DRAFT
FIM4Rv2 Assessment for Internet2 Trust and Identity

(DRAFT - 10/13/2018)

Repository ID: TI.112.1
DOI: 10.26869/TI.112.1
Persistent URL: http://doi.org/10.26869/TI.112.1
Authors: Warren Anderson, Jill Gemmill, Karen Herrington, Chris Phillips, Nick Roy, David Walker
Publication Date: TBD
Sponsors: Community Architecture Committee for Trust and Identity (CACTI)

Background

On July 9, 2018, version 2.0 of Federated Identity Management for Research Collaborations (FIM4Rv2) was released by several authors representing research communities, Research Services, Infrastructures, Identity Federations and Interfederations, all with a joint motivation to ease collaboration for distributed researchers. The white paper was edited collaboratively by the Federated Identity Management for Research (FIM4R) Community, with input sought at conferences and meetings in Europe, Asia and North America. This paper has arrived at an important time for Trust and Identity, as Internet2 seeks to sharpen its focus for InCommon and the TIER initiative to address the community's projected future needs. Engaging researchers regarding middleware design is difficult, so having shared requirements identified and vetted by the research community is extremely valuable at this time. The FIM4Rv2 paper provides a consolidated view into several research-related organizations and their use of or need for federation.

On July 16, 2018, Kevin Morooney, Vice President of Trust and Identity Services for Internet2, requested the Community Architecture Committee for Trust and Identity (CACTI), to conduct a gap analysis and develop recommendations for meeting the requirements contained in the FIM4Rv2 paper. This is the result of that work.

Why Research Is Important to Internet2 Trust and Identity

> "The challenge of sharing resources within [LIGO] is formidable. One of the best tools for managing this challenge is federated identity." - David Reitze, Director of LIGO Laboratory, *et al*.

Research is an increasingly collaborative endeavor, spanning institutional and national boundaries. Large projects like the Laser Interferometer Gravitational Wave Observatory (LIGO) must respond to an ever-evolving community of researchers in need of access to LIGO's data, software, and collaboration tools. In instances where researchers are affiliated with institutions that have embraced federated identity management and the R&S profile, LIGO has been able to respond quickly, effectively, and securely to these needs. However, despite considerable effort and advocacy by LIGO and other large research collaborations, such as NIH's National Institute of Allergy and Infectious Diseases, CERN, and the Large Synoptic Survey Telescope (LSST), many institutions still lag behind in their IdP support for research. Thus, LIGO must continue to allocate significant resources toward enabling collaboration rather than directing those resources toward valuable research efforts.

Smaller research collaborations have similar needs for software and collaboration tools but are even more challenged in their ability to fulfill those needs. These smaller groups lack the resources to build their own tools and lack the necessary clout to advocate effectively for increased federation support from participating institutions. Even sharing one institution's resources using federated IAM (beyond a website) has proven to be difficult. As a result, smaller collaborations have adopted *ad hoc* tools that fail to provide a complete solution and fall outside of federated identity and access management infrastructure - for example, Google groups and Google docs. Where sensitive and/or

regulated data is concerned, CISOs are increasingly paying attention to how data is stored and accessed but may assert requirements that make collaboration even more difficult - eg: a university ‘X’ user account is required.

Internet2 is in a unique position to foster the InCommon federation’s support for research, particularly for smaller research projects and large projects with participants from small institutions. The Internet2 organization can lead efforts to create information resources, software, and services in support of the research collaborations themselves. Internet2 can advocate for support from home institutions and provide international leadership for coordination with other national federations. Collaboration infrastructures like eduroam that are readily deployed, and therefore pervasive, serve as a model for what is desirable and achievable.

Additionally, high quality services are the driving force behind adoption of Trust and Identity services. Improvements to services will aid in attracting new federation participants seeking services, as well as increase the usage and relevancy of services by new and existing participant institutions.

Our Approach

CACTI requested input from InCommon Technical Advisory Committee (TAC), the Community Trust Advisory Board (CTAB), and the TIER Component Architects, focusing on the FIM4Rv2 recommendations from section *5.6 Mapping of Groups to Recommendations* and listed in the table below.

Groups	Recommendations
GÉANT, Internet2, NRENS	● Increase research representation in FIM governance ● 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

The input we received from these groups is summarized in Appendix: Summary of consultation from INC-TAC, CTAB, TIER Tech-Archs.

Priority Recommendation: Invest in Areas to Support Collaboration-as-a-Service

While the Internet2 Trust and Identity Program does well overall, institutional IdP deployment choices have been driven primarily by important, but siloed, institutional requirements and risk-averse policy that may not have considered the value proposition of research collaboration. Most impacted are Researcher collaboration platforms. These platforms or instances of them delivered as-a-service are critical and continue to be difficult to find, challenging to implement, and often funding and resource starved. These factors hamper researchers and their ability to maximize their impact through collaboration both domestically and globally.

Internet2 should actively promote secure collaboration via the Trust and Identity Program, focusing on collaboration as a service that uses the following guiding principles:

- Research collaborations are fundamental to new knowledge discovery; thus, collaboration is core to student training and university research portfolios.
- Global collaboration solutions should be sustainable and evolve with current and future needs. This is a worthwhile investment for Internet2 and member institutions.
- A "ready for collaboration" reference best practice model for InCommon IdPs should be developed and maintained.
- New and existing components/tools for federated collaboration should be encouraged, incubated, or enhanced.
- Cataloging and adding to the set of collaboration tools able to use federated IAM will increase usefulness of InCommon to university faculty investigators.
- Expertise in use and implementation of these solutions in the field should be cultivated.

Internet2 can provide leadership by renewing its' focus in this direction. CACTI's recommendations in this context are:

1. **Internet2 should increase research representation in all levels of FIM governance**, including adding such representation to the Trust & Identity PAG and the Board of Trustees. Additional FIM governance groups such as CACTI, InCommon Steering, InCommon CTAB, TAC, and TIER Architects should continue to include representation and/or regular engagement with researchers and research infrastructure developers.

2. **Support for collaboration must include services as well as underlying infrastructure**
    - IdP-as-a-service is needed so that researchers from institutions both large and small can easily participate in collaborations both large and small.
    - Existing resources should be aggregated, documented and promoted (eg: federated IAM plug-in for WordPress, HubZero with a Federated identity module).
    - New applications need to be "domesticated" so that there are federated alternatives to Google docs. This will require on-going software development and a vehicle for discovering researchers' preferred applications.
    - Create an Internet2 "virtual office" or "non-profit marketplace" type center where research projects could go for service. (see TechSoup.org as an example) This could serve as a model for how campus IT can support their researchers.

    - Recruit pilot campus demonstration projects where COmanage (standalone and/or via CILogon) is used to support a campus collaboration.
    - Do rigorous promotion of current pilots that are using COmanage to replace parent/affiliate/guest account approaches.
    - Non-web applications, such as ssh, are not well supported. The existing technical solutions still need work and reference practices promoted as best practices.
3. **CILogon has become a critical service for existing collaborations as well as a foundation for broader collaboration**, **but there is currently no sustainability model.**
    - Internet2 should provide financial and staff support for CILogon, including developing a plan for assuming support and operation of CILogon.
    - COmanage and CILogon are underutilized TIER components. Internet2 should lead campuses in using identity mapping (associating multiple global identifiers, including gmail and OAUTH2 ids, with campus EPPNs).
4. **Establish TIER packaging default settings and profiles that support easy use of COmanage and CILogon.** TIER software is currently able to support these requirements, as evidenced by how well CILogon works for many large collaborations today. However, use of TIER software to support research collaborations will be a new approach for many campus IdPs. These expectations should currently include
    - support for R&S
    - ECP on
    - Follow Metadata requirements
    - Follow SIRTFI requirements
    - Support Multi-Factor Authentication, important for collaboration with sensitive data

    As FIM4R requirements are updated in the future, Internet2 Trust and Identity should review and update the baseline expectations.

Recommendation: Increase Focus on Sustainability Practices

The process to produce this one time report has been helpful to highlight opportunities to institutionalize some of the practices we are employing to assemble this report. CACTI believes that by choosing carefully what to engage on first we can act more quickly and be more informed to the benefit of our participants and have a more active role in the T&I outcomes and landscape.
To facilitate such an environment CACTI recommends:

- Assessments of the Internet2 trust and identity solutions be performed at predetermined intervals (if they are not already) to identify critical components that may have emerged since last review. This assessment should consider existing T&I portfolio items as well as emerging technologies and consider publishing it as a report publicly.
- The creation of a curated set of endorsed Best Community Practices (BCP) and tools for various components and solutions. This should encompass:
    - Internet2's technology portfolio and advocated as endorsed solutions.
    - A starting set of profiles as reference implementation profiles for configuring 'collaboration ready' IdPs and SPs and any other profiles as deemed necessary (e.g. eduroam configurations, proxy configurations etc)
- Mechanisms to assess and evolve with current and future needs should be embodied in the I2 technology portfolio described above.
- Communication and advocacy of the recommended patterns and practices should be explored to improve reach and adoption levels of tools and services.

- Improving discoverability of services and tools both domestically and globally will uncover new or existing components that we may be able to take advantage of or highlight partnerships.
- Actively cultivating expertise and in house knowledge of these solutions and BCPs in the field through
    - more self-paced training or partnering with bodies to grow our T&I professional capabilities from within our community.
    - Identifying partnerships with emerging or existing national platforms

Conclusion / In Summary

CACTI thanks the many Internet2 T&I working group subject matter experts who have been instrumental in reviewing and responding to the FIM4Rv2 work. Our recommendations are based on *your* insight and input. Our charge was to conduct a gap analysis and produce a set of recommendations. As we worked to get our arms around the many details involved, it became clear over time that providing Collaboration-as-a-service and increasing sustainability for these services addressed the most important gaps between FIM4Rv2 requirements and Internet2's current Trust and Identity program. For those who are interested in increasing levels of gap analysis detail we have included the contributions that we drew from in the appendices.

The FIM4Rv2 document while taking the better part of a year to gather and distill to its recommendations is a moment in time snapshot of researcher challenges. CACTI's recommendations embody a viewpoint that we should formalize regular assessment of how the T&I program is meeting community identified researcher requirements in addition to other university IAM needs.

With its renewed focus on support for university research, Internet2 and its member institutions can significantly address CACTI's recommendations by prioritizing existing people and resources to this purpose. For example, collaboration-as-a-service that addresses local researcher needs could be provided by campus IAM in coordination with Internet2 and other research support organizations. Should additional investments be needed, we hope all decision makers will recognize that support for research is a differentiator and also a growth opportunity.

While pragmatically selecting things that we know can be done with resources available to Internet2, T&I challenges are not limited to one organization but span the global ecosystem as inter-federation and interoperability are now table stakes. To address the challenges highlighted in the FIM4Rv2 report with the limited resources we have, global coordination and orchestration will be the most effective. Coordination should be with our global peers, organizations such as REFEDS, other NRENS and within the US, to national platform projects (eg: Science Gateways, Globus) so that we can maximize benefits for all partners if not all of the T&I ecosystem and reduce the overall energy to sustain such activities.

Appendix: Kevin Morooney's Request to CACTI

On 2018-07-16, "Kevin Morooney" <kmorooney@internet2.edu> wrote:

Hi Chris,

This note is a follow up on the FIM4R discussion that CACTI had at their July 10, 2018 call and a request to you for action.

The FIM4R document and the work that it represents is immensely important to Internet2 Trust and Identity. Engaging research alone is difficult and having them identify shared requirements is even more rare. It provides a consolidated view into several research-related organizations and their use of or need for federation that is very difficult to find.

CACTI is uniquely positioned to review the requirements and develop next steps, given the international representation and broad view of the body.

Engaging the Trust and Identity working groups (InCommon TAC and CTAB and TIER Component Architects), I request that CACTI conduct a gap analysis of and develop recommendations for meeting the requirements contained in the FIM4R paper. The final deliverable would contain an assessment that includes current support for the requirements (non gaps), planned support (activities in the workplan that are shortly to be kicked off), and recommended (new) activities that CACTI identifies as needing attention.

Ideally, I'd like to share the recommendations two weeks prior to TechEx, so we can have discussions there about how to address the new items. Please let me know if this timeframe is an issue.

I understand this is a big ask, so let me know if you need additional staff support outside Emily.

Many thanks for your support,

-kevin

Appendix: Summary of consultation from INC-TAC, CTAB, TIER Tech-Archs

What follows below is a record in one location results of our consultation with InCommon TAC, CTAB and TIER Technical Architects that contributed to forming the recommendations above. Not everything made it to the recommendation section and during the draft stage encourage review and questions. These do not appear in priority order and have allocation of contribution in the associated spreadsheet used during collection.

- **Partnership**. The needs of researchers evolve rapidly. All constituents (GÉANT, Internet2, NRENS, Home organisations, and R&E federations) must engage at multiple levels with researchers and their IT staffs on a continuing basis to assure that the needs continue to be met. The following recommendations from the FIM4Rv2 paper fall under this theme:
    - Increase research representation in FIM governance (GÉANT, Internet2, NRENS; R&E Federations)
    - Provide avenues for ongoing coordination (GÉANT, Internet2, NRENS; R&E Federations)
    - Admit research organisations to federation (R&E Federations)
- **User Experience and Functionality**. A user's experience with federated identity management is often difficult. This is, at times, related to gaps in the functionality, but is often related simply to lack of deployment of existing functionality Attention to this not only make the experience more pleasant, it can actually increase researchers' productivity. The following recommendations from the FIM4Rv2 paper fall under this theme:
    - Release Research & Scholarship attributes (Home Organizations; R&E Federations)
    - Provide usability essentials (Home Organizations; R&E Federations)
    - Sensitive Research User Experience (Home Organizations)
    - Remove interoperability barriers in eduGAIN metadata processes (R&E Federations)
- **Operations**. The infrastructure that supports federated identity management is crucial to successful research. It must operate reliably and be funded appropriately to sustain the infrastructure. The following recommendations from the FIM4Rv2 paper fall under this theme:
    - Sustain operation of critical FIM services (GÉANT, Internet2, NRENS; R&E Federations)
    - Security Incident Response Readiness (Home Organizations; R&E Federations)

In consultation with the InCommon Technical Advisory Committee (TAC), the Community Trust Advisory Board (CTAB), the Trust and Identity for Education and Research (TIER) Architects, and others, CACTI has identified the following gaps that currently affect research, along with potential actions for closing those gaps.

Partnership

Gap 1: Inadequate research representation in Trust and Identity's governing bodies and other activities.

- **FIM4Rv2 Recommendation**
    - Increase research representation in FIM governance.
    - Provide avenues for ongoing coordination (GÉANT, Internet2, NRENS; R&E Federations)
- **Observations**
    - This is crucial for continuing alignment with research's evolving needs.
    - The emphasis here not only on gathering research requirements; it is also on governance, *i.e.*, contributing to priority setting.
    - We need to take the cross-product pollination model from TIER and apply it to more. What if we had a forum for different research-based SPs to collaborate as well as to make their federation and identity needs known to the community?
    - While this feels like an item that Refeds, not InCommon, should be responding to, we clearly need some internationally agreed upon interop standards. All the work that has come out of InCommon WGs for interoperability should be considered for aligning eduGAIN metadata.
- **Potential Actions to Address This Gap**
    - Add researchers (practitioners and infrastructure providers) in the Trust & Identity PAG and any new TIER leadership bodies.
    - Increase research representation in the InCommon TAC, particularly representatives working on sensitive research.
        - Add a requirement in the TAC Operating procedures that requires at least one research representative on TAC.
        - Add language in the TAC Nominations template to request nominations of/from the Research community.
    - Create a research focused work group to give the community a common place to discuss these issues.
    - Identify champions from the research community to help coordinate and lead these efforts.
    - Need a pathway, steps by which further communities become aware of and vested in federation, before they might understand a reason for helping guide Internet2. CTAB should agendize an attempt to figure out such a pathway.

GAP 2: It is difficult for multi-institutional research collaborations to join InCommon.

- **FIM4Rv2 Recommendation**
    - Admit research organizations to federations.
- **Observations**
    - In order to preserve InCommon's trust model, any solution needs to address both policy/assurance, as well as providing useful services.
- **Potential Actions to Address This Gap**
    - InCommon should examine the possibility of extending the nascent Steward Program to allow one or more Research Community Stewards to onboard research IdPs and SPs in their community directly to InCommon.
    - Aggregate available resources and create an Internet2 "virtual office" or "non-profit marketplace" type center where research projects could go for service. (see TechSoup.org as an example)
    - Explore/discuss any expectations for SP Proxies, explore SNCTFI for inclusion into Baseline Expectations or FedOp

User Experience and Functionality

Gap 3: Current software and federation practice do not support inter-institutional collaboration well.

- **FIM4Rv2 Recommendation**
  - Provide usability essentials.
- **Observations**
  - Current group management software was designed more for intra-institutional use cases than inter-institutional use cases.
  - InCommon Participants are not required to provide the errorURL entity attribute in their metadata.
  - The InCommon community has adopted the Baseline Expectations for Trust in Federation (https://spaces.at.internet2.edu/display/TI/TI.34.1) to improve interoperability; however, adoption is currently at 75%.
  - Internationally, the vast majority of LIGO related IdPs do not conform to the InCommon Baseline in terms of Metadata, R&S attributes, and SIRTFI.
  - Non-web applications, such as ssh, are not well supported. The existing technical solutions still need work, but existing solutions should be promoted as best practices.
  - Things like logos, clear descriptions of the roles of different on-campus IdPs, meaningful failure modes, etc can be facilitated by home organizations and make user experience far less frustrating.
  - Best practices for logos and pages reference by error URLs are needed for international adoption.
  - Researchers from institutions that have not federated their IAM systems are not well served. An IdP of Last Resort that releases R&S attributes and can be used internationally is needed.
  - InCommon members need to be more educated related to the release of R&S attributes. GDPR and related regulations for privacy and consent need to be reviewed carefully and consent modules added to TIER or refeds.
  - Researchers' federated identifiers change when the researchers move to new institutions, causing administrative and technical issues for virtual organizations. ORCIDs, being institution-independent identifiers, are a potential mitigation for this.
- **Potential Actions to Address This Gap**
  - Make release of the R&S attributes a requirement under Baseline Expectations (as recommended by the Attributes for Collaboration working group).
  - CTAB will initiate a Community Consensus Process on requiring release to R&S (or MORE) for IdPs in the next version of Baseline Expectations
  - Create a pilot that uses CoManage at a campus for identity aggregation and inter-institutional collaboration and/or guest/affiliate accounts.
  - TIER architects should clearly document how federation and multiple IdP provisioning can be handled in the TIER components.
  - Home institutions should provide errorURL (as defined in the SAML "MDUI Information" specification) in their the entity attributes in addition to those required by Baseline Expectations.
  - Add errorURL into Baseline Expectations. Identify a group or instantiate a group to solve this problem. Next step: raise issue at REFEDS18.

    - InCommon should coordinate with eduGAIN to adopt similar baseline requirements and recommend the same to other federations.
    - The release of ORCIDs and their aggregation in community proxies should be prioritized.
    - Promote deployment of ECP in IdPs.
    - Promote international best practices for logos and pages referenced by error URLs.
    - Promote deployment of consent (or dissent) mechanisms by home institutions to facilitate attribute release when institutional policy requires individuals' permission.
    - Promote deployment of attribute release base on groups whose membership is determined by virtual organizations.
    - Provide an IdP of Last Resort that releases R&S attributes and that can be used internationally.

Gap 4: Sensitive research is not supported well.

- **FIM4Rv2 Recommendation**
    - Sensitive Research User Experience
- **Observations**
    - This is a multi-faceted issue, but broad support for multi-factor authentication is a big step forward.
- **Potential Actions to Address This Gap**
    - Home organizations should support the REFEDS MFA profile.
    - InCommon can help home organizations by providing encouragement and technical resources.
    - Add support for MFA to baseline.
    - Continue monitoring of and participation in REFEDS Assurance WG.

Gap 5: Access to services across national borders is inconsistent.

- **FIM4Rv2 Recommendation**
    - Remove interoperability barriers in eduGAIN metadata processes
- **Observations**
    - R&E federations export and import eduGAIN metadata according to local policies. This causes confusion for international research collaborations, as researchers may or may not have access to services, depending on their home country.
    - The R&S bundle needs to easily flow from IdPs to SPs without regard to their nationalities.
- **Potential Actions to Address This Gap**
    - InCommon should advocate that R&E federation participants in eduGAIN need to establish common policies metadata import and export. Where possible, the implementation of these common policies should be moved to eduGAIN.
    - InCommon should advocate release of the R&S attribute bundle without regard to their nationalities. More outreach of the risk analyses performed by GÉANT and REFEDS about R&S + CoCo entity categories is needed to increase adoption.

Operations

Gap 6: Services critical to research do not always have sustainable funding.

- **FIM4Rv2 Recommendation**
  - Sustain operation of critical FIM services
- **Observations**
  - The InCommon fees increase enacted by Steering in late 2016 was a good start on this, but further sustainable funding for operations and new initiatives need to be sought out.
  - One or more "component" services, *i.e.*, that are integrated with others to produce a valuable result, such as CILogon, have become established as a critical element of federated e-Infrastructure. Research communities look to Federations to ensure sustainable operations of those services.
  - The CILogon service integrates COmanage, which also requires sustainable funding.
  - Research infrastructure builders must operate their own IdPs of Last Resort to accommodate researchers whose home organizations do not support federation.
  - Charity begins at home: InCommon needs to set an example for others to follow. Sustainable federation-operated services like an MDQ service is a start. If TIER proves to be sustainable, it offers another model that others can follow.
- **Potential Actions to Address This Gap**
  - Find additional, sustainable funding for some research-specific needs.
  - An IdP of last resort with good identity vetting should be provided with sustainable funding. High value identities require strong identity registration, which InCommon is not set up to do. However, a third party such as MorphoTrust could be engaged to investigate some kind of a partnership to enable this.
  - Ensure ongoing support and development for CILogon and COmanage.
  - Continue publishing health check information while useful to promote the health of the FIM services.

Gap 7: An international, efficient incident response system is needed.

- **FIM4Rv2 Recommendation**
  - Security Incident Response Readiness
- **Observations**
  - A coordinating body for proactive security measures is needed--should be the same group. InCommon, REN-ISAC and Trusted Introducer have had some initial conversations about this, and the SIRTFI tabletop that was conducted in early 2018 is a step in a good direction, but there has been little to no follow-up on the results of that tabletop.
  - The scale of the research matters a lot here. If you are large enough to have representation in REN-ISAC, or even dedicated security persons employed, this is less necessary, but small research groups are in a far more precarious position if their is a vulnerability in their FED-ID software or if there is an incident that might affect them.

    - This is actually quite challenging in the US. Principle Investigators don't prioritize security, and CSOs focus on sensitive data.
    - We need more campaigning of SIRTFI from InCommon to our members. Clearly, SIRTFI becomes more valuable as more members adopt it, and it seems like the federation can provide more guidance and resources to help with that. Also, once we have more SIRTFI adopters, we need a well-defined international clearing house.
- **Potential Actions to Address This Gap**
    - InCommon should facilitate/lead development of an international organization (similar in function to REN-ISAC) that can provide an effective, global response team. Ensure that such an organization can address the needs of both large and small research groups.
    - Implement the ability to disable all logins from an identified Idp as part of a SIRFTI response.
    - Require SIRTFI as part of Baseline Expectations.
    - Queue up Community Consensus Process on adding SIRTFI into Baseline Expectations.
    - Recommend InCommon establish a SIRTFI dashboard.
    - Continue monitoring of and participation in the SIRTFI WG.