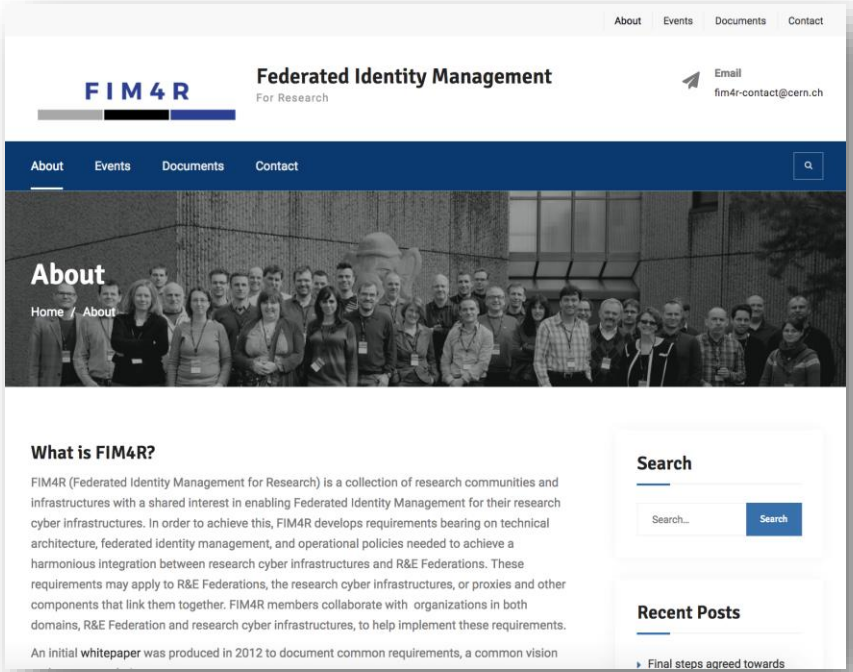
FIM4R

Progress towards the version 2 Whitepaper

Background

- The Federated Identity Management for Research Community
  - Wrote a whitepaper in 2012 that guided the direction of identity federation for research *https://fim4r.org/documents/*
  - Formed the RDA FIM IG
  - Currently writing an updated version of the whitepaper



https://fim4r.org/about/

Who is represented?

Research Fields

- High Energy Physics
- Life Sciences
- Humanities
- European Neutron and Photon Facilities
- Climate Science
- Earth Observation (EO)
- Gravitational Wave Astronomy
- Nuclear Physics
- Gamma-Ray Astronomy
- Infectious Disease Research
- Radio Astronomy
- Virtual Atomic and Molecular Data Centre
- Ionospheric and Atmospheric Science

Experiences from Research Driven Services

- ORCID
- HNSciCloud

Identity Federation Projects/Communities

- AARC (Authentication & Authorisation for Research Collaboration, European Commission Project)
- GN4 (GEANT 4, European Commission Project)
- REFEDS (Research and Education Federations Group)

Current Status of FIM4R v2

- Requirements have been gathered since September 2017
- Requirements analysis has taken place at
  - Pre-meeting & RDA 10th Plenary (Montreal, September 2017)
  - Internet2's TechEx (San Francisco, October 2017)
  - TIIME (Vienna, February 2018)
  - Multiple online meetings
- Research Communities are finishing their contributions to the paper
- Aiming to publish by June in an open repository

Frozen as of March 1st 2018

REQUIREMENTS

Requirements Summary

Identity Lifecycle
- Linking & ORCID

Discovery & Usability
- Service Catalogues, Identity Provider 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 (Enhanced Client Proxy for non-web), translation & delegation

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

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

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.

Authorization

Realtime authorization	AuthZ decisions at an SP must be based on identity credentials, attributes or assertions that have a short lifetime, i.e. they are valid now and not for too long into the future. Even within this short period it should be possible for the SP to look up realtime status information, e.g. revocation lists and/or suspension lists.
User blocking	It must be possible for an Infrastructure or Research Community to block access to a service based on the presence of an identity credential in an operational suspension list or revocation list.
Service Provider Quota Management & Resource allocation and accounting	It must be possible for an SP operator to limit access of an individual identity or a group, or by attributes or roles allocated to the identity by the IdP or the research community AA/Proxy, to subject them to quotas and make resource allocations. Usage records (accounting) must be possible at the same granularity.

Authorization

Deprovisioning	Deprovisioning of AuthZ attributes, assertions, credentials, tokens, or other artifacts is an essential part of access life-cycle management. It must be possible to suspend or remove an individual's access when they no longer possess right of access, e.g. because they have left the research community. Some use cases may require immediate removal of access while others may only require removal in an identified determinate period of time.
Bona-Fide users for registered access	For controlled access ("registered" access) to a dataset or other resources, it must be possible to grant this only to those users have been proven to have bona fide rights to access. Bona Fide researchers must be identifiable.
Group Management	Research Communities must be able to add individuals to Groups, for use in AuthZ, Quota management and Accounting. Groups should be hierarchical and users can belong to more than one group.
Active role selection	Individual users must be able to select which attributes, groups or roles are "active" for a particular connection request and AuthZ decision. For example, a user may wish to separate sessions as a researcher and as an administrator for a service.

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 Research & Scholarship 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 Research &Scholarship 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 (Security Incident Response Trust Framework for Federated Identity) 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.

Research e-Infrastructure

IdP/SP Proxies must be allowed to join edugain	We require support of an IdP/SP Proxy so that only the proxy has to join eduGAIN. This pertains to both federations and Research Communities.
Research Communities voice	Representation of Research Communities needs should be incorporated into eduGain governance with the ability to influence (inter)federation. Similar for REFEDS.
Snctfi (Scalable Negotiator for a Community Trust Framework)	Research Communities should become Snctfi compliant for scalability and ease of management, enabling a Proxy to meet operational and policy obligations of both worlds that it interconnects: the Research Comunity and eduGain. Federations should accept a Snctfi'd Proxy as meeting its R&S, Sirtfi, and CoCo obligations.
.int for R&E federation	Some research organisations have parts in multiple countries, making membership in one national R&E federation problematic. eduGain should provide a federation home for them.

Assurance

Assurance Framework	The international community should continue work on developing assurance profiles to meet the evolving requirements of research communities.
Step up Auth/MFA (Multi Factor Authentication)	Strong authentication, eg MFA, is required for some research community activities. The inclusion of MFA information in authentication tokens and metadata should be supported.

Usability

Consistent metadata handling practices	Federations should support standard metadata propagation processes and, where out of bands actions are required, provide clear documentation and support in order to avoid user and interoperability issues due to inconsistent handling.
Identity Provider deployment profile	Specify precisely what conditions IdPs must meet in order to provide federated credentials in research collaborations. Eg, Sirtfi + R&S. FIM4R to define the deployment profile and IdPs to adopt it.
Federation entity attributes designed to enhance user experience should be populated	Eg, the entity attributes defined in the SAML "MDUI Information" specification and errorURL should be populated, at least.

Beyond Web

Non-web use cases & support	Many interactions between clients and servers are via the user's command-line or via interacting applications using API access to AAI. Cannot assume that all access will be via a web browser interface, or that a web browser will be part of the authentication flow, even beforehand to set things up. Strong authentication (not necessarily MFA) may be required for some use cases.
! ECP	One way of solving non-web access is via the use of SAML-ECP, which is not widely adopted by IdPs. Certain services currently depend on this, but other good means are available that should be used in preference. Hence, this requirement is to retool where ECP is currently present.
Delegation	Delegation here means providing end-entities (users) ability to give a constrained portion of their access to another entity acting on their behalf. This might be reasonably accomplished either by impersonation or by proper delegation. This is required in any use case in which a work-flow continues without the presence and direct connection of a user.
Credential translation	Services will not always be able to consume the credentials the user currently has. Translations from one type of credential to another is a very common and important requirement.

Onboarding & Support

Non-legal entity participation in eduGain	Research Communities are often not legal entities. This causes problems should they wish to join federations and eduGAIN. One insititute does not wish to take on liability for the actions of others in the community.
eduGain test/dev environment	Easy-to-use testing environments to allow new Proxies and new SPs to experiment with their Federation-facing parts without interfering with existing production deployments.
Simple process for scientific SPs to become relying parties	Develop guidance and corresponding on-boarding process to address questions such as: How does a new research SP become a relying party? And an RP of what? Relying parties through a Federation, or behind a proxy?
Help Desk	Federations and eduGAIN should provide a Help Desk capability suited to supporting interactions between federations and research communities.

Critical Collateral Infrastructure

IdPoLR (Identity provider of last resort)	Provide sustained services to meet the many cases where global researchers do not have access to an acceptable Home Organization IdP, as an alternative to each Research Community solving this problem for itself.
IdPoLR not-a-robot	Google-based captcha is not available to some users in China, so another approach to not-a-robot must be determined.
Sustainable operation of specified critical services	When a "component" service, i.e., one that is integrated with others to produce a valuable result, becomes established as a critical element of federated e-infrastructure, Research Communities look to Federations to provide sustainable operations.

NEXT STEPS

Have we missed anything?

- If your research community is struggling with an issue not mentioned, please speak out!
- Join the fim4r community, emailfim4r-contact@cern.ch

Next Meetings

1. The FIM4R activities will be presented at ISGC in Taipei, Taiwan on March 20th
2. The FIM4R version 2 whitepaper will be published on Zenodo
3. The completed version 2 whitepaper will be presented at the FIM4R session at TNC18, in Trondheim, Norway on June 12th.

We hope to see you there!