The rapidly changing face of identity management for Higher Education and Research

Ric Phillips
MONASH University

Terry Smith
AUSTRALIAN ACCESS FEDERATION

Maria Corpuz
QUT

Neil Witheridge
aarnet
Digital Identity

Moonlight Towers and Horseless Carriages

Ric Phillips | Monash University
Hot Topics
in Federated IDM

Theta 2015
Terry Smith
Australian Access Federation
What we do

We provide the trusted authentication framework for education and research
150+ Services

Astronomy services
Research cloud
Virtual labs
Journals
Mass-storage servers
Animal databases
High performance computing labs
DNA systems

AAF Connecting researchers to Australia’s NCRIS capabilities

AUSTRALIAN ACCESS FEDERATION
• AAF is only for Web based services
• Non-web services?
• Other Protocols?
• Researchers outside the federation?
• Who are the researchers?
• Access control?
• Internationalisation?
Information Security and Privacy
Challenges for next generation IAM

Maria Corpuz
Queensland University of Technology
Traditional IAM

Create identities based on user’s personal information

Identity-based access – user authentication
Open access

Information Security risks/breaches:
- Cyber hacking
- Web site defacements, plagiarism
- Loss of intellectual property e.g. plagiarism
- Identity fraud in social media
- Copyright infringements

User requirements:
- Open access anywhere, anytime on any device
- Online collaboration, cloud services
- Single sign-on and federated access
- Social log-in
Legislation

“Australian Privacy Principle 8 — cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):
who is not in Australia or an external Territory; and
who is not the entity or the individual;
the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

……

Australian Privacy Principle 11 — security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:
from misuse, interference and loss; and
from unauthorised access, modification or disclosure. … “

Compliance Checklist

Information Security and Privacy:
- State and Federal standards:
  - Qld Govt Information Security Standard 18
  - Privacy Act
  - Qld Financial Mgt Act and Standards
  - Education Act
- Organisational:
  - Information Security (including Access Mtg policy)
  - Privacy policy
  - Fraud Management policy
  - Records Management
  - Code of Conduct
Solutions

Mitigations:
Information Security and Privacy:
- Security policy and guidelines (data classification, mobility, BYOD, social media etc)
- User awareness training
- Security architecture

Maria Corpuz
Institutional Challenge: End-User Support

Neil Witheridge, AARNet
(eduroam AU administrator)
How End-User support has changed

Before federated access:

- Same and Single Sign On
- Proliferation of services, not all delivering training and support capabilities (global service accessibility, a strength and a weakness)
- Authentication & access infrastructure involves 3rd party operators & complex components

After federated access:

- Support (L1)
- Institutional IT Support Helpdesk
- Training
- Access & Use
- Login using institutional account (integrated with institutional authentication infrastructure) or service-specific credentials

- Support (L2)
- Institutional Service Admin or ‘Owner’
- Training
- Service deployed / managed locally or hosted

- Support (L3)
- Institutional Identity Mgmt & Authentication Infrastructure Admin
- Training

- Service Vendor

Institutional IT Support
Helpdesk

6th May 2015
The Rapidly Changing Face of Identity Management in R&E
Federated Access: Support challenge

• Ability of an institution to provide effective end-user support in access to & use of federated services
  – Support roles:
    - institutional ITS provides support to end-users
    - institutional service admins provide support to ITS
    - institutional service admins are supported by service providers/owners & federated authentication & access infrastructure operators.

• Aspects of end-user support
  – Support roles & responsibilities
  – ITS knowledge & training
  – Trouble-shooting capabilities
  – Escalation path & process

• Global inter-federation exacerbates the challenge
Current & Emerging Solutions

• eduroam (currently institutional support is limited)
  – eduroam Policy defines support roles (Operator, Institution)
  – AARNet provides informational resources, support request system, 9:00-5:00 support, troubleshooting via National RADIUS Server logs

• SAML Federation (AAF) Services
  – AeRO User Support Project, AeRO Tick Accreditation
Candidate Solutions

• Training and troubleshooting enablement of institutional support staff

• eduroam
  — Reduce support demands by effective operability auditing
  — Automate troubleshooting between IdPs and SPs
  — Globally standardised trouble-shooting mechanisms
    • standard test authentication triggers & accounts
    • access to information from infrastructure & institutional logs

• SAML Federation
  — Globally standardised trouble-shooting mechanisms
    • Service Provider: standard test end-points, access to information from infrastructure & institutional logs