

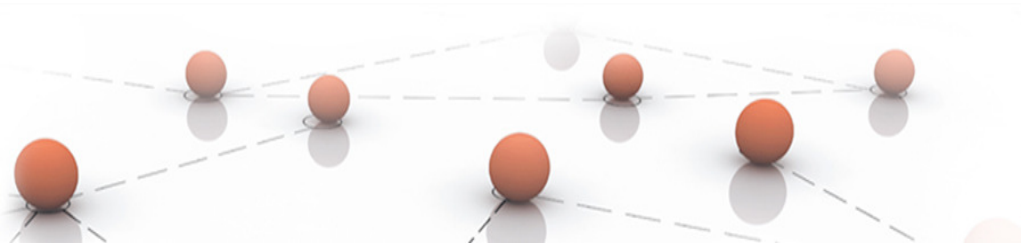
Federated Identity Management for Research Collaborations

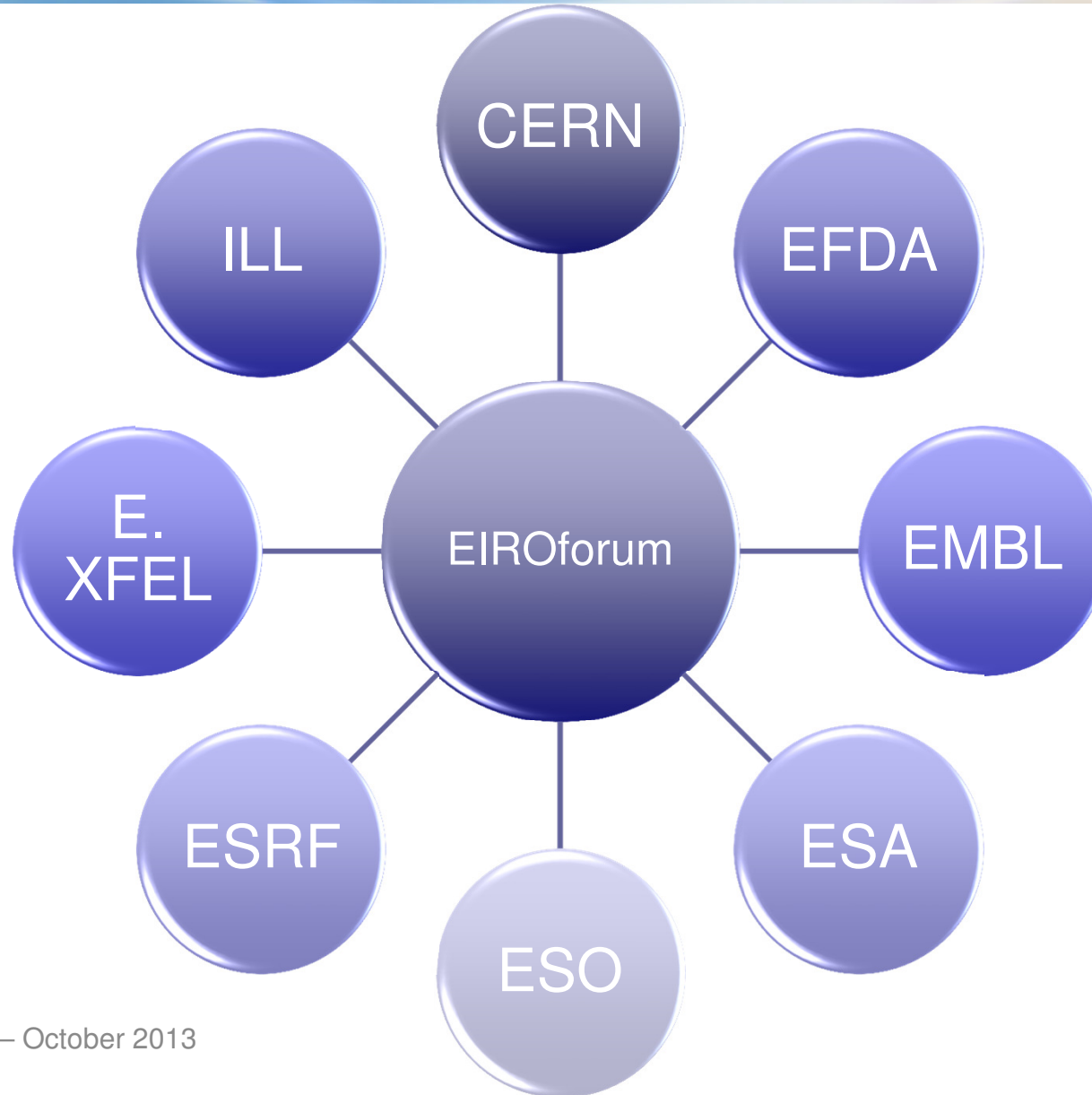
Bob Jones

IT dept

CERN

29 October 2013







FIM₄R workshops

CERN Climate
Jun'11
HEP

STFC
Nov'11

ASGC
Feb'12
Asia

MPI
Jun'12
Social S &
Humanities

PSI
Mar'13
Photon/
Neutron
facilities

CSC
Oct'13
BioMedical
Science

<https://indico.cern.ch/event/129364>

<https://indico.cern.ch/event/157486>

<https://indico.cern.ch/event/177418>

<http://www.clarin.eu/events/3501>

<http://indico.psi.ch/event/2230>

<https://refeds.org/meetings/oct13/>

Federated Identity Management for Research Collaborations

Paper Type: Research paper

Date of this version: 28 August 2013

Abs

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

Federated
subsc
group
For ex
resour

A num
deluge

organisational and national boundaries.

lets
the
ers.
n of

of a
ross

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

Authors: Daan Broeder, Bob Jones, David Kelsey, Philip Kershaw, Stefan Lüders, Andrew Lyall, Tommi Nyrönen, Romain Wartel, Heinz J Weyer

Bob Jones (CERN) – March 2013

CERN-OPEN-2012-006
28/08/2013



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



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.



Prioritisation of FIM₄R requirements

- **User friendliness (high)**
 - Support for citizen scientists and researchers without formal association to research labs or univ
- **Browser & non-browser federated access (high)**
- **Bridging communities (medium)**
 - Bridging is a central issue with an efficient mapping of the respective attributes
- **Multiple technologies with translators including dynamic issue of credentials (medium)**
- **Implementations based on open stds and sustainable with compatible licenses (high)**
- **Different Levels of Assurance with provenance (high)**
 - Credentials need to include the provenance of the level under which it was issued
- **Authorisation under community and/or facility control (high)**
- **Well defined semantically harmonised attributes (medium)**
- **Flexible and scalable IdP attribute release policy (medium)**
 - Bi-lateral negotiations between all SPs and all IdPs is not a scalable solution
- **Attributes must be able to cross national borders (high)**
 - Data protection considerations must allow this to happen.
- **Attribute aggregation for authorisation (medium)**
 - Attributes need to be aggregated from different sources of authority including federated IdPs and community-based attribute authorities.
- **Privacy and data protection** addressed with community-wide individual ids (medium)

Technologies being piloted by research communities

	Technology	Inter-federation	Status	Plans
ELIXIR	SAML2	Joined to the HAKA federation.	Development	Join eduGAIN and Kalmar union.
ESA	Shibboleth		Production	Join NASA and EUMETSAT
WLCG	Web based and non-web based. Pilot project on non-web based. SAML2.		CLI solution achieved, but looking into alternatives.	Refocus on web-based use case.
DARIAH	Shibboleth		Development	Implement DARIAH-EU
SWITCH	Shibboleth	Open to inter-federation with eduGAIN.	Production (for the majority of Swiss Universities)	Moonshot and Interfederation with eduGAIN
CLARIN	Shibboleth		Implementation	Interconnection through Service Provider Federation (SPF)
Umbrella	Shibboleth	Bridging concept being developed.	Implementation	Affiliation Database, Sync with other programs iCAT, Moonshot. Bridging. Implementation up to Sept. 2013.
WeNMR	Drupal based WeNMR VRC, Shibboleth authN, phpCAS authN, robot certificates.	Flexibility to connect to a wide set of federations (from Drupal).	Production	
SyBIT	Azure	Any federation could be easily integrated.	Microsoft product.	Self-federation model.

1st wave:

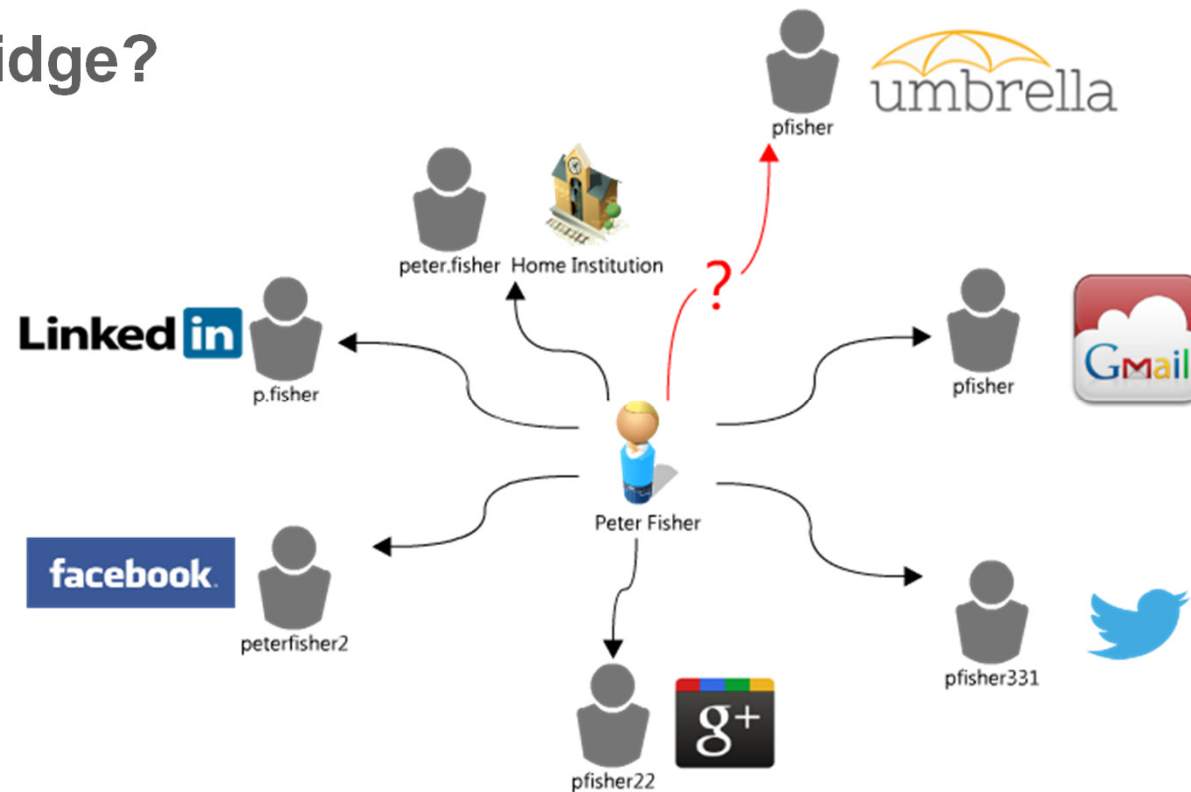
ILL, ESRF, PSI
online since
August 2013

2nd wave:

DESY, ISIS,
Diamond,
HZB, Elettra
(Nov 2013 –
Jan 2014)

Full
deployment
end of
March
2014

Why to bridge?



Creating a new account is often criticized



A Vision for a European e-Infrastructure for the 21st Century

Sustainable - RIs currently in construction (FAIR, XFEL, ELIXIR, EPOS, ESS, SKA, ITER, HiLHC and upgrades to ILL and ESRF etc.), need to be convinced that e-Infrastructure will exist and continue to evolve throughout their construction and operation phases if they are to take the risk and invest in its creation & exploitation

Inclusive - Need an e-Infrastructure that supports the needs of the whole European research community, including the *“long tail of science”*, and interoperate with other regions

Flexible - Cannot be a one-size-fits-all solution

Integrated - Coherent set of services and tools must be available to meet the specific needs of each community

Innovative - Essential that European industry engages with the scientific community to build and provide such services

User driven - The user community should have a strong voice in the governance of the e-Infrastructure

See <https://cds.cern.ch/record/1550136/files/CERN-OPEN-2013-018.pdf>



What do we have already?

- Existing European e-infrastructure *long-term* projects
 - GEANT, EGI, PRACE
- Many “pathfinder” initiatives have prototyped aspects of what will be needed in the future
 - Includes much of the work in the existing e-Infrastructure projects but also projects such as EUDAT, Helix Nebula, OpenAIRE+, etc
 - Thematic projects such as BioMedBridges/ CRISP/ DASISH/ ENVRI, as well as Transplant, VERCE, GenesIDEC and many others



How can we create e-infrastructures that overcome fragmentation?

- Fragmentation of users (big science vs. long tail)
- Fragmentation of infrastructure (not integrated services)
- Common platform (*e-infrastructure commons*) with 3 integrated areas
 - **International network, authorization & authentication, persistent digital identifiers**
 - **small number of facilities to provide cloud and data services of general and widespread usage**
 - **Software services and tools to provide value-added abilities to the research communities, in a managed repository**
- Need a *data continuum* - linking the different stages of the data lifecycle, from raw data to publication, and compute services to process this data

ESFRI Cluster projects




Cross-Disciplinary Challenges

A matrix showing the interest in common topics for the four cluster initiatives

	CRISP	ENVRI	DASISH	BioMed
Data identity				
Data identity continuum				
Software identity				
Concept identity				
User identity management				
Common data standards and formats				
Service discovery				
Service market places				
Integrated data access and discovery				
Data storage facilities				
Data curation				
Privacy and security				
Volatile data management				
User Community Body				
Semantic annotations and bridging				
Reference models				
Education & training				


A European cloud computing partnership: big science teams up with big business






Strategic Plan


- ▶ Establish multi-tenant, multi-provider cloud infrastructure
- ▶ Identify and adopt policies for trust, security and privacy
- ▶ Create governance structure
- ▶ Define funding schemes



To support the computing capacity needs for the ATLAS experiment


EMBL 

Setting up a new service to simplify analysis of large genomes, for a deeper insight into evolution and biodiversity



To create an Earth Observation platform, focusing on earthquake and volcano research

Adopters





<http://www.helix-nebula.eu>
contact@helix-nebula.eu



@HelixNebulaSC
 HelixNebula.TheScienceCloud



Research Infrastructures need a **common AAI service**

Technology is not the problem!

- **Risk Analysis** - *implications of having a malicious SP in a federation*
- **Traceability** - *identifying the cause of any security incident*
- **Security Incident Response** – *including all IdPs and SPs*
- **Transparency** - *essential to gain the trust of the users and service providers*
- **Reliability and Resilience** - *of the framework services*
- **Smooth Transition** - *of the existing production systems to a federated identity management model*
- **Easy integration with local SP environment** - *SPs will want to support multiple means of authentication*
- **Specific requirements** - *from some communities*



Next steps

- FIM4R is proposing to establish an interest group within RDA
 - Ensure interaction with USA and Australia
 - Hopefully to part of RDA event in Dublin in March 2014
- 7th FIM4R workshop to be hosted by ESA in Frascati in April 2014



Summary

The Research Communities have

- **Highlighted identity mgmt as a *common* service**
- **Aligned their basic requirements**
- **Undertaken a series of prototypes/pilots with providers**
- **Confirmed that suitable technologies are available**

But the real issue is to establish *policies* and networks of *trust* between users, SPs and IdPs

We need a common federated identity management service for the whole of the e-infrastructure