AARC Authentication and Authorisation for Research and Collaboration

FIM4R Update

Authentication and Authorisation for Research and Collaboration

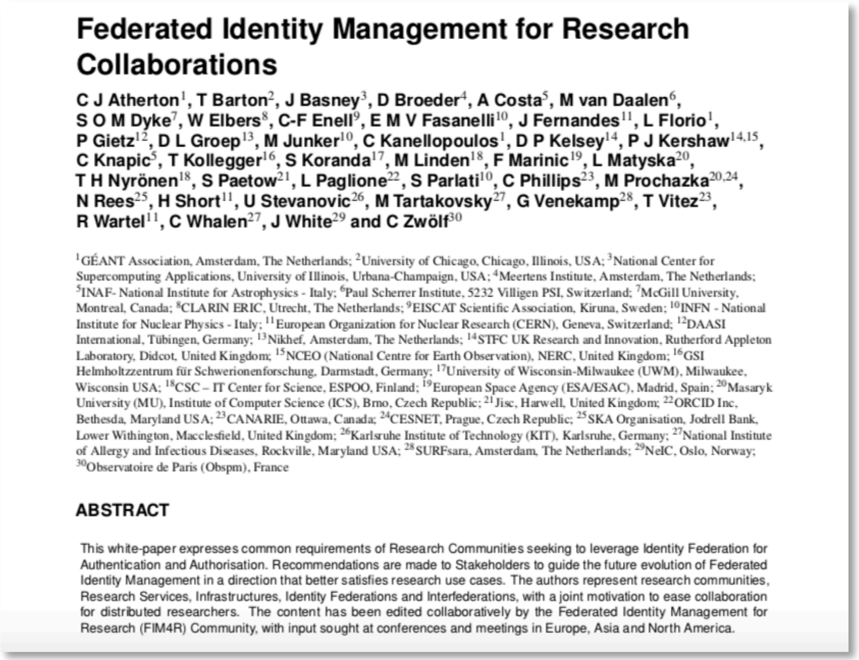
Presented by David Kelsey (STFC UK Research and Innovation)

Co-authors: Tom Barton, Peter Gietz, Hannah Short

REFEDS40, TNC19, Tallinn, Estonia
June 16th 2019

FIM4R.org

- *FIM4R (Federated Identity Management for Research) is a collection of research communities and infrastructures with a shared interest in enabling Federated Identity Management for their research cyber infrastructures*
- FIM4R version 1 paper – presented at TNC2012 in Reykjavik
- FIM4R version 2 paper – final draft published at TNC18
- http://doi.org/10.5281/zenodo.1296031
  - Published on 9 July 2018
- *40 Authors*
- *~40 Pages*
- *~40 Requirements*



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]Meertens Institute, 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]Jisc, 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.

13th FIM4R Meeting at TIIME event, Vienna – 11th February 2019

- Agenda and presentations at https://indico.cern.ch/event/775478/
- Many presentations from research communities, infrastructures and solution providers
- Discussion on tracking/monitoring the impact of the version 2 paper
- How do we track the solutions and improvements that address the 9 recommendations and 40 requirements expressed?
  - continued later in the week in a session during the TIIME 2019 conference
- Agreement:
  - FIM4R to survey/consult the stakeholders to whom the 9 recommendations were aimed
  - To be launched soon after REFEDS meeting at TNC19
  - The responses will be analysed in the form of a short status report (a version 2.1 paper) in 2020 (for TNC20?)

Recommendations from FIM4R version 2

Stakeholders/Groups

- GÉANT, Internet2, NRENs
- Research funding bodies
- Home organisations
- R&E federations
- eduGAIN operator
- Research e-Infrastructures
- Research community proxies
- Research communities
- REFEDS

Categories of Recommendation

- Governance and coordination
- Baseline of research user experience
- Security incident response readiness
- Harmonisation of research community proxy operations and practices
- Sensitive research user experience

Stakeholders, groups and recommendations (1)

Groups	Recommendations
GEANT, 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

Stakeholders, groups and recommendations (2)

Groups	Recommendations
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

Feedback on the impact of version 2 paper?

- Identifying/reaching out to stakeholders
  - Some are clear and obvious
  - We are asking REFEDS and R&E Federations today
  - Research communities – we will ask FIM4R
  - Research and e-Infrastructures – we know who they are
- Home organisations, funding bodies, NRENs …
  - Ask FIM4R and REFEDS members for info re these Stakeholders and their response to FIM4R v2
- We need your help today! Discussion now and "Sticky Notes" (all day!)
- What has changed in response to the V2 paper?
- Is there other FIM4R version 2 impact we are not yet aware of?
  - Even if not directly related to the recommendations/requirements
  - CACTI paper and Internet2 response has happened
- What should have happened by now and has not?

Sticky-note input

- Available all today
- Please contribute your knowledge, observations, thoughts
    - Please add your name (for contact/follow-up) if you are happy to (we will not publish your name)
- What impact have you witnessed (are you aware of) following publication of FIM4Rv2?
- What recommendations have already been satisfied?
- What has not yet been addressed (and should have been)?

- Or send e-mail to contact@fim4r.org

Other info and future meetings

- FIM4L (later today)
- (*Announcement from Hannah Short*) MFA chat on Tuesday 18th June - lunch with AAF
- (TBC) AAI meeting with DUNE (HEP Experiment) and others at FNAL or in the area
  - Certainly involves HEP community plus Infrastructures/federations – others?
  - A “mini” FIM4R
  - September 12th
- 14th FIM4R at Internet2 TechX – full day meeting – December 8th
- (TBC) 15th FIM4R at TIIME (whenever, wherever that is) – Feb 2020?
- Then finalise our V2.1 paper before TNC20

Following slides are the words used in the V2 paper to describe the recommendations aimed at R&E Federations and REFEDS

Increase research representation in FIM governance

- Organisations that envision or sustain critical FIM operations should plan and prioritise with input from all key stakeholders, including funders, planners, operators, architects, engineers and representatives of those to whom value of FIM is intended to accrue. At the time of this writing, some of the larger organisations in this space, such as GE´ ANT, Internet2, and some national R&E federations, include few researchers or research e-Infrastructure operators among those they consult with or are governed by. This has contributed to an increased focus on developing R&E federation to support enterprise applications. While that is valuable, it is incidental to the research and scholarly aspects of the academic mission. The expense and effort to provide a trustworthy infrastructure on which to securely manage collaborative access to research assets should be substantially undertaken by organisations whose mission it is to provide operational support to help enable research. Having sufficient research representation in their governance and advisory functions helps ensure the continued alignment of their actions with that mission.

Sustain operation of critical FIM services

- The availability of FIM is increasingly critical for researchers to perform their workflows. It is essential that FIM services be operated sustainably, reliably and with a level of user support appropriate for the breadth of research use cases. Testing environments, help desks and accessible documentation are highly important for new communities to navigate the policies and technologies underpinning FIM.
- The footprint of what needs to be sustained is also increasing as new elements of the overall FIM ecosystem become critical to research workflows. Researcher and research e-Infrastructure operator participation in an organisation’s governance processes can help identify operations that have become critical to the overall research enabling ecosystem and assess consonance with the organisation’s mission and its existing services to focus effort to create business or funding models to sustain them.
- By suitably highlighting and including FIM as direct costs for projects, programs, and solicitations, research funding bodies can also bring substantial influence and focus to critical FIM capabilities that should be sustained. Future e- Infrastructure projects should develop an interoperable mesh of complementary AAI solutions, building upon recognised best practices and supporting global research needs. The diversity of the research communities should be reflected in the AAI offerings; we do not see a single solution as a sustainable future.

Provide avenues for ongoing coordination

- To produce and maintain current and coherent actionable plans, collaboration among parties across the FIM ecosystem, including federations, research e-Infrastructures, and research communities, should be on a continuing rather than episodic basis. Interested parties who sustain FIM and AAI operations should programmatically establish avenues for this ongoing coordination.
- The mutual benefit of exchanging AAI experiences has been felt both by the research communities themselves and by the wider community, as projects and initiatives have been generated to resolve common issues. Such a forum should continue to be owned, supported and attended by research communities.

Release Research & Scholarship attributes

- Some research communities rely on their underlying proxies to obtain basic user attributes directly from users when users' home organisations do not supply them. However, the value of federation is maximised when all home organisations participate in the R&S Entity Category, removing that impediment from downstream operations and from the users. R&E federations should increase efforts to get all of their identity provider members who employ researchers and scholars to participate in this well-established program.
- To help identity providers in the EU address their obligations under the GDPR and so remove a further obstacle to releasing R&S attributes, research service providers and proxies that directly participate in any R&E federation and whose users include EU citizens and residents should support the Data Privacy Code of Conduct by implementing its recommendations and asserting a corresponding entity tag in their federation metadata. R&E federation operators must offer their service provider members a satisfactory means of adding this tag to their entity metadata.

Provide usability essentials

- Identity and service provider logos help users find their way and error URLs help them to get the right person's attention when something goes wrong. R&E federation members should ensure that all of their entity metadata includes these basic aides to good user experience. R&E federation operators can help by making this the objective of outreach campaigns with their members.

Remove interoperability barriers in eduGAIN metadata processes

- Users from different home organisations are not always able to access the same set of services because of the diversity of inconsistent practices followed by R&E federations in their handling of eduGAIN metadata. eduGAIN receives entities exported by each R&E federation and publishes an aggregate metadata file that R&E federations each import and publish within their federations. Different R&E federations implement different policies for determining which of their entities to export to eduGAIN, and similarly some R&E federations filter some entities from the eduGAIN aggregate before publishing the result to their members. When a research service is not exported to eduGAIN, no users from other R&E federations can access that service. When a research service is filtered, no user in the local federation can access it. When an identity provider is filtered, its users cannot access research services within the local federation.
- R&E federation operators should harmonise their eduGAIN export/import practices and ensure that eduGAIN itself addresses risks presented by entities sourced elsewhere, rather than each R&E federation doing so unilaterally. All R&E federations should support the ability of researchers and scholars at their member identity providers to access research services they need for their work.

Admit research organisations to federation

- Some research e-Infrastructure operators and research communities that are not legal entities also do not have their FIM interests represented by a legal entity participating in an R&E federation that can act on their behalf. This lack of legal standing can result in not meeting membership requirements for their national R&E federation, which precludes associated research communities from benefiting from FIM. Similarly, some research organisations, legally recognised or not, are intrinsically and essentially transnational, not aligned with membership of any specific national R&E federation. One or more R&E federations, or perhaps eduGAIN, should provide reasonable processes to include such cases into FIM and widely promulgate them across R&E federation operators. That way a positive answer can be given to the initial overture from such an organisation seeking to benefit from FIM.

Security Incident Response Readiness

- Organisations participating in R&E federations should apply best practices in operational security to their federated entities. They should also participate in security incident response frameworks such as Sirtfi and should be supported by their R&E federation operators in doing so.
- Each R&E federation operator, and the eduGAIN operator, should have a security incident response plan. These plans should be tested periodically.

Sensitive Research User Experience (aimed at REFEDS)

- The research community has substantial need to employ strong forms of authentication and access control to manage confidentiality of restricted research data sets and of preliminary results prior to publication, integrity of basic scientific data to ensure fidelity of its influence on public policy and to preserve academic attribution, and availability of specialised and expensive instruments and computing resources. Identity provider organisations are encouraged to provide strong authentication credentials to their researchers and implement the REFEDS MFA Profile to enable research service providers and proxies to signal when a user needs strong authentication to continue their activity and to acknowledge whether that has occurred. Identity assurance frameworks such as the REFEDS Assurance Framework should continue to be developed to respond to these needs.

Thank you

Any Questions?

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).