UW System Identity & Access Management (IAM)

Recommended Strategic Roadmap

Fall 2015

ITMC
Our challenge

- CIOs charged IAM-TAG with recommending an IAM strategy that would:
  - Establish an identity that’s honored by all UW System institutions
  - Ensure that campuses could brand that identity
  - Ensure that campuses could define their own populations and access control requirements
  - Integrate with cloud providers and other external entities
  - Leverage infrastructure, staff resources and expertise wherever possible
Today's Infrastructure

Campus-Hosted IdP

- Campus SIS
- Campus Supplemental Data
- Campus IdM System / Process
- Person Registry
- Discovery Service
- Hosted Identity Provider
- Reverse Proxy
- Attribute Authority

System-Hosted IdP

- Campus SIS
- Campus Supplemental Data
- Campus IdM System / Process
- Attributes
- Authentication

External Service Providers

HRS

Employee Data

Student Data

PKI Requests
Our Methodology

- Environment Scans
- Campus Surveys
- Design Sessions
- Membership expansion
- Campus consultations
Additional Improvements Needed

• Strong authentication
• Sensitive data policies
• Audit and deprovision
• Loosely affiliated populations
• Improve identity data quality
• Directory interop (AD and others)
• Integration governance
External Benchmarks

• US Higher Education
  – University of California System – UCTrust Federation
  – University of Texas System – UTFed
  – University of Nebraska System – NU Federation Project
  – Penn State - Central Person Registry
  – Indiana University – Common ID
  – University of North Carolina – Onyen (Common ID)
  – University of Minnesota – Common ID
  – MNSCU – StarID

• Internet2 - TIER
  – Sustainable Federation
  – IAM Infrastructure for HE
External Benchmarks

• Identity Federations Internationally
• Industry Trends
  – Greater support for federated / external authentication from key vendors
    • Azure AD Authentication Library (ADAL)
    • Greater adoption of open standards (SAML2, OAuth)
  – Other standards eroding in favor of cloud lock-in (XMPP federation, CalDav, etc)
  – Tremendous variability in vendor ability to integrate with external authentication / authorization
  – Organizations need a rich toolkit to provide integration to meet varied application needs and capabilities
Summary Findings

- Federation can achieve some of what’s asked, but there are limitations
- Federation will always be part of our strategy
- Common UW System Credential is the most straightforward way to meet most of CIOs’ request
- Value of a ‘common credential’ is greatly diminished at < 100% adoption
- There are things we can do now to improve interoperability

- Metcalfe’s Law:
## Risk / Benefit Matrix

<table>
<thead>
<tr>
<th>Alternative</th>
<th>Benefits</th>
<th>Risks / Complications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Federation between campuses</td>
<td>- Much infrastructure exists today</td>
<td>- Service Provider Complexity</td>
</tr>
<tr>
<td></td>
<td>- Required for federation with external partners</td>
<td>- Application compatibility</td>
</tr>
<tr>
<td></td>
<td>- Preserves independent campus infrastructure / direction</td>
<td>- Some 3\textsuperscript{rd} party integration scenarios not possible</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Alternative</th>
<th>Benefits</th>
<th>Risks / Complications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common UW System Credential</td>
<td>• Increased application compatibility (system-wide apps)</td>
<td>• Major infrastructure change</td>
</tr>
<tr>
<td></td>
<td>• Less service provider complexity</td>
<td>• Major business process change – not just for IT</td>
</tr>
<tr>
<td></td>
<td>• Pushes common infrastructure direction</td>
<td>• Tight coupling between campuses</td>
</tr>
<tr>
<td></td>
<td>• Pushes common business process definition</td>
<td>• Implies closer coordination for other systems</td>
</tr>
<tr>
<td></td>
<td>• Increased mobility between campuses</td>
<td>• Implies standardization or centralization of other business processes (SIS)</td>
</tr>
<tr>
<td></td>
<td>• Increased collaboration opportunities between campuses</td>
<td>• Possible restrictions with individual campus software implementations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• InCommon certification complications</td>
</tr>
</tbody>
</table>
Graphic Roadmap

YEAR 1
- Component Integration
- Two Factor Auth
- Internet2
- TIER
- UW System

YEAR 2
- Campus Management UI
- Self-service credentialing
- Person Registry
- TIER Provisioning
- Directory Interop (AD and others)
- MFA for Pilot Campuses
- Extend IdP Hosting to Support Local Apps
- Metadata Governance
- Standard Attribute Release Policy
- Master Data Management (MDM) Pilot
- Establish Identity Integration Center Of Excellence (CoE)
- Promote CommIT / External ID

YEAR 3
- Research Connector
- Provisioning Service Pilot
- MFA for All Campuses
- Provisionsing Service Deploy
- Standard Attribute Release Policy
- Master Data Management (MDM) Deployment
- Pilot external / self-service creds

YEAR 4
- Decision Point
- Common UW System Credential?
- External / Self-Managed ID
Current Status

• Definition / early stages of Y1 – Y2 Strategic Projects
  – Multi-Factor for Pilot Campuses
  – Directory Interoperability
  – Exploration of IdP Hosting Options
  – Enhancing Person Data Delivery (PICH and others)
  – Integration Standards / Guidelines for Applications
  – Metadata / App Onboarding Technical Governance / Operations

• Foundational work with I2 TIER Initiative
  – Integration architecture through CIFER / TIER API
Questions?

• For additional information:

  Tom Jordan, IAM-TAG Chair

  tom.jordan@wisc.edu