



7th FIM₄R meeting summary

23-24 April 2014

ESRIN

Frascati



Meeting agenda

Agenda page online with material:

<https://indico.cern.ch/event/301888/>

A written summary of this event will be produced



The FIM₄R 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.

Still valid though we may think to extend:

- lifetime of **unique electronic identities** to cover whole career of a researcher
- **Common policy and trust framework** also includes operations
- **authorize access to digital resources** may imply legal constraints

Being able to estimate the cost of transition to FIM may be an indication of maturity



Prioritisation of FIM₄R requirements

- **User friendliness (high)**
 - Support for citizen scientists and researchers without formal association to research labs or univ

Homeless-IdP tested in pilots

- **Browser & non-browser federated access (high)**

Testing in Pilots

- **Bridging communities (medium)**
 - Bridging is a central issue with an efficient mapping of the respective attributes

Not tested in Pilots

- **Multiple technologies with translators including dynamic issue of credentials (medium)**

Testing in Pilots

- **Implementations based on open stds and sustainable with compatible licenses (high)**

OpenID & SAML can interop.

- **Different Levels of Assurance with provenance (high)**
 - Credentials need to include the provenance of the level under which it was issued

Testing in Pilots

- **Authorisation under community and/or facility control (high)**

Testing in Pilots



Prioritisation of FIM₄R requirements

- **Well defined semantically harmonised attributes** (**medium**)

Limited success with subset of eduPerson but believe it is better to aim for consistency within a community

- **Flexible and scalable IdP attribute release policy** (**medium**)

- Bi-lateral negotiations between all SPs and all IdPs is not a scalable solution

Not Yet ☹️

- **Attributes must be able to cross national borders** (**high**)

- Data protection considerations must allow this to happen.

Not Yet ☹️

- **Attribute aggregation for authorisation** (**medium**)

- Attributes need to be aggregated from different sources of authority including federated IdPs and community-based attribute authorities.

Works for Active Directory Federation Services

- **Privacy and data protection** addressed with community-wide individual ids (**medium**)

Testing in Pilots



Actions from this meeting

- As input for Terena H2020 AAI & GN4 proposals:
 - Each research community to provide by email a short list of key commercial Service Providers (including cloud services) they would like to see integrated with eduGAIN

[Deadline: end May]



Actions from this meeting (II)

Consensus among FIM4R communities that:

- Sufficient level of operation security is essential for inter-fed production services
- Lack of minimal requirements for eduGAIN IdPs/SPs poses unacceptable risks
- FIM4R should leverage the current practices based on existing efforts & expertise
- The SCI work is relevant and could perhaps be extended to incorporate FIM

Proposal:

- FIM4R to jointly propose common operational security requirements for IdPs/SPs

Action:

- Romain/Dave to circulate the latest version of the SCI paper [mid May]
- Romain/Dave to compose + propose a draft document: [end June]
 - Based on the SCI paper
 - In collaboration with Geant/eduGAIN (Leif Nixon/Leif Johansson)
- FIM4R communities to give feedback and eventually endorse document

Following the approach of the original FIM4R paper

[feedback end August]



Actions from this meeting (III)

- Formulate RDA Working Group focused on extension of FIM4R pilots to USA partners and adoption of minimal set of security operations requirements for IdPs
- Schedule next FIM4R meeting in Amsterdam to coincide with RDA 4th plenary (22-24 Sept 2014)
[discuss common operational security requirements for IdPs/SPs]