FIM4R

Presenting the 2nd Whitepaper

With thanks to the FIM4R Editors and Contributors for their collaboration on the whitepaper and the following slides.

LIGO VIRGO

EISCAT SCIENTIFIC ASSOCIATION

umbrella

DARIAH-DE
Digital Research Infrastructure
for the Arts and Humanities

WLCG
Worldwide LHC Computing Grid

elixir

SKA
SQUARE KILOMETRE ARRAY

KAGRA

CLARIN

INFN
Istituto Nazionale di Fisica Nucleare

VAMDC
Virtual Atomic and Molecular Data Centre

FAIR

LIGO

cta
cherenkov telescope array

HELIX NEBULA
THESCIENCECLOUD

CORBEL

ESGF
Earth System Grid Federation

esa

National Institute
of Allergy and
Infectious Diseases

*** Not all contributors' logos represented*

Agenda

- Introduction & Motivation
- Progress since 2012
- Research Community Use Cases
- Common Requirements
- Recommendations
- Next Steps

Introduction & Motivation

Motivation

- Research Communities provide complex use cases where federated identity can be leveraged to great effect
  - Distributed users
  - Distributed services
- The specific way of working brings specific challenges that go beyond the functionality typically offered by federations and interfederation
  - Global accessibility
  - Non-web use cases

FIM4R provides a forum for Research Community representatives to exchange experiences of implementing AAI and by combining our voices we hope to influence the future direction of FIM in a way that meets the needs of our Users

“Every researcher is entitled to focus on their work and not be impeded by needless obstacles nor required to understand anything about the FIM infrastructure enabling their access to research services.” **FIM4R version 2**

2012: FIM4R version 1

- 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

2018: FIM4R 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
- A new distillation of specific requirements and a set of recommendations is the result of this process

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

Who is represented?

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

Others

Research Driven Services

- HNSciCloud
- ORCID

Identity Federation Projects/Communities

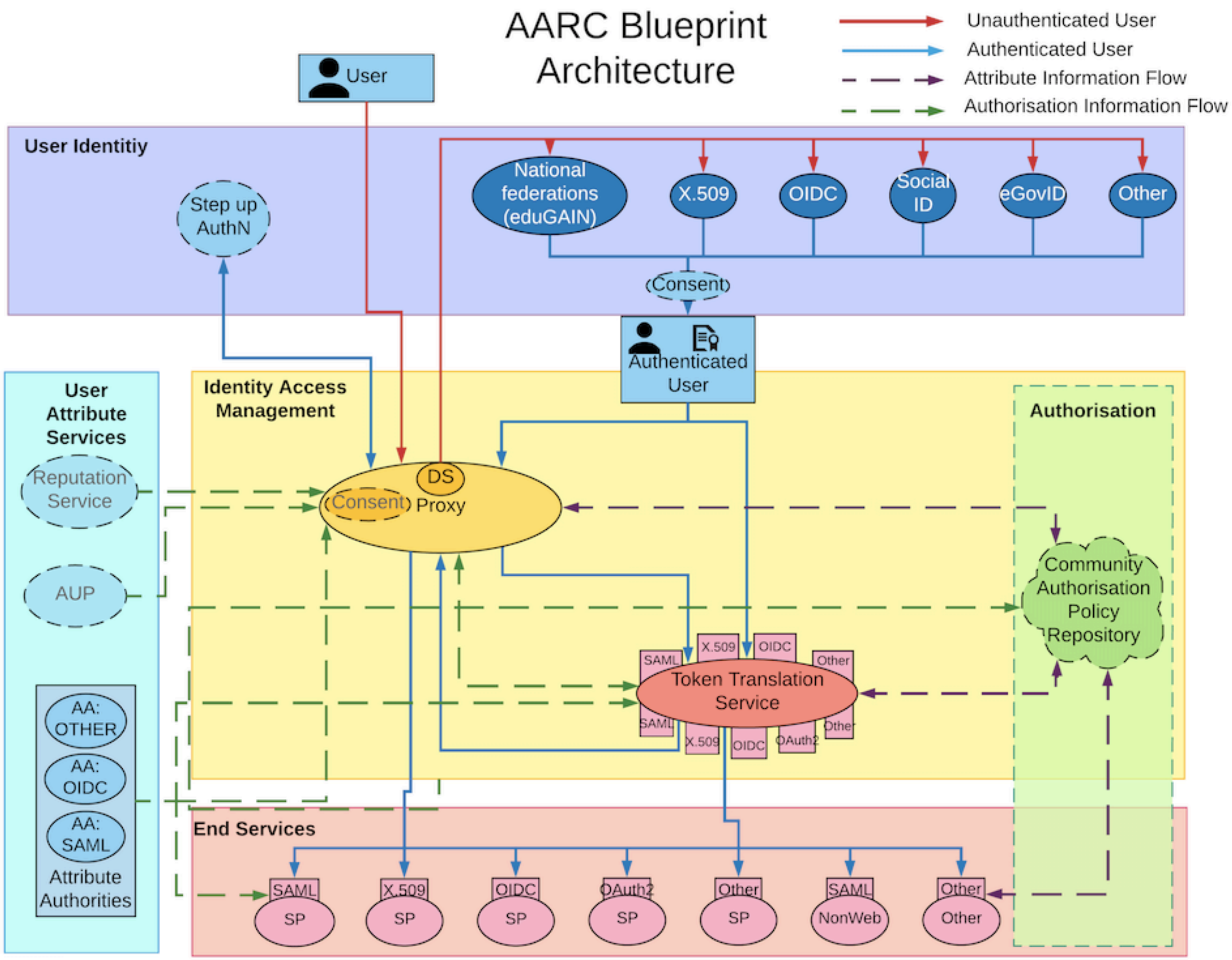
- AARC(2)
- GÉANT-GN4
- InCommon/Internet2
- REFEDS

Progress since 2012

Successes

Much has changed since 2012. The FIM4R paper was taken seriously – AAI now more mature and many successes

- European Commission funding (H2020) for the AARC/AARC2 projects
- Federations and interfederation have found their role as an Authentication infrastructure; Authorisation managed by Communities
- eduGAIN’s operational support capability is now in place and maturing
- e-Infrastructures are deploying shared AAI services (EGI, EUDAT, GÉANT, EOSC-hub, …)
- Specific successes include: Sirtfi and Snctfi trust frameworks
- Standardisation and best practices for the emerging trend of “proxy” architecture (The AARC Blue Print Architecture)



https://aarc-project.eu/architecture/

Outstanding Challenges

- Usability & User Experience
- Data Privacy and EU GDPR
  - Better data access and privacy expectations need to be balanced, E.g. ELIXIR Human Data resources are potentially liable for breaches
  - Attribute release by risk averse IdPs is already problematic, this may be aggravated
- Interfederation and many federations do not offer an adequate level of operational support and security
- Several generic AAI infrastructures are evolving but their respective advantages and availability are unclear

Research Community Use Cases

NIAID

- National Institute of Allergy and Infectious Diseases Virtual Research Organization Platform
- International Centers for Excellence in Research built in Bamako, Mali; Entebbe, Uganda; and Chennai, India
- Key challenges
  - Many independent research institutions and foundations are unable to join their domestic federations
  - No attribute release led to creation of NIAID accounts for many users, rendering FIM pointless
  - Commercial software expecting 1 IdP (e.g. cloud services), implementing proxy architecture helped

WLCG

- Worldwide LHC Computing Grid
- Certificate federation in use, looking to move to a multi-credential proxy model leveraging eduGAIN
- Key Challenges
  - Security Incident Response at all Identity Providers
  - Sustainably operated components, such as Token Translation
  - Robust operational support for federations and interfederation

Common Requirements

FIM4R Version 2 – Frozen draft on 1st March 2018
https://fim4r.org/documents/ (11 groups, 39 requirements)

- Identity Lifecycle & Linking
- Discovery & Usability
- Authorization & De/provisioning
- Attribute Release
- Security Incident Response
- Research e-Infrastructure Proxies
- Assurance & MFA
- Consistent Operations
- Non-Web
- Onboarding & Support
- Sustaining Critical Infrastructure

Some examples - 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.

Recommendations

Overview

Governance & Sustainability

- Research representation, funding for sustainable operation, ongoing coordination

Baseline of User Experience

- Attribute release, remove interoperability barriers, non-legal status, user mobility

Security Incident Response Readiness

- For federations, interfederation and organisations

Harmonisation of Proxy Operations & Practices

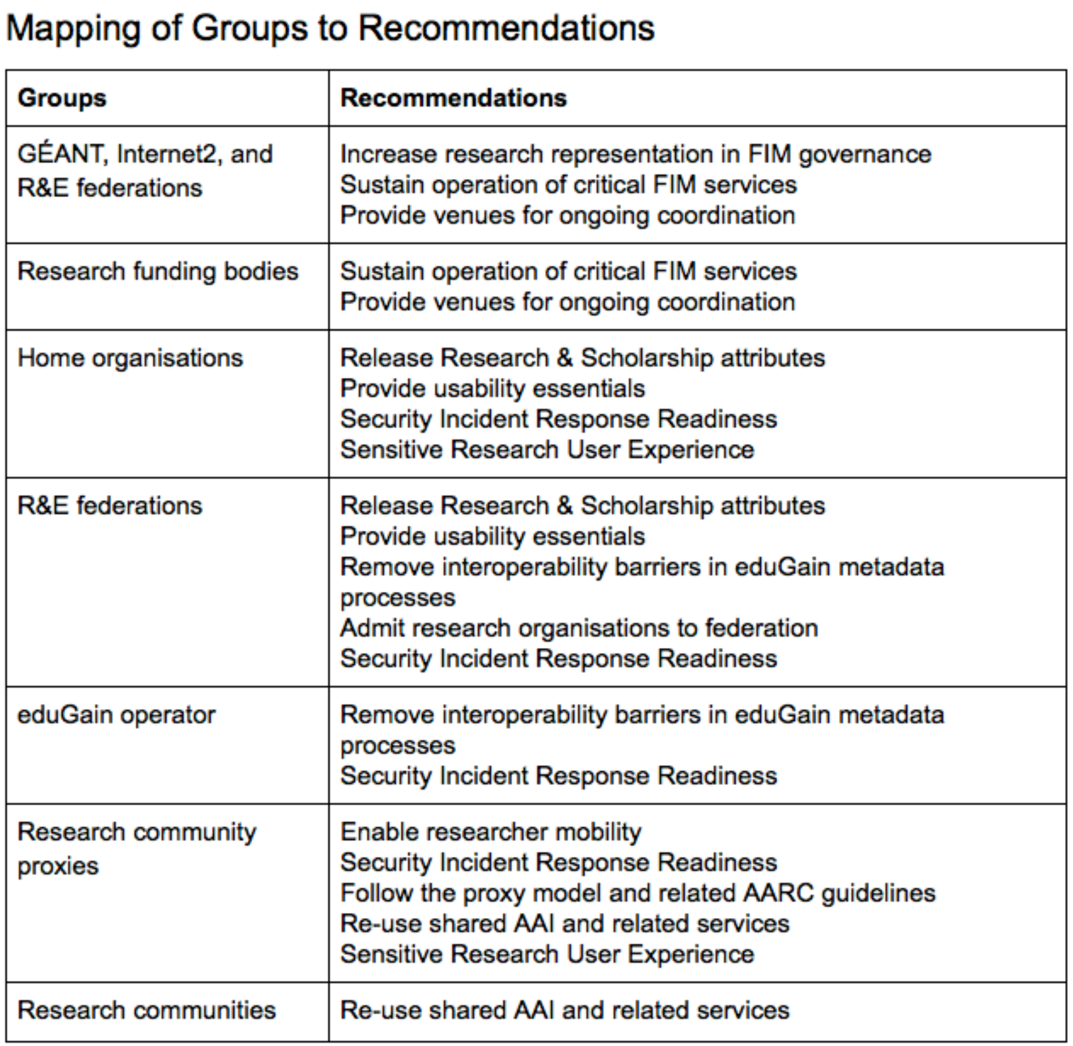
- Reuse generic services, follow best practices for interoperability

Sensitive Research User Experience

- Support multifactor authentication and publish Assurance Profiles

Recommendations

- Landscape changes, and those providing a service do too
- Recommendations mapped to current stakeholders for ease



Mapping of Groups to Recommendations

Groups	Recommendations
GÉANT, Internet2, and R&E federations	Increase research representation in FIM governance Sustain operation of critical FIM services Provide venues for ongoing coordination
Research funding bodies	Sustain operation of critical FIM services Provide venues for ongoing coordination
Home organisations	Release Research & Scholarship attributes Provide usability essentials Security Incident Response Readiness Sensitive Research User Experience
R&E federations	Release Research & Scholarship attributes Provide usability essentials Remove interoperability barriers in eduGain metadata processes Admit research organisations to federation Security Incident Response Readiness
eduGain operator	Remove interoperability barriers in eduGain metadata processes Security Incident Response Readiness
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

Next Steps

Next Steps

- Currently finalising the draft
- Aiming to publish on Zenodo in the coming weeks
- Whitepaper will be widely circulated
  - Federation and interfederation governance
  - Technology Providers
  - The FIM Interest Group of the Research Data Alliance (RDA), with the aim to publish as an RDA Document

Questions?

hannah.short@cern.ch