Executive Summary

• Much of the current auth_n, auth_z, provisioning, identity management and directory infrastructure will be replaced or upgraded over a two-year period
• Several pieces of the SUN One platform will be licensed
• LDAP will play a key role, including white pages (replacing Ph)
• Many policy and governance rules need to be worked out…
Is This…

• Necessary? Yes, to standardize, reduce costs and ease maintenance.
• Innovative? No, is a proven approach in higher-ed, commerce and government.
• Only technical? No, it has significant governance and data administration facets.
LDAP Components

• Enterprise-level community directory based on authoritative identity management
• White pages services (Ph replacement)
• Authentication (auth_n)
• Authorization (auth_z)
• Attribute housing
Information Technology

LDAP Directory Structure

root

ou=people
- uid=tboard,
  cn="Board, Thomas E"

ou=organizations
- uid=biology,
  cn="Department…"

ou=services
- uid=hris
- uid=lookup

dc=northwestern, dc=edu
Information Technology

Information Flow

HR

Meta-directory & enterprise directory

Meta-directory & enterprise directory

SES

SSO Auth_n Auth_z

Active Directory forests

Application directory

Enterprise white pages

Web
<table>
<thead>
<tr>
<th>Attribute/Org.</th>
<th>CAESAR (Registrar)</th>
<th>HRIS (HR)</th>
<th>Lookup (NUIT)</th>
<th>Parking (B&amp;F)</th>
<th>MyXXX (School)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetID (NUIT)</td>
<td>✓ s</td>
<td>✓ s</td>
<td>✓ s</td>
<td>✓ s</td>
<td>✓ s</td>
</tr>
<tr>
<td>DisplayName (HR)</td>
<td>✓ s</td>
<td>✓ w, s</td>
<td>✓ s</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OfficeAddress (HR)</td>
<td>✓ w</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Emplid (HR)</td>
<td>✓ s</td>
<td>✓ w, s</td>
<td>✓ s</td>
<td>✓</td>
<td>✓ s</td>
</tr>
<tr>
<td>SchoolPhone (Registrar)</td>
<td>✓ w</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Information Technology

Browser

Web auth_n - now

Option 1

Proxy CGI

Web Server

Application

Option 2

Web Server

Application
Information Technology

Identity Sources
- End Users
- Administrators

Connectors
- Web

Identity Management Business Rules

Oracle Meta-Directory Database

Provisioning
- Directory Management
- LDAP Directory
- SSO

Non-NetID
- Email
- Servers
- AD
- NT4
- Kerberos
- Portal
- SES/Bb
- Radius
- Web Svc
- Auth_n
- Auth_z
- Attrs
- White Pages
- SES/Bb
- Radius
- Web Svc
- Auth_n
- Auth_z
- Attrs
- White Pages
Information Technology

Oracle Meta-Directory Database

Identity Management Business Rules

Provisioning & Directory Management

Identity Sources
End Users
Administrators

Connectors
Web
Non-NetID

LDAP Directory

Email
Servers
AD

Federated
Portal
SES/Bb
Radius
Web Svc
Auth_n
Auth_z
Attribs
White Pages
## Implementation Timeline

<table>
<thead>
<tr>
<th>2003</th>
<th>2004</th>
<th>2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
</tr>
<tr>
<td>FY2003</td>
<td>FY2004</td>
<td>FY2005</td>
</tr>
</tbody>
</table>

- Deploy dual central LDAP directories
- Deploy LDAP mirror on directory.northwestern.edu
- IdM deployment
- SSO deployment
- Federated authentication deployment
- LDAP becomes primary white pages service
- Ph retirement
- Email delivery to nwu.edu domain retired
- End NT4 password synchronization
- Kerberos retirement
- Change directory.northwestern.edu mirror to real-time update
- Mail routing conversion to LDAP
- Develop LDAP white pages management
- LDAP becomes primary white pages service
- Ph retirement
- Email delivery to nwu.edu domain retired
Questions & Contact Info

• Phil Tracy <ptracy@northwestern.edu>
• Albert Steiner <a-steiner@northwestern.edu>
• Xiaoxia Dong <x-dong@northwestern.edu>