Identity Management in the Higher Education Experience

Renee Woodten Frost
Internet2/University of Michigan

Ron Yanosky
ECAR Research Fellow, EDUCAUSE
• Copyright Renee Woodten Frost and EDUCAUSE 2006. This work is the intellectual property of the authors. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the authors. To disseminate otherwise or to republish requires written permission from the authors.
Topics

• What is IdM and Why does it matter?
• IdM Architecture
• Institutional Motivations, Challenges, Plans
• Resources and Project Management
• A Look to the Future
• Moving Forward
Identity Management: What is it?

*The business processes and infrastructure required to support the creation, maintenance, and use of digital identities.*  
(Courtesy The Burton Group)

A *collection* of *technologies, business processes, and underlying policies* that enables *networked systems* to determine who has *access*, when they get and lose access, and what they are *authorized* to access, while *protecting* individual privacy and access to confidential information.
Knock, knock. Who *is* there?

- Internet users grew from 45 million to over 1 billion 1995-2005
- Annual cost of U.S. identity theft is about $50 billion

Sources: eTForecasts; US Federal Trade Commission; Privacy Rights Clearinghouse
Digital Identity in the Spotlight

- EDUCAUSE 2005 Current Issues #1 “greatest potential to become more significant” & 2006 “most significant”
- Federal leadership/coercion:
  - HSPD-12 and federal Personal Identity Verification
  - E-Authentication Levels of Assurance
  - FDIC/FFIEC recommendations for 2-factor AuthN
- Identity federation a la Shibboleth and Liberty Alliance
The Key Functions

- **Who** am I - *Identification*
- Am I really **who** I say I am - *Authentication*
- **What** am I allowed to do - *Authorization*
- **When** do I get an account, when do I get authorization, and when is my authorization changed - *Provisioning*
- **When** is my account, and the resources associated with it, removed – *De-provisioning*
- **How** does everything work together to provide an effective, accurate, secure set of services - *Technology and Business Processes*
- The **Why** - The underlying *Policy*
Identity Management
Architecture
An Introduction to IdM Architecture

- A. Michael Berman

![Diagram showing data sources, person registry, directories, and apps & platforms]
Potential Simplification: Using a Core System as the Registry

Data sources —> Person Registry —> Directories —> Apps & Platforms
Potential Simplification: Use Directory as Person Registry
Institutional Motivations, Challenges, & Plans
## Motivation to Pursue IdM

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security/privacy best practices</td>
<td>80.9</td>
</tr>
<tr>
<td>Enhanced user services and satisfaction</td>
<td>60.8</td>
</tr>
<tr>
<td>Regulatory compliance (e.g. HIPPA, GLB Act, FERPA)</td>
<td>42.7</td>
</tr>
<tr>
<td>Strategic value/opportunities</td>
<td>22.8</td>
</tr>
<tr>
<td>Improvements in our technical environment</td>
<td>20.3</td>
</tr>
<tr>
<td>Keeping current with generally accepted IT directions</td>
<td>18.9</td>
</tr>
<tr>
<td>Cost reduction/increased efficiencies</td>
<td>18.6</td>
</tr>
<tr>
<td>Position the institution for implementation of federated identity</td>
<td>14.6</td>
</tr>
<tr>
<td>Strategy of early adoption/experimentation</td>
<td>1.2</td>
</tr>
<tr>
<td>Reduce vendor dependencies</td>
<td>0.5</td>
</tr>
</tbody>
</table>

*Total percentage of respondents ranking item as first, second, or third highest motivation*

Source: EDUCAUSE Center for Applied Research
12345
Decentralize user acct mgmt and authZ
Allow non-inst users access to our inst resources requiring our authN
Give visitors only access required and disable at correct time
Strong authN
Allow inst users access to off campus resources requiring sep authN
User authN and authZ processes scalable
Immed change auth services for user who changes roles
Provide self-service functions
Immed enable auth new user services
Single authoritative source for affiliated persons
Track illegal or unauth network activity to person responsible
Prior to issuing credentials, have confidence in user identity
Immed disable all services & IDs when user no longer affiliated

Respondents uniformly assessed the importance of IdM benefits higher than their capability to them.

1=very low, 2=low, 3=medium, 4=high, 5=very high

Source: EDUCAUSE Center for Applied Research
Senior Management Understanding

- **Understands benefits**: 9.5% Strongly Agree, 31.8% Agree, 23.3% Neutral, 31.3% Disagree, 4.1% Strongly Disagree
- **Understands the costs**: 2.8% Strongly Agree, 14.1% Agree, 26.7% Neutral, 46.7% Disagree, 9.7% Strongly Disagree
- **Willing to address related policy issues**: 8.9% Strongly Agree, 46.2% Agree, 31.3% Neutral, 11.2% Disagree, 2.3% Strongly Disagree

Source: EDUCAUSE Center for Applied Research
IdM Documentation

- Documented data owners/custodians:
  - Completed: 32.5%
  - In progress: 33.5%
  - Planning to do: 23.8%
  - Not planning to do: 6.5%

- Documented data definitions, reconciling differences:
  - Completed: 15.0%
  - In progress: 38.3%
  - Planning to do: 28.8%
  - Not planning to do: 10.8%

- Risk assessment of data access security and privacy practices:
  - Completed: 12.8%
  - In progress: 34.4%
  - Planning to do: 36.2%
  - Not planning to do: 11.8%

- Released an RFI or RFP for Identity Management:
  - Completed: 5.5%
  - In progress: 16.1%
  - Planning to do: 62.0%
  - Not planning to do: 11.8%

Source: EDUCAUSE Center for Applied Research
RSSO, Enterprise Directories, RBA

Source: EDUCAUSE Center for Applied Research
Plenty of IdM Work on the Table

- 64% of respondents were either implementing ED, RSSO, or RBA, or planning to in some time frame
- Majorities with operational EDs plan to enhance them
- Almost nobody entirely rules out at least considering these technologies

Source: EDUCAUSE Center for Applied Research
Authentication: How many arrows in the institutional quiver?

- 28% use one or more multi-factor authN technologies specified; only 1% use more than two such methods
- Of those using no such methods, 63% either have no plans to use them, or don’t know their plans
- 10% use PKI in some form, somewhere for user network authentication (15% planning)

Source: EDUCAUSE Center for Applied Research
Resources and Project Management
IdM Project Highlights

- 89% of respondents were engaged in “efforts or projects related to identity management”
- Only 28% report stand-alone IdM projects; the rest are bundled with other projects
- 42% have used consultants or external services for IdM projects

Source: EDUCAUSE Center for Applied Research
Expected central IT spending on IdM projects in the next 3 years (N=339)

<table>
<thead>
<tr>
<th>Category</th>
<th>Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>$50,000 or less</td>
<td>26.5</td>
<td>26.5</td>
</tr>
<tr>
<td>$50,001 to $100,000</td>
<td>20.6</td>
<td>47.2</td>
</tr>
<tr>
<td>$100,001 to $500,000</td>
<td>28.3</td>
<td>75.5</td>
</tr>
<tr>
<td>$500,001 to $1 million</td>
<td>5.9</td>
<td>81.4</td>
</tr>
<tr>
<td>Between $1 million and $2 million</td>
<td>2.9</td>
<td>84.4</td>
</tr>
<tr>
<td>Between $2 million and $5 million</td>
<td>1.5</td>
<td>85.8</td>
</tr>
<tr>
<td>More than $5 million</td>
<td>0.3</td>
<td>86.1</td>
</tr>
<tr>
<td>Don’t know</td>
<td>13.9</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Percentage of project-active respondents choosing each category

*Source: EDUCAUSE Center for Applied Research*
IdM Project Sponsorship

- CIO (or equivalent)
- Director/manager of IT networking
- Director of administrative computing
- Other IT management
- Administrative functional area executive
- Other administrative management
- Chief information security officer
- Other academic management

Percentage of project-active respondents selecting item; multiple responses allowed

Source: EDUCAUSE Center for Applied Research
Getting Value from IdM Project Investments (N=254)

Source: EDUCAUSE Center for Applied Research
A Look to the Future
Leveraging For The Future

- Be prepared
- New technologies are in development now
- New business processes and policies will need to be incorporated
- Think about how whatever you implement now will fit in with future requirements and solutions
Federated Identity Management

- Federated Identity Management
  - A system that allows individuals to use the same user name, password, or other personal identification to authenticate and be authorized to use services hosted by another organization.

- Single Sign-on or Initial Sign-On for the Web
  - Institutional applications
  - External partner applications
  - Can protect privacy and not give away your data
Inter-institutional Collaboration Drives Federations

• One institution hosting course-content for another
• Students at one college taking an on-line course from another college
• Libraries purchasing licenses for multiple vendors with specific access policies
• Researchers making resources available to project members at other schools
• Schools in state systems or articulation relationships that require mutual access to services
When Will You Need a Federated ID Solution?

<table>
<thead>
<tr>
<th>When</th>
<th>DR</th>
<th>MA</th>
<th>BA</th>
<th>AA</th>
</tr>
</thead>
<tbody>
<tr>
<td>We do not envision a need</td>
<td>6.1</td>
<td>19.8</td>
<td>18.9</td>
<td>17.0</td>
</tr>
<tr>
<td>We have a need now</td>
<td>30.3</td>
<td>6.3</td>
<td>6.8</td>
<td>10.6</td>
</tr>
<tr>
<td>In the next 12 months</td>
<td>11.1</td>
<td>4.5</td>
<td>8.1</td>
<td>0.0</td>
</tr>
<tr>
<td>Between 1 and 2 years from now</td>
<td>19.2</td>
<td>15.3</td>
<td>14.9</td>
<td>8.5</td>
</tr>
<tr>
<td>Between 2 and 3 years from now</td>
<td>19.2</td>
<td>16.2</td>
<td>16.2</td>
<td>8.5</td>
</tr>
<tr>
<td>More than 3 years from now</td>
<td>5.1</td>
<td>11.7</td>
<td>10.8</td>
<td>10.6</td>
</tr>
<tr>
<td>Don’t know</td>
<td>9.1</td>
<td>26.1</td>
<td>24.3</td>
<td>44.7</td>
</tr>
</tbody>
</table>

Percentage of respondents in category

Source: EDUCAUSE Center for Applied Research
What is a Federation?

- An association of organizations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions.
- Uses common policy, technology, and business practices to establish trust
- Access services from (or provide services to) other institutions, corporate partners, government organizations
- A contractual arrangement
Federated Model

• Enterprises and organizations provide local authentication and attributes, namespaces, etc.
• Uses a variety of end-entity local authentication – PKI, username/password, Kerberos, two-factor, etc.
• Enterprises within a vertical sector federate to coordinate LOA’s, namespaces, metadata, etc.
• Provides a scalable alternative to multiple bilateral technical relationship management
• Prepares for inter-federation exchange
InCommon

• InCommon: US Research & HE Federation
  – www.incommonfederation.org
  – More than 20 higher-ed institutions, plus several service providers

• Shibboleth: common technology that supports local authentication with remote authorization
  – shibboleth.internet2.edu

• Requires an institutional commitment
  – specific policy requirements relatively lightweight (but evolving)
More Functions/Technologies Leveraging IdM Infrastructure

• Directories/Schema
  – edu*: person, org, course, group
  – schema coordination efforts

• Signet™  Grouper™

• Provisioning: Nexus

• Workflow

• Messaging/event services

• Virtual Organization Support

• Lionshare, Medical Middleware, Connective or Real Time Middleware, Digital Rights Mgmt, Learning Mgmt (ie, SAKAI)
Moving Forward
Identify Goals

• Identify objectives and constraints
  – Single common userid? Will all stakeholders agree?
  – Single common password? Is that a desirable goal?
  – Identify systems & applications that will be integrated
  – How do we deal with FERPA & other external reqs?
  – What are the tolerances for real-time response & outages?

• Identify possible future initiatives such as
  – Inter-institutional federation
  – Integration with ID card (if not already part)
  – Integration with government systems
  – Etc.
Other Preparatory Steps

- **Describe Current Conditions**
  - identify existing directories, directory-enabled technologies, resources, network infrastructure condition, etc

- **Document Systems**
  - unique user identifier; events, triggers to include; tables, schemas, crosswalks with registry; possible integration points, existing automated data exchange with other systems in the scope, security requirements, etc.

- **Document Policy and Business Processes**

- **Assess Candidate Technologies**
  - embrace standards and flexible architectures
Open and Commercial Standards

• Consider how a technology you select for IdM will incorporate new open standards:
  – SAML – Security Assertion Markup Language
  – Shibboleth – Federated IdM based on SAML
  – SOAP – Simple Object Access Protocol
  – EduPerson LDAP Schema
  – XML

• Proprietary Standards should be considered also
  – Microsoft ADFS, Active Directory Federation Services
  – Liberty Alliance
  – WS-Federation – WS-trust, WS-Policy
Other Technology Considerations

- **Strong authentication = at least 2-factor**
  - What You Know = the first factor and is usually a password
  - What You Are = biometrics (ie, Fingerprint, Retinal print, Facial characteristics, DNA?)
  - What you have = the second factor (or third) (ie, Smart cards, RFID, One-time password generator, Certificate on a stick)

- **Public Key Infrastructure (PKI)**
  - Many are already using at least some PKI in the form of SSL Certificates
  - PKI is used for digital signatures and will be important in
  - federated identity management
  - Identity & access management is a prerequisite to many uses of PKI

How will these technologies factor into your IdM plans?
Create the Vision

• Document the envisioned environment
  – Which identity objects will be synchronized across apps?
  – What are the canonical sources for identity information (identity objects)?
  – How will information flow through the system?
  – Where and how can an identity object be modified and how will those modifications propagate?
  – What are the new business processes for identity management?
  – How will endpoint application authorities authorize identity objects for their domain?
  – How will security be maintained?
NMI-EDIT:
HE Community Resources

• National Science Foundation Middleware Initiative (NMI)

• Enterprise and Desktop Integration Technologies Consortium (NMI-EDIT)
  – Internet2 and EDUCAUSE

• Project Goals
  – Create a common, persistent and robust core middleware infrastructure for the R&E community
  – Provide tools and services in support of inter-institutional and inter-realm collaborations
MACE Advisory Group

- Promote deployment of common middleware infrastructure across higher ed
- Practices, standards, models, tools, documentation to facilitate campus design & implementation
- Community-based, community-driven
  - Early adopters, working groups
- Liaison, collaboration with other middleware communities
- Demonstrate viable models to vendor community
NMI-EDIT Deployment Guidance

- Enterprise Directory Implementation Roadmap

- DRAFT Enterprise Authentication Implementation Roadmap
NMI-EDIT Tutorials, Seminars, and Workshops

• EDUCAUSE regional and annual conferences
  – Look for NMI-EDIT in the abstract
  – Track sessions and preconference seminars

• 2006 CAMP (Campus Architecture and Middleware Planning) Workshops
  – June 26 - June 30, Burlington VT
    • CAMP Shibboleth
    • Advanced CAMP on Workflow
  – November TBD
    • CAMP Signet/Grouper

• Open workshops preceding Internet2 meetings
  – December 4-7 in Chicago IL
    events.internet2.edu/2006/fall-mm/index.html
Websites

- Internet2 Middleware Initiative
  - middleware.internet2.edu
- NMI-EDIT
  - www.nmi-edit.org
- NSF Middleware Initiative
  - www.nsf-middleware.org
- Net@EDU Identity Management Working Group
  - www.educause.edu/idm
Email Lists

• Net@EDU Identity Management Working Group
  – General discussion on middleware
  – www.educause.edu/idm

• Internet2 MACE-Dir
  – Technical directory discussion
  – middleware.internet2.edu/dir

• NMI lists
  – Information about NMI releases, press announcements, and upcoming events