Federated Identity Management for Research Collaborations

Bob Jones, CERN

Daan Broeder, Max-Planck Institute for Psycholinguistics

David Kelsey, Particle Physics, STFC

Philip Kershaw, CEDA, RAL Space, STFC

Stefan Lüders, CERN

Andrew Lyall, European Bioinformatics Institute

Tommi Nyrönen, CSC

Romain Wartel, CERN

Heinz J Weyer, PSI

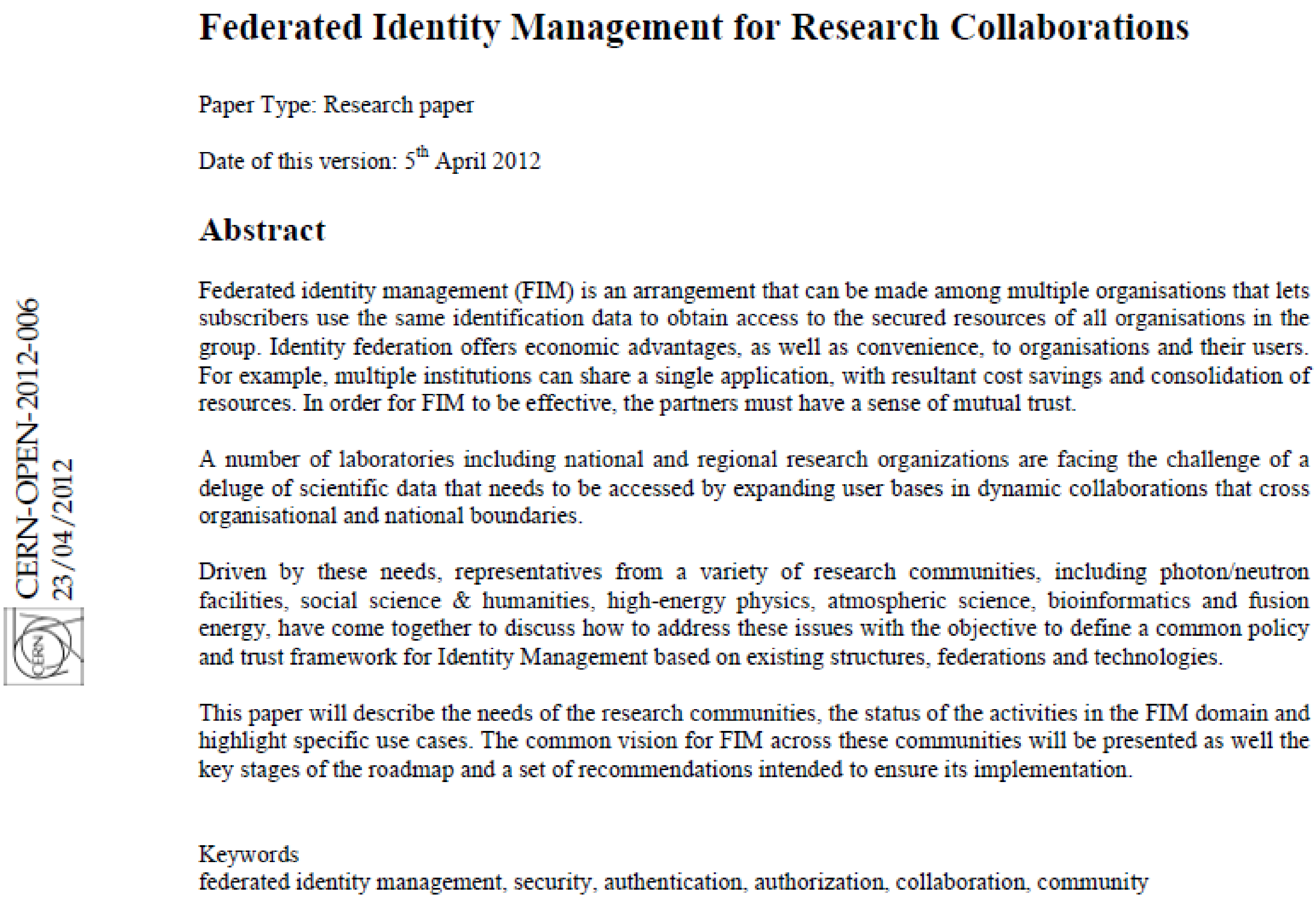
Background

- Issue of identity management raised by IT leaders from EIROforum labs during their IT working group meeting in January 2011

- These laboratories, as well as national and regional research organizations, are facing similar challenges
  - Scientific data deluge means massive quantities of data needs to be accessed by expanding user bases in dynamic collaborations across organisational and national boundaries
  - "Facebook" generation demands all the tools (work & social) integrate smoothly

Fed Id Mgmt Workshops

- Three Federated Identity Management workshops already held:
  - **June 2011, CERN (High Energy Physics)**
    - Identified needs of users communities
    - Current state of usage explored
    - Scope for commonality and willingness to work together expressed
  - **November 2011, RAL (Climate Science)**
    - Uses cases presented
    - Common vision developed
    - Architects/contacts from each community agreed to produce a common paper
  - **February 2012, Taipei (Asian input**)
    - Input from Asian colleagues
    - Vision, recommendations and position paper refined



Federated Identity Management for Research Collaborations

Paper Type: Research paper

Date of this version: 5th April 2012

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.

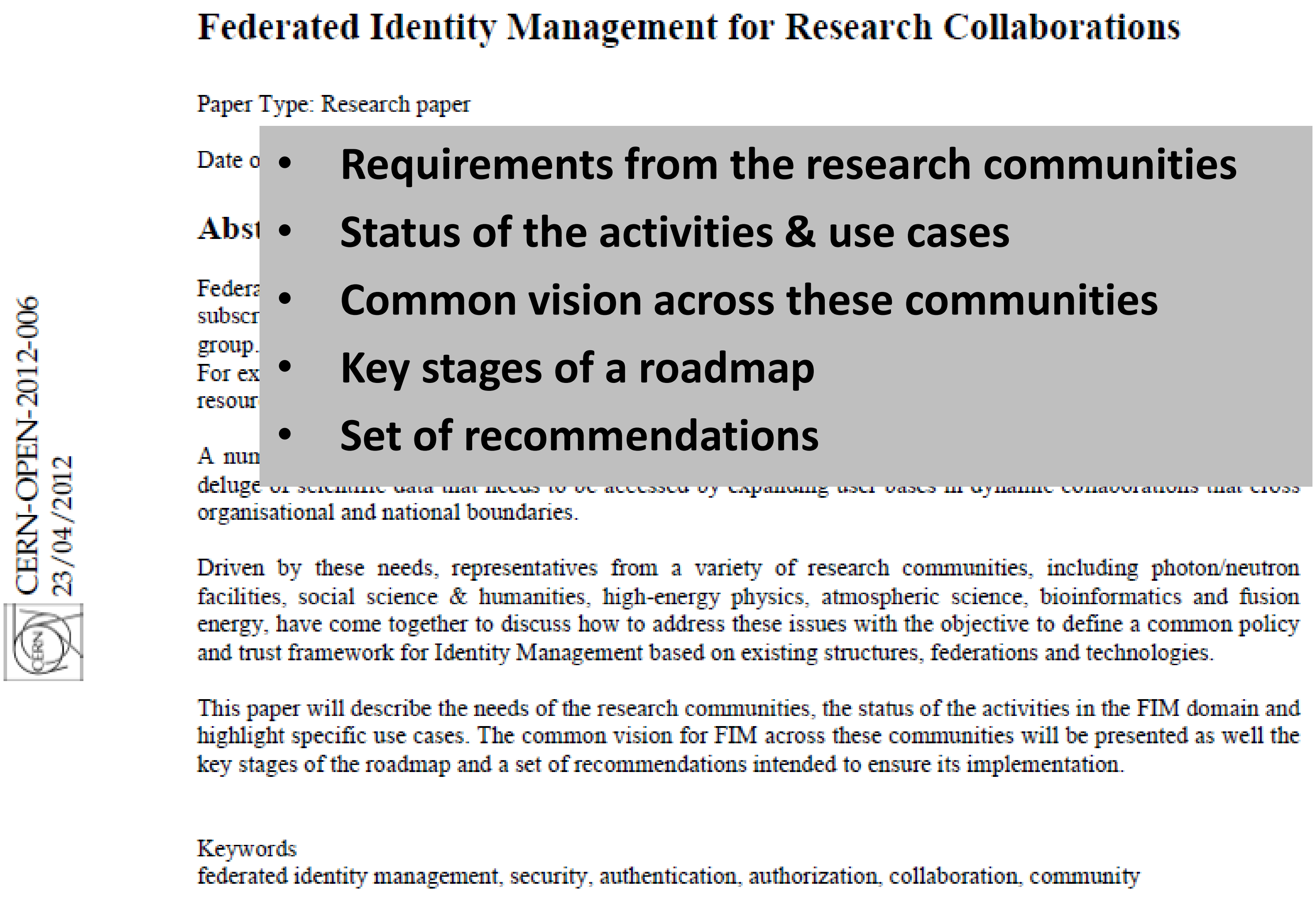
Driven by these needs, representatives from a variety of research communities, including photon/neutron facilities, social science & humanities, high-energy physics, atmospheric science, bioinformatics and fusion energy, have come together to discuss how to address these issues with the objective to 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

https://cdsweb.cern.ch/record/1442597/files/CERN-OPEN-2012-006.pdf

You can provide feedback here https://cdsweb.cern.ch/record/1442597/comments



Federated Identity Management for Research Collaborations

Paper Type: Research paper

Date o

Abst

Federa
subscr
group.
For ex
resour

A nun
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

- **Requirements from the research communities**
- **Status of the activities & use cases**
- **Common vision across these communities**
- **Key stages of a roadmap**
- **Set of recommendations**

https://cdsweb.cern.ch/record/1442597/files/CERN-OPEN-2012-006.pdf

You can provide feedback here https://cdsweb.cern.ch/record/1442597/comments

User Communities Represented

- Representatives from a number of research communities:
  - photon/neutron facilities
  - social science & humanities
  - high-energy physics
  - atmospheric science
  - Bioinformatics
  - fusion energy

The 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.

Recommendations

- For each stakeholder group
  - Research Communities
  - Technology Providers
  - Funding Agencies

Recommendations: research communities

- **Risk Analysis**
  - Needed to reassure the security officers at participating sites
  - Prioritise the various risks and hence focus available effort
  - The research communities should work with technology providers, IdP and SPs to perform such a risk analysis and the results used to improve the deployed FIM
  - Particularly important for the Life Sciences community
    - early stage of FIM uptake, unfamiliar with FIM technologies
  - Low Level of Assurance concerning people's identities is not going to be legally acceptable if the service distributes sensitive data
- Pilot projects – see later

Recommendations: technology providers

- **Separation of AuthZ and AuthN**
  - The need for external attribute authorities managed by the research community
    - formal separation of the AuthN by the IdP and the AuthZ on behalf of the SP
- **Credentials revocation**
  - The credentials issued by the IdP to the user or the SP should be revocable
- **Attribute delegation to the research community**
  - Need for personal information to be aggregated with community defined attributes in order to grant access to digital resources and services
  - Semantic harmonisation of federated attributes and local attributes and metadata is needed
- **Levels of Assurance**
  - A *one size fits all* model for levels of assurance will not scale
    - E.g. the biomedical community where there is a wide range of security levels needed
  - Essential for FIM systems are re-used across multiple domains and communities
  - More work is required on the standardisation efforts for Levels of Assurance – its communication and enforcement

Recommendations: funding agencies

Funding model and governance structure

- **A clear funding model is required with an appropriate governance structure**
  - Who pays for what, who manages the services and who decides?
- **Sensitive data in Life Sciences**
  - Critical that infrastructure technology pilots start a dialogue with a recognised 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 a template policy to the ethical committee
- **Focus of this work has been usability and deployment aspects with a desire to stay technology neutral**
  - But technology which can simplify the administration of policies for IdPs will definitely contribute to the acceptance and uptake of FIM systems
  - Funding for FIM technologies should be focused on solving the described needs of the research communities

FIM and European Policy

- Vital to engage with the national and international infrastructures that provide identity related services, standards forums
- Potential Wider Impact:
  - European E-infrastructure Forum report (2010) on the requirements for Pan-European e-infrastructure resources and facilities: http://www.einfrastructure-forum.eu/documents/EEF-report
  - Gathered input from **28 ESFRI projects**
  - Highlighted **consistent identity management and single sign-on** as a fundamental **requirement** for **all the ESFRI projects**

FIM and European Policy (cont.)

e-Infrastructure Reflection Group (e-IRG) white paper, 2011

- Includes a section on AAI with objectives that are consistent with those in the FIM paper:
- *“The overall objective is to establish and maintain the level of mutual trust amongst users and service providers that is needed for an open ecosystem to function. As an e-Infrastructure matures and its user community grows, requirements for aligning authentication and authorisations grow as well. This must translate into:*
  - *Improved usability, lowering the threshold for researchers to use the services.*
  - *Improved security and accountability, which often conflicts with the usability requirement.*
  - *Leveraging of existing identification systems, such as that of the employing organisation.*
  - *Enhanced sharing, allowing willing users to minimise the burden of policy enforcement.*
  - *Reduced management costs, freeing resources for other service or research activities, and providing a sound basis for accounting.*
  - *Improved alliance with the commercial Internet, which also improves interaction between scientists and society.”*

http://www.e-irg.eu/publications/white-papers.html

FIM Pilot Projects

- Several pilot studies are underway or planned:
  - Neutron/proton facilities community: Umbrella project
  - Life sciences and medical research: ELIXIR/BioMedBridges projects
  - CLARIN & DARIAH humanities project
- Pilot projects will
  - Explore the requirements on FIM services in more detail
  - Provide feedback on the technologies and services available
  - Engage more potential stakeholders to FIM
- This approach should be adopted across all the research communities

Progress since the workshop in Taipei

- Paper has been revised and made available in an open access repository
- Presented to the European Geosciences Union (EGU, Austria Apr’12) and European network community (TNC2012 & REFEDs, Iceland May’12)
- Research communities have discussed the paper internally (minor updates provided from humanities & neutron/photon communities) and advanced with their pilot projects

Objectives for this workshop (II)

- Gather further input from the research communities
- Plan how to implement the recommendations:
  - Research Communities
    - Prepare the risk analysis
    - Review the status of the pilot projects
  - Technology providers
    - Are the recommendations accepted and if so what is the timeline for implementation?
      - Separation of AuthZ and AuthN
      - Credentials revocation
      - Attribute delegation to the research community
      - Levels of Assurance
  - Funding agencies – explore sustainability aspects
- Determine which aspects of the financial model are in place and what else is needed
- Plan the next workshop