Authentication and Authorisation for Research and Collaboration

FIM4R Version 2

Federated Identity Requirements for Research

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

https://fim4r.org

AARC2 All Hands Meeting, Athens
11 April 2018

ISGC2018 talk (20 Mar 2018) With many thanks to all FIM4R colleagues

- Co-authors: Tom BARTON (UChicago & Internet2); Peter GIETZ (DAASI & DARIAH); Scott KORANDA (LIGO & MWA); Hannah SHORT (CERN & WLCG)
  - Especially for material for these slides (Hannah and Tom)
- And other Version 2 paper authors/editors:

C Atherton (GÉANT)
J Basney (NCSA)
D Broeder (KNAW)
S Dyke (McGill)
W Elbers (CLARIN)
E Fasanelli (INFN)
H Flanagan (IETF)
L Florio (GÉANT)
D Groep (Nikhef)
M Hardt (KIT)
N Harris (GÉANT)
C Kanellopoulos (GÉANT)
P Kershaw (STFC)
C Knapic (INAF)
M Linden (CSC)
F Marinic (ESA)
B Moyer (NIH)
T Nyronen (CSC)
S Paetow (Jisc)
U Stevanovic (KIT)
G Venekamp (SURFsara)
C Wahlen (NIH)
J White (EISCAT 3D)
K Wierenga (GÉANT)
C-M Zwolf (VAMDC)

Outline

- What is FIM4R?
- FIM4R version 1 white paper (2012)
- FIM successes since version 1
- Aims of/methods used for version 2 paper
- The current list of V2 requirements
- Next steps

What is FIM? What is FIM4R?

- *"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*
- Founded in 2011, FIM4R (Federated Identity Management for Research) is a collection of research communities (and some infrastructures)
  - with a shared interest in enabling use of Federated Identity Management
- FIM4R collects requirements both on technical architecture and on operational policies
  - Relating to Federated Identity Management
- Note: these requirements may apply to R&E Federations or to the Research/e-Infrastructures
  - or to proxies and/or other components that link them together

FIM4R & AARC2 – The Community Engagement Forum

The **Community Engagement Forum** helps AARC to best support the authentication and authorisation needs of research communities by allowing communities to:

- **provide feedback** on AARC developments in policies, architectures and technical pilots
- **alert AARC** to new requirements
- **receive information about AARC** developments and opportunities to participate in AARC pilots and training
- Research communities that participate in the Community Engagement Forum meet within the FIM4R (Federated Identity Management For Research) group, which provides a **central reference point**
- In this way, AARC also supports and promotes FIM4R, making a win-win situation for the continuous engagement of everyone concerned

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
- 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

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).

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

Successes since FIM4R version 1

Much has changed since 2012 – and many successes

- eduGAIN evolves towards an operational infrastructure
- Several research community successes, e.g. Life Sciences, LIGO
  - Life Science AAI - Requirements specification
- Emergence of a “proxy” architecture (The AARC Blue Print Architecture)
- eduGAIN (as an Authentication infrastructure)
  - now augmented by other components
  - Critical components, especially Authorisation, are operated by Research Infrastructures
  - e-Infrastructures deploying AAI services (EGI, EUDAT, GÉANT, EOSC-hub, …), e.g. for Life Sciences
- FIM4R paper was taken seriously
  - Research Communities working together, timely input to funding agencies and federations
  - Paper was important input to the TERENA/EC “Study of AAA”
  - European Commission funding (H2020) for the AARC/AARC2 projects

Some specific successes

- Development and implementation of the Research & Scholarship Category
- Development and implementation of Sirtfi, a security incident response framework
- Snctfi, a trust framework for integration of Infrastructures with R&E Federations
- GÉANT Data Protection Code of Conduct to address data privacy issues
- Various solutions to non-browser federated access needs
- Experiments with defining solutions to Level of Assurance

Ongoing challenges

- eduGAIN still in process of becoming an operational service
  - With support and security operations
- National federations still vary a lot
- Some difficulties joining federations and/or eduGAIN
- Take-up of entity categories has been slow
  - R&S, Sirtfi
- Data Protection and Attribute Release is still a problem
  - Will EU GDPR and GÉANT DP Code of Conduct version 2 fix it?
- Must we give up on attribute release from Institute IdPs?

- Research Communities just want all this FIM/AAI “stuff” to be easy to use and just work!
- We still have a long list of requirements!

Aims & Methods – for version 2

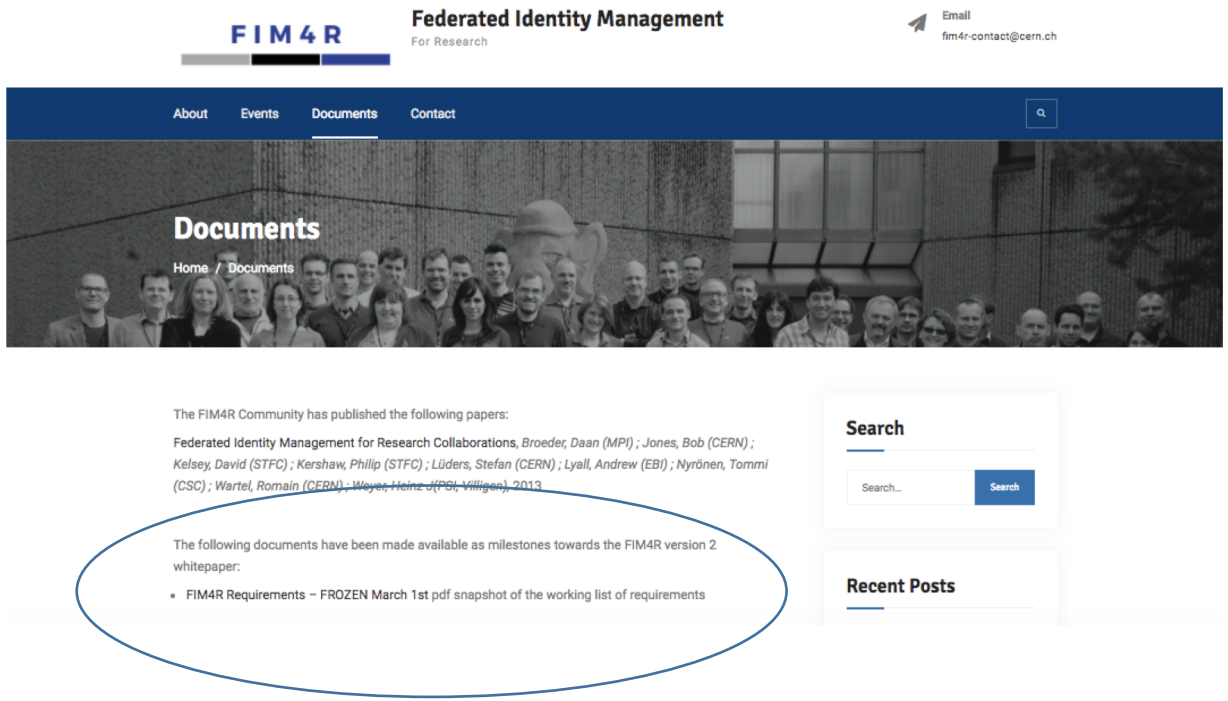
- In early 2017 FIM4R decided to start work on a Version 2 paper
  - 5 years on, much had changed & time to review progress
- Representatives of more than 20 research communities have provided input
- Four face to face meetings in Europe and North America
  - Presentations by research communities and e-Infrastructures were heard
  - discussion to integrate specific requirements within a stalking horse catalogue
  - sets of specific requirements were assigned to break-out group to reconsider
  - some requirements were removed, others merged, and language was sharpened
- An (almost) final distillation of specific requirements is the result of this process
  - those providing input are assigning endorsements to specific requirements
  - to ensure that each expresses a concrete need that is valuable to address

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

- Trust & Internet Identity (TIIME), Vienna – Feb 2017
- Montreal – Sep 2017
- Mini-meeting @ Internet2 TechX meeting
  San Francisco – Oct 2017
- Trust & Internet Identity (TIIME), Vienna – Feb 2018

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

FIM4R version 2 requirements – frozen draft on 1st March 2018



https://fim4r.org/documents/

Number of groups 11

Number of requirements 39

FIM4R Version 2 - Requirements Summary

Identity Lifecycle
- Linking & ORCID

Discovery & Usability
- Service Catalogues, IdP Logos & Smart Discovery

Authorization
- Realtime, deprovisioning, bona fide & resource allocation

Attribute Release & Adoption
- Attributes across borders & Entity Attributes

Security
- Suspension & Incident Response Channels

Research e-Infrastructure
- Federation support & proxy frameworks

Assurance
- Step-up & framework adoption

Usability
- Metadata handling & user experience

Beyond Web
- Alternative to ECP, translation & delegation

Onboarding & Support
- Federation dev environment, interfederation support & documentation

Critical Collateral Infrastructure
- IdP of last resort for all, sustainable operation

Some example requirements

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.

Have we missed anything? Would you like to join FIM4R?

- If your research community is struggling with an issue not mentioned, please speak out!
- Have all AARC2 communities contributed to FIM4R V2?
- All communities are very welcome
- Join the FIM4R community, email fim4r-contact@cern.ch

Next steps

- Complete and publish the version 2 white paper by end of May 2018
- Members of the editorial team plan a set of presentations at meetings in Europe (TNC18, RDA, CHEP), North America (PEARC18), and Asia Pacific (ISGC2018) to inform more communities and seed further input
- A version 2.1 of the white paper is also envisioned
  - To incorporate input received too late for the version 2
- In addition, major organizations that support R&E Federation such as Internet2, GÉANT, and REFEDS are already taking the version 2 preliminary findings into account as they plan their further activities.

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).