

Real-World Identity Management Solutions

John A. Lewis
Chief Software Architect
Unicon, Inc.

28 July 2009
Campus Technology
Boston, Massachusetts

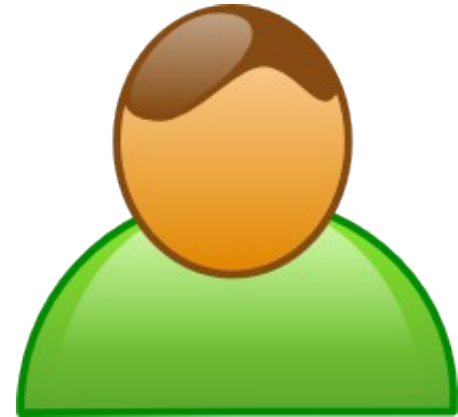


© Copyright Unicon, Inc., 2009. Some rights reserved.
This work is licensed under a Creative Commons Attribution-Noncommercial-
Share Alike 3.0 United States License. To view a copy of this license, visit:
<http://creativecommons.org/licenses/by-nc-sa/3.0/us/>



Why Makes Identity Important?

- **Connects**
 - **Users**
 - **Applications**
- Lots of other things
 - security, privacy, spam,
 - secrecy, trust, authority,
 - collaboration, convenience,
 - ...



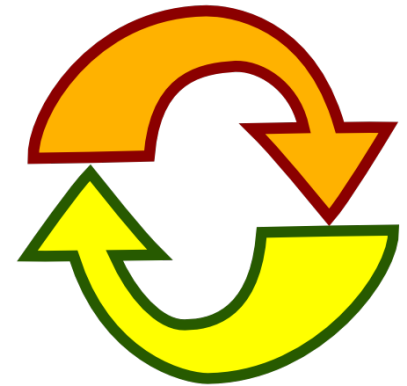
What *Is* Identity Management?

“A set of processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities.” – Burton Group

- Account creation, directories, authentication, authorization access controls, ...
- Includes policy, process, governance, trust
- Need new ways of thinking about controlling access to IT services

Identity Management Lifecycle

- Provisioning
 - Initial Account creation
 - When to establish a persistent identity?
- Account updates
 - Self-service? For which attributes?
 - Central administrative changes
- Role maintenance
 - Adding, changing, removing roles
- Suspending / Removing / Restoring
 - When to do this? How long to retain it?



Policy and Governance

PRESIDENT
PROVOST



REGISTRAR



HUMAN
RESOURCES



FACULTY
AFFAIRS



CIO



...

Establish identity

Determine policy

Source Systems

HR

faculty, staff

SA

student,
postdoc

Finance

PI, approver

Courses

instructor,
enrolled

⋮

Reflect
& Join

Manage Identity

Persons

Accounts

Organizations

Groups

Privileges

Authenticate
Authorize
Provide
Federate

Systems and Services

Business
systems

Network
services

Library

⋮

Federated
partners

Enrich identity

SCHOOLS
DEPARTMENTS



PROJECTS



PROGRAMS



TEAMS



USERS



...

Manage Groups

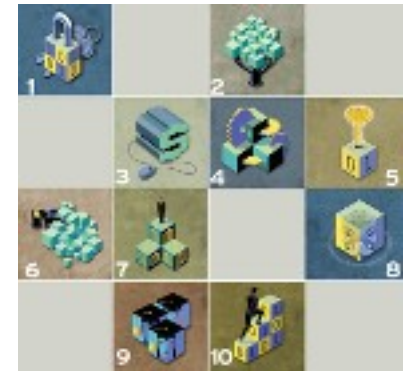
Apply policy

Manage Privileges

• EDUCAUSE Top 10 IT Issues

- **2003 #3**
Security & Identity Management
- **2004 #3**
Security & Identity Management
- **2005 #2**
Security & Identity Management
- **2006 #1**
Security & Identity Management
- **2007 #4**
Identity / Access Management (Security at #2)
- **2008 #5**
Identity / Access Management (Security at #1)

TOP
10 IT
ISSUES



Challenge & Goal

- Challenge: **Fragmented Identity Landscape**
 - Many systems of records
 - Many applications
 - Many passwords
 - Many overlapping roles
- Goal: **Ease-Of-Use for Students/Faculty/Staff**
 - Enable seamless access to resources
 - Enforce security and privacy
 - Create a sense of a unified Enterprise

Evolution of User Identity

- Application Silos
 - Each with their own logins and passwords
- Common Directories / Databases
 - Central store for person information
- Single Sign-On
 - Central login system for multiple applications
- Federated Identity
 - Trusted identity information from others

Emerging Best Practices

- Automate Provisioning across systems
- Separate Authentication and Authorization
- Use Roles for Access Control & Dynamic Rules
- Provide Delegated Administration
- Multiple Authoritative Sources for Attributes
- Allow Account Names to change

Federated Identities

Developing a Coherent Cyberinfrastructure from Local Campus to National Facilities: Challenges and Strategies

A Workshop Report and Recommendations

EDUCAUSE Campus Cyberinfrastructure Working Group
and Coalition for Academic Scientific Computation

February 2009



Short Link: <http://bit.ly/jsTvH>

Strategic Recommendation 2.3.1

“Agencies, campuses, and national and state organizations should adopt a single, open, standards-based system for identity management, authentication, and authorization, thus improving the usability and interoperability of CI resources throughout the nation.”

Tactical Recommendation 2.3.1a

The global federated system for identity management, authentication, and authorization that is supported by the InCommon Federation should be adopted with an initial focus on major research universities and colleges. After an initial deployment in research-oriented functions involving research universities, such an identity management strategy for CI should be implemented generally within funding agencies and other educational institutions.

Why Federated Identity?

- *Authoritative* information
 - Users, privileges, attributes
- Improved security
 - Fewer user accounts in the world
- Privacy when needed
 - Fine control over attribute sharing
- Saves time & money
 - Less work administrating users

What Is SAML?

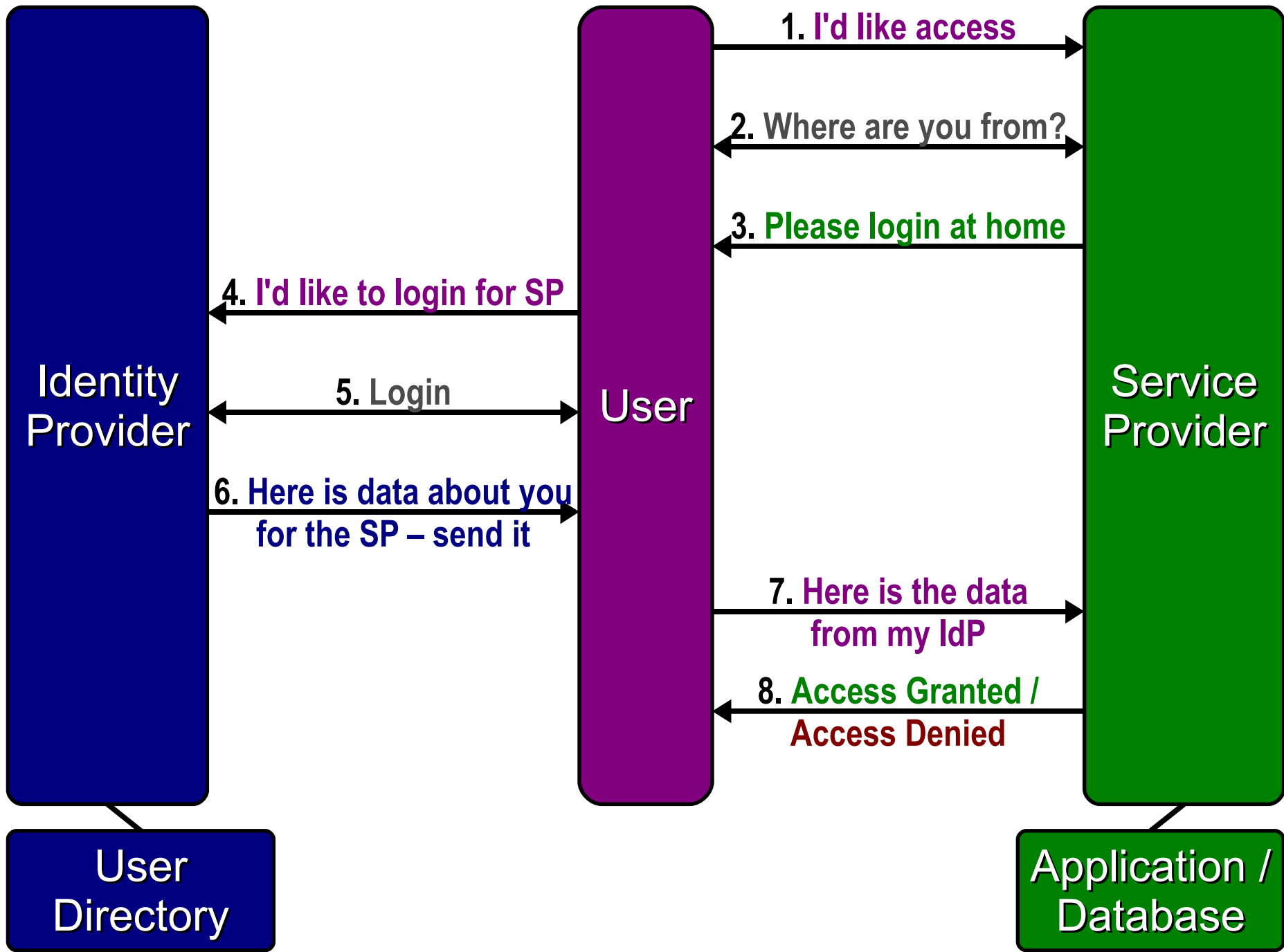
- Security Assertion Markup Language (SAML)
- XML-based Open Standard
- Exchange authentication and authorization data between security domains
 - Identity Provider (a producer of assertions)
 - Service Provider (a consumer of assertions)
- Approved by OASIS Security Services
 - SAML 1.0 November 2002
 - SAML 2.0 March 2005

Major SAML Applications

- Proquest
- Project MUSE
- Thomson Gale
- Elsevier ScienceDirect
- Google Apps
- ExLibris MetaLib
- Sakai & Moodle
- uPortal
- DSpace, Fedora
- Ovid
- Microsoft DreamSpark
- Moodle, Joomla, Drupal
- JSTOR, ArtSTOR, OCLC
- Blackboard & WebCT
- WebAssign & TurnItIn
- MediaWiki / Confluence
- National Institutes of Health
- National Digital Science Library

How Federated Identity Works

- A user tries to access a protected application
- The user tells the application where it's from
- The user logs in at home
- Home tells the application about the user
- The user is rejected or accepted



Shibboleth

Shibboleth

- Enterprise federated identity software
 - Based on standards (principally SAML)
 - Extensive architectural work to integrate with existing systems
 - Designed for deployment by communities
- Most widely used in education, government
- Broadly adopted in Europe
- 2.0 release implements SAML 2
 - Backward compatible with 1.3



Shibboleth Project

- Free & Open Source
 - Apache 2.0 license
- Enterprise and Federation oriented
- Started 2000 with first released code in 2003
- Excellent community support
 - <http://shibboleth.internet2.edu>
 - shibboleth-announce@internet2.edu



Join the Federation!



Role of a Federation

- Agreed upon Attribute Definitions
 - Group, Role, Unique Identifier, Courses, ...
- Criteria for IdM & IdP practices
 - user accounts, credentialing, personal information stewardship, interoperability standards, technologies, ...
- Digital Certificates
- Trusted “notary” for all members
- Not needed for Federated IdM, but does make things even easier

InCommon Federation

- Federation for U.S. Higher Education & Research (and Partners)
- Over Three Million Users
- 163 Organizations
- Self-organizing & Heterogeneous
- Policy Entrance bar intentionally set low
- Doesn't impose lots of rules and standards
- <http://www.incommonfederation.org/>



Other Emerging Projects / Standards

- **Grouper**
grouper.internet2.edu 
 - Access Management via sophisticated group structures, protocols
- **Comanage**
middleware.internet2.edu/co 
 - Collaborative Organization Management Platform with wide variety of “domesticated” applications
- **XACML** - eXtensible Access Control Markup Language
 - declarative access control policy language and a processing model for interpret the policies
- **SPML** - Service Provisioning Markup Language
 - framework for exchanging user, resource, and service provisioning information between organizations

Questions & Answers



John A. Lewis
Chief Software Architect
Unicon, Inc.

jlewis@unicon.net
www.unicon.net