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.
Self-Service Identity: Join The Community

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

January 12, 2012
Presentation Outline

- The Landscape – The environment
- The Problem – What we are trying to address
- The Destination – Where we want to go
- The Roadmap – How we get there
- Conclusion
The Landscape – Current Scope

- UM Directory in production since 2004
- Central authN/authZ
  - 36 enterprise applications
  - Hundreds of internal web applications
  - 16 inter-institutional/government applications
- 58,532 total identities (41,544 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
The Landscape – Current Authoritative Sources

eUM HRMS (Employees & Affiliates)
UM Stub Records (Incoming Employees)
UM SIMS (Students)
UM DIRECTORY
The Landscape – Current Authoritative 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 eUM affiliates ONLY
    - Security precautions are typically overkill for user’s needs
    - Cumbersome process (paper, signatures, slow = days)
    - Sponsorship renewals are not consistently performed
    - 6,544 identities created to date
    - Established 2005 – average ~80 per month
The Landscape – Current Authoritative 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)
  - 3,750 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
The Landscape – Current Directory Architecture

- Majority of applications use either native LDAP or Shibboleth for authN

- Directory Architecture
  - All users are in single OU (no hierarchy)
  - Many applications cannot filter authN requests based on complex queries (e.g. Status=A, CurTermReg=True)
    - These applications rely on basic account controls to determine access (e.g. loginDisabled=True)
    - Requires all applications to play by the same rules for how long users have valid credentials (e.g. Students have 3 years after graduation)
The Landscape – Current Directory Architecture
The Problem

- Almost all enterprise applications leverage the enterprise IdM system, therefore an identity is required for all users for authN/authZ

- Issues:
  - Many users of campus resources are not present in traditional authoritative sources (HRMS, SIMS)
  - Current eUM Affiliate creation process is cumbersome (many steps, paper, slow, once-in/never-out)
  - Employee hiring process is not timely (could be weeks/months after start date to completion)
The Problem – Issues To Address

- 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
The Problem – Issues To Address

- 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*
The Destination

- 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
The Roadmap – Future Authoritative Sources
The Roadmap – UM Community System
The Roadmap – UM Community System

USER
(Self or On-Behalf)
User goes to a web page and self-registers for an account

SPONSOR
Sponsor is emailed approval request, use UM Directory authN to validate identity, sponsor approves user, and sets account expiration

UM Community System
Data is captured in UM Community System DB

User is emailed account has been approved and directed to myUM Acct Mgmt Site to set up their credentials

Electronic Approval Workflow
User LOA is raised based on sponsorship

UM Directory
User is created in UM Directory (UM-LOA0)
The Roadmap – Levels of Assurance

- Levels of Assurance
  - Based on NIST SP800-63 and InCommon Assurance Program
  - Definition: The confidence in the vetting of the identity and the ownership of the credential

- Implementation
  - Categorize applications by their respective security requirements
  - Classify security of identities based on confidence in that identity and corresponding credential
## The Roadmap – Levels of Assurance

<table>
<thead>
<tr>
<th>Description</th>
<th>InCommon Level</th>
<th>Vetting</th>
<th>Proofing</th>
<th>Creation</th>
<th>authN</th>
<th>TTL</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>UM-LOA0</td>
<td>No assurance of identity</td>
<td>Basic</td>
<td>N</td>
<td>N</td>
<td>Self-registered or registered on user's behalf</td>
<td>U/P, lower security scheme</td>
<td>90 days, unlimited renewal</td>
</tr>
<tr>
<td>UM-LOA1</td>
<td>Moderate level of assurance</td>
<td>Bronze</td>
<td>Y</td>
<td>N</td>
<td>sponsorship of LOA0 or authoritative source</td>
<td>U/P, moderate security scheme (current)</td>
<td>governed by authoritative sources</td>
</tr>
<tr>
<td>UM-LOA2</td>
<td>High level of assurance</td>
<td>Silver</td>
<td>Y</td>
<td>Y</td>
<td>elevation from LOA1</td>
<td>U/P, moderate security scheme (current)</td>
<td>governed by authoritative sources</td>
</tr>
<tr>
<td>UM-LOA3</td>
<td>Very high level of assurance</td>
<td>Gold</td>
<td>Y</td>
<td>Y</td>
<td>elevation from LOA1/2</td>
<td>2 factor - U/P and PKI, password resets cannot be performed via self-service</td>
<td>governed by authoritative sources</td>
</tr>
</tbody>
</table>
The Roadmap – Levels of Assurance

- **UM-LOA0**
  - No assurance of identity = InCommon Basic
  - No identity vetting or proofing
  - Accounts created via UM Community System – self register or registered on other’s behalf
  - U/P authN, password scheme is low
  - TTL is 90 days, unlimited renewal
  - Low security services provided
    - E2Campus
    - Wireless (DMZ)
    - Guest Access
The Roadmap – Levels of Assurance

- UM-LOA1
  - Moderate level of assurance = InCommon Bronze
  - Identity vetting required, no identity proofing
  - Accounts created via sponsorship of LOA0 account or entry into authoritative source
  - U/P authN, password scheme is high (current password controls – complexity, history, expiration)
  - TTL is dictated by sponsorship and/or authoritative source
  - Moderate security services provided
    - Most applications fit here
The Roadmap – Levels of Assurance

- UM-LOA2
  - High level of assurance = InCommon Silver
  - Identity vetting and proofing required
  - Accounts created via elevation from LOA1
  - U/P authN, password scheme is high (current password controls – complexity, history, expiration)
  - TTL is dictated by sponsorship and/or authoritative source
  - High security applications fit here
    - More sensitive applications – applications dealing with financial information, HIPAA, etc
The Roadmap – Levels of Assurance

- UM-LOA3
  - Very high level of assurance = InCommon Gold
  - Identity vetting and proofing required
  - Accounts created via elevation from LOA1/2
  - 2 factor authN – U/P and PKI, password resets cannot be done via self-service
  - TTL is dictated by sponsorship and/or authoritative source
  - Extremely sensitive applications fit here
    - Enterprise-wide, state/regional/national impact applications that require the highest degree of security
The Roadmap – Future Directory Architecture

- Directory Architecture
  - Each UM LOA will have its own part of the Directory (OU)
  - Users will have identities in each OU at or below their current LOA
  - Applications can decide which LOA fits their needs best and authN ONLY against that OU – filter by membership
The Roadmap – Future Directory Architecture
The Roadmap – Issues Addressed

- **Who can create identities?**
  - *Current:* HRMS, SIMS, Affiliate System (IT Helpdesk)
  - *Future:* 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?**
  - *Current:* Days → Weeks
  - *Future:* Immediately (real-time)
The Roadmap – Issues Addressed

- **Who needs to be involved in identity creation?**
  - **Current:** User, Payroll Reps, Registrar, School/Dept Sponsor, IT Helpdesk
  - **Future:** User, Payroll Reps, Registrar, School/Dept Sponsor (eliminate IT Helpdesk and OneCard Office from process)
    - All stakeholders remain involved, IT Helpdesk and OneCard Office is removed as the ‘baby-sitters’ of the process
    - All electronic workflow
    - HRMS-aware security model to determine eligible sponsors
The Roadmap – Issues Addressed

- **How long will the identity be valid?**
  - *Current:* At least 1 year, maybe forever
  - *Future:* Lifespan of identity can be chosen at time of sponsorship and renewed/revoked anytime

- **What privileges should the identity have?**
  - *Current:* No hierarchy in directory architecture, application has to make the determination
  - *Future:* Start with UM-LOA0 (minimal access) and elevate LOA based on sponsorship
Conclusion

- **Goals – The Destination**
  - 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
Conclusion

- Solution
  - 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 150 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
THANK YOU

Brian Coats
bscoats@umaryland.edu