FIM4R Version 2: Federated Identity Requirements for Research

Thomas Barton[1], Peter Gietz[2], David Kelsey[3], Scott Koranda[4], Hannah Short[5]

What is FIM4R?

Federated Identity Management (FIM) is an evolving set of technologies, policies, and services that national Research & Education Federations implement to produce a global trust infrastructure for the R&E sector that enables login to (federated access to) protected resources with users' home organization credentials [1]. FIM4R (FIM for Research) is a collection of individuals from research communities, research cyber infrastructures that support them, and R&E Federations with a shared interest in enhancing how R&E Federations and research cyber infrastructures integrate to support the work of research communities. A key measure of success for R&E Federation is its uptake among research and academic communities. To promote this, FIM4R collects and rationalizes requirements bearing on technical architecture, services, standards, and operational policies needed to produce harmonious integration between research cyber infrastructures and R&E Federations. These requirements may apply to R&E Federations, the research cyber infrastructures, or proxies, portals, gateways, and other components that link them together. FIM4R members collaborate with organizations in both domains, R&E Federation and research cyber infrastructures, to help implement these requirements. A version 1 white paper [2] was produced in 2012 to document common requirements, a common vision, and recommendations.

FIM4R members are currently working on a second white paper to highlight the progress since 2012 and update requirements and recommendations to reflect current and anticipated trends and challenges.

FIM4R Version 1 and its Impact

The version 1 white paper was the result of gathering input from a variety of research communities and cyber infrastructures and distilling common high level requirements and recommendations from the input. These include

- User friendliness
- Federated access enabled with and without need for browsers

[1] Thomas Barton, University of Chicago and Internet2, tbarton@uchicago.edu
[2] Peter Gietz, DAASI International, peter.gietz@daasi.de
[3] David Kelsey, STFC Rutherford Appleton Laboratory, david.kelsey@stfc.ac.uk
[4] Scott Koranda, LIGO, scott.koranda@ligo.org
[5] Hannah Short, CERN, hannah.short@cern.ch

- Support for the multiple credential types in use by research cyber infrastructures
- Support for multiple Levels of Assurance to match different levels of risk associated with protected resources
- Control over authorization by research communities or research cyber infrastructure operators
- A well-defined set of user attributes that are appropriately available across the entire architecture
- Risk assessment, traceability, and a security incident response capability suited to this environment
- Transparency of the various policies by which organizations manage their users' federated credentials
- Reliable and resilient operations
- Scalable means by which to address legal, policy, and trust concerns with ensuring suitable security and privacy across this international and heterogeneous infrastructure

Substantial developments on all of these have occurred since the v1 white paper's publication. Highlights include:

- Development and implementation of the Research & Scholarship Category [3], a globally adopted program that defines a set of user attributes and helps to manage user privacy by disclosing them only to federated services independently vetted to be purposed for research or scholarly use.
- Development and implementation of SIRTFI [4], a security incident response framework adopted by R&E Federations, SNCTFI [5], a suite of policies that facilitate successful integration of cyber infrastructures with R&E Federations, and the GÉANT Data Protection Code of Conduct [6] to address data privacy compliance needs of federated organizations in the EU.
- Various solutions to non-browser federated access needs.
- Experiments with defining and fielding solutions to Level of Assurance needs [7], [8].
- Emergence of a proxy architecture [9] as the approach taken by multiple research cyber infrastructures to simplify their integration with R&E Federations.
- European Commission funding for the AARC and AARC2 projects [10], which convened and focused FIM4R members and others on identifying means to address the various requirements of the version 1 white paper, whose efforts helped to produce several of the above items and more.

FIM4R Version 2: It's Time to Update

Although the developments listed above are quite substantial, they have not fully addressed the problems at which they are aimed. Most R&E organizations do not yet participate in the Research & Scholarship Category or SIRTFI programs, and the Data Protection Code of Conduct has had to be revised in light of the General Data Protection Regulation [11], a process that is incomplete and whose outcome is as yet uncertain. The InCommon Federation

developed its Bronze and Silver Levels of Assurance but discovered that most of its member organizations found them too onerous to implement absent evidence of uptake by resource providers, and resource providers similarly did not rely on them because of, among other reasons, insufficient uptake by users' home organizations.

Whereas in 2012 many practitioners envisioned that every service in a research cyber infrastructure would directly join an R&E Federation, experience has shown that it is more practical and scalable to implement a proxy for them that is joined to R&E Federation. This centralizes credential translation, authorization management, and other functions in one place, avoiding the need to do so in each service within a cyber infrastructure and join it to R&E Federation. And a proxy helps to mitigate the shortcomings of the Research & Scholarship Category program by providing an alternate locus for managing needed user attributes. More generally, standards, technologies, architectures, and services have evolved over six years, as has what practitioners can envision. There are now good open source proxy platforms that address these needs, for example, and services such as ORCID [12] that provide new approaches to meeting some of the needs of research communities.

In early 2017 FIM4R members determined that it is time to look anew at how integration of FIM and research cyber infrastructures should continue to evolve and began a new cycle of gathering input from research communities and cyber infrastructures. Representatives of more than 20 research communities across physics, astronomy, climate and planetary science, life sciences, infectious diseases, and humanities, and their supporting research cyber infrastructures, have provided input thus far. Four face to face meetings in Europe and North America focused on this effort have occured. At three of them presentations by research communities and cyber infrastructures were heard, followed by discussion to appropriately integrate their specific requirements within a stalking horse catalog aggregating such. At another meeting sets of specific requirements were assigned to break-out groups to reconsider whether these were the right requirements, which lead to some requirements being removed, others merged, and sharpening of the language used to express those remaining. A nearing-final distillation of specific requirements [13] is the result of this process, and those who have provided input are in process of assigning endorsements to specific requirements to ensure that each expresses a concrete need that would be valuable to address.

An editorial team was established and is working towards completing 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 (ISGC) to inform further communities and seed further input. A version 2.1 of the white paper is envisioned in which input received too late for the version 2 paper can be incorporated. In addition, major organizations that support R&E Federation such as Internet2 [14], GÉANT [15], and REFEDS [16] are already taking the version 2 preliminary findings into account as they plan their further activities.

[1] http://doi.org/10.26869/TI.3.2
[2] https://fim4r.org/wp-content/uploads/2017/07/CERN-OPEN-2012-006-2.pdf
[3] https://refeds.org/category/research-and-scholarship
[4] https://refeds.org/sirtfi
[5] https://wiki.geant.org/display/AARC/Snctfi
[6] https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home
[7] https://www.incommon.org/assurance/
[8] https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group
[9] https://aarc-project.eu/architecture/
[10] https://aarc-project.eu/
[11] https://www.eugdpr.org/
[12] https://orcid.org/
[13] https://fim4r.org/wp-content/uploads/2018/03/FIM4R-Requirements-FROZEN-March-1st-TIIME-2018.pdf
[14] https://www.internet2.edu/
[15] https://www.geant.org/
[16] https://refeds.org/