Identity Management

Conference Report

Conference
Hosted by the Chief Information Officers of the Committee on Institutional Cooperation

June 5-6, 2006
University Place Conference Center and Hotel
Indianapolis, IN
Conference Planning Committee

Chair
Annie Studden, Chief Information Officer
University of Wisconsin-Madison

Members
Tom Barton
University of Chicago

Mike Grady
University of Illinois at Urbana-Champaign

Alan Walsh
Indiana University, Bloomington

Chris Pruess
University of Iowa

Liz Salley
University of Michigan

Luke Tracy
University of Michigan

Matt Kolb
Michigan State University

Christopher Rigsby
University of Minnesota

Tom Board
Northwestern University

Mitch Dysart
Ohio State University

Kevin Morooney
Pennsylvania State University

Mike Carr
Purdue University

Mairead Martin
University of Wisconsin-Madison

Jim Phelps
University of Wisconsin-Madison

Ann West
Educause/Internet2

CIC Headquarters Staff
Karen Partlow
Associate Director, Technology Collaboration

Galen Rafferty
IT Specialist
Contents

INTRODUCTION 1

CIC CHIEF INFORMATION OFFICERS 2

CIC MEMBERS (PROVOSTS) 3

CONFERENCE AT A GLANCE 4

CAMPUS IDM PRIORITIES 5

CAMPUS IDM MATRIX 6

CAMPUS IDM PRIORITIES - INDIVIDUAL 7

UNIVERSITY OF CHICAGO 7

UNIVERSITY OF ILLINOIS 9

INDIANA UNIVERSITY 11

UNIVERSITY OF IOWA 12

UNIVERSITY OF MICHIGAN 13

MICHIGAN STATE UNIVERSITY 14

UNIVERSITY OF MINNESOTA 15

NORTHWESTERN UNIVERSITY 16

OHIO STATE UNIVERSITY 17

PENNSYLVANIA STATE UNIVERSITY 18

PURDUE UNIVERSITY 19

UNIVERSITY OF WISCONSIN-MADISON 21

RESOURCES SHARED IN PRESENTATIONS 21

ATTENDEES BY UNIVERSITY AND CAMPUS AREA 23

ATTENDEES 24
A warm welcome to the first CIC Identity Management Conference. This conference came about as the result of an idea brought forward from a group of senior IT leaders in our institutions (they are known as the AIS Directors) to the CIOs last fall. The CIOs agreed this was a hot topic at our universities, and that we would sponsor a conference to discuss the issues and concerns around building a strong identity management program on our campuses, a program that could provide secure access to information and services based on individual and group roles and responsibilities. This is a big task to accomplish at our universities, and it is our hope that this conference will push us all a bit further in our knowledge about the issues as well as our understanding of development and implementation concerns.

Solving the identity management puzzle isn’t only an IT challenge. It is a challenge for our campus partners who collect and provide information and services to our campus communities. The IT challenge is to provide an IT infrastructure that allows our campus identity management programs to be technically implemented. It is our student service colleagues, our human resource colleagues, our campus security and police agencies, our librarians, and other campus partners who need to define the identity management program for our campuses.

We are most fortunate to have three national leaders in the thinking about identity management as keynote speakers for this conference, Peter Alterman, Michael Gettes, and Ken Klingenstein. In addition to being leaders in moving us forward nationally on identity management, these three folks are also great fun to listen to.

So, enjoy this conference. We hope that it will give all of you the opportunity to think well about the identity management issues on our campuses – and beyond – and bring all of us new ideas and opportunities for moving identity management initiatives forward.

Annie Stunden,
Chief Information Officer, Office of Information Technology
University of Wisconsin-Madison; and Chair, Conference Planning Committee
CONFERENCE GOALS:

- To develop a common language around Identity Management.
- To share what is happening on each CIC campus in terms of identity management and middleware.
- To identify the intramural collaboration opportunities as well as what the CIC universities might do jointly to push the current state of the art.

WHAT DOES “IDENTITY MANAGEMENT” MEAN?

Identity Management is an integrated system of business processes, policies and technologies that enable organizations to facilitate and control their users’ access to critical online applications and resources while protecting confidential personal and business information from unauthorized users. It represents a category of interrelated solutions that are employed to administer user authentication, access rights, access restrictions, account profiles, passwords, and other attributes supportive of users’ roles/profiles on one or more applications or systems.

WHAT IS MIDDLEWARE?

Middleware is the technology used to implement Identity Management policies. Middleware, or “glue,” is a layer of software between the network and the applications. This software provides services such as identification, authentication, authorization, directories, and security. One instance of process improvement through middleware is Single Sign On (SSO). SSO between applications allows users to authenticate once, then move seamlessly from service to service without having to login repeatedly. SSO between institutions is now technically feasible through “federation” middleware. This allows students and faculty to securely access a partner university’s library, data and computing resources across the Internet. Identity management policies are an important aspect of the trust needed between universities to join in a federation.
CIC Chief Information Officers

University of Chicago
Gregory A. Jackson, Chair, Chief Information Officer

University of Illinois at Chicago
Ahmed S. Kassem, Vice Provost & CIO, Director, Academic Computing & Communications Center

University of Illinois—Urbana-Champaign
Peter M. Siegel, Chief Information Officer

Indiana University, Bloomington
Brad C. Wheeler, Acting Chief Information Officer, IU Bloomington Dean of Information Technology

University of Iowa
Steve Fleagle, Associate Vice President and CIO

University of Michigan
James L. Hilton, Associate Provost, Academic, Instructional and Information Technology

Michigan State University
David Gift, Vice Provost, Libraries, Computing & Technology

University of Minnesota
Steve Cawley, Associate Vice President & CIO, Office of Information Technology

Northwestern University
Mort A. Rahimi, Vice President & Chief Technology Officer, Information Technology

Ohio State University
Ilee Rhimes, Jr., CIO, Office of Information Technology

Pennsylvania State University
J. Gary Augustson, Vice Provost, Information Technology

Purdue University
James R. Bottum, Vice President for Information Technology

University of Wisconsin-Madison
Ann Studden, Chief Information Officer, Division of Information Technology
University of Chicago
Richard P. Saller, Provost

University of Illinois
University of Illinois - Chicago: R. Michael Tanner, Provost and Vice Chancellor for Academic Affairs
University of Illinois-Urbana-Champaign: Linda Katehi, Provost and Vice Chancellor for Academic Affairs

Indiana University, Bloomington
Michael A. McRobbie, Interim Provost and VP for Academic Affairs, Bloomington

University of Iowa
Michael J. Hogan, Provost

University of Michigan
Teresa A. Sullivan, Provost and Executive Vice President

Michigan State University
Kim Wilcox, Provost

University of Minnesota
E. Thomas Sullivan, Executive Vice President and Provost

Northwestern University
Lawrence B. Dumas, Provost

Ohio State University
Barbara R. Snyder, Executive Vice President and Provost

Pennsylvania State University
Rodney A. Erickson, Executive Vice President and Provost

Purdue University
Sally Mason, Provost

University of Wisconsin-Madison
Patrick Farrell, Provost and Vice Chancellor for Academic Affairs

The CIC is a consortium of 12 research universities, including the 11 members of the Big Ten Conference and the University of Chicago. With campuses in 8 states, CIC universities enroll more than 300,000 undergraduates and 76,000 graduate students, and employ some 33,000 full-time faculty and 139,000 full-time staff.

The CIC is guided by the Provosts of the member universities.
## Conference at a Glance

### Monday, June 5, 2006

<table>
<thead>
<tr>
<th>Time</th>
<th>Plenary session (Room #137)</th>
<th>Process Track (Room #208)</th>
<th>Policy Track (Room #216)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:30 – 9:45a</td>
<td>BREAK (outside of session rooms)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9:45-10:45a</td>
<td>Plenary Panel: Services and Privileges and Managing Groups and Roles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00-Noon</td>
<td>Assigning Identity and ID Cards</td>
<td>Governance Processes</td>
<td></td>
</tr>
<tr>
<td>Noon – 1:00p</td>
<td>LUNCH (Bistro; second floor, hotel lobby)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:00 – 2:00p</td>
<td></td>
<td>Identity Silos</td>
<td>Federated Identity and Sharing Resources Beyond Campus</td>
</tr>
<tr>
<td>2:00-3:00p</td>
<td></td>
<td>Risks and Trends in Authentication</td>
<td>Big Policy Issues</td>
</tr>
<tr>
<td>3:00 – 3:15p</td>
<td>BREAK (outside of session rooms)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:15-4:15</td>
<td>Functional Peer Group Discussions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:15-5:15</td>
<td>Campus Team Discussions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:15-6:30p</td>
<td>Reception (Bistro; second floor, hotel lobby)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6:30p - ??</td>
<td>Dinner on your own</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Tuesday, June 6, 2006 (Room #137)

<table>
<thead>
<tr>
<th>Time</th>
<th>Plenary session</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00-8:15a</td>
<td>West: Recap of Day 1 activities, overview activities and goals for day 2</td>
</tr>
<tr>
<td>8:15-9:00a</td>
<td>Klingenstein: “Bob’s and Keith’s (and many others’) Excellent Adventure”</td>
</tr>
<tr>
<td>9:00-10:00a</td>
<td>Plenary Panel: Protecting Identities</td>
</tr>
<tr>
<td>10:00-10:15a</td>
<td>BREAK (outside of session Room #137)</td>
</tr>
<tr>
<td>10:15-11:30</td>
<td>Campus Team Discussions and reporting out</td>
</tr>
<tr>
<td>11:30-1:00p</td>
<td>West: Summary, next steps and box LUNCH</td>
</tr>
</tbody>
</table>
One of the important outcomes for the conference came from the Campus Team Discussions, which gave each team an opportunity to identify its campus priorities for future Identity Management initiatives. As part of these sessions, each campus identified at least three priorities which the conference moderator summarized in the final session. Attendee feedback indicated great interest in having these campus priorities published for all to read. So after the conference, each member of the planning committee briefly summarized the top Identity Management priorities for their respective institutions. These summaries appear on pages 7-20.

In addition, a summary matrix of these priorities on page 6 identifies recurring or common items, providing a view of which campuses are planning or implementing initiatives on similar priorities. Although past or completed initiatives are not captured here, this matrix may be useful in identifying potential for collaboration among campuses who wish to share plans or solutions to the upcoming planned Identity Management issues they have in common.
<table>
<thead>
<tr>
<th>Wisc-Mad</th>
<th>Purdue</th>
<th>PSU</th>
<th>OSU</th>
<th>NWU</th>
<th>Minn</th>
<th>MSU</th>
<th>Mich</th>
<th>Iowa</th>
<th>Indiana</th>
<th>Illinois</th>
<th>Chicago</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Achieve level 2 CAF assessment</td>
<td>Develop a common IdM governance and policy</td>
<td>Reposition and improve new IdM governance and policy for nontraditional communities</td>
<td>Implement appropriate policies and procedures</td>
<td>Determine need for governance structure</td>
<td>Join InCommon Federation</td>
<td>Continue Two-Factor validation</td>
<td>Complete identity deployment</td>
<td>Complete implementation of e-Auth</td>
<td>Federaing with the Fed</td>
<td>Establish UC-wide person ID</td>
<td>Establish UC-wide directory and IdM services</td>
<td>Align CAF assessment with e-Auth</td>
</tr>
<tr>
<td>Develop an activity for the purposes of persistency and exchanging</td>
<td>Improve nontraditional communities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Build a comprehensive and effective IdM structure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Join InCommon Federation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continue Two-Factor validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Co建立健全 IdM governance and policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The University of Chicago delegation used a “weighted priority” voting scheme to identify the 1st, 2nd, and 3rd priorities among the dozen or so important Identity & Access Management issues it identified during the Functional and Campus Break Out Sessions. The result includes two-way ties for 2nd and for 3rd place, and so 5 items are presented below numbered 1, 2a, 2b, 3a, and 3b.

1. Establish the UCID

UC has a database called the Master Constituency Database (MCDB) that lists all of the people associated with UC, including present and past faculty, staff, students, hospital employees, alumni, persons in affiliated organizations, and others. The MCDB is also where CNetIDs are authoritatively housed. The UCID is an identifier associated with each person in this database that (1) never changes, (2) is 9 characters, and (3) can be stored in other databases containing information about UC people to indicate which UC person the information pertains to. Currently, SSNs and CNetIDs are often used for this purpose, but CNetIDs can change, not every UC-associated person has one, and use of SSN for this purpose is at odds with good stewardship of personally identifying information. The UCID will be used to logically integrate several databases and will be used as a replacement for SSN in many contexts in separate projects.

2a. Security Integration of Vendor Applications

Many applications are architected to internally provide security services such as authentication, groups, and roles. Many of those do so in a tightly-integrated, proprietary way, making it difficult or impossible to integrate these functions with external, campus-operated infrastructure. We need to teach vendors how to do so in a more loosely-coupled manner that supports both a vendor-provided self-contained configuration and a campus-integrated configuration. The objective of this item is to develop documentation describing the desired style and function of a set of interfaces in collaboration with other CIC institutions, and to use this document in meetings with vendor product managers and product architects to communicate our needs and suggest means of addressing them.

2b. CNet Adoptability

This is an overarching and long-term program that guides enhancements to “all things CNetID” towards those that are most needed to meet adoption requirements by distributed IT operations. The chief program elements remaining to reach completion are

- Distributed groups management—to enable others to create and maintain groups for local purposes, optionally combining them with centrally-maintained groups.
- Distributed account management—to enable distributed IT support staff to help end-users with password resets and email settings.
- Password policy classes—to enable each CNet account to be in one of several different password policy groups matched to high-watermark requirements of the applications accessed by the account holder.
3A. **Integrate Chicago Card & CNetID Management Operations**

The Chicago Card Office and Network Systems Databases department (NSD) separately join employee and student information to form a comprehensive view of who’s at UC for purposes of issuing Chicago Cards and CNetIDs, respectively. An extract of the Chicago Card database is imported into NSD’s MCDB database, so that Chicago Card ISO numbers are among the identifiers associated with each person in the MCDB. But the current arrangement ill disposes us to take several valuable steps:

- Leverage the in-person identification process of the Chicago Card to benefit CNetID assignment in some circumstances.
- Provide feeds associating CNetIDs with Chicago Card ISOs or with Library bar codes (on the Chicago Card).
- Reduce the number of fundamental identities assigned to the same person, both within the Chicago Card and MCDB databases separately, and between them.

A logical or perhaps physical merging of these databases and appropriate changes to organizational and automation processes are needed to address these service issues.

3B. **Policy & Practice Gap Analysis**

The Federal e-Authentication program’s Credential Assessment Framework and a UC-specific authentication service (to enable UC Hospitals and UC to run applications whose userships cross both organizations) need to provide strategic objectives for our identity and access management operations. We will use a deliberate and transparent process to identify and assess gaps between current and potentially required policies & practices needed to meet those objectives.
The University of Illinois Urbana-Champaign and Chicago groups (which also included representatives from our University Administration, which spans the campuses) met together to generate the list. We collected the “top three” (sometimes more) from each of the team “functional area reps,” and then synthesized those through discussion into the following three overall top priority items. We have included the individual “by functional area top three lists” after the top three so that we don’t lose that input as we go forward.

1. **Education/Data Stewardship**

Good data stewardship practices (including security/privacy issues) is a key topic where an educational campaign would be valuable. One audience to target would be the AITS unit security contacts. But decision makers are also important to target, so that they understand the issues and needs. It is also important to educate decision makers on the components that make up an identity management infrastructure, and on a common vocabulary to be used. This provides necessary background for the next item.

Education should be two-way though, and we need to have good ways to get feedback/needs from the users of our identity management infrastructure as a key input into the planning and prioritization of changes/enhancements/evolution of that infrastructure.

2. **Governance/Policy**

Set up an “identity management leadership group” (UWisc’s name) to help provide a governance structure for identity management within the University. The general sentiment was that this was best structured with campus-specific groups that have oversight from a University-wide group—something akin to the I-Card committee structures. This group would guide policy for identity management, and create working groups as necessary in areas where expertise is needed that is not within the group. (Would this/these groups be helping to prioritize work to be done?)

Some specific policy areas were identified, such as lifecycle of a person’s affiliations and identifiers with the University (one comment was a “life view of identity”), and perhaps policy concerning the importance of documentation of our identity management processes and workflows, including provisioning and de-provisioning of services. A CAF (credentials assessment framework) would be one tool/approach to use to help guide where policy/procedures/documentation are most in need of work. Or perhaps these last two are really part of the next item.

3. **Solidify the Foundation**

Not that we can’t do research and use case/requirements gathering for new functionality, but unless we start with a rock solid foundation to our University identity management infrastructure, the whole “stack” of identity management services will be fragile. Part of solidifying the foundation is establishing clear policy and documented processes for implementing that policy in our identity management framework. Perhaps a CAF-like assessment (as mentioned above) would help to expose areas where work is needed—although we already know a number of areas needing work. Feedback from users of the infrastructure is also likely to identify areas needing work.
Following are the lists from each of our representatives in the different functional areas

Note that we did not have a Human Resources or Library representative that was able to attend, so we don’t have functional lists in those areas.

**Registrars**
- Education, particularly on proper data stewardship
- Policy on lifecycle of individuals and their affiliations
- Policy/governance and management in a de-centralized environment

**ID Centers**
- High level of assurance in identity vetting
- Renewal process (identity needing to be re-affirmed?)

**IT Managers**
- CAF process
- Identifying and documenting workflow
- Provisioning and de-provisioning

**IT Directors**
- Education/Communication
- Governance/Authority management
- Agility to make changes
- Non-traditional ("external") identity
- Lifeview of identity
- Customer relations

**IT Security**
- Multifactor authentication
- Central authorization database (managing privileges in a central place rather than within each application)

**IT IdM (1)** *(IdM group was so big that there were 2 tables of discussion)*
- Policies for NetID and its lifecycle
- Password synchronization
- Single signon/WebSSO

**IT IdM (2)**
- Governance structure
- Common vocabulary/education on components of identity management
- Documentation/CAF as process to help drive
- Levels of Assurance (LOA) and Risk Assessments, and then matching risk to an appropriate LOA per application.

**CIOs**
- Data stewardship, and better policies (best practices) on it
- Multifactor authn not worth it yet (can be/is being "gamed," so a sufficient cost/benefit ratio not clearly established yet)
- Password synchronization
- Rock solid identity management components and processes
- Roles based (including group management) authorization
- Federated services
1. **Authorization (AuthZ) Management**

Overall we would like to have a more robust system for managing authorization. Ideally this solution would allow us to grant and revoke privileges automatically as people come and go or change roles.

There is a particular concern that authorizations are not removed appropriately as people leave the institution or change jobs within the institution.

2. **Automatic Provisioning and De-Provisioning of Any IT Related Accounts**

Consistent with each unit’s respective business practice, we would like to have an automated process for both the creation and deletion of accounts. Today we do have a process for our most common accounts, but there are still numerous systems that fall outside of the scope of the automated system. Many of those systems are among the most critical in terms of security and exposure of sensitive data.

On a related note, there is a desire to speed up the account creation process, in order to better meet the expectations of new users.

3. **Federating with the Fed**

Many people are concerned with IU's ability to federate with the federal government. As the E-Authentication initiative moves forward, there is an expectation that IU faculty, staff, and students will need to be able to participate, particularly in regards to research-related work.

Will Shibboleth (and InCommon) be the answer???

4. **Reporting and Support Related Tools**

From both an auditing and support perspective, there is a need to allow support staff to see an individual's identity and (as appropriate) manage that information with online tools. This would need to include authorization data, which seems to be one of the key missing elements today.
1. **EDUCATION**

One priority is the need for additional educational efforts focused on the protection of data. We identified these priority areas:

- Instruction regarding protection of institutional data (data of others); making certain that staff are using data appropriately and minimizing exposure in shadow systems.
- Development of stronger checks and balances when educational data is shared as part of collaborative efforts.
- Instruction regarding measures available to individuals for protection of their personal data.

The development of a common set of vocabulary is important to us as we balance the needs and responsibilities of the Enterprise Identity Management and Provisioning Service and campus services reliant on the IdM Service. Provisioning, and especially deprovisioning, are not well understood.

We will evaluate existing campus governance for applicability to Identity Services, but anticipate that a new Identity Services Management Group may be appropriate.

2. **MANAGEMENT OF IDENTITY FOR SPECIAL POPULATIONS**

In our discussion, special populations are those communities needing services from the institution but who do not have a current student enrollment or employment relationship. Examples include: 1) alumni; 2) prospective students; 3) roving scholars/research collaborators; 4) parents; 5) other guests; 6) students and staff from other higher education institutions; 7) high school counselors and others in K-12; 8) other recruitment task requirements; 9) VA Hospital staff collaborations with UI Hospital/College of Medicine; and 10) conferences, summer programs, and other campus events.

The policy and technical requirements include, but are not limited to,

- Determination of Identity Service boundaries: to whom does the University provision services? This identifies the community of persons to be included within the identity service.
- How we create and maintain the identity information: policy, process, and toolsets.

3. **BENCHMARK ANALYSIS OF CAMPUS IDENTITY SERVICES**

The UIowa Directory Services group is in the middle of a directory infrastructure upgrade project to migrate much of the legacy directory scripts and processes into a Microsoft Identity Integration Server (MIIS) based environment. When completed, we intend to benchmark the UIowa state of Identity Management Services with standards such as:

- Federal e-Authentication program's Credential Assessment Framework
- InCommon Software Guidelines
- “No Child Left Behind” national ID requirements, relative to student identification

We anticipate that the analysis will help determine the development roadmap needed to position UIowa for Federation of Identity for grant submissions and collaborations with the CIC and other educational institutions.
1. **IMPLEMENT A NEW ENTERPRISE-WIDE DIRECTORY AND IDENTITY MANAGEMENT SYSTEM**

UM has established a comprehensive project plan for implementing a new Enterprise Directory and Identity Management system. ([http://www.itd.umich.edu/enterprisedir/](http://www.itd.umich.edu/enterprisedir/)) The system will include:

- Real-time data updates from authoritative systems to support real-time service provisioning, de-provisioning, and access control
- Distributed Roles and Group Management
- Distributed Identity Creation and Lifecycle Management

The University of Michigan is well poised to succeed in this endeavor. We have a time-tested policy and principles of data management. We have an effective, committed governance board structure that has proven capable of resolving issues. We have a record of cross-institutional project success. We have a comprehensive and widely adopted Web Single-Sign On system (i.e., CoSign). We have managed a centralized identity management system for over a decade.

2. **EDUCATION/AWARENESS ON OUR CAMPUS**

We need to do a better job of communicating and educating our campus about IdM issues. Decision makers need a better understanding of why a robust campus IdM infrastructure is important and why it should be funded. Individual departments on campus need to understand how a campus-wide system will solve their local access management issues.

3. **PREPARING FOR FEDERAL E-AUTHENTICATION**

We need to examine our policies and practices in light of e-Authentication and the Credential Assessment Framework and set a roadmap federated identity capabilities in general.

4. **STAFFING**

Finding highly-qualified technical staff for IdM projects has been a challenge.
1. **DATA COHERENCE**

Articulate a larger vision of information resource management that includes identity management.

Increasingly, information is being recognized as an important component of products and services and an asset of the organization. For all of Michigan State University (MSU)’s assets to be effectively and efficiently utilized to support its mission, goals, objectives and strategies, the management of information as a resource needs to be consistent and integrated enterprise-wide with the management of MSU’s other assets—human, financial and physical resources, customer relationships and intellectual property.

Data governance, data stewardship, together with technology and standards, are essential factors for coherent data resource management. Coherent data resource management is needed to bring various pieces of information together, across MSU’s business functions and offices, in a logical, consistent and integrated manner to form an efficient, effective and harmonious whole. It also promotes and maintains the integrity of the information while facilitating accessibility of the information for those who need it in the performance of their job responsibilities.

2. **GOVERNANCE**

Define and implement a prototype governance program to begin developing vision, policy, guidelines and procedure, and addressing issues related to identity and data coherence. The prototype will facilitate education and awareness across university offices and functions.

Information resource management in an organization includes data governance and data stewardship programs. As with managing any asset, a pragmatic and practical approach includes authority and accountability. Data governance is the execution of authority over the management of data assets and performance of data functions. Data stewardship is formalizing accountability for the management of data resources. Both programs include formalization of roles, responsibilities and procedures. Note that the programs cover both data and metadata, and that the programs themselves have data and metadata.

Identity is an important, fundamental information resource with many attributes that spans all offices and the majority of functions of the institution. It will need to be managed as a component within the overall data governance and data stewardship framework.

3. **TECHNOLOGY**

Continue efforts to identify and understand identity management technology, including identification and implementation of identity management technology standards.

- Perform a United States federal government e-Authentication Credential Assessment Framework (CAF) self-assessment and gap analysis to assist in identifying and setting directions and objectives.
- Explore ISO 17799 – “a comprehensive set of controls comprising best practices in information security.” This internationally recognized generic information standard covers ten security areas:
  - Security Policy
  - System Access Control
  - Computer & Operations Management
  - System Development and Maintenance
  - Physical and Environmental Security
  - Compliance
  - Personnel Security
  - Security Organization
  - Asset Classification and Control
  - Business Continuity Management
The University of Minnesota contingent met on campus both before and after the conference. The pre-conference meeting was a discussion about what we each hoped to gain from the conference and briefly review what had been done recently. The post-conference meeting was to review the take-aways and “to-do” list that we compiled.

The following are the significant outcomes and planned activities from attending the conference:

- Review the outcomes and recommendations from a 2005 mid-year review of our existing enterprise directory infrastructure – a small group was charged in spring of 2005 to review and document our existing Enterprise Directory infrastructure, then do a comparative analysis of our capabilities with some Identity Management product packages on the market. A list of about 15 recommendations was produced by that group.

- Re-start/continue our Two-Factor Authentication initiative—in late 2004 through 2005, a group of 4 or 5 individuals successfully ran a pilot project to use a USB SmartCard-based PKI token for two-factor authentication with our existing Web Signon system. The purpose was to study the feasibility and necessary controls for using the PKI client to enhance the security of our most critical web-based business systems. The pilot was successful, and the report delivered to the CIO contained the recommendation of also investigating One-Time Password (OTP) technologies. This recommendation has now been accepted, and a group of people will begin this work in August, with the goal of using some form of two factor authentication for critical systems and server administrators (about 300 people) by the end of June 2007.

- Join the InCommon Federation—This would provide two opportunities. The first would be to understand where we stand today in our Identity Management practices, since all members of InCommon must post a “Participant Operating Practices” document describing their Identity Management systems and processes. We have many systems and processes, but little documentation. The next opportunity is to become more involved in the federated identity space, placing the institution in a position to take full advantage of those capabilities when needed. We hope to leverage InCommon’s work with the Fed E-Auth group for future eGovernment interaction.

- Evaluate our Identity Management practices against the federal E-Auth Credentials Assessment Framework—many in our group were interested to understand how we stack up against the CAF requirements.

- Explore using Signet for privilege management—Initial interest is in tracking and interfacing with our central ERP systems, such as PeopleSoft Student Administration and HR.

- Develop a “common vocabulary” for talking about Identity Management Issues on our campus—IdM is a hard thing to explain and discuss without a common understanding of the topics and challenges. We decided to start with small discussions that may evolve into presentations that highlight the benefits of good identity management practices, as well as the consequences of less-than-good practices.

Parting comments: it was observed by our leadership that nothing on this list is a trivial effort, and our resources are already stretched by existing efforts. It will be challenging to find the time and people to accomplish these goals.
SHORT TERM

Identified as priorities for the next 12 months:

- Complete initial two-factor authentication deployment within an ERP system under the new Web SSO system. Northwestern has just deployed the SUN Access Manager product intends to put one ERP system behind it with two-factor authentication for administrative access protections. Once this has been demonstrated, other ERP systems will join this infrastructure. Funding for the two-factor service will be determined after the demonstration is complete.

- Complete implementation plans for real-time interchange of information between the authoritative systems (HR, student records) and the IdM system. Long in the planning, real-time data interchange is now recognized as a necessary compliance and customer service factor. As Northwestern changes its IdM software these sources will be connected.

- Pursue a risk analysis of current downloading practices for HR and student records data with the goal of targeting certain data items for higher protection via encryption. The security of personally-identifiable information (PII) is vital and while IdM can address ACCESS, it cannot solve protection of downloaded information. What protections can be built in that will raise awareness and perhaps given some greater assurance that PII is protected?

- Determine need for a governance structure to define and grant access to student data. Because the issue is a community concern, perhaps the community should be involved in the policy decision-making.

- Assemble a program for users on data sensitivity and regulatory awareness. An education program can be developed once data is classified (already in motion at NU), and could be a requirement for ACCESS and renewal of access as policed by the IdM system. This is a regulatory requirement in some research situations and we want to see if it can be extended further to general data custodianship. [Note: an educational program of this sort — especially in electronic form — could be a valuable CIC-wide resource/initiative.]

LONG TERM

Additional projects and concerns in motion or on the docket of lower priority or timeline longer than 12 months:

Identity Management Services

- Review the current culture of identity management practices under the e-gov CAF for passwords.
- Complete implementation of the SUN Identity Manager replacement for the legacy IdM system and then:
  - Implement workflows for requesting new identities and granting access to ERP systems
  - Use group memberships or roles to provision services on school/division Windows servers (e.g. file space, Sharepoint, etc.)
  - Implement enterprise roles as defined by a governance body
  - Create “trustworthiness” and/or “level-of-assurance” metrics within IdM business processes and expose them in the directories for use by access control services.
  - Replace the ID-card management software with workflows within the IdM system to unify the overall identity space.

Access Control Services

- Implement SAML 2.0 federation technologies for internal use, use with vendors, and in preparation for joining inCommon.
- Educate University legal counsel about forthcoming needs for federation contracts.
- Support security services required within the University’s forthcoming Service-Oriented Architecture of Web Services.

Directory Services

- Complete deployment of a delegated-OU central Active Directory infrastructure.
- Deploy Oracle Internet Directory as a specialized user profile database for Oracle applications.
The Ohio State University has identified the following areas as important priorities in the area of Identity Management. We would not necessarily consider these to be “ordered priorities” but rather important points of consideration:

1. **Securely Integrate Various Applications**

There are mainly applications in existence at The Ohio State University. These include vendor purchased software as well as home-grown applications. Nowadays, most applications revolve around web access. However, not all applications do, and these also need to be considered. Federated access is the key to relatively easy implementation across a whole range of applications.

2. **Secure Stakeholder Buy-in for the Identity Management Concept**

It is very important that all major stakeholders buy in to the IdM concept. This not only includes traditional application and business process owners such as the Registrar and the Office of Human Resources, but it also includes such important system owners as the University ID card and maintainers of various physical access control systems on campus. Given the current climate surrounding the risks associated with identity theft, acquiring this buy-in will likely be easier than it would have been previously.

3. **Implement Appropriate Policies and Practices to Support an Identity Management Approach**

Without appropriate supporting policies and procedures, an Identity Management system would soon become less than useful. Given the certain growth in federation, and the likely requirements of the federal government in this regard, implementing adequate proofing methodologies, as well as ancillary procedures such as identity management database auditing, tight password controls, and classification of identifiable information is a must.

4. **Establish Mechanisms to Support Central Identity Accounting, Account Provisioning and De-Provisioning, and Federated Access**

These constitute the core components of an Identity Management system. It is very important for an IdM system to assist participating application systems in establishing identities across multiple systems. A big benefit to the implementation of an IdM system will be the ability to provision accounts through an automated workflow process. Even more important, given the current climate regarding security, is the ability to terminate access for a given user to all systems at the touch of a button. Finally, federated access is the lynchpin to making an IdM system work seamlessly across multiple environments.
Arguably the best aspect of this conference was the opportunity to spend some time with Penn State colleagues who are similarly passionate about a complex yet important topic. One exercise in which we participated was to discuss, institution by institution, those issues surrounding IdM which are important to us and then try to quickly agree as to what our institutional priorities would be for the coming year. The three we agreed on were:

**Priorities**

1. Achieve a Level of Assurance of 2 in the eyes of the Credential Assessment Framework
2. Reposition and improve how it is we deal with non-traditional communities (for example, people at collaborating institutions/organizations and other communities served)
3. Develop an active community of people at Penn State for the purposes of persistently exchanging bilateral requirements for IdM

**Other Issues Discussed**

1. Achieve level-2 level of assurance in the eyes of the CAF
2. Implement two factor in cosign/WebAccess
3. Establishing a governance structure
4. Managing loosely couple communities, non-traditional accounts
5. Education on IdM
6. Partnership with IT when creating roles and responsibilities
7. Guiding principle for access regarding stakeholders
8. Persistent requirements gathering for improved influence for stakeholders
9. Doing for academic process what workflow is doing for business processes
10. Webrat up and running in a year
11. Improved understanding with the feds on direction in IdM
12. Deal better with special populations of users (patients, roaming physicians and roaming lecturers)
13. Connectivity with PSU and external collaborations
14. Community education on IdM, establishing better IdM policies and processes
15. FERPA test in order to allow staff access to certain kinds of data determining what kinds of data people
16. Engage non-traditional groups for id card provisioning - both how and who
17. Development of process/procedures for single place for “supervisor” of identity
18. Utilization of second factor for more than just what it’s currently used for
19. Improved fraud detection
20. Being prepared for legislative changes and landmark legal cases
21. Universal data classification that ties back to regulatory and legal requirements
22. Trusted federated state between HMC and PSU
23. Improved understanding of the relationship between the Nittany Medical Center and various PSU entities (i.e. HMC/COM); and intentions as they relate to the sharing electronic information and resources
24. Who is really paying for the children’s hospital and the cancer center—who gets accounts, who gets what services
25. Leveraging the signature station process for Hershey
For the CIC Identity Management Conference, Purdue University sent staff from several areas, including Information Technology, Registrar, Business and Student Services Computing, and Research. The group gave the following three recommendations as its top issues in identity management.

1. **Identity Management Governance and Policy**

   Purdue must work to establish appropriate guidelines, governance, policies, and procedures to ensure that our campus constituents work together to address identity and access management issues and needs. Specifically, those areas that need to work together include our Information Technology, Identity Management, Registrar, Research, and Human Resource groups.

2. **Process and Procedure Improvement**

   In order to better serve all its affiliates, Purdue must continually review, assess, and improve the processes and procedures used to provision access to its resources. Purdue University provides services not only to our students, but also to its employees and the general public. It also collaborates with various external groups in research projects and teaching and learning activities.

3. **Develop a Common Understanding**

   Because of its complexity, Purdue must work to develop a common understanding of identity management across all campuses. This can be accomplished by educating its constituents about items one and two above, specifically the processes and procedures used in providing identity management services.
The University of Wisconsin - Madison originally had seven issues. This have been re-factored into the following list. Note this list is only sort-of prioritized in that we think each of these are important and there is a lot of overlap between the activities.

1. **MEET THE CRITERIA TO JOIN THE INCOMMON FEDERATION AT A BASIC LEVEL**

Ongoing discussions between the federal government and the InCommon people have displaced the “do the CAF analysis” with joining InCommon. This also includes our previous item of “Understand the federal requirements and consequences for meeting those requirements.”

2. **BUILD A BUSINESS CASE OF IDENTITY AND ACCESS MANAGEMENT (IAM) ON CAMPUS**

We are working on documentation around our PASE (Populations Affiliations and Service Entitlements) project. This will be broadened to include governance and policy needs as well as technical needs. This will include business process models to show where the Identity and Access Management pieces fit. This includes the previously separate item, *From a campus governance perspective, better understand how all of the IAM pieces fit together and within the enterprise as a whole.*

3. **MORE COMPLETELY BUILD OUT THE CAMPUS TECHNICAL INFRASTRUCTURE FOR IAM**

We need to continue our work on PASE and our authentication and authorization technologies.

4. **AUTOMATE PROVISIONING WORKFLOW AND ACCESS MANAGEMENT**

This is a specific project to streamline the management of service entitlements (access to specific forms, fields and/or systems).

5. **PUT IN PLACE ID PROOFING FOR PROSPECTIVE EMPLOYEES**
GENERAL

- EDUCAUSE Identity Management Working Group and mail list
  This is probably the best mail list to use for comparing notes on IdM practices with peer institutions.
- NMI-EDIT Authentication Roadmap
- NMI-EDIT Directories Roadmap
- Info on upcoming CAMPs and other good stuff
- Jim Phelps blog: http://arch.doit.wisc.edu/jim/
- Sample Incident Response Protocol Document: http://www.it.northwestern.edu/policies/index.html

FEDERAL IDENTITY MANAGEMENT INITIATIVES PLENARY

- www.cio.gov/eauthentication
- http://csrc.nist.gov/pki
- www.cio.gov/ficc
- www.smartcardalliance.org

BIG POLICY ISSUES

- External Issues
  - USA-Patriot Act
    http://www.cit.cornell.edu/oit/policy/PatriotAct/
  - Digital Copyright
    http://www.cit.cornell.edu/oit/policy/copyright/
  - Privacy in the Electronic Realm
    http://www.cit.cornell.edu/oit/policy/privacy/
  - CALEA: Communications Law Enforcement Assistance Act
    http://www.cit.cornell.edu/oit/policy/calea/
- Institutional Policy (Cornell Model)
  - Centralized University Policy Office
    http://www.policy.cornell.edu/
  - Famous “policy on policies!”
    http://www.policy.cornell.edu/vol4_1.cfm
- Parker Brothers Problem
  - “Significantly more work may be needed to empower applications to use Signet.”
Resources Shared in Presentations (cont.)

FEDERATED IDENTITY

- [http://arch.doit.wisc.edu/jim/](http://arch.doit.wisc.edu/jim/)
- E-Authentication
  - [www.cio.gov/eauthentication](http://www.cio.gov/eauthentication)
- Credential Assessment Framework (CAF)
  - [http://www.educause.edu/LibraryDetailPage/666?ID=EAF0628](http://www.educause.edu/LibraryDetailPage/666?ID=EAF0628)

PROTECTING IDENTITIES

- NU [Protocol for Data Exchange](http://www.protocolfordataexchange.com)
- PSU Hershey Med Center Risk Assessment Tools
- The risk landscape is fluid – tools should be too!
  - Risk Valuation Matrix
  - HIPAA Compliance Assessment Tool
- EDUCAUSE [Data Incident Notification Toolkit](http://www.educause.edu)
  - Includes links to policy and incident sites at several universities, Federal & state notification regulations, related articles and presentations
- [National Conference of State Legislatures Privacy Site](http://www.ncsl.org)
  - Security breach laws introduced in 25 states
  - SSN mitigation legislation introduced in 38 states
  - Other scary stuff!

RISKS AND TRENDS IN AUTHENTICATION

- Moving toward user-centric identity
  - [www.identitygang.org](http://www.identitygang.org)
  - [www.eclipse.org/higgins](http://www.eclipse.org/higgins)
  - [www.sxip.com](http://www.sxip.com)
  - [www.identityblog.com](http://www.identityblog.com)
- One-time password device
  - [http://www.safehaus.org](http://www.safehaus.org)
<table>
<thead>
<tr>
<th>Name</th>
<th>Position/Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob Bartlett</td>
<td>Director, Network Based Services</td>
</tr>
<tr>
<td>Tom Barton</td>
<td>Sr. Director, IT Integration</td>
</tr>
<tr>
<td>David Larsen</td>
<td>Head of Access Services</td>
</tr>
<tr>
<td>Cheryl Malmborg</td>
<td>Programmer/Analyst</td>
</tr>
<tr>
<td>Mark Norem</td>
<td>Manager, Chicago Card</td>
</tr>
<tr>
<td>Tod Olson</td>
<td>Programmer/Analyst</td>
</tr>
<tr>
<td>Ron Thielen</td>
<td>Enterprise Architect</td>
</tr>
<tr>
<td>Robert Goldstein</td>
<td>Assistant Director</td>
</tr>
<tr>
<td>Michael Kamowski</td>
<td>Director</td>
</tr>
<tr>
<td>Janet Shaw</td>
<td>Supervisor, Client Services Office, academic Computing</td>
</tr>
<tr>
<td>Karen Athy-Penrose</td>
<td>Project Manager</td>
</tr>
<tr>
<td>Kimberly Blum</td>
<td>i-Card Program Support Coordinator</td>
</tr>
<tr>
<td>Les Cromwell</td>
<td>Assistant Registrar</td>
</tr>
<tr>
<td>Linda Fletcher</td>
<td>AITS Technical Analyst</td>
</tr>
<tr>
<td>Michael Grady</td>
<td>Senior Technology Architect and Strategist</td>
</tr>
<tr>
<td>Ken Gustin</td>
<td>Program Director</td>
</tr>
<tr>
<td>Carol Malmgren</td>
<td>Registrar</td>
</tr>
<tr>
<td>Stacey Neil</td>
<td>Enterprise Systems Coordination Specialist</td>
</tr>
<tr>
<td>Eugene Roeder</td>
<td>Research Programmer</td>
</tr>
<tr>
<td>Marya Ryan</td>
<td>Director, i-card Programs</td>
</tr>
<tr>
<td>Peter Siegel</td>
<td>CIO</td>
</tr>
<tr>
<td>Ryan Thomas</td>
<td>Associate Director of IT (OET, College of Ed)</td>
</tr>
<tr>
<td>Charles Thompson</td>
<td>Manager of Systems Services</td>
</tr>
<tr>
<td>Keith Wessel</td>
<td>Directory Service Manager</td>
</tr>
<tr>
<td>Nat Francis</td>
<td>Analyst/Programmer</td>
</tr>
<tr>
<td>Patricia Goodall</td>
<td>Academic HR Systems Data Manager</td>
</tr>
<tr>
<td>Laura Klein</td>
<td>Computer Accounts Manager</td>
</tr>
<tr>
<td>Robert Lowden</td>
<td>UIS Director of Development, Operations, and Administration</td>
</tr>
<tr>
<td>Stephen Martino</td>
<td>Business Systems Director</td>
</tr>
<tr>
<td>Susan McCammon</td>
<td>Assistant Dean of the Faculties</td>
</tr>
<tr>
<td>Mark McConahay</td>
<td>Sr. Associate Registrar</td>
</tr>
<tr>
<td>Alan Walsh</td>
<td>Manager of Identity Management Systems</td>
</tr>
<tr>
<td>Karen Watkins</td>
<td>HRMS/SIS Project and IPS Manager</td>
</tr>
<tr>
<td>Steve Fleagle</td>
<td>CIO</td>
</tr>
<tr>
<td>Larry Lockwood</td>
<td>University Registrar</td>
</tr>
<tr>
<td>Ken Nickels</td>
<td>Applications Developer/Support IV</td>
</tr>
<tr>
<td>Phyllis Davidson</td>
<td>Asst. Dean - Library DL &amp; IT Services</td>
</tr>
</tbody>
</table>
Attendees

MIchigan state university

Pamela Beemer
Assistant VP for Human Resources

Thomas Block
HR Assistant Director

Mike Bosko
Division Manager, Technical Services

David Gift
Vice Provost, Libraries, Computing and Technology

John Griffith
Data Administration Team Leader

Matt Kolb
Identity and Messaging Systems Team Leader

Steve Kurncz
Information Technology Auditor

Dugald McMillan
Senior Associate Registrar

Pat Murphy
Information Technologist

Scott Sowulewski
Director, Employee Relations

Michele Berner
OIT Data Security, Security Analyst

Steve Cawley
CIO

Kevin DeJong
AD Admin

Tina Falkner
Associate Director

Brian Hayden
E-mail/Unix Sys Admin

Kevin O’Rourke
IT Manager

Mark Powell
Director, OIT Data Security

Christopher Rigsby
Systems Architect

Scott Ruud
Deputy CIO

Dennis Skovsted
IS Audit Manager

northwestern university

Thomas Board
Director, Information Systems Architecture

Dave Kovarik
Director, Information Security

Paul Matijevic
Director, Development Information Services

Mort Rahimi
CIO

David Takehara
Director, Financial Systems

Kathy Tessendorf
Director of HR Information Systems

university of Michigan

Amy Brooks
Director, UM Computing Environment

Daniel Drumm
Information Security Officer
Michigan Administrative Information

Robert Korniski
Manager

Justin Laby
Senior Helpdesk Support

Sue MacDavitt
Senior Director, Human Resources

Paul Robinson
University Registrar

Elizabeth Salley
Product Manager

Luke Tracy
Enterprise Directory Technical Lead
Attendees

**Ohio State University**

Scott Cantor  
Senior Web Data Access Developer

Mitch Dysart  
Operations Director

Howard Imhoff  
Director HR IT Services

Robert Kalal  
Director of IT Policy

Charles Morrow-Jones  
Director, Security

Brad Myers  
University Registrar

Ilee Rhimes, Jr.  
CIO

Valerie Shafer  
Director Student Affairs Information Tech

Tremayne Smith  
Senior Data Security Analyst

Steve Kellogg  
Director, Applied Information Technologies

Kathleen Kimball  
Senior Director, ITS Security Operations and Services

Kevin Morooney  
Senior Director, Academic Svcs

Scott Smith  
Deputy Director

Shawn Wagner  
Assistant Registrar, User Support Services

Matthew Weber  
Information Security Officer

Joel Weidner  
Assoc. Dir. Information Systems

**Purdue University**

Michael Carr  
Chief Information Security Officer

Peter Dunn  
Associate Vice President for Research

Susan Gothard  
Application Services Manager

Cheryl Gray  
Human Resource Operations Manager

**University of Wisconsin-Madison**

Joanne Berg  
Associate Vice Chancellor for Enrollment Management and Registrar

Karen Hanson  
Assistant Registrar for Enrollment Services

Chris Holsman  
Director, Enterprise Internet Services

Ron Kraemer  
Deputy CIO

Jim Lowe  
Chief Security Officer

Mairead Martin  
Assistant Director Middleware Systems Technology

Wayne Hilt  
Card Services Manager

Bob Kubat  
University Registrar

Terry Schroeder  
Assistant Director, Business Services Computing

Rob Stanfield  
Interim Director, Identity and Access Management

Daniel Whiteley  
Data Steward
Attendees

Bob Mayville
Manager of Student Applications

Jim Phelps
Senior Architect

Carla Raatz
Director, Human Resources

GUESTS
Diane Beckman
Director University Information Systems
Iowa State University

Vicki Brubaker
Associate Director - Human Resource Services
Iowa State University

Kathleen Jones
Asst VP for Enrollment and Registrar
Iowa State University

Kent Ziebell
Software Analyst
Iowa State University

CIC STAFF
Amber Marks
Program Manager, Interinstitutional Course Sharing

Karen Partlow
Associate Director, Technology Collaboration

Galen Rafferty
IT Specialist