
esa


umbrella


DARIAH-DE
Digital Research Infrastructure
for the Arts and Humanities

FIM4R v 2.0


WLCG
Worldwide LHC Computing Grid


egi


LIGO


elixir

Background

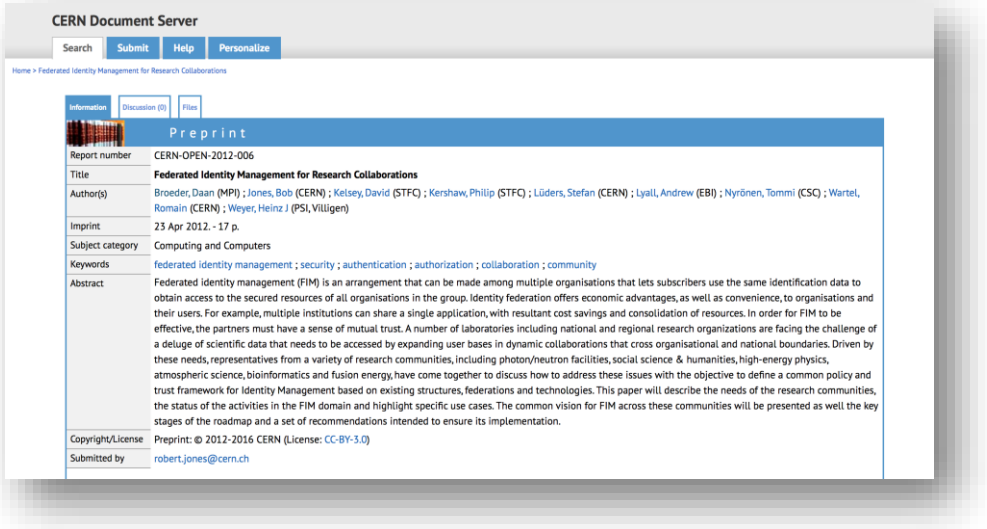
- The first workshop was held at CERN in June 2011 (https://indico.cern.ch/event/129364),
- the second at RAL in November 2011 (https://indico.cern.ch/event/157486),
- the third at ISGC in February 2012 (https://indico.cern.ch/event/177418),
- the fourth at MPI Psycholinguistics Nijmegen in June 2012 (http://www.clarin.eu/events/3501),
- the fifth at PSI Villigen in March 2013 (http://indico.psi.ch/event/2230),
- the sixth at CSC in Helsinki in October 2013(https://refeds.org/meetings/oct13/index.html),
- the seventh at ESRIN in Franscati in April 2014 (https://indico.cern.ch/event/301888/),
- the eighth at CERN on 3-4th February 2015 (https://indico.cern.ch/event/358127).
- the 9th FIM4R meeting 30th November 2015 (https://indico.cern.ch/event/450600/).

Through these workshops, the research communities have converged on a common vision for FIM, enumerated a set of requirements and proposed a number of recommendations for ensuring a roadmap for the uptake of FIM is achieved. These points have been documented in a paper (https://cdsweb.cern.ch/record/1442597).

https://indico.cern.ch/event/358127/

Background

Requirements documented published in 2012 and now due an update!



CERN Document Server

Search | Submit | Help | Personalize

Home > Federated Identity Management for Research Collaborations

Information | Discussion (0) | Files

Preprint

Report number	CERN-OPEN-2012-006
Title	**Federated Identity Management for Research Collaborations**
Author(s)	Broeder, Daan (MPI) ; Jones, Bob (CERN) ; Kelsey, David (STFC) ; Kershaw, Philip (STFC) ; Lüders, Stefan (CERN) ; Lyall, Andrew (EBI) ; Nyrönen, Tommi (CSC) ; Wartel, Romain (CERN) ; Weyer, Heinz J (PSI, Villigen)
Imprint	23 Apr 2012. - 17 p.
Subject category	Computing and Computers
Keywords	federated identity management ; security ; authentication ; authorization ; collaboration ; community
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.
Copyright/License	Preprint: © 2012-2016 CERN (License: CC-BY-3.0)
Submitted by	robert.jones@cern.ch

2012 Requirements

- **User friendliness (high)**
- **Browser & non-browser federated access (high).**
- Bridging communities (medium).
- Multiple technologies with translators including dynamic issue of credentials (medium).
- **Implementations based on open standards and sustainable with compatible licenses (high).**
- **Different Levels of Assurance with provenance (high).**
- **Authorisation under community and/or facility control (high).**
- Well defined semantically harmonised attributes(medium).
- Flexible and scalable IdP attribute release policy(medium).
- **Attributes must be able to cross national borders(high).**
- Attribute aggregation for authorisation(medium).
- Privacy and data protection to be addressed with community-wide individual identities(medium)

2012 Requirements: how have we done?

- **User friendliness (high) - *Good but varies wildly, citizen scientists partially addressed***
- **Browser & non-browser federated access (high). – *Mostly requires web intervention***
- Bridging communities (medium). – *eduGAIN addresses R&E but little interaction with commercial/social*
- Multiple technologies with translators including dynamic issue of credentials (medium).
- **Implementations based on open standards and sustainable with compatible licenses (high).**
- **Different Levels of Assurance with provenance (high).**
- **Authorisation under community and/or facility control (high).**
- Well defined semantically harmonised attributes(medium). – R&S, not so much for other attributes
- Flexible and scalable IdP attribute release policy(medium). – *R&S seems to have reached happy medium*
- Attributes must be able to cross national borders(high). - *Good work from AARC but GDPR problematic for intergovernmental organisations*
- Attribute aggregation for authorisation(medium). – *Case by case basis*
- Privacy and data protection to be addressed with community-wide individual identities(medium)

2012 Recommendations

- Recommendations to the research communities
  - Conduct Risk Analysis
  - Run Pilot Studies coordinated by experts
- Recommendations to the technology providers
  - Separation of Authorization and Authentication
  - Credentials revocation
  - Attribute delegation to the research community
  - Standardise efforts in Levels of Security/Assurance
- Recommendations to funding agencies
  - Fund FIM technologies that are focused on solving the described needs of the research communities

2012 Recommendations: how have we done?

- Recommendations to the research communities
  - Conduct Risk Analysis – SCI
  - Run Pilot Studies coordinated by experts - AARC
- Recommendations to the technology providers
  - Separation of Authorization and Authentication – as per attribute delegation
  - Credentials revocation
  - Attribute delegation to the research community – partially done within the context of pilots
  - Standardise efforts in Levels of Security/Assurance – Minimal LoA, Sirtfi
- Recommendations to funding agencies
  - Fund FIM technologies that are focused on solving the described needs of the research communities – AARC/AARC2

Recommendations 2016

- Address command line and non-web use cases
- Integrate FIM with existing Community Membership Management Tools
- Build operational security
- Support GDPR adequacy certification for intergovernmental organisations
- Commercial IaaS interaction
- Make FIM a production service and a corner stone of the European Open Science Cloud
- …

Next Steps

- Run a 10th FIM4R Workshop to start defining an updated whitepaper
- When?
  - FIM4R Workshop @ TIIME (old EWTI) in February, Austria
  - Feedback @ WISE Workshop in March, Amsterdam
  - Feedback @ RDA Session in April, Barcelona
- Who? Representatives of Research Communities and Infrastructures
- Timeline?