Shibboleth and the Australian Access Federation

James Dalziel
Macquarie University
james@melcoe.mq.edu.au

CAUL Meeting 2008/1,
Sydney University Village, April 4th, 2008
Shibboleth Key Principles

• Home institution (“Identity Provider”) login
• Institution-backed identities (not self-assertion)
• Services trust Identity Providers, rather than manage local user accounts
• Privacy preservation where required

• MAMS Testbed Federation currently has 1,000,000+ identities across 26 IdPs (inc 14 Aust unis & 2 NZ unis) and 27 SPs (eg, institutional repositories, Grid services, datasets, project wikis, online librarian, etc)
Key questions for Libraries

• Why the move to Shibboleth?

• Will libraries be required to know anything about it?

• Will libraries be required to do anything about it?

• What will we be able to do that we cannot do now?

• What is the time scale for implementation - in our universities, for libraries?
Key questions for Libraries

• Why the move to Shibboleth?
  – Too many user accounts and passwords!
  – Poor security arising from too many user accounts
  – Management overheads from too many accounts
    • Up to 75% of helpdesk calls are password related
  – Libraries can focus on providing access, not managing identities
  – Shibboleth can provide strong privacy protection
    • Allows for “trusted anonymous” access
    • This requirement came directly from librarians in 2000
  – Shibboleth was built for higher education, 10+ federations around the world and growing
Key questions for Libraries

• Will libraries be required to know anything about it?
  – Useful to understand high level concepts, especially the distinction between an Identity Provider (IdP) and a Service Provider (SP)
  – Don’t need to know details for managing IdP
    • This is normally the task of IT Services/HR
  – Do need to know details of SP management
    • In Shibboleth, a library is a large collection of SPs
    • Over time, many library services that currently manage their own user accounts will move to become Shibboleth Service Providers
Key questions for Libraries

• Will libraries be required to do anything about it?
  – Not normally – Shibboleth adoption should be a choice due to its benefits, not a forced requirement
  – Initial focus is likely to be on new Services that require secure access, or existing services with burdensome account management issues
  – Library technical staff should begin to learn about how to implement a Service as a Shibboleth SP
    • MAMS training workshops
  – Long term, IT Services will provide user attributes; libraries will be the experts in deciding policies about who gets access to what, based on user attributes
Key questions for Libraries

• What will we be able to do that we cannot do now?
  – Less time on account management, so more time for other library priorities
  – Provide access to secure resources based on identity rather than physical location
    • Eg, able to support home access, as no longer rely on IP address based authentication
  – Support secure access for users from other institutions
  – Provide a wider range of access policies, implement them more easily, and change them easily if required
  – Support more complex eResearch access requirements
Key questions for Libraries

- What is the time scale for implementation - in our universities, for libraries?
  - MAMS Testbed been in operation for 2.5 years – a number of libraries use it for production services today:
    - UQ Institutional Repository
    - Macquarie + Murdoch shared online librarian service
    - WAGUL reciprocal borrowing
  - AAF begins rollout later in 2008
    - Subject to legal agreements and establishment
  - Your local IT Services is a likely first point of contact with AAF (to establish the university’s IdP)
  - For libraries, I would encourage technical staff to seek SP training this year so they are ready for projects in 09
    - Could do a libraries SP workshop – just tell us when!