Case Study – Identity Management at Texas A&M University

Susan Neitsch
Lead Software Applications Developer, Texas A&M University
The Problem: delivering a centralized email service

• Climate
  – Late 1990s
  – Students didn’t have accounts
  – Employees had accounts but the group managing those accounts did not want to be involved in managing student accounts

• Our answer
  – Create and manage separate email login account
The Next Problem: World Wide Web

• Climate
  – WWW gaining popularity
  – Campus entities wanting to start delivering web-based services
  – We managed a giant credential store with both employee and student accounts

• Our Answer
  – Leverage email login accounts for accessing web apps
  – Rebrand account the ‘NetID’
Texas A&M IdM Infrastructure ~ 2002

- RAs
  - Employee system
  - Student system
  - ROTC
  - Assoc Former Students
  - A&M Foundation
  - 12th Man Foundation
  - USDA-ARS facility
  - Visiting scholars

- IdMS/Attribute Service (OpenLDAP)

- Verifier (CAS)

- Credential Store (Kerberos)

- Campus web apps
The Next Problem: Communicating with groups

- Climate
  - 2004 - 2005
  - Campus entities wanted to communicate with their students and employees via email

- Our answer
  - Utilize mailing lists that would dynamically build email recipients at message distribution to eliminate manual list subscriber maintenance
Texas A&M IdM Infrastructure ~ 2005

- RAs
  - Employee system
  - Student system
  - ROTC
  - Assoc Former Students
  - A&M Foundation
  - 12th Man Foundation
  - USDA-ARS facility
  - Visiting scholars

- IdMS/Attribute Service (OpenLDAP)
- RDBMS
- Verifier (CAS)
- Credential Store (Kerberos)

Data to campus entities via feeds/SQL/LDAP binds

Campus web apps
The Next Problem: support federated authN

- Climate
  - 2005 - 2006
  - InCommon Federation existed
  - Shibboleth 1.3 released
  - Statistics department wanting to use WebAssign

- Our answer
  - Join InCommon Federation
Texas A&M IdM Infrastructure ~ 2007

- **IdP** (Shibboleth)
- **IdMS/Attribute Service** (OpenLDAP)
- **RDBMS**
- **Verifier (CAS)**
- **Credential Store (Kerberos)**

**RAs**
- Employee system
- Student system
- ROTC
- Assoc Former Students
- A&M Foundation
- 12th Man Foundation
- USDA-ARS facility
- Visiting scholars

**Data to campus entities via feeds/SQL/LDAP binds**

- **Service Providers**
- **Campus web apps**

**Service Providers**

**Campus web apps**
The Next Problem: address growing pains

• Climate
  – 2009 - 2010
  – Perl script fragile, need something more robust and flexible
  – Improve data stewardship
  – Simplify access management

• Our answer
  – Move to a two directory (Enterprise and White Pages) system
  – Adopt Python as our coding language
  – Set up web services
  – Set up a true Identity Management System/Person Registry
Texas A&M’s Identity Management System

System of Record/Registration Authority

IdMS NetID account/credential management applications
customer-facing tools
administrative tools

credential lifecycle event management

account lifecycle event management

IdMS Subject database (mergedPerson)

Credential Store

Attribute Service(s)

<table>
<thead>
<tr>
<th>id</th>
<th>uin</th>
<th>feed</th>
<th>attribute</th>
<th>last_updated</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>66720131</td>
<td>301008264</td>
<td>lifecycle</td>
<td>confirmedEnrolledSemester</td>
<td>2011-07-27 17:16:51</td>
<td>200411 IT Infrastructure &amp; Operation</td>
</tr>
<tr>
<td>99983535</td>
<td>301008264</td>
<td>bpp-employee</td>
<td>deptName</td>
<td>2013-01-31 01:11:33</td>
<td>employee</td>
</tr>
<tr>
<td>19937272</td>
<td>301008264</td>
<td>derived</td>
<td>eduPersonAffiliation</td>
<td>2009-12-19 01:38:59</td>
<td>member</td>
</tr>
<tr>
<td>19937280</td>
<td>301008264</td>
<td>derived</td>
<td>eduPersonAffiliation</td>
<td>2009-12-19 01:39:00</td>
<td>member</td>
</tr>
<tr>
<td>19937282</td>
<td>301008264</td>
<td>derived</td>
<td>eduPersonAffiliation</td>
<td>2009-12-19 01:39:00</td>
<td>staff</td>
</tr>
<tr>
<td>53959690</td>
<td>301008264</td>
<td>derived</td>
<td>eduPersonPrincipalName</td>
<td>2013-05-17 15:07:33</td>
<td><a href="mailto:sneitsch@samu.edu">sneitsch@samu.edu</a></td>
</tr>
<tr>
<td>22088714</td>
<td>301008264</td>
<td>bpp-employee</td>
<td>firstName</td>
<td>2010-07-05 16:06:20</td>
<td>Susan</td>
</tr>
<tr>
<td>22088829</td>
<td>301008264</td>
<td>bpp-employee</td>
<td>lastName</td>
<td>2010-03-18 13:04:39</td>
<td>Neitsch</td>
</tr>
<tr>
<td>38270549</td>
<td>301008264</td>
<td>bpp-employee</td>
<td>middleName</td>
<td>2010-07-21 15:06:40</td>
<td>L</td>
</tr>
<tr>
<td>17512922</td>
<td>301008264</td>
<td>derived</td>
<td>tamuEduPersonAffiliation</td>
<td>2009-12-09 13:49:33</td>
<td>employee:staff:active</td>
</tr>
<tr>
<td>74101708</td>
<td>301008264</td>
<td>derived</td>
<td>tamuEduPersonAffiliation</td>
<td>2011-11-09 10:17:34</td>
<td>affiliate:formerstudent</td>
</tr>
<tr>
<td>26500433</td>
<td>301008264</td>
<td>ldap</td>
<td>tamuEduPersonNetID</td>
<td>2013-05-17 15:07:33</td>
<td>sneitsch</td>
</tr>
<tr>
<td>24535585</td>
<td>301008264</td>
<td>bpp-employee</td>
<td>title</td>
<td>2010-03-18 13:04:38</td>
<td>Lead Software Applications Developer</td>
</tr>
</tbody>
</table>

2014 TECHNOLOGY exchange
Texas A&M IdM Infrastructure ~ 2011

Service Providers

IdP (Shibboleth)

Attribute Services (OpenLDAP, web services, AD DS)

Verifier (CAS)

Credential Store (Kerberos)

Data to campus entities via feeds/web services

RAs
Employee system
Student system
ROTC
Assoc Former Students
A&M Foundation
12th Man Foundation
USDA-ARS facility
Visiting scholars

IdMS (the merge)
The Next Problem: improve customer support

• Climate
  – 2011 - today
  – Organizational change: outsourcing, restructuring
  – Shared services initiative/Wide-spread adoption of cloud services
  – Increasing regulatory requirements
  – Departmental use of NetID accounts increasing

• Our answer
  – Create Identity Management Office
Current Problems

• Climate
  – The (Near) Future
  – Higher assurance accounts for researchers

• Our answer
  – Pursuing InCommon Bronze and Silver certification
In Summary – Texas A&M’s IdM Philosophy

An organization engages in Identity Management to solve a problem. No one ‘does’ Identity Management just for the sake of Identity Management.

If you are interested in getting into Identity Management . . .

. . . . find a really unpleasant problem and make that your project.
Case Study – Identity Management at Texas A&M University

Susan Neitsch
Lead Software Applications Developer, Texas A&M University