

A view of access management from Europe

James Farnhill
JISC Programme Manager (e-Research)
j.farnhill@jisc.ac.uk

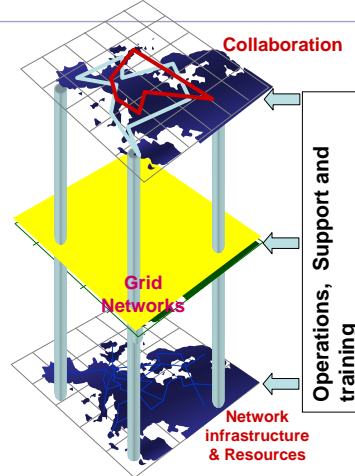
- Key concepts
- European groups
- European activities in access management
- UK Access Management Federation
- JISC and eResearch
- JISC AAI Activities for eResearch
- Lessons learned
- Future directions
- Questions

What is e-Research?

- Collaborative research that is made possible by the sharing across the Internet of resources (data, instruments, computation, people's expertise...)
 - Crosses organisational boundaries
 - Often very compute intensive
 - Often very data intensive
 - Sometimes large-scale collaboration

What is e-Infrastructure?

- Grids: permit resource sharing across administrative domains
- Networks: permit communication across geographical distance
- Supporting organisations
 - Operations for grids, networks
- Resources
 - Computers
 - Digital libraries
 - Research data
 - Instruments
- Middleware
 - Authentication, Authorisation
 - Registries, search engines
 - Toolkits



Examples of Specific Research Tasks Requiring AAI and IDM

- Workflow automation
 - Managing large scale workflow execution from resource provisioning to provenance tracking
- Access to remote instrumentation
- Supporting creation and management of decentralized, dynamic VOs across the Grid
- Job submission -batch queue on a site's computers where the user's job is executed
- Delegated administration

Virtual organisations

- People in different organisations seeking to cooperate and share resources across their organisational boundaries E.g. A research collaboration
- Each grid is an infrastructure enabling one or more “virtual organisations” to share and access resources
- Key concept: The ability to negotiate resource-sharing arrangements among a set of participating parties (providers and consumers) and then to use the resulting resource pool for some purpose. (Ian Foster)

e-Research Challenges Relating to AAI and IdM 1/2

- Security challenges tend to be very user identity-specific in e-Research
 - E.g. making sure that only those users who have the proper credentials are granted access to the resources
 - No agreed way to determine the user’s access rights from their e-Science certificate alone
 - User can be assigned to:
 - a particular network; to a particular technology; to a certain VO (or multiples!); resource; usage rights; security domain, etc
- Abstracting multiple identity systems behind a single, open interface
- Simplified authentication tools
 - single sign-on to integrate grid, network and campus resources in a seamless system
 - access to grid facilities/resources securely through the Shibboleth authentication mechanisms

e-Research Challenges Relating to AAI and IdM 2/2

- how to cross administrative domains in a well understood way
 - administrative challenges when trying to interoperate with various other identity systems
- defining a set of recognised roles, actions, and relationships to support VOs, and for multi-institutional collaboration
 - Address user and security policy requirements in VOMS
 - License management software, across a site and across a VO
 - Mechanisms to support controlled and convenient sharing of files between groups
- Need to tackle non-technical issues, to boost adoption

- Switzerland - SWITCH-AAI
- Finland – HAKA
- Norway – FEIDE
- Denmark – DK-AAI
- Holland – SURFederation
- Sweden – SWAMID
- Spain - CBIC
- Europe – TERENA and TF-EMC2
- EGEE
- EU Framework Programmes (FP6, FP7)
-and others to follow

- Primarily federation and basic access management based on a range of technologies from commercial (eg Sun) to open source (eg Shib)
- VOs –
 - EGEE
 - SWITCH – Group Mgt Tool, SLCS/VASH
- SCHAC – attribute exchange internationally
- Kalmar Union - confederation
- Identity
- Technologies and standards

- Has grown out of previous activity in access management:
 - 05/99 and AAA programmes
 - Core Middleware Technology Development and Infrastructure Programmes
- Run as a service by JA.NET for JISC
- Currently has 78 members
 - 48 IDPs – 40 HEIs and 8 FEs
 - 30 SPs
- Main focus on access management and providing a replacement service for ATHENS
- Main technology used is Shibboleth but SAML compliant and gateways exist for ATHENS users
- Access Management Transition Programme run by Nicole Harris to establish federation
- Main activity is outreach and training with some development

- JISC's mission is to provide world class leadership in the innovative use of ICT to support education and research
- eResearch team formed to address the challenges in research
- Manages a broad portfolio of projects that focuses on five main themes:
 - Community Engagement and Support
 - Collaborative Research Technologies
 - Authentication, Authorisation and Identity Management
 - Data, Knowledge and Information Management
 - Infrastructure Development.
- I head up the AA and IDM theme

UK Research Community is the primary beneficiary

- Arts & Humanities;
- Biotechnology and Biological Sciences;
- Engineering and Physical Sciences;
- Medical Sciences;
- Natural Environment;
- Particle Physics and Astronomy;
- Social Sciences.

RCUK www.rcuk.ac.uk

- Core Middleware Technology Development
 - SHIBGRID – better access to grid with Shib credentials via portal
 - SHEBANGS – better access to grid with Shib credentials via temp certificate
 - FAME-PERMISS – technology for levels of assurance
 - DyVOSE – demonstrator of dynamic delegation of trust for VOs
 - DyCOM – dynamic delegation of privileges for VOs
 - ESP-GRID - investigated how Shibboleth offers solutions to issues of grid authentication, authorisation and security
 - SPIE - demonstrated the use of Shibboleth in providing integration between institutional and national information environments.

■ eInfrastructure

- The Identity Project – managing identity within and between institutions
- ES-LoA – defining and agreeing levels of assurance
- CUCKOO – exploring practical implementation of VOs
- G-FIVO – creating VO services tied in with a virtual home for identities
- SHINTAU – using multiple attribute sets from multiple sources
- VPMAN – exploring use of PERMIS for VOs
- Grid accounting and usage study

■ Federation

- Don't re-invent the wheel; use what is already there in other federations
- Keep it simple – UK AM Federation has only 4 core eduPerson attributes
- Social issues (data protection, policy, training) are more important than technology
- Policy needs to be right first time
- Work to standards not technologies (SAML, eduPerson)
- Make a technology choice and give users practical help on that technology whilst allowing them to use their own

■ eResearch

- Use cases first, technology second
- Grid world and federated world have very different approaches (x509 v AM)
- Have a roadmap and keep updating it
- eResearch, as with research, is international – work with other countries
- eResearch tools are there to complement other research tools
- Don't reinvent the wheel – many tools, marketing, policy are already out there

- OpenID and Cardspace
- Researcher access to virtualised data
- Inter-federation
- Identity
- SCHAC and using new attributes
- Capabilities of Shib 2.0, as and when it is released!
- AAI tools

- Rest of the JISC eResearch team who can't be here!
- Ann Borda and Nicole Harris for slides and info
- TERENA
- Thomas Lengenhagger at SWITCH, Mikael Linden at CSC, David Simonsen at UNI-C, Diego Lopez at PAPI, Ingrid Melve at FEIDE, Klaas Wierenga at SURFnet, Victoriano Giralt at Uni of Malaga
- Thanks to the MAPS project for inviting me

- Questions?

- JISC www.jisc.ac.uk
- More details on TERENA and TF-EMC2 www.terena.org
- eInfrastructure programme - <http://tinyurl.com/36qn6z>
- UK Federation - <http://tinyurl.com/323mtn> and <http://www.ukfederation.org/>
- Identity Project – www.identity-project.info
- ES-LoA – www.es-loa.org
- Internet2 Shibboleth Roadmap - <http://tinyurl.com/3cpllx>
- EGEE - <http://www.eu-egee.org/>
- Kalmar Union Presentation at TF-EMC2 - <http://tinyurl.com/2shmfu>

James R.B. Farnhill
e-Research Programme Manager

JISC Executive,
j.farnhill@jisc.ac.uk
Tel: +44 77 66 44 22 59