InCommon®

IAM Online

Thursday, June 10, 2010 – 1 p.m. EDT

Handling Affiliate Populations

Questions via Adobe Connect chat
Audio via Adobe Connect – preferred

Conference phone bridge also available (listen-only)
Dial-in numbers:
+1-734-615-7474 Preferred (from any phone where long distance has no add'l cost)
+1-866-411-0013 (US/Canada only if you pay for long distance)
Access Code: 0157272#

UNICON®

Thank you to our InCommon Featured Affiliate for June, Unicon, for supporting IAM Online

InCommon®

Handling Affiliate Populations

- capabilities of a guest and affiliate system
- methods to track these populations, including provisioning and deprovisioning services.

Today's Speakers

Liz Salley, University of Michigan

Brendan Bellina, University of Southern California

MCommunity

University of Michigan MCommunity: Affiliate Management

Liz Salley (salley@umich.edu)
Product Manager, Information and Technology Services

Overview

- **Who's in, who's out.** MCommunity will allow the University to know who is and is not a member of the U-M community so that central University offices, departments, schools, colleges, and campuses can grant and remove access to online resources as needed and appropriate.
- **Affiliate Management is key.** In order to effectively support the identity and access needs for the entire community, the creation of an affiliate management system was considered a key building block for our entire enterprise IAM project.
- **A collaborative effort.** MCommunity is a collaborative effort across U-M IT units and the many academic and non-academic units that use it.

http://www.itd.umich.edu/mcommunity/

Problem Statements

- **Time-consuming to get access.** Going through "official" channels to provision accounts to the extended University community, including parents, visiting faculty, volunteers, etc., is time-consuming and unrealistic.
- **Local control wanted.** Units demand local control of access to IT services.
- **Better life cycle management needed.** Consistent and predictable life cycle management practices are needed.
- **Varying Levels of Identity Assurance Required**
  - Staff contractors require a UM credential, expect a similar user experience, and require the same identity assurance as staff or faculty.
  - Short-term affiliates often require a UM credential, but are only granted limited access and do not require strong identity assurance.
  - Many services do not require a UM-issued credential at all.

Affiliate Types

- **Sponsored Affiliates**
  - Examples: Contractors, Visiting Researchers, conference attendees, short-term guests.
  - Must be identified by a recognized UM department who agrees to actively manage the identity life-cycle.
  - UM credential created in the central IAM system.
  - Future: Potential to meet InCommon Silver Assurance.
- **Self-Registered Affiliates**
  - Examples: Parents or other family members, Donors, Library Patrons.
  - Affiliate "self-registers" with the target system. May require delegation of access from a person with a UM credential, or a UM unit.
  - Uses a non-UM credential (ie, a valid non-umich e-mail address).

Sponsored Affiliates

Relationship/Business Reason	Uniqname Type	Identity Type	Default Sponsorship Length*
Contractors	Regular	Strong	30 days
Incoming Faculty/Staff	Regular	Strong	6 months
Temporary Staff	Regular	Strong	1 year
Visiting Researchers/Scholars	Regular	Strong	1 year
U-M Online Subscribers**	Regular	Strong	1 year
Associates	Regular	Weak	1 year
VIPs	Regular	Weak	1 year
Conference/Program Participants	Temporary	Weak	30 days
Wireless Users	Temporary	Weak	10 days
Other Short-Term Guests	Temporary	Weak	90 days

- **Additional details about UM Sponsor system and sponsorship types available at: http://www.itd.umich.edu/itcsdocs/r1458/**

Authority and Accountability

- How do we enforce standards in a highly decentralized environment?
- System enforcement vs. guidelines and best practices.
- Decentralized authority and accountability to ensure guidelines and best practices are followed.
- Resources for IT directors.
- See “MCommunity Sponsoring Authority Policies and Agreement” http://www.itcs.umich.edu/itcsdocs/r1460/

Self-Registered Affiliates

- Example: Parent (Family and Friend) Access to Student Information.
- Limited to Student Accounts and Financial Aid.
- Student must first authorize (delegate) access by registering the delegate's e-mail address in the student information system.
- An e-mail is automatically generated to the delegate inviting them to self-register for a **UM Friend Account** (http://www.itd.umich.edu/itcsdocs/s4316/)

Self-Registered Affiliates

- UM Friends is an extension of our CoSign web single sign-on implementation (http://cosign.sourceforge.net/).
- Any CoSign-protected web resource on campus can take advantage of UM Friends accounts.
- The owner of the web resource defines policy and lifecycle for UM Friend Account access.
- Other Examples:
  - Library staff "delegate" access to public Library resources without needing to create a UM credential.
  - The UM Alumni Association can link a Friends Account to non-alumni donor records.

Questions?

University of Southern California: Handling Affiliate Populations IAMOnline June 10, 2010

Brendan Bellina
ITS Identity Services Architect
Mgr, Enterprise Middleware Identity Management
Information Technology Services
University of Southern California
Los Angeles, California, USA
bbellina@usc.edu

University of Southern California

- Private research university, founded 1880
- 35,000 students
- 21,100 employees
- 229,000 alumni
- 19 academic units
- Two major Los Angeles campuses; six additional US locations; four international offices

Source: http://www.usc.edu/about/ataglance/

Populations of Interest

- Members:
  - Students, Faculty, Staff employees
- Affiliates/Associates:
  - Student Lifecycle related: Admits, Alumni, former students
  - Employee Lifecycle related: Incoming faculty and staff; Emeriti and retirees
  - Visitors - Visiting scholars and researchers, summer program attendees, volunteer faculty, vendors, etc.
  - Library Patrons
  - Parents, Donors, etc.

How NOT to Establish the Identity Record

- "Force Square Peg into Round Hole" Method
  - Incomplete record of individual forced into a system of record such as the Student System or Payroll/HR
  - Creates problems:
    - Mixes non-members into member populations
    - Undermines common assumptions
      - Student Record => Student ID => Student
      - Employee Record => Employee ID => Employee
    - Requires special activation/deactivation practices
    - May inappropriately provide/constrain service access

How NOT to Establish the Identity Record

- "Manage Accounts not People" Method
  - Create accounts in electronic service systems
  - Gap between Identity System and Account store
    - Identity information stored in the Account store
    - Conflicts when the account holder becomes a member
    - Can result in privileges being given out for longer than needed
    - Difficult to determine all services accessible by the person
  - Gap between Identity System Policy and Account Practices
    - Application account administrator acts as policy maker in a policy vacuum

Trends and Requirements

- Common movement between member and non-member roles
- Wider range of eServices that departments want to extend to non-members
- More services becoming integrated with IAM for SSO, authentication, authorization, and personalization
- Potentially a large and growing population of affiliates
  - University of Salford (20,000 students, 2,500 employees) estimated 2,500-5,000 affiliates of 12 types accessing 15 resources and later found it to be closer to 40,000 (excluding alumni) of 77 types accessing 85 resources

USC Sponsored Guest System: iVIP

- Requirements established by a committee of academic and administrative leaders
- Developed by Central IT resources in Identity Services
- Integrated with Person Registry for Identity Resolution
- Integrated with Enterprise Directory “GDS” for authorization to services
- Web interface delegated to trained department administrators for data entry and maintenance
- Web interface for service providers
- Application owner is for the time being the Office of Organization Improvement

iVIP Steering Committee

- Chaired by Margaret Harrington, the Director of the Office of Organization Improvement Services
- Management committee meets monthly
  - Focuses on requirements of the iVIP system to allow services to be extended to non-members, establishes practices, recommends policy
  - Attendees include representatives from ITS, academic schools, administrative departments
- Technical sub-committee meets monthly
  - Focuses on technical development, establishes development priorities
  - Attendees include members of the ITS development group and representatives from the Office of Organization Improvement Services

iVIP Policies

- Required attributes - Name (first and last), Date of Birth, and two forms of contact - email address, telephone number, or physical mail delivery address
- All iVIP administrators must complete iVIP training and be employed by the University
- All granted iVIP services must have a start date (within a year) and an end date (within a year of start date)
- One sponsoring department acts as primary sponsor for the VIP
- Sponsor must be a benefits eligible USC employee and be identified by the department dean or Vice-President
- VIPs are outside standard active lifecycle of Student and Employee Systems

iVIP Roles

- Program Director
  - Primary Data Steward for Guest/Affiliate system
- System Director
  - Technical manager of Guest/Affiliate System
- Department Executive
  - Delegates authority to sponsors and lead administrator; typically a dean, chair, or vice president
- Department Lead Administrator
  - Manages the sponsorship process for the department and assigns department administrators. Must be a full-time USC employee. Must complete iVIP training.

iVIP Roles

- Department Sponsor
  - Faculty or staff member with authority to sponsor a guest/affiliate on behalf of a department
- Department Administrator
  - Responsible for operational interface between sponsors and the Guest/Affiliate system. Enters requests into the iVIP system. Must be a full time USC employee. Must complete iVIP training.
- Service Manager
  - Responsibility for a service such as Email, Blackboard, White Pages, Portal. May determine additional requirements for Guest/Affiliates requiring access to a service. Can remove a Guest/Affiliate from a service if need be.
- Service Administrator
  - Administrator of a service. Has responsibilities regarding the accounts within a service.

iVIP Services

- Any department can sponsor an iVIP for any services defined in iVIP
- iVIP services:

Blackboard instructor	University Email
MyUSC Portal	White Pages listing
University VPN	White Pages Retrieval
USCard	USCWeb
University Hospital Exchange	Departmental Services

Current Status

- Number of Services defined in iVIP: 10
- Number of roles defined: 16
- Number of identities entered into iVIP: 8,363
- Number of active affiliates: 4,400
- Number of departments using iVIP: 147 out of 230
- Number of department sponsors: 321
- Number of department administrators: 112
- Number of potential services for affiliates: 100+

Challenges we face

- Resolving duplicates requires participation from all Systems of Record – *Maintain good communication and appropriate steering committees*
- Some applications assume information is available that is not available for affiliates – *Require developers to understand the attributes that are available for affiliates*
- Unknown affiliate types appearing with little warning, usually challenging practice and policy – *Pursue senior level backing for policies*

Challenges we face

- Difficulty establishing a permanent home for the system
- Departments wanting affiliates to have services but access them in non-standard ways
- Departments using the affiliate system rather than establishing their own SOR
- Department administrators fabricating VIP data
- Data and service access issues when people transition from VIP to member or vice versa

Questions?

InCommon®

Please complete the survey about today's IAM Online:
http://www.surveymonkey.com/s/FFGQCCT

Shibboleth Workshop Series

Shibboleth®

Northwestern University Library
Evanston, Illinois

Identity Provider July 28, 2010 (9 a.m. - 6 p.m.)
Service Provider July 29, 2010 (9 a.m. - 6 p.m.)

www.incommon.org/educate/shibboleth

InCommon®

Please complete the survey about today's IAM Online:
http://www.surveymonkey.com/s/FFGQCCT

Upcoming IAM Online

www.incommon.org/iamonline

July 8, 2010 – 1 p.m. (ET) eduRoam
August 12, 2010 – 1 p.m. (ET) Federated Identity Management Essentials

Thank you to InCommon Affiliates for helping to make IAM Online possible.

UNICON® aegisUSA™

Brought to you by InCommon, in cooperation with Internet2
and the EDUCAUSE Identity and Access Management Working Group