Integrating Identity Management – Aspirations and Issues

James Dalziel
Professor of Learning Technology, MAMS CI and Director, Macquarie E-Learning Centre Of Excellence (MELCOE)
Macquarie University
james@melcoe.mq.edu.au
www.melcoe.mq.edu.au

Presentation for Open Repositories 2006, University of Sydney, 2nd February 2006
Overview

• Aspirations for repositories
• Where are we today – identity and access?
• What could the future be?
• Any reason for optimism?
  – Directory/SSO
  – Shibboleth
  – XACML
  – Open Source Software
• MAMS
Some Aspirations

• Staff and students can share a compound (multi-part) resource (e.g., PhD) where some parts are openly available, and some parts require restricted access
  
  *(Restrictions could be by country, institution, time, role, discipline)*

• A researcher can share a valuable, restricted availability dataset with colleagues at partner institutions and/or discipline peers – easily, securely, automated

• A librarian can manage access policies for protected resources in a single, unified way regardless of the type of resource, repository software, location of resource, etc
Some Aspirations

- IT managers can provide a central, secure identity service which provides Single-Sign-On to all applications and repositories, and application/repository owners don’t manage identities, just access policies based on attributes.

- Access to federated search facilities that work across many repositories; including the new problem of “authenticated federated search” across protected repositories.

- Solve DRM without lock-ins, preserve privacy and maintain openness wherever possible and appropriate.
Two More Aspirations....

• Identity and Access Management solutions for institutional repositories should also work for:
  – Dataset repositories
  – Learning Object Repositories
  – Online collaborative “Virtual Organisations”
  – Grid/High Performance Computing services
  – Campus portals
  – Etc

• Solutions should work across institutional boundaries (not just within)
  – Therefore open standards are crucial, as the systems will be different
### Convergence of Higher Education Domains

<table>
<thead>
<tr>
<th>IT Services</th>
<th>E-RESEARCH</th>
<th>SCHOLARLY INFORMATION</th>
<th>E-LEARNING</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Interfaces</td>
<td>User Interfaces</td>
<td>User Interfaces</td>
<td>User Interfaces</td>
</tr>
<tr>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
</tr>
</tbody>
</table>

#### Middleware

<table>
<thead>
<tr>
<th>Common services</th>
<th>Common services</th>
<th>Common services</th>
<th>Common services</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>Infrastructure</th>
<th>Infrastructure</th>
<th>Infrastructure</th>
</tr>
</thead>
</table>

- Enterprise Info DBs
- Datasets Repositories
- Knowledge Repositories
- Learning Object Repositories
What is typical today - identity?

• Well managed central directory of identities is rare, mainly a fairly messy set of identity silos across campus
  – Eg, nine different identity silos just within the library

• Identity management processes are weak and inconsistent
  – “Evidence of identity” is uneven, “provisioning” uneven, lots of security holes (but mainly in low risk contexts, eg e-journals)

• Repository systems are hard (or impossible) to link to external directories of identities (…hence silos)

• IP address, not person-based, access to protected content
What is typical today - access?

• Repository software has its own (usually closed) approach to controlling “who gets access to what” (authorisation)
  – Open source software, while helpful, is not necessarily a solution if a repository’s authorisation mechanisms are not cleanly separated

• Access to protected resources usually requires personally identifying information (typically a name and password)
  – Privacy implications for search; intellectual property disclosure issues (bio)

• Library-managed protected resources involve a nightmare of access management issues (both contracts and technical)

• **Many researchers have valuable resources/datasets sitting on their desktops because they don’t have a simple method for restricted sharing
What could the future be?

- One central identity store (managed by IT Services)
- Single-Sign-On across all appropriate applications
- Able to share (open and) restricted-access resources
  - Easily, automated, preserve privacy where relevant
- Able to easily manage access policies
  - A new key role of the librarian?
- Traditional and authenticated federated search

No more identity duplication or hard-wired access control!
Any reason for optimism?

1. Central Directories/Single-Sign-On
2. Shibboleth
3. XACML
4. Open source software
Directory/SSO

• Examples of one, centralised, well managed directory of identities providing Single-Sign-On now exist in universities
• Most university IT managers have identity projects on their list of priorities (although rarely at the top yet)
  – **Now is the time to push for these projects to start
• Many applications are getting better at working with external identities and SSO (if not, question their future value)
• E-Security concerns are becoming a new driver
• SAML V2 incorporates SSO
Shibboleth (SAML) 101

- Open source software based on an open security standard (SAML – Security Assertion Markup Language)
- Allows an identity system (eg, directory) to pass attributes to service system (eg, repository)
- World-class privacy preservation
  - Core use case: A researcher at University A wants to access a restricted resource in a repository at University B; where the repository needs to know the request comes from a trusted partner institution, but without necessarily identifying the individual

- Shibboleth is crucial, but not the whole solution
  - (Shibboleth manages and transmits the attributes only)
XACML 101

• Open standard for policies to control access (XACML – eXtensible Access Control Markup Language)
  – Open source XACML processor available

• Allows access to repository resources to be controlled by a separate, flexible, easily-edited language

• Can receive SAML attributes to process yes/no access decisions

• SAML + XACML provides an alternative solution to DRM
  – IFFFFFFFFF….. web based access control is sufficient for now…..
Open Source Software

• Open source software has a range of potential benefits
  – Innovation
  – Total cost of ownership
  – Re-use and adaptation of software

• In the particular case of repositories and access control, open source is useful for two reasons:
  – Access rights associated with resources remain open (no risk of closed rights being used for proprietary software lock-in)
  – Open source allows developers to build access control software modules that are not hard-wired into the rest of the repository
    • Potential for a single access control system and a unified set of access policies, regardless of repository software chosen
      – But – requires repository to allow for modular access systems
MAMS

- MAMS (Meta Access Management System) is a 3 year DEST funded project to solve end-to-end identity/access issues
- Working on Directories/SSO (with IT Managers); Shibboleth (including easy install CD, national testbed federation, ShARPE); Shibbolising repositories; XACML for repositories; authenticated federated search
- Testbed federation is available (400,000 identities so far)
  - Use easy install CD to join (www.federation.org.au for more details)
- Various workshops and roadshows throughout 2006
  - Eg, technical workshop on shibbolising services in February
- The vision described today already works – rollout is the key
Collated Votes for MAMS Service Prioritisation

<table>
<thead>
<tr>
<th>Subject</th>
<th>Number of votes</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Sign-On</td>
<td>129</td>
<td>1</td>
</tr>
<tr>
<td>DRM &amp; Repository Access</td>
<td>100</td>
<td>2</td>
</tr>
<tr>
<td>Federation Policy</td>
<td>76</td>
<td>3</td>
</tr>
<tr>
<td>Virtual Organisations</td>
<td>59</td>
<td>4</td>
</tr>
<tr>
<td>Attribute management</td>
<td>57</td>
<td>5</td>
</tr>
<tr>
<td>Accountability/Audit</td>
<td>47</td>
<td>6</td>
</tr>
<tr>
<td>Visiting Academic</td>
<td>45</td>
<td>7</td>
</tr>
<tr>
<td>User Preferences</td>
<td>32</td>
<td>8</td>
</tr>
<tr>
<td>Messaging</td>
<td>12</td>
<td>9</td>
</tr>
<tr>
<td>Calendaring</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>Anonymous Access</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>Presence</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>AV conferencing</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>Whiteboard</td>
<td>1</td>
<td>14</td>
</tr>
</tbody>
</table>