FIM4R - success of V1?

David Kelsey STFC-RAL

TIIME, February 5/6 2018

FIM4R V1 Vision

- **A common policy and trust framework for Identity Management based on existing structures and federations either presently in use by or available to the communities. This framework must provide researchers with unique electronic identities authenticated in multiple administrative domains and across national boundaries that can be used together with community defined attributes to authorize access to digital resources**
- ***Is this still OK for version 2?***

BUT first – some discussion of aims, timetables and publication plans

- We submitted abstracts to conferences (all successful)
  - ISGC 2018, Taipei, 20-23 March 2018
  - Note: there is also RDA 11th plenary – Berlin (21-23 March 2018)
    - No abstract submitted, but FIM-IG will meet?
  - Internet2 Global Summit, San Diego (6-9 May 2018)
    - As part of AARC2 session
  - TNC 2018 - Trondheim (11-14 June 2018)
    - We have a whole session
  - PEARC 2018 – Pittsburgh (22-27 July 2018)
- Version 2 paper
  - We have promised to publish before TNC 2018
  - For PEARC we have been asked to submit a paper by 19 March

Publication plans

- Aim – write paper in terms of requirements and recommendations
  - Not propose solutions
- For PEARC 2018 (by 19 March)
  - We need to transfer copyright to ACM
  - In conflict with continuing to own our “requirements”
  - Proposing to write a “meta” paper
    - Describes the aims and procedures of gathering requirements
    - With pointer to a web-based (and copyright still owned by FIM4R authors) current list
    - Not the final list of requirements
    - Do we include recommendations? (or leave for May)
  - This can then also be used for the talk at ISGC2018
- Then publish the final paper before end of May 2018
    - We need to agree where

What has FIM4R version 1 done for us?

Successes

Some personal views

- FIM4R paper was taken very seriously
  - Research Communities working together, timely input to funding agencies and federations
- The whole AAI world has changed a lot since 2012
- Paper was important input to the TERENA/EC study of AAAI
- Proposal and EC call to create AARC project was great source of funding
- InCommon activities in USA have been very important too
- eduGAIN moves towards behaving as an operational infrastructure
- Many community successes, e.g. LIGO
- Infrastructures deploying AAI services (EGI, EOSC-hub, …)

Successes (2)

- Many AARC successes
  - BPA, Sirtfi, Snctfi and other policy work, pilot studies, …
  - The IdP/SP Proxy becomes a standard approach (in use by many)
  - AARC2 project includes more Research Communities
- FIM is today in production use
  - see Scott's MWA talk earlier today
  - But is at as successful as we would like?

Still ongoing

- Research Communities just want all this AAI stuff to be easy and just work!
- We still have a long list of requirements (see Hannah later)
- eduGAIN still in process of becoming an operational service
  - With support and security operations
  - National federations still vary a lot
  - Lots of difficulties joining eduGAIN
- Takeup of entity categories has been slow
  - R&S, Sirtfi
- Data Protection and Attribute Release still a problem
  - Will EU GDPR and GEANT DP CoCo version 2 fix it?
  - Have we given up on attribute release?

Look at Requirements from version 1 – in detail

Requirements from 2012

User Friendliness	Browser & non-browser	Bridging communities	Multiple Technologies with Translators	Open Standards	Different LoAs
Authorization under community control	Well defined, semantically harmonised attributes	Flexible and scalable attribute release policy	Attribute flow across borders	Attribute aggregation for authorisation	Risk analysis of using FIM
Security Incident Response policies and procedures	Traceability	Policy Transparency, i.e. why and what is FIM	Reliability and Resilience	Smooth Transition to FIM	Easy Integration of services

Contracts between communities & federations

FIM4R mini-meeting

- Before AARC2 All Hands meeting (Nikhef)
  - 21 Nov 2017
- Some of us went through the V1 requirements and gave our impressions of whether the requirement has been resolved or not

REQ (1)

- **User friendliness (high).** The attitude of end-users towards FIM tools has changed. Single-Sign On is assumed to be the basis of interaction with the suite of digital services. The tools that support the FIM framework should be simple and intuitive and integrate with the many other IT tools used in daily life. Ease of use will be particularly important since many researchers only access the ICT systems concerned infrequently or on a part-time basis. Support for citizen scientists and researchers without formal association to research laboratories or universities is essential.
- *STILL IMPORTANT. Progress underway, give examples (e.g. Social IdPs)*

REQ (2)

- **Browser & non-browser federated access (high).**The wide-range of applications in use in the various communities includes many which do not have a simple web-browser front-end. Non-browser based interfaces are essential to support machine-machine interactions in secured workflows.
- *STILL IMPORTANT. Many ways to do it, some have reasonable solutions.*

- **Bridging communities (medium).** FIM is important and will be even more important in many research fields, commercial sections and social groupings. Therefore, bridging between the various communities is a central issue with an efficient mapping of the respective attributes. Here, again user friendliness is an issue with the goal of maximum transparency and with requiring minimum actions by the users of these systems.
- *DO WE HAVE USE CASES? There are not workable, harmonised attributes… this may have been assumed in v1.*

REQ (3)

- **Multiple technologies with translators including dynamic issue of credentials (medium).**No single technology can meet the need of all communities. Translators between one type and another will be required to allow credentials from one community to be used on other services and this translation will often need to be dynamic.
- *THIS IS NOW STANDARD. Certain shared components available for the communities. Community proxies play a central role in translation and generating consistent identities for the community.*
- **Implementations based on open standards and sustainable with compatible licenses (high)**. These are essential for interoperability and sustainability.
- *STILL TRUE. Don't want to be locked into a specific implementation.*

REQ (4)

- **Different Levels of Assurance with provenance (high).** A single Level of Assurance in the quality of authentication cannot meet the need of all communities. Credentials issued under different levels will need to include the provenance of the level under which it was issued.
- *STILL TRUE, now includes Step-Up Assurance injected by community in addition to IdP Assurance.*
- **Authorisation under community and/or facility control (high).**The assignment of attributes to individual users within a given community for use in authorisation decisions needs to be managed by that community. Externally managed federated IdPs cannot fulfil this role.
- *NOW STANDARD. Success!*

REQ(5)

- **Well defined semantically harmonised attributes(medium).**For interoperable authorisation across many service providers it is necessary for the names and possible values of attributes to be well understood and standardised. This may be very difficult to achieve between different research communities but convergence is important.
- *It would be nice but is now managed by the communities*

- **Flexible and scalable IdP attribute release policy(medium).**Different communities and indeed SPs within a community are likely to require a different set of attributes from the IdPs. The IdP policy related to the release of user attributes and the negotiation mechanism needs to be able to provide this flexibility. Bi-lateral negotiations between all SPs and all IdPs is not a scalable solution.
- *PARTIALLY. Bi-lateral negotiations are limited by proxies. R&S helps with scaling*

REQ(6)

- **Attributes must be able to cross national borders(high).**Many of the research use cases require user attributes from an IdP in one country to be used by an SP in another country. Data protection considerations must allow this to happen.
- *BIGGER PROBLEM, attribute release in general, we need a v2 to address new laws*

- **Attribute aggregation for authorisation(medium).**Attributes will need to be aggregated from different sources of authority including federated IdPs and community-based attribute authorities. Privacy and data protection to be addressed with community-wide individual identities(medium). There are many use-cases identified which will require the release of personal data to identify individual users. Clearly this has to be managed in a way that satisfies all legal requirements for data protection.
- *NOW STANDARD.*

REQ(7)

- **Privacy and data protection to be addressed with community-wide individual identities(medium).** There are many use-cases identified which will require the release of personal data to identify individual users. Clearly this has to be managed in a way that satisfies all legal requirements for data protection
- *STILL TRUE*

REQ(8)

There are various essential operational aspects that need to be addressed in the common framework, including:

- **Risk Analysis**. This needs to include consideration of the use of an identity federation from the point of view of the community infrastructure. The implications of having a malicious SP in a federation, for example, need to be considered. This risk analysis will help prioritise the efforts needed to deal with various risks that have already been identified.
- **Traceability**. Identifying the cause of any security incident is essential for containment of its impact and to help prevent re-occurrence. The audit trail needs to include the federated IdPs.
- Appropriate **Security Incident Response policies and procedures** are required which need to include all IdPs and SPs.
- *GETTING THERE, Sirtfi is baseline but more needed*

REQ(9)

- **Transparency of the policies**, e.g. the “what” and “why” of identity management, is essential to gain the trust of the users and service providers.

- **The Reliability and Resilience** of the framework services are essential usability issues that must be addressed. For example, SPs are dependent on the availability of IdPs in order to grant access to their services.
- **Smooth Transition.** There is a wide range of tools and technologies already deployed in production use. A smooth transition of the existing systems to a federated identity management system while maintaining continuous production usage will facilitate its introduction.
- **Easy integration with local service provider (SP) environment.** The ease with which federated authentication and the related authorisation services can be used is an important consideration in the design of any new system. SPs are likely to want to support multiple means of authentication. Controlling access to data sets or repositories is the most foreseen use of identity management across the user communities. In terms of privacy and security, the common policy and trust framework also needs to meet specific requirements from some communities, such as the biomedical community, where competition between different research groups requires scoping within a given trust context.

REQ(10)

A number of legal, policy and trust issues must also be addressed, including:

- **Contracts or SLAs between communities and federations.** These agreements should be developed in a scalable way, so that the maximum number of participants can be included. Bi-lateral agreements between many different communities and many identity federations may be difficult to achieve.
- One attractive way of addressing scalability could be to define **Standards of Trust** or codes of conduct similar to the Authentication profiles and guidelines developed and maintained by the IGTF.
- *Success here has been the adoption and recognition of the proxy model, and Snctfi*

Common Requirements

- Might be a good place to add that the AARC Blueprint Architecture expresses the breadth of technologies required to operate a mature AAI for Research. Could use BPA components as table columns.
-

And what about Recommendations?

Version 1 Recommendations

Research Communities

- Risk Analysis
- Pilot Studies

Recommendations (2)

Technology Providers

- *e-Infrastructures & Federation Operators*

- Separation of AuthN and AuthZ
- Revocation is required
- Attribute delegation to Research Community
- Levels of security

Recommendations (3)

Funding Agencies

- **Funding model and governance structure**
- In order to implement this common policy and trust framework for Identity Management an agreed funding model is required with an appropriate governance structure.
- Life Sciences, it is critical that infrastructure technology pilots start a dialogue with a well-established ethical committee. Pilots should try to find a set of attributes and metadata that are adequate for granting access to sensitive data, and can then propose this as a template policy when new ethical committees are established.
- technology which can simplify the administration of policies for IdPs will definitely contribute to the acceptance and uptake of FIM systems. Hence funding for FIM technologies that are focussed on solving the described needs of the research communities is required.