Science & Technology Facilities Council

Federated Identity Management for Research Communities (FIM4R)

David Kelsey (STFC-RAL)

EGI TF, AAI workshop

19 Sep 2012

Overview

- FIM4R
  - “Federated Identity Management for Research”
- Some background
- FIM4R workshops and our paper
- The Research Communities
- Vision and Common Requirements
- Next steps

Background

- Issue of IdM raised in EIROforum (Jan 2011)
  - CERN, EFDA-JET, EMBL, ESA, ESO, ESRF, European XFEL and ILL
- 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
- Also encouraged by EEF and eIRG
- Global problem, not just EU

Workshops and Paper

- 4 workshops to date
  - link to Jun 2012 agenda below (other links contained within)

https://indico.cern.ch/conferenceDisplay.py?confId=191892

- Prepared a paper that documents common requirements, a common vision and recommendations
- Paper: CERN-OPEN-2012-006: *https://cdsweb.cern.ch/record/1442597*

The communities

user community	other projects	# users	chosen technology	status	IGTF
photon/neutron facilities	EUROFEL, PanData, CRISP	>30,000 visiting researchers per year	Shibboleth/SAML	Umbrella prototype	no
Social Sciences and Humanities	DARIAH, CLARIN, CESSDA, DASISH, Bamboo	hundreds now, potential for 10000+ across SSH	Shibboleth/SAML	Prototype CLARIN Service Provider federation deployed in 3 countries	yes
high energy physics	WLCG	10,000+ globally	X509	production	yes
earth sciences	Federation, GENESI-DEC, CMIP5, Metafor, IS-ENES, CORDEX, Exarch, Climate Data Exchange	5000+ for CIMP5	OpenID, X.509 and SAML	production - earth system grid	not yet but foresee for EGI integration
life sciences	ELIXIR, BioMedBridges, BBMRI, NCoEDG & potentially 10 BMI ESFRI projects	3 million researchers access data via EBI website each year	not chosen yet	Security is included in BioMedBridges project workplan and a pilot project is being planned with EGI	no

Common vision statement

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

Common Requirements

- User friendliness
  - Many users use infrequently
- Browser and non-browser federated access
- Bridging between communities
- Multiple technologies and translators
  - Translation will often need to be dynamic
- Open standards and sustainable licenses
  - For interoperability and sustainability
- Different Levels of Assurance
  - When credentials are translated, LoA provenance to be preserved
- Authorisation under community and/or facility control
  - Externally managed IdPs cannot fulfil this role
- Well defined semantically harmonised attributes
  - For interoperable authorisation
  - Likely to be very difficult to achieve!

Requirements (2)

- Flexible and scalable IdP attribute release policy
  - Different communities and different SPs need different attributes
  - Negotiate with IdF not all IdPs – for scaling
- Attributes must be able to cross national borders
  - Data protection/privacy considerations
- Attribute aggregation for authorisation
- Privacy and data protection to be addressed with community-wide individual identities
  - We need to identify individuals
    - E.g. ethical committees can require names, addresses, supervisors to grant access
- Legal issues and contracts
  - Data protection, scalability, …

Operational Requirements

- Risk analysis
- Traceability
  - Audit trails include IdPs
- Security incident response
  - To include all IdPs and SPs
- Transparency of policies
  - To gain trust of SPs and users
- Reliability and resilience
- Smooth transition (from today's production)
- Easy integration with local SP
  - SP likely to want to support multiple AuthN technologies

Example FIM Pilot Projects

- Life Sciences
  - Users authenticate with FIM to access sensitve data
  - Automated electronic workflow for authenticated user to be granted access to a dataset (Data Access Comm)
- Photon and Neutron facilities
  - *Umbrella* system being developed
  - A common Federated IdM system across all facilities
    - with all facility User Offices linked
- Humanities
  - CLARIN is gradually building a federation of SPs

Next steps

- Awaiting response from REFEDS
- Can then jointly prioritise requirements
- Pilot projects are very important
  - Simple way to engage both sides
- Next FIM4R meeting – 20/21 March 2013 (PSI, Switzerland)

Questions?