Copyright: Brian Coats – 2013

This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.
UM Community System: Expanding Identity Boundaries

Brian Coats
Director, Identity Management & System Integration
University of Maryland

January 17, 2013
Agenda

- Introduction
- UM Community System Objectives
- Design Framework
- Timeline & Outcomes
- Challenges
- Conclusion
Introduction to the Environment

- UM implemented Directory Services in 2004
- Central authN/authZ

<table>
<thead>
<tr>
<th>Internal Apps</th>
<th>Internal Web sites/apps</th>
<th>External Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>61</td>
<td>Hundreds</td>
<td>100+</td>
</tr>
<tr>
<td>Shibboleth/LDAP</td>
<td>Shibboleth/LDAP</td>
<td>Shibboleth</td>
</tr>
</tbody>
</table>

- 65,686 total identities (39,812 are active)
  - Student identities have a minimum 3 year lifespan following last activity (admission → graduation)
  - All other accounts are immediately disabled upon termination of employment or non-renewal of sponsorship
Identity Sources

UM Community System
(Affiliates, Anyone/Everyone)

eUM HRMS
(Employees)

UM SIMS
(Students)

UM DIRECTORY
Identity Sources

- eUM HRMS (Employees & Affiliates)
  - Employee records are only sent once entire hiring process is complete – could be weeks or months from start date
  - Affiliate system is bolt-on app originally designed for HRMS users ONLY
    - Security precautions are typically overkill for user’s needs
    - Cumbersome process (paper, signatures, slow = days)
    - Sponsorship renewals are not consistently performed
    - 12,992 identities created to date
    - Established 2005 – average ~135 per month
Identity Sources

- UM Stub Record App (Incoming Employees)
  - Created to compensate for slow hiring process
  - Administered by OneCard Office
    - Priorities tend to be more customer-centric than security-centric
    - Data inconsistencies due to lack of vested interest
    - Cumbersome process (paper/email, multiple hops, data entry on behalf of users, slow = hours)
  - 4,549 identities created to date
  - Established 2006 – average ~55 per month

- UM SIMS (Students)
  - Many stages in student lifecycle, many variations to the order
  - Some services/applications should retain perpetual access
Problems Faced

- Who can create identities?
  - eUM HRMS, eUM Affiliate System (IT Helpdesk), UM Stub Records (OneCard Office), UM SIMS – Too Restrictive

- How long does it take to create an identity?
  - Days to Weeks – Too Long

- Who needs to be involved in identity creation?
  - User, Payroll Reps, Registrar, School/Dept Sponsor, IT Helpdesk, OneCard Office – Too Many Players
Problems Faced

- How long will the identity be valid?
  - At least 1 year, maybe forever – *Not Flexible/Insecure*

- What privileges should the identity have?
  - No hierarchy in directory architecture, application has to make the determination – *Not Flexible/Insecure*
UM Community System Objectives

- Anyone can register for an UM identity (self or on other’s behalf)
- Identity creation is immediate
- All electronic workflow (registration, sponsorship, credentialing, renewals, revocations)
- Identity lifespan can be customized and is regularly validated
- Identities have varying levels of privileges based on sponsorship
UM Community System Objectives

- Incoming Employees
- Emeritus Faculty
- Visiting/Adjunct Faculty
- Temp/Contractual Employees
- Partner Organization Employees
- Prospective Students
- Pre-Directory (2004) Alumni
- Visiting Students
- Library Patrons
- Volunteers
- Vendors
- All other needed users that aren’t captured in our other Identity Sources that need access to UM resources
### Design: Registration Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Register</th>
<th>View</th>
<th>Edit</th>
<th>Sponsor</th>
<th>Approve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Approver</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Sponsor</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>App Owner</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Editor</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Helpdesk</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reviewer</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Approvers** = School/Dept designee that has final authority to grant identity creation
- **Sponsors** = School/Dept user that can vouch for connection to university (anyone that can approve timesheets)
- **Editors** = Someone that can edit records for accuracy (admin assistants)
- **Reviewers** = Someone that can view records only
Design: Identity Registration

1. Web Registration
   - Data Validation & Duplicate Checking
   - Create/Modify CS Record
2. Sponsor Emailed or Self-Initiated
3. Sponsorship Decision
4. Sponsorship Info Recorded
5. Approval Emailed or Self-Initiated
6. Approval Decided
7. Approval Info Recorded
8. Web Approval
9. User Emailed
   - CS Record is Registered in Directory

Registrand (self or on someone’s behalf)
Design: Application Provisioning

New User
Web Registration → Data Validation & Duplicate Checking → Create/Modify CS Record → Sponsorship/Approval Workflow

Existing User
Web Application Request → CS Application Request Record Created → Directory Object updated with App Request Data

Registrant (self or on someone’s behalf)
Sponsor/Approver
User feed to relevant App
Project Timeline

- **Phase 1:** *Spring 2011 – Fall 2012*  
  - System Design/Web Development
  - Pilot
    - HS/HSL Patrons
    - USM Library-Shibboleth Project
    - Vibe Users
  - Sponsor/Approver-driven Registration

- **Phase 2:** *Winter 2012 – 2013*  
  - Levels of Assurance
  - System of record for all non-eUM Affiliates
  - Electronic workflow for sponsorship and approval
  - Retire eUM Affiliation System and introduce HRMS Person Module
  - Application/Service Request module

- **Phase 3:** *2013 – 2014*
  - Self-registration
  - Replace and retire Stub Record Application

**COMPLETE**

**UNDERWAY**
Outcomes

- **Who can create identities?**
  - *Problem:  HRMS, SIMS, IT Helpdesk, OneCard Office – Too Restrictive*
  - *Solution:  HRMS, SIMS, UM Community System*
    - Anyone can self-register for an UM identity
    - Identities can be registered on someone else’s behalf

- **How long does it take to create an identity?**
  - *Problem:  Days → Weeks – Too Long*
  - *Solution:  Immediately (real-time)*
Outcomes

- Who needs to be involved in identity creation?
  - Problem: User, Payroll Reps, Registrar, School/Dept Sponsor, IT Helpdesk – Too Many Players
  - Solution: User, Payroll Reps, Registrar, School/Dept Sponsor (eliminate IT Helpdesk and OneCard Office from process)
    - All stakeholders remain involved, IT Helpdesk and OneCard Office removed as the ‘baby-sitters’ of the process
    - All electronic workflow
    - HRMS-aware security model to determine eligible sponsors
Outcomes

- **How long will the identity be valid?**
  - *Problem:* At least 1 year, maybe forever – *Not Flexible/Insecure*
  - *Solution:* Lifespan of identity can be chosen at time of sponsorship and renewed/revoked anytime

- **What privileges should the identity have?**
  - *Problem:* No hierarchy in directory architecture, application has to make the determination – *Not Flexible/Insecure*
  - *Solution:* Start with UM-LOA0 (minimal access) and elevate LOA based on sponsorship
Challenges

- Logistical/Political
  - Competing projects/priorities
  - Resources

- Functional
  - Develop a sponsorship framework and workflow that didn’t exist reliably
  - School/dept-specific vs. One-size-fits all
  - Retrain school/depts on where/what/who/how to get their users accounts (Affiliates & Stub Records)
  - Culture change for users to renew accounts

- Technical
  - Potential configuration changes to existing applications to leverage UM-Levels of Assurance
Conclusion

- Create new authoritative source – UM Community System
  - Immediate identity creation
  - All electronic workflow
  - Customizable identity lifespan with required renewals
- Retire ineffective authoritative sources
  - UM Stub Records & eUM Affiliate System – approx 190 accounts per month
  - Remove non-stakeholders from process
- Introduce UM Levels of Assurance
  - Segregate applications of like security to appropriate LOA OU’s
  - Allow perpetual access as appropriate
Questions?

Brian Coats
Director, Identity Management & System Integration
University of Maryland
bscoats@umaryland.edu