Australian Access Federation
For Research and Higher Education

Identifying Researchers

Presented at APSR Workshop, National Library of Australia
3 June 2008

Patricia McMillan
The University of Queensland
patricia.mcmillan@uq.edu.au

Australian Government
Department of Innovation, Industry, Science and Research

aaf australian access federation

What is the AAF?

Facilitates trusted electronic communications and collaboration within and between institutions of higher education and research in Australia and other organisations worldwide.

- User logs in to access resources

- Institution manages user's identity and credentials
  - Username and password and/or certificate
  - Attributes and other details that affect resource access

- Resource manager controls authorisation
  - What rules determine who may access a resource?
  - E.g., who you are or characteristics you have

- Federation sets policies and provides services
  - How members agree to exchange and handle information
  - Operates the central technology infrastructure
  - Provides support, packaging, training

Some AAF use cases

- Research data and facilities

- Institutional repositories

- Cross-institutional course delivery

- Collaboration tools and shared services

- Scholarly and information resource licensing

- Trusted electronic communications

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

AusCERT

MAMS
META ACCESS MANAGEMENT SYSTEM

MACQUARIE
UNIVERSITY · SYDNEY

Federations are about trust

- Details about you are asserted by your research org
  - Not self-asserted

- Defined levels of identity proofing
  - Examples:
  - In-person identification upon commencing work
  - 100 points test

- Relying party trusts the information

Do I need to know who you are?

- AAF supports anonymous, authenticated access
  - Sometimes it's not important to know who you are
  - e.g. access institution's subscription to Elsevier

- AAF supports identified access
  - Sometimes it's very important to know who you are
  - Scientific instrumentation, e.g. Synchrotron
  - Accessing one's own data objects in data grid
  - Viewing sensitive data, e.g medical linkage

Identifiers used with the AAF

- When I do need to know who you are

- PKI user certificate
  - Requires passing 100 points test
  - Two types: digital and crypto token
  - AusCERT provides root Certificate Authority (CA)

- Attributes asserted in SAML (Shibboleth) transaction
  - eduPersonTargetedID
  - auEduPersonSharedToken

eduPersonTargetedID

- From eduPerson international de facto std schema

- Different value for each combination of
  - User, Identity provider, and Service provider

- Privacy-preserving
  - Because each Service gets a different ID for a user

- Difficult to do linkage across services (e.g. Grids)

- Difficult to link objects and services to a user over time
  - Because users move around

auEduPersonSharedToken

- Part of new AAF auEduPerson schema

- Unique, opaque value for each user

- Non-targeted
  - Each Service gets the same ID for a user

- Portable (at user's option)
  - When a user changes organisations

- Enables linkage across services (e.g. Grids)

- Enables linkage of objects and services to users over time

Thank you!

www.aaf.edu.au

aaf.@aaf.edu.au

THE UNIVERSITY
OF QUEENSLAND
AUSTRALIA

AusCERT

Copyright © 2008 AusCERT

10

MAMS
META ACCESS MANAGEMENT SYSTEM

MACQUARIE
UNIVERSITY · SYDNEY