

Leveraging Identity Management for Privacy, Security, and Compliance

John Suess, VP of IT and CIO, UMBC

What I Will Focus On

- An overview of identity management
- How identity management can help improve security, protect privacy, and ensure compliance
- The crisis in managing and protecting privacy
- The concept and use of level of assurance
- The concept and use of federated identity management

Overview of Identity Management Systems

- What do we mean by Identity Management?
 - **California State University** definition - An identity management *infrastructure* is a *collection* of *technology and policy* that enables *networked computer systems* to determine who has *access* to them, what resources the person is *authorized* to access, while *protecting* individual privacy and access to confidential information.

Analyze the Definition

- **Infrastructure** - software and hardware
- **Collection** - not just technology
- **Technology and policy** – policy plays a critical role and is an essential element of the solution
- **Networked computer systems** - implies distributed technology systems communicating over a network
- **Access** - Who am I
- **Authorized** - What can I do
- **Protecting** - limiting access and protecting information

Three Core Concepts

- People and Relationships
- Creation and Management of Identities
- Access to Data and Applications

People and Relationships

- Different types of affiliations
 - Formal vs. Casual
- Multiple affiliations
- Affiliation life-cycles

Creation & Management of Identities

- Vetting – collection and validation of identity information
- Proofing – aligning collected data and matching an actual person
- Issuance of credentials
 - ID/password pair
 - ID card
 - 2nd factor token

Access to Data & Applications

- Connecting people to data and services
- Authentication decisions
 - Knowing who
- Authorization decisions
 - Affiliation type, status, level of assurance, roles and other attributes.

Benefits of Identity Management?

- Centralize directory services
 - One authoritative source for applications
 - One stop shopping for students and employees!
- Single sign-on
- Remote access
- Inter-institutional access
- Lifecycle issues: “from cradle to grave”
- Enhance privacy of personal information
- Improve security and safeguarding of information
- Compliance with federal and state laws and regulations

Emerging Uses of IdM

- Building Access Controls
- Federal Government Agencies
 - NIH and NSF
- Software-as-a-Service (SaaS)
 - National Student Loan Clearinghouse
 - Parking, billing, career services, emergency notification
 - Educational tools
- Research
 - access to special resources

Managing and Protecting Privacy

- Higher education has had a large number of non-public information (NPI) data releases. Primarily this is associated with our past heavy use of social security numbers.
- Privacyrights.org lists 314 releases 2008, 95 were universities.

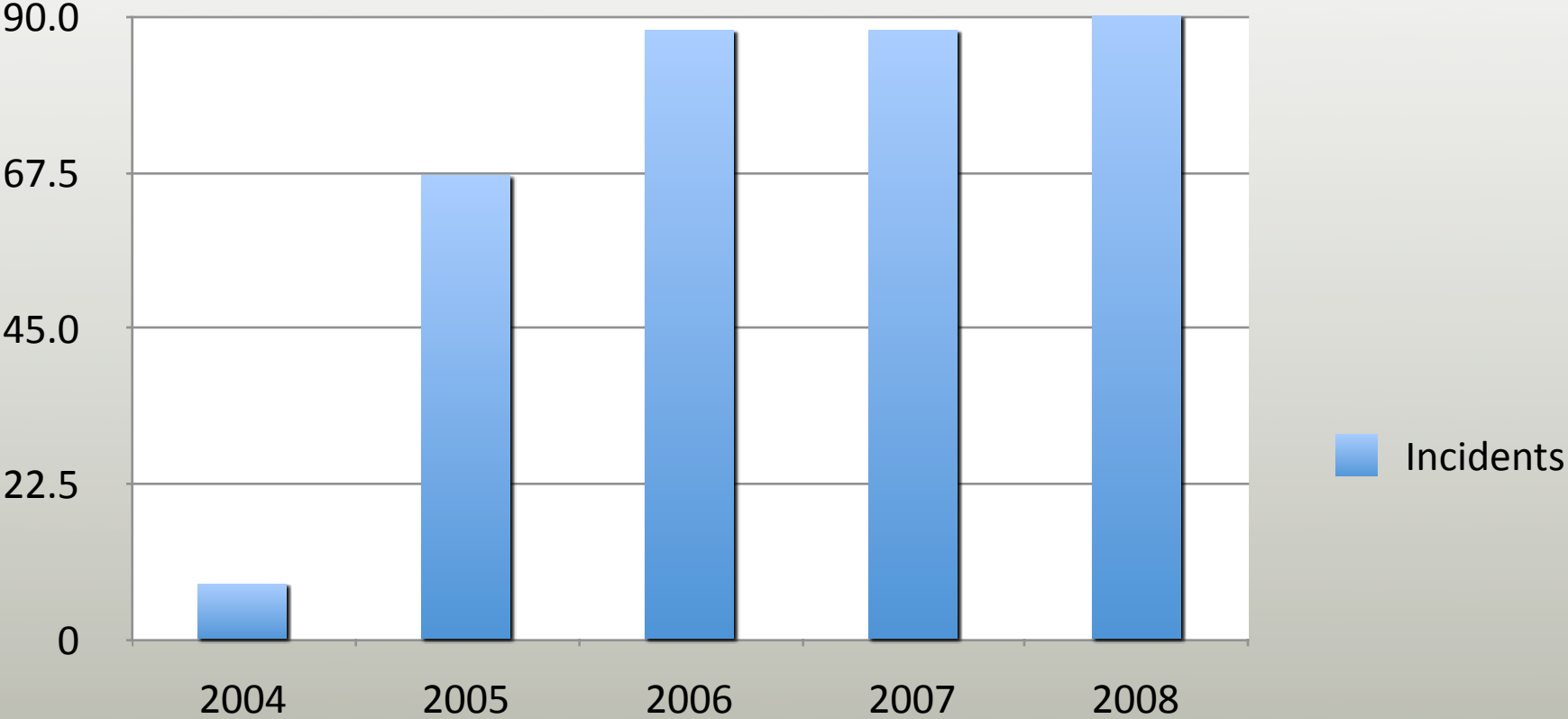
Chronology of Data Breaches

Go to Breaches for [2005](#), [2006](#), [2007](#), [2008](#) or [2009](#)

DATE MADE PUBLIC	NAME(Location)	TYPE OF BREACH	NUMBER OF RECORDS
2005			
Jan. 10, 2005	George Mason University (Fairfax, VA)	Names, photos, and Social Security numbers of 32,000 students and staff were compromised because of a hacker attack on the university's main ID server.	32,000
Jan. 18, 2005	Univ. of CA, San Diego (San Diego, CA)	A hacker breached the security of two University computers that stored the Social Security numbers and names of students and alumni of UCSD Extension.	3,500
Jan. 22, 2005	University of Northern Colorado (Greeley, CO)	A hard drive was apparently stolen. It contained information on current and former University employees and their beneficiaries -- name, date of birth, SSN, address, bank account and routing number..	30,000
Feb. 12, 2005	Science Applications International Corp. (SAIC) (San Diego, CA)	On Jan. 25 thieves broke into a SAIC facility and stole computers containing names, SSNs, and other personal information of past and current employees. Stolen information included names, NNS, addresses, phone numbers and records of financial transactions.	45,000 employees

Higher Education Data Security Incidents

Title



Interesting Statistics

- Data as of July 2007
- Higher education was responsible for 5.8 million of the “official” 140 million identities that had been released.
- The median size of a data release in higher education was 4719.
- 5% of the incidents accounted for 2.7 million of the 5.8 identities that were released (47% of the total).
- 20% of the incidents accounted for 80% of the identities released (4.8 million)

What Do These Statistics Imply?

- Small incidents dominate the statistics.
- Many of the incidents revolve around individuals having access to data that had sensitive information (NPI) and not taking adequate security procedures.
- Data management – knowing who has access to sensitive data, and then taking appropriate measures, is a key aspect of protecting that data.
- Large incidents often revolve ancillary business systems that are run outside of central IT.

Identity Management and NPI

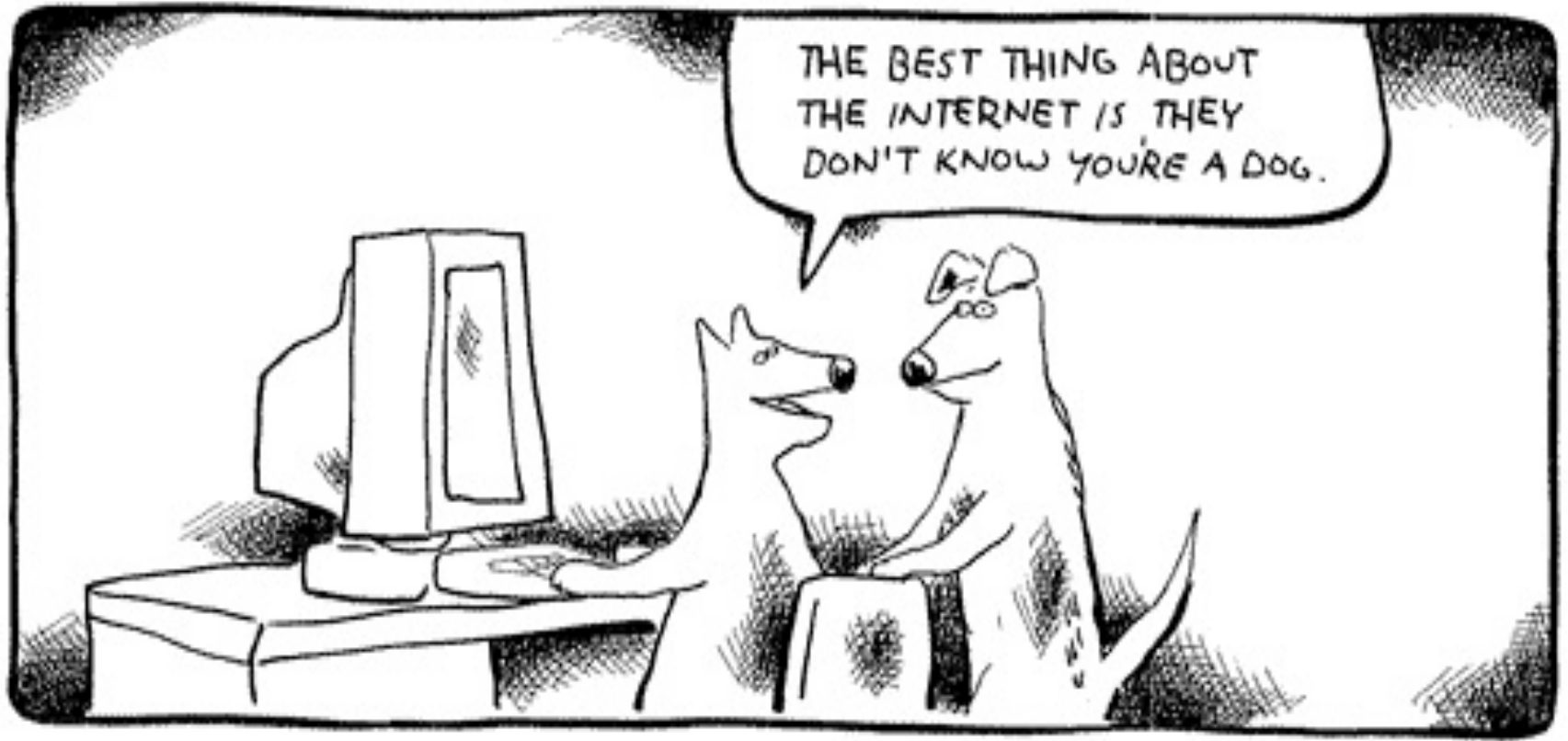
- At UMBC, our Identity Management system was instrumental in remediating our use of SSN across different business systems. We integrated our ID card into the system and did away with the using SSN as a primary identifier.
- We built better tools for identity lookup, including presenting the ID picture to validate the person, through the Identity Management system. As part of this effort we built in strict controls on who has access to view someone's full or partial SSN.

Future Directions for Identity Management and NPI

- At UMBC, we have purchased a tool, Asarium, that allows us to track whether NPI is on a device.
- We want to integrate data management privileges into our IDMS and use the IDMS to verify who has gone through formal data management training and who has NPI on their machine.
- We will then use the IDMS to show us who is and isn't allowed to have NPI on their machine and use that to inform our compliance efforts – either removing the NPI or making certain that compliance training has occurred.

Broader Privacy Issues

- Increasingly through either state laws or as a result of the European Union privacy efforts we are going to have to manage varying rules for what is private information and how to manage that information based on the relevant jurisdiction of the individual.
- Additionally, as the EU rules take hold we will need to recognize what outside groups we can share information with and what attributes can be released on individuals to different entities.



"The best thing about the Internet is they don't know you're a dog."

Tom Toles. Buffalo News, April 4, 2000.



“You’re a four-year-old German Shephard-Schnauser mix, likes to shop for rawhide chews, 213 visits to Lassie website, chatroom conversation 8-29-99 said third Lassie was the hottest, downloaded photos of third Lassie 10-12-99, e-mailed them to five other dogs whose identities are...”

Kim Cameron's Identity Blog

Kim Cameron is Microsoft's Chief Architect of Identity.

His blog is a very good place to get thoughtful discussion on identity.

<http://www.identityblog.com/>



Kim Cameron's Laws of Identity

Whitepaper

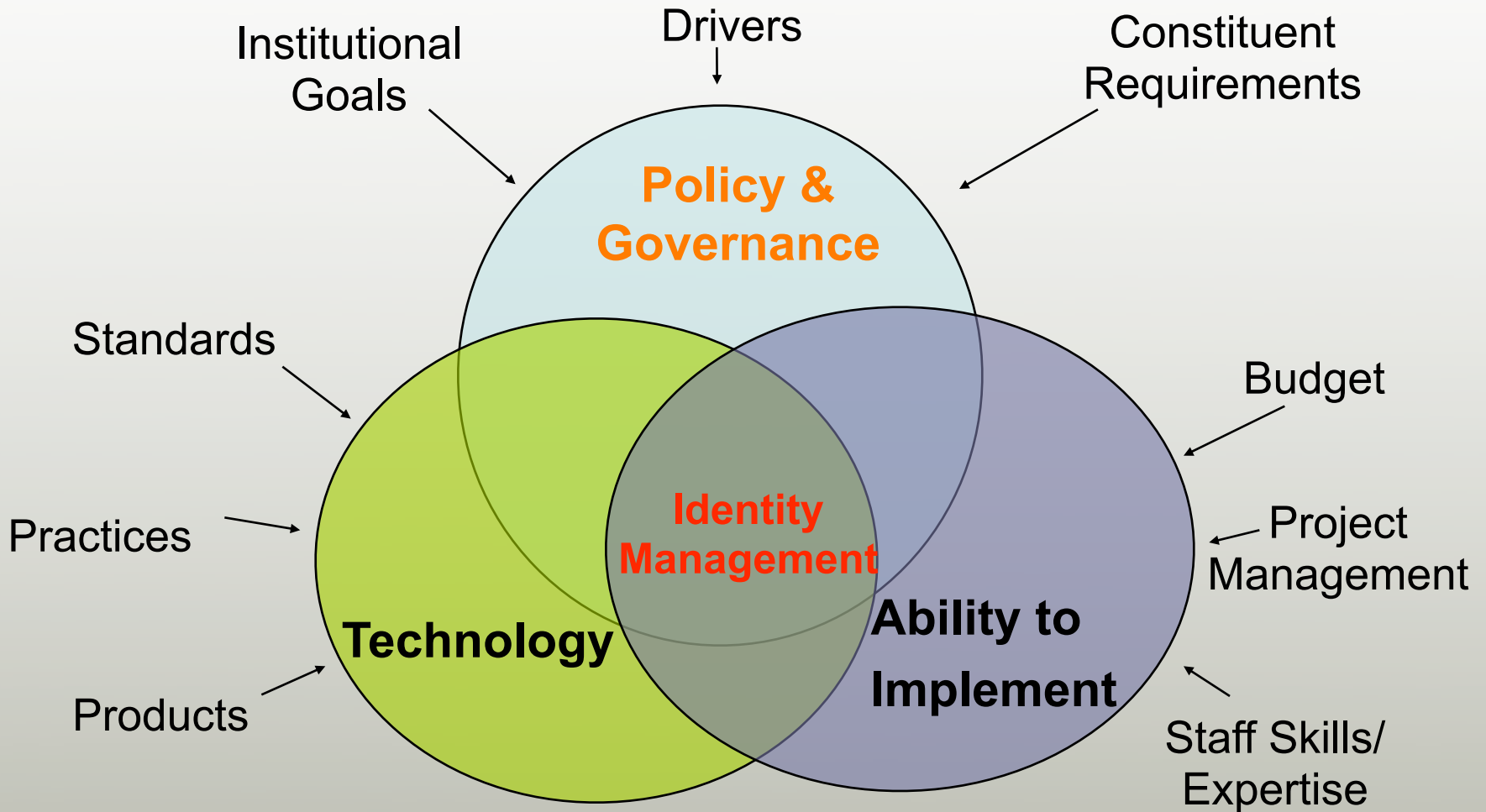
Seven Laws of Identity

1. User control and consent
2. Minimal disclosure for a constrained use
3. Limit relationships to justifiable parties
4. Control over who can see my identifier, directed identity
5. Pluralism of operators and technologies
6. Human integration
7. Consistent experience across contexts

Implications for IDMS

- We are in the beginning stages of managing identity.
- There won't be a single identity provider solution.
- The human integration component is critical and we need to create something flexible that people can consistently use.
- We will see a lot of products and technologies over the next 5 years because this is a critical component in making the Internet usable.

Identity Management Factors



Review of Factors

- As we find with security, identity management is at the intersection of policy and governance, technology, and people.
- Amongst these factors, the technology is maturing and is becoming the easiest of the three as vendors develop better cross-vendor solutions.
- Staffing still requires highly-qualified IT architects that can work across technical and functional areas.
- Policy and governance – of which audit is a key tool, is the most challenging of the three.

Policy frameworks to Build On

- The evolution of security processes and procedures from ISO 27002 provides a strong foundation for risk management and developing strong internal controls as these pertain to security.
- While much of the ISO 27002 program is helpful to building a strong identity management function it was not necessarily written for this function. As the IDMS becomes a key business driver we will see the frameworks evolve.
- We are looking at internal audit to help us bridge some of these gaps while the policy approaches are resolved.

ISO 27002: Access Control

- Business requirement for access control
 - Access Control Policy
- User access management
 - User registration
 - Privilege management
 - User password management
 - Review of user access rights
- User responsibilities
 - Password use
 - Unattended user equipment
 - Clear desk and clear screen policy

ISO 27002: Access Control (cont'd)

- Network access control
 - Policy on use of networked services
 - User authentication for external connections
 - Equipment identification in networks
 - Remote diagnostic and configuration port protection
 - Segregation in networks
 - Network connection control
 - Network routing control

ISO 27002: Access Control (cont'd)

- Operating system access control
 - Secure log-on procedures
 - User identification and authentication
 - Password management system
 - Use of system utilities
 - Session time-out
 - Limitation of connection time
- Application and information access control
 - Information access restriction
 - Sensitive system isolation

Technical Frameworks to Build On

- I have been following the work of the Burton group since 2000 and feel they are among the thought leaders in this space.
 - 2002 – their whitepaper on Virtual Enterprise Networks
 - 2003 – updated to consider SOX
 - 2004 – worked with Network Applications Consortium to develop a white paper titled *Enterprise Security Architecture*.
 - 2007 -The Open Group Architecture Forum
<http://www.opengroup.org/togaf>

<http://www.opengroup.org/togaf/>

The screenshot shows the TOGAF website's Architecture Forum page. At the top, the logo for 'THE Open GROUP' is displayed with the tagline 'Making standards work®'. Navigation links include HOME, SITE MAP, and a SEARCH box. A secondary navigation bar contains 'Sponsor an Event', 'Become a Member', and 'Member Area'. A main navigation bar lists 'About', 'Forums', 'Certification', 'Services', 'Government', 'Events', 'Bookstore & Downloads', 'Newsroom', and 'Contact'. A breadcrumb trail reads 'You are here: Home > Forums > Architecture Forum > TOGAF 8.1.1'. The left sidebar contains links for 'TOGAF 8 About TOGAF 8', 'TOGAF 8 Certification', 'TOGAF 7 TOGAF 7 Web Site', and 'Other Links'. The main content area features a banner for the 'Architecture Forum' with a photo of people working. Below this is a 'Welcome to TOGAF™ Version 8.1.1 "Enterprise Edition"' section. This section includes a 'TOGAF SHOWCASE' box, a globe image, and text stating that the full text of TOGAF 8.1.1 Enterprise Edition is available as a book or PDF. A 'Top of Page' link is located at the bottom right of the main content area.

THE Open GROUP
Making standards work®

HOME | SITE MAP | SEARCH

Sponsor an Event | Become a Member | Member Area

About | Forums | Certification | Services | Government | Events | Bookstore & Downloads | Newsroom | Contact

You are here: Home > Forums > Architecture Forum > TOGAF 8.1.1

Architecture Forum

Welcome to TOGAF™
Version 8.1.1 "Enterprise Edition"

TOGAF SHOWCASE
Certified training courses, tools, and service providers
TOGAF™

TOGAF™ -- "The Book" 2007 Edition (incorporating 8.1.1)
The full text of TOGAF 8.1.1 Enterprise Edition is now available as a perfect bound, soft cover book; over 500 pages, with full color illustrations.
→ order now or buy the PDF Edition and download now.
Also now available the TOGAF 8 Study Guide (8.1.1 Edition) and more...

About TOGAF™
TOGAF, The Open Group Architecture Framework, is an industry standard architecture framework that may be used freely by any organization wishing to develop an information systems architecture for use within that organization.
TOGAF has been developed and continuously evolved since the mid-90's by representatives of some of the world's leading IT customer and vendor organizations, working in The Open Group's Architecture Forum. Details of the Forum, and its plans for evolving TOGAF in the current year, are given on the Architecture Forum web site.

The Open Group's Platinum Members

Top of Page

A Model Architecture for Identity Management

- Identity management systems aggregate information across disparate systems. Requirements include:
 - High performance – these systems drive all web-facing customer applications and customers (or employees) won't wait.
 - High reliability – these systems often provide all authentication and authorization services. When down, nothing can occur.
 - High security – these systems may maintain a large number of person attributes, sometimes including personally protected information.

Level of Assurance in IDMS

- IDMS systems have often been business enablers for connecting customers or external business partners.
- Questions?
 - Do all account holders have access to all services and generate the same level of risk?
 - Do you have the same level of confidence that the identity associated with an account is who they purport to be for all your account holders?
- If you answered no, you might look at integrating level of assurance into your IDMS.

Overview of Level of Assurance in IDMS

- Two distinct uses
 1. For a **service provider**, the level of risk to the application or organization if an incorrectly identified user is allowed to access the application or perform a transaction. This can happen if someone compromises an account password.
 2. For an **identity provider**, the risk that the person is not who they claim to be – in this case the person has legitimate credentials that they acquired frauduantly
- Organizations often perform both functions and must look at both risks.

U.S. Federal Government eAuthentication Initiative

<http://www.cio.gov/eauthentication/>



Today's Date is: 24-June-2008

Authentication
SECURE GOVERNMENT ACCESS ONLINE

Home Key Personnel Federation Applications Federation Links Federation Members Newsroom

ANNOUNCEMENTS

GSA's HSPD-12 MSO wins Outstanding Issuing Organization Award
The HSPD-12 MSO won the 2008 Smart Card Alliance Outstanding Issuing Organization award at the CTST 2008 Americas Conference and Exhibition currently taking place in Orlando, Florida. The HSPD-12 MSO won for its role in personalizing and issuing the federal government's Personal Identity Verification cards for more than 65 federal agencies and departments; the PIV is a common, government-wide smart card credential for both physical access control and information security that is being issued to all federal government employees and subcontractors. [For more information...](#)

Background on E-Authentication Solution and the US E-Authentication Identity Federation

US E-AUTH IDENTITY FEDERATION

- Membership Documents
- Technical Architecture
- E-Authentication Portal
- Interoperability Testing
- Approved Product Vendors
- FIDCS Acquisition Information

POLICY

- Guidance for Federal Agencies
- NIST Special Publication 800-63
- X.509 CP for E-Governance CA's

Assurance as an Identity Provider

- A combination of assurance that the person presenting their credentials is who they say they are AND they are the person presenting the credentials.
 - The degree of confidence in the vetting process; and
 - The degree of confidence that the person presenting the credential is the person you issued the credential too
- Level 1 – little or no assurance
- Level 2 – some confidence
- Level 3 – high confidence
- Level 4 – very high confidence

Assurance as an Identity Provider

- eAuthentication guidelines require that everyone is identity proofed.
- We define another group – level 0. Level 0 has no assurance the person is who they say they are. These are guests that assert their identity and want a portal account. We have no way of verifying they are who they say they are
- Audit plays an important role in assessing and validating the procedures for initial identity proofing. We do this when issuing our ID card.

Assurance of Credentials

- The second component of assurance is the assurance of the credential as presented by the person it was issued too.
- Traditional authentication focuses on password management. Level 2 is the highest assurance a text-based password can achieve.
- For level 3 or 4 assurance eAuthentication requires two-factor authentication. The second factor must be some token that is issued to the user. The US government is moving to smart ID-cards under the auspices of HSPD-12.

Credential Assurance

NIST 800-63 guide provides excellent framework for managing credentials.

The entropy spreadsheet is a great tool for reviewing password practices and looking at how subtle variations in policy practices change the strength of the credentials.

This is a great tool for auditors!

THE E-AUTHENTICATION CREDENTIAL ASSESSMENT SUITE

- [Guide to Preparing for a Credential Assessment](#)
- [Certificate Credential Assessment Profile](#)
- [Password Credential Assessment Profile](#)
- [Credential Assessment Framework](#)
- [Entropy Spreadsheet, v2.0.0](#)

An Example – Password Resets

- Forgotten passwords are often amongst the most common call to the helpdesk.
- Creating a self-service method to reset your password often is essential for improving customer service and reducing helpdesk costs.
- However, this creates an opening for attacks to compromise accounts. We are integrating level of assurance into our process.
 - The 10% of total account holders that have LOA of 2 have a different process than the 90% with LOA of 1.

Assurance for Service Providers

- Service providers follow traditional risk management approaches such as NIST 800-30 to assess the risk associated with an authentication error:
 - The potential harm or impact, and
 - The likelihood of such harm or impact.
- Potential categories of harm include: reputation, financial loss, organization harm, release of sensitive information, risk to personal safety, and criminal or civil violations.
- Ratings use values of low, moderate, or high.

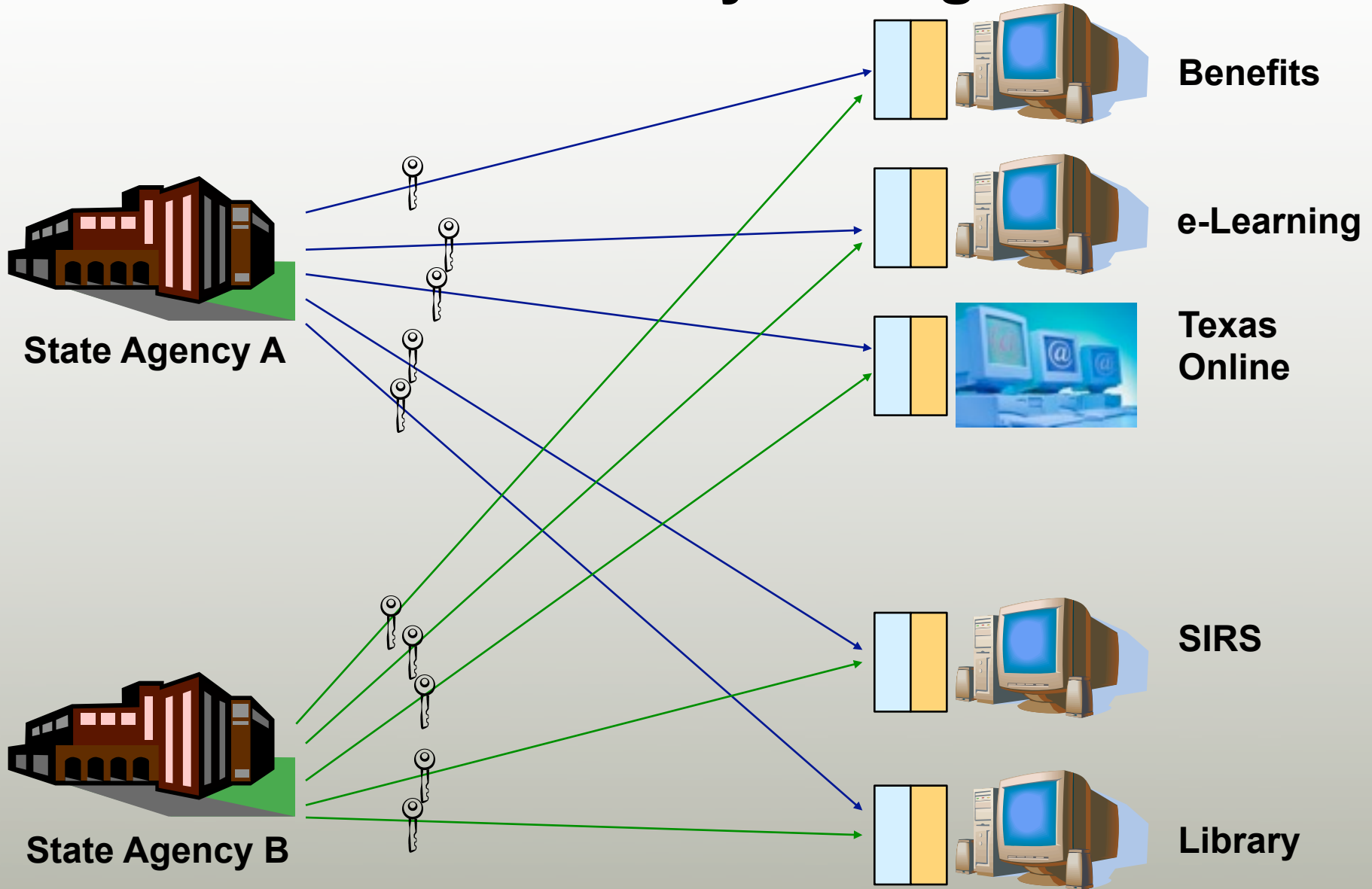
Setting Level of Service Assurance


Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Federations and Identity Management

- Federations – definition
 - *Dictionary.com* - a federated body formed by a number of nations, states, societies, unions, etc., each ***retaining control*** of its own internal affairs.
 - *Incommon.org* - a federation is an association of organizations that come together to exchange, as appropriate, about their users and resources in order to enable collaborations and transactions.

Traditional Identity Management

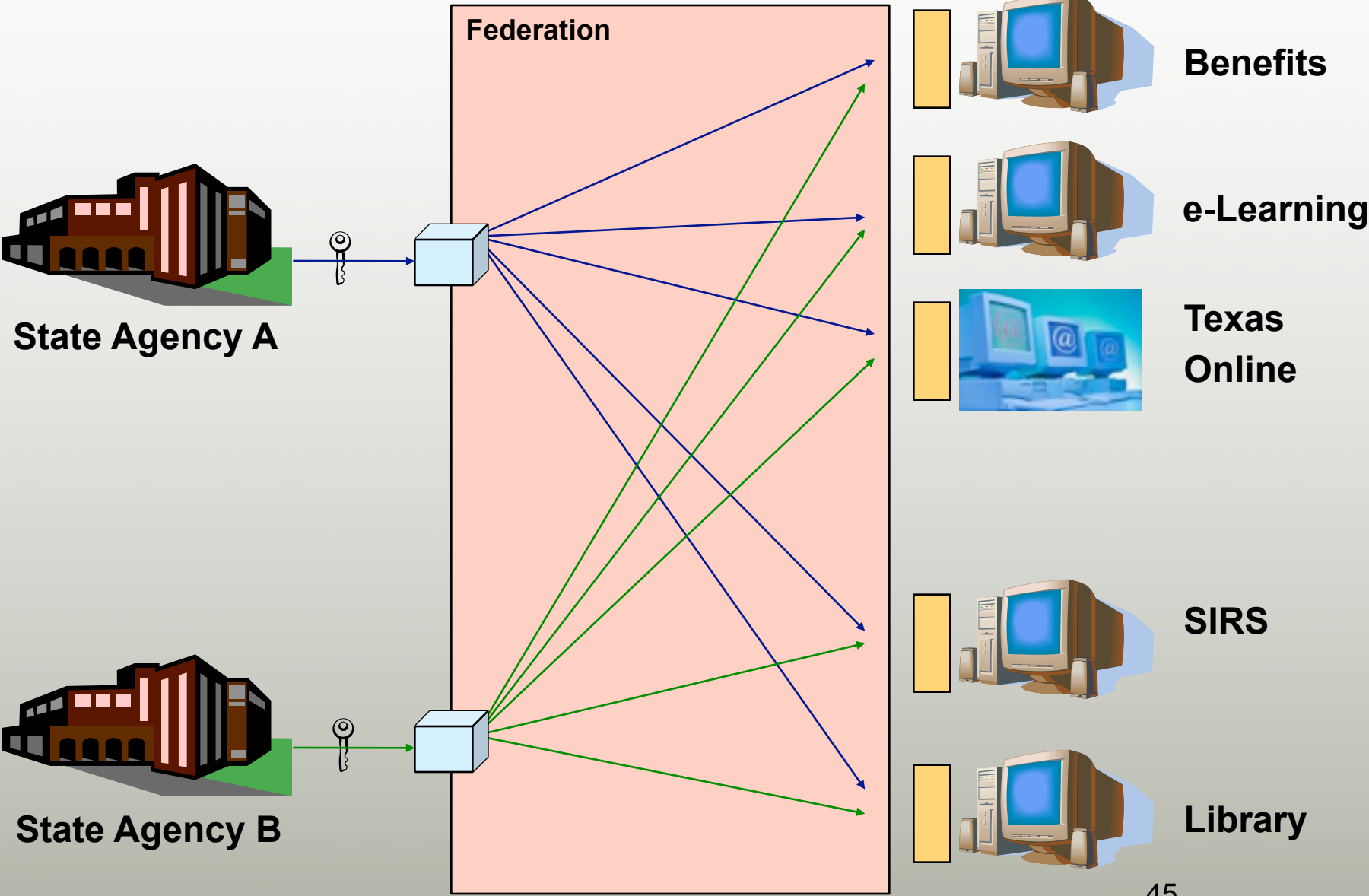


 = Credentialing / Authentication

 = Authorization

 = User Credential

Federated Identity Concept



 = Credentialing / Authentication  = Authorization  = User Credential

Federations

- **InCommon Federation**
 - HE & Research Emphasis
- **UT System Identity Management Federation**
 - Business Emphasis
- **State of California Federated IdM Vision**
(http://www.cio.ca.gov/stateIT/pdf/California_SOA_and_IDM_Vision_122007.pdf)
- **State of New York IdM Model**
(<https://www.oft.state.ny.us/Policy/G07-001/>) Trust Model
(<http://www.oft.state.ny.us/OFT/PrinciplesoftheNYSEnterpriseIAMArchitecture.pdf>)
- **State of Nebraska Federated Services**
(http://www.nitc.state.ne.us/events/conferences/egov/2004/files/345_UserAuthentication_Hartman-FedID.ppt)

InCommon Federation – An Example

www.incommonfederation.org

- Presently about 141 members, approximately 101 higher education institutions, 5 government agencies or non-profit laboratories, and 35 corporations (public and non-profit) representing 3 million individuals.
- Entities agree to a common participation agreement that allows each to inter-operate with the others.
- InCommon sets basic practices for identity providers and service providers. The primary focus has been technical and focuses on campus identity management procedures and attributes.

[Join InCommon](#)

[Participants](#)

[Policies and Practices](#)

[Technical Information](#)

[Metadata, WAYF, & CA](#)

[Frequently Asked Questions](#)

[Benefits](#)

[Site Administrator Login](#)

[Collaboration Wiki](#)

[Glossary](#)

[Contact](#)

[About](#)

InCommon makes sharing protected online resources easier.

InCommon eliminates the need for researchers, students, and educators to maintain multiple, passwords and usernames. Online service providers no longer need to maintain user accounts. Identity providers manage the levels of their users' privacy and information exchange. InCommon uses SAML-based authentication and authorization systems (such as [Shibboleth®](#)) to enable scalable, trusted collaborations among its community of participants.

Of Interest

- [Public Draft](#) InCommon is developing a program, tentatively called the [InCommon Defined Identity Assurance Program](#), to define and certify standard practices for "identity assurance" (aka InCommon Bronze and Silver). DRAFT documents describe the program and profiles and are available for comment from the community at the link above.
- [Update: Software & Protocol Support](#)
- [InCommon and Microsoft's DreamSpark FAQ](#)
- Attribute [Overview](#) and [Summary](#) documentation
- [Joining the InCommon Federation](#) (Eligibility Criteria and Process)
- The InCommon Participation Agreement [[pdf](#)]
- [The InCommon Fee Schedule](#)
- [Sponsorship Information](#): How to sponsor or be sponsored for federation participation

Case Studies

Read about current InCommon Participants and how they are implementing innovative approaches to federating identity and access management systems.

[Screenshot](#)
VIVA Library Consortium federates PBS video content [[pdf](#)]



UCTrust
Federation built on a Federation [[pdf](#)]



InCommon Federation – How is it Used?

- InCommon uses a technology called Shibboleth (shibboleth.internet2.edu) that uses the security access markup language (SAML) to exchange information.
- A student at my institution can access external content providers and request information. When they do this the user is directed to authenticate at UMBC and UMBC provides some agreed upon attribute to the content provider validating access (or not).
- Shibboleth is designed so that you can release the minimal amount of information as necessary.

Benefits of Federations

- For organizations, without a federation, organizations that want to share information must enter into bilateral agreements. These agreements are difficult to achieve and greatly complicate the work of insuring compliance if each has slightly different terms.
- For individuals, without a federation, individuals must establish a relationship with each organization, often providing duplicate information to multiple organizations.

InCommon Federation

- It has taken three years to reach this point. Recent interest from Microsoft, Google, and Apple will dramatically increase membership.
- We anticipate that InCommon could double in size every 6 months for the next 3 years, when it could ultimately reach 1000 universities and represent at least 10 million individuals.
- We are adding new categories for members that need greater security. “Silver” membership will require higher level of assurance for credentials and require an annual audit of practices.

The Evolution of Federations

- As I look at InCommon I can see the possibility of InCommon becoming a meta-data service and supporting a variety of federations. A major research project is inter-federation trust support.
- As the broad use of federation becomes more commonplace we envision that across our users there will be range of applications available through the federation that require different levels of assurance.
- As a result, managing compliance requires validating each identity is managed appropriately and assigned the proper level of assurance.

Vendor Offerings

- Higher education has often built these identity management system as custom software projects.
- Many agencies require vendor support or COTS products to begin deployment.
- Major vendors are developing comprehensive products -- I will speak to two of the larger vendors, Oracle and Microsoft.

Vendor Solutions for Managing Application Security - Oracle

- Oracle has purchased a number of the leading companies in the middleware space – Oblix and BEA to name a few and has a well thought out plan.
- Oracle's Fusion Middleware product is moving to redefine the way that security is provisioned in Oracle Fusion applications. There will be mechanisms for provisioning non-Oracle applications

Oracle Middleware

Oracle has one of the most comprehensive set of IDMS solutions among vendors. It is quite complete but also quite complex and in my opinion requires strong technical resources to implement.

▲ ORACLE IDENTITY MANAGEMENT SOLUTIONS

- [Oracle Access Manager](#)
- [Oracle Adaptive Access Manager](#)
- [Oracle Identity Manager](#)
- [Oracle Role Manager](#)
- [Oracle Identity Federation](#)
- [Oracle Internet Directory](#)
- [Oracle Virtual Directory](#)
- [Oracle Web Services Manager](#)
- [Oracle Enterprise Single Sign-On Suite](#)
- [Oracle Entitlements Server](#)
- [Oracle Management Pack for Identity Management](#)
- [Oracle Identity & Access Management Suite](#)
- [Oracle I&AM Suite for Mid-Sized Businesses](#)
- [Oracle Authentication Services for Operating Systems](#)

Microsoft Identity Lifecycle Manager

- Microsoft has been building a solid system by leveraging its investment in Active Directory. Microsoft released the Microsoft Identity Management System a few years ago and in higher education we see increased adoption.
- Microsoft has recently announced the Microsoft Identity Lifecycle Manager 2.0 (ILM) system. This builds on the prior system and adds much better provisioning, credential management, and support for some of the emerging web-services standards. Groups making heavy use of Windows Server and/or Sharepoint will be targeted.



Identity Lifecycle Manager "2"

Identity Management is about to get a lot easier

ILM "2" Feature Highlights:

Policy Management

- SharePoint-based console for policy authoring, enforcement & auditing
- Extensible WS-* APIs and Windows Workflow Foundation workflows
- Heterogeneous identity synchronization & consistency

Credential Management

- Heterogeneous certificate management with 3rd party CA support
- Management of multiple credential types, including OTP
- Self-service password reset integrated with Windows logon

User Management

- Integrated provisioning of identities, credentials, and resources
- Automated, codeless user provisioning and deprovisioning
- Self-service user profile management

Group Management

- Rich Office-based self-service group management tools
- Offline approvals through Office
- Automated group and distribution list updates

Concluding Remarks

- Identity management should be integral to your security and privacy architecture and the cornerstone of compliance.
- Levels of assurance is a key concept in managing risk and balancing ease-of-use versus security.
- Federation is an essential tool for SaaS and cloud computing.
- Vendor products are emerging but there is no single solution for all needs.

More Information

Jack Suess, VP of IT, UMBC

Phone – 410.455.3208

Email – jack@umbc.edu

URL – <http://userpages.umbc.edu/~jack>

Questions?