dept. of Physics, McGill University, Montreal (Sep 2017)

Successes since FIM4R version 1

Much has changed since 2012 – AAI now more mature and many successes

- FIM4R paper was taken seriously
  - European Commission funding (H2020) for the AARC/AARC2 projects
- eduGAIN evolves towards an operational infrastructure
- Several research community successes
- Emergence of a “proxy” architecture (The AARC Blue Print Architecture)
- eduGAIN (as an Authentication infrastructure) – Authorisation by Communities
- e-Infrastructures deploying AAI services (EGI, EUDAT, GÉANT, EOSC-hub, …)
  - e.g. for Life Sciences
- Specific successes include: Sirtfi and Snctfi trust frameworks
- **But still many ongoing issues** – including 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

The Research Community SP/IdP Proxy



FIM4R version 2

- Published 9 July 2018
- https://doi.org/10.5281/zenodo.1296031

Federated Identity Management for Research Collaborations

C J Atherton[1], T Barton[2], J Basney[3], D Broeder[4], A Costa[5], M van Daalen[6], S O M Dyke[7], W Elbers[8], C-F Enell[9], E M V Fasanelli[10], J Fernandes[11], L Florio[1], P Gietz[12], D L Groep[13], M Junker[10], C Kanellopoulos[1], D P Kelsey[14], P J Kershaw[14,15], C Knapic[5], T Kollegger[16], S Koranda[17], M Linden[18], F Marinic[19], L Matyska[20], T H Nyrönen[18], S Paetow[21], L Paglione[22], S Parlati[10], C Phillips[23], M Prochazka[20,24], N Rees[25], H Short[11], U Stevanovic[26], M Tartakovsky[27], G Venekamp[28], T Vitez[23], R Wartel[11], C Whalen[27], J White[29] and C Zwölf[30]

[1]GÉANT Association, Amsterdam, The Netherlands; [2]University of Chicago, Chicago, Illinois, USA; [3]National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign, USA; [4]Nikhef, Amsterdam, The Netherlands; [5]INAF-National Institute for Astrophysics - Italy; [6]Paul Scherrer Institute, 5232 Villigen PSI, Switzerland; [7]McGill University, Montreal, Canada; [8]CLARIN ERIC, Utrecht, The Netherlands; [9]EISCAT Scientific Association, Kiruna, Sweden; [10]INFN - National Institute for Nuclear Physics - Italy; [11]European Organization for Nuclear Research (CERN), Geneva, Switzerland; [12]DAASI International, Tübingen, Germany; [13]Nikhef, Amsterdam, The Netherlands; [14]STFC UK Research and Innovation, Rutherford Appleton Laboratory, Didcot, United Kingdom; [15]NCEO (National Centre for Earth Observation), NERC, United Kingdom; [16]GSI Helmholtzzentrum für Schwerionenforschung, Darmstadt, Germany; [17]University of Wisconsin-Milwaukee (UWM), Milwaukee, Wisconsin USA; [18]CSC – IT Center for Science, ESPOO, Finland; [19]European Space Agency (ESA/ESAC), Madrid, Spain; [20]Masaryk University (MU), Institute of Computer Science (ICS), Brno, Czech Republic; [21]Inc, Harwell, United Kingdom; [22]ORCID Inc, Bethesda, Maryland USA; [23]CANARIE, Ottawa, Canada; [24]CESNET, Prague, Czech Republic; [25]SKA Organisation, Jodrell Bank, Lower Withington, Macclesfield, United Kingdom; [26]Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany; [27]National Institute of Allergy and Infectious Diseases, Rockville, Maryland USA; [28]SURFsara, Amsterdam, The Netherlands; [29]NeIC, Oslo, Norway; [30]Observatoire de Paris (Obspm), France

ABSTRACT

This white-paper expresses common requirements of Research Communities seeking to leverage Identity Federation for Authentication and Authorisation. Recommendations are made to Stakeholders to guide the future evolution of Federated Identity Management in a direction that better satisfies research use cases. The authors represent research communities, Research Services, Infrastructures, Identity Federations and Interfederations, with a joint motivation to ease collaboration for distributed researchers. The content has been edited collaboratively by the Federated Identity Management for Research (FIM4R) Community, with input sought at conferences and meetings in Europe, Asia and North America.

E-mail: contact@fim4r.org

For the ORCID® identifiers and author affiliations of the "Federated Identity Management for Research" collaboration to their various Research Communities and e-Infrastructures, see Appendix A.

Document details - Version: 2.0. Date: 9 July 2018
doi: 10.5281/zenodo.1296031

40 requirements in 11 groups

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

Some examples - Identity Lifecycle

Account Linking	The ability, for one entity, to link credentials from multiple IdPs to one account on an SP. More generically, the ability for a researcher to link multiple identities together, whether held in parallel or succession.
ORCID	ORCIDs have become a common requirement. There are several ways by which they can arrive at Research SP: from the home org IdP, integrated by a proxy, user login at ORCID IdP. The release of ORCIDs and their aggregation in community proxies should be prioritised.

Discovery & Usability

Smart discovery	IdP discovery should be "smart enough" to quickly and easily take a user to their appropriate home IdP. For example, show the user a short list tailored to them by home country, institute, e-Infrastructure, research community, project, or other hints.
Logo in metadata	Discovery services should display organization logos to aid the user in choosing the IdP. IdPs should provide a logo of an agreed standard size.
Service catalogue	Each research community should provide a service catalogue to help users find relevant resources, ie, service discovery.

Attribute Release & Adoption

Attribute Release	IdPs must release a unique, persistent, omnidirectional identifier, email address, and name for users when accessing research services. For example, ensure that R&S is widely adopted, or other means.
Entity Attribute Adoption Streamlining	Federations can take a long time to implement support for new entity tags and entity attributes, so in addition to federations implementing support for new entitiy attributes as soon as possible, the requirement is to find a work around to that problem that enables dependent research activities to proceed pending Federations completing their implementation.
Attribute release across borders	The R&S bundle, especially, needs to easily flow from IdPs to SPs without regard to their nationalities. More outreach of the risk analyses and R&S + CoCo entitiy categories is needed to increase adoption.

Security

Sirtfi adoption	To be acceptable to Research Comunities, an IdP must meet the requirements of Sirtfi and assert this in metadata.
Peer assessment of incident response performance	Provide a way for participants in a federated security incident response to provide feedback on how well each participant has performed, as an incentive to maintain good op sec processes.
Incident response communication channels	Next step after Sirtfi is to require the definition and maintenance of IR communication channels. These channels should be tailored to the incident scenario, involving only necessary people, and the contact points should be periodically checked for responsiveness. Assume that Snctfi addresses this with Proxied Research SPs.
IdP suspension	Abilty to disable all logins from identified IdPs as part of managing a security incident. Can happen by home federation or by Proxy.

Recommendations to Stakeholders

5.6 Mapping of Groups to Recommendations

Groups	Recommendations
GÉANT, Internet2, NRENS	Increase research representation in FIM governance Sustain operation of critical FIM services Provide avenues for ongoing coordination
Research funding bodies	Sustain operation of critical FIM services Provide avenues for ongoing coordination
Home organisations	Release Research & Scholarship attributes Provide usability essentials Security Incident Response Readiness Sensitive Research User Experience
R&E federations	Increase research representation in FIM governance Sustain operation of critical FIM services Provide avenues for ongoing coordination Release Research & Scholarship attributes Provide usability essentials Remove interoperability barriers in eduGAIN metadata processes Admit research organisations to federation Security Incident Response Readiness
eduGAIN operator	Remove interoperability barriers in eduGAIN metadata processes Security Incident Response Readiness
Research e-Infrastructures	Sustain operation of critical FIM services Re-use shared AAI and related services
Research community proxies	Enable researcher mobility Security Incident Response Readiness Follow the proxy model and related AARC guidelines Re-use shared AAI and related services Sensitive Research User Experience
Research communities	Re-use shared AAI and related services
REFEDS	Sensitive Research User Experience

FIM4R - Next steps

- A version 2.1 of the white paper is envisioned (next year?)
  - We still invite more contributions from other Research Communities
  - To incorporate input received too late for the version 2
- Also need to decide how best to track requirements and solutions
- Next F2F meeting of FIM4R during Trust & Identity Meeting in Vienna – Feb 2019

Thank you

Any Questions?

David.Kelsey@stfc.ac.uk

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).