FIM4R workshop Geneva

February 16th 2023

A libraries principle: protecting academic freedom

Authentication should be managed in the right way, protecting privacy. The FIM4L working group helps libraries with this by providing recommendations. We serve a global community with an email list of about 70 people. (www.fim4l.org)

Organization and strategy

The FIM4L initiative is born as a spin-off from the AARC project as a global initiative from librarians. A Working Group was formed under LIBER (Association of EU libraries) by whom we are governed.

We have close ties with Seamless Access, REFEDS and GEANT.

We are a library-led community for librarians. Creating awareness, explain SSO possibilities and providing recommendations for both IdP's and SP's.

Active working groups / Inactive working groups

DIGITAL SCHOLARSHIP AND DIGITAL CULTURAL HERITAGE COLLECTIONS WORKING GROUP

Digital Scholarship and Digital Cultural Heritage Collections Working Group

ARCHITECTURE WORKING GROUP

LIBER Architecture Working Group (LAG)

CITIZEN SCIENCE WORKING GROUP

LIBER Citizen Science Working Group

COPYRIGHT & LEGAL MATTERS WORKING GROUP

LIBER Copyright & Legal Matters Working Group

DATA SCIENCE IN LIBRARIES WORKING GROUP

LIBER Data Science in Libraries Working Group

The LIBER Data Science in Libraries (DSLib) working group explores and promotes library engagement in applying data science and analytical ..

EDUCATIONAL RESOURCES WORKING GROUP

LIBER Educational Resources Working Group

FIM4L WORKING GROUP

LIBER FIM4L Working Group

LEADERSHIP PROGRAMMES WORKING GROUP

LIBER Leadership Programmes Working Group

OPEN ACCESS WORKING GROUP

LIBER Open Access Working Group

https://libereurope.eu

Introduction

The FIM4L (Federated Identity Management for Libraries) Working Group aims to develop a library policy for federated authentication which is broadly supported by libraries and publishers. As Working Groups are the primary units to conduct work on the LIBER strategy, ours will operate under the Steering Committee for the direction, State-of-the-art Services, as defined in LIBER's 2023-2027 Strategy.

This is a library-led working group to further the usage of FIM technologies by providing guidelines for libraries on how to deploy such technologies while at the same time preserving the privacy of users.

The key concern of FIM is that libraries must be at the core of managing the privacy of users when they access library e-resources. When federated authentication is implemented, users authenticate with the Single Sign-On (SSO) service of their institution. Depending on the configuration of this SSO, a user can remain anonymous or not. It is up to the institution, the library, to maintain this and protect the privacy of its users. As such, FIM4L contributes to upholding the principle of academic freedom.

The group was initiated within the AARC project and now maintains its own website.

Feel free to view the group's latest publication, LIBER FIM4L Recommendations 2020 v.01, which is also available on Zenodo.

Join our group

Are you interested in identity management, and how we can support research librarians in acquiring the training they need? We need your energy!

Contact us

Group chairs

View all group members

Jos Westerbeke
Library IT specialist / manager, Erasmus University Rotterdam
Contact →

Office liaisons

View all group members

Andrej Vrčon
Head of International Projects, LIBER
Contact →

Priorities

1. Consensus
2. Support

Priority 1

To come to a consensus on library policy for federated authentication that protects users identities. T

policy should help libraries and publishers and needs to be clear for account managers, license managers, etc. (those who make the deals), while also including enough technical information for IT staff.

fim4l.org

FRONTPAGE RECOMMENDATIONS DOCUMENTS EVENTS ABOUT CONTACT

FIM4L

Federated Identity Management for Libraries

FIM4L (Federated Identity Management for Libraries) is a library-led working group that aims to further the usage of Federated Identity Management technologies by providing guidelines for libraries on how to deploy such technologies while in the same time preserve the privacy of the users. FIM4L was initiated in the AARC project.

FIM4L is an international activity with members from at least 4 continents. The European branch has also organized as a LIBER working group. Further information on that LIBER working group can be found at https://libereurope.eu/strategy/research-infrastructures/fim4l/

FIM4L recommendations are endorsed by Canadian Association of Research Libraries (CARL-ABRC), Council of Australian University Librarians (CAUL), LIBER, and Research Libraries UK (RLUK) members of International Alliance of Research Library Associations.

In 2020 we published the first version of the Recommendations.

In 2022 the second and current version has been published.

Published on Zenodo:
https://zenodo.org/record/7313371

The recommendations' core principles can be summarized as:

- ➔ Federated access is a viable alternative to IP based access with benefits for users, libraries and publishers, but
- ➔ correct configuration is key to the successful operation of a Single Sign-On connection, and
- ➔ user privacy should always be protected by all parties involved.

Recommendations
zooming in to 4.A and 4.B

- An IdP can be configured to release either a transient (4.A anonymous) or a persistent (4.B pseudonymous) alphanumeric identifier.

- We don't make a recommended choice in the document, but most libraries prefer option 4.B: pseudonymous. Which
  - enables the use of user profiles and
  - gives the possibility to track down a user who breached the licence.

Where are we now

- ➔ Talks with Elsevier about "agile" access
- ➔ Published as a blogpost on LIBER website
- ➔ By "agile" we mean that an IdP can release a persistent identifier or not. Or, at the publishers' website, to login to a user profile or not. The user has a choice.
- ➔ Results Elsevier talks:
  - ○ Anonymous works for some products, some not.
  - ○ You cannot change during a session, and you can't login anonymous anymore after a pseudonymous session.
  - ○ There's a need for building trust between libraries and publishers to solve the difficulties.
  - ○ This can be done by contracts and technical transparity. (See Seamless Access)
  - ○ User awareness and communication should be part of SSO implementation.
- ➔ We are working on educational material.

Federated Identity Management (FIM)

IdP

SP's

Taylor & Francis
Taylor & Francis Group

Springer

- National NREN federations
- Global federations

Seamless Access.org

NON SOLUS

ELSEVIER

WILEY

EBSCOhost

Private

Anonymous

An IdP (library) manages authentication and provisioning of attributes to an SP.

=> Minimal disclosure policy

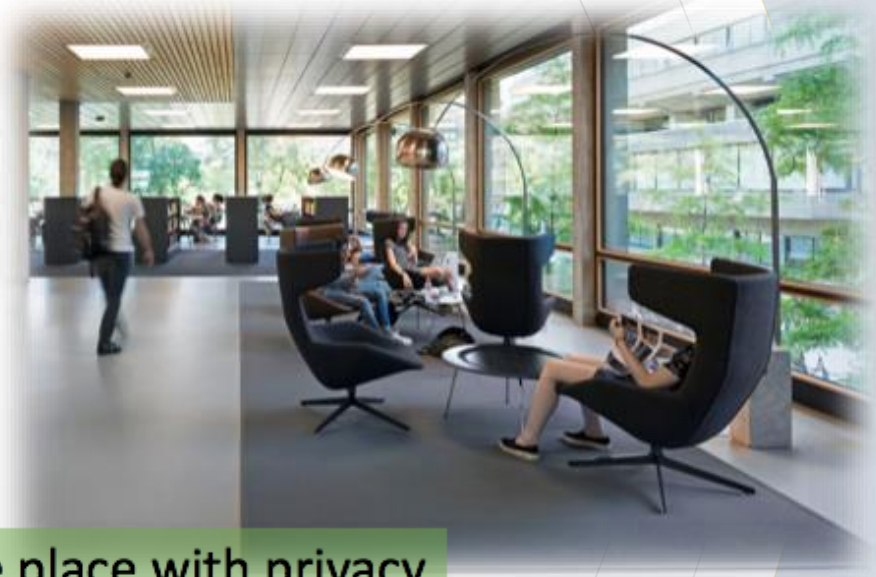
Library patron

FIM4L

The library as a trusted place

The library has to

- Provide a private place, even online
- Protect its patrons



A trusted safe place with privacy

Trust relationship with publishers via contracts

Pseudonymous access at Elsevier ScienceDirect

ERASMUS
UNIVERSITEIT
ROTTERDAM

Live showcase (if time permits)

Discussion

- What role can libraries take in FIM4R?
- What topics are we interested to discuss with you:
  - General privacy and consent technologies.
  - Selective attribute release.
  - Open Access/Science and FIM Use cases.
  - Setting up a consortium for HORIZON Call on Privacy Enhancing Technologies.
  - New Entity Categories anonymous, pseudonymous (and personalized) What are REFEDS's plans for roll-out across eduGAIN?
  - schacLocalReportingCode attribute status. - vut.cz (Jiri) is interested in the attribute roll-out and usage across publishers' platforms.

THANKS!

Jos Westerbeke

Erasmus University Rotterdam, Netherlands
https://www.linkedin.com/in/jwesterbeke/