Identity and Security Management at Duke University

Session ID: T-1
About Duke University

- University and Health System
- 14,950 undergraduate and graduate students
- 36,000 employees
- $5.4 billion operating budget
- Three hospitals in Durham and Raleigh
- Clinics in North Carolina and Virginia
Identity Management Challenges

- Variety of identity types
- Numerous systems/services
- Multiple physical locations
- Decentralized management
# Identity Management Challenges

## Identity types and provisioned services - examples

<table>
<thead>
<tr>
<th>Employees</th>
<th>Campers</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Students</td>
<td>Temporary staff</td>
<td>Email groups</td>
</tr>
<tr>
<td>Patients</td>
<td>Visiting professors</td>
<td>Class rosters</td>
</tr>
<tr>
<td>Contractors</td>
<td>Weekend MBA's</td>
<td>Class materials</td>
</tr>
<tr>
<td>Affiliates</td>
<td>Corporate education</td>
<td>Computing resources</td>
</tr>
<tr>
<td>Alumni</td>
<td></td>
<td>Network</td>
</tr>
<tr>
<td>Donors</td>
<td></td>
<td>Filesystems</td>
</tr>
<tr>
<td>Volunteers</td>
<td>Temporary staff</td>
<td>Applications</td>
</tr>
<tr>
<td>Media</td>
<td></td>
<td>Streaming media</td>
</tr>
<tr>
<td>Visitors</td>
<td></td>
<td>Building access</td>
</tr>
<tr>
<td>Parents</td>
<td></td>
<td>Room access</td>
</tr>
<tr>
<td>Doctors</td>
<td></td>
<td>Sporting events</td>
</tr>
<tr>
<td>Residents</td>
<td></td>
<td>Other special events</td>
</tr>
</tbody>
</table>
Identity Management Challenges

Campuses, hospitals and clinics in North Carolina and Virginia
Identity Management Challenges

Decentralized management

Two separate central IT departments, University and Health System

Many local IT departments in various schools, departments, etc.
IDM System Components

- Oracle IDM 9.1
- MIT Kerberos5 12.2
- Shibboleth 3.1.2
- Duke Unique ID
- Microsoft Active Directory 2008r2/2012r2
- Grouper 2.1.5
- SUN LDAP 6.3 (changing to 389 DS)
IDMS Architecture

Authoritative Sources

Oracle IDM

Kerberos /SHIB
Duke UniqueID
Active Directory
Grouper
LDAP

Authentication

Provisioned Systems, Services

Duke UNIVERSITY
OFFICE OF INFORMATION TECHNOLOGY
Administrative Systems Challenges

- Large number of users
- High turnover
- Complex authorization requirements
- Multiple applications
- Need a single point of entry for maintenance
Administrative Systems Components

- SAP ECC 6.0
- SAP BW 7.3 & BI Java
- SAP Enterprise Portal
- SAP BO Enterprise
- SAP CRM 7.0
- SAP SRM 7.0
- SAP PI 7.0
- Kofax (scanning, fax)
- Mobius (content repository)
- IBM Brass Ring (candidate selection)
- ECRT (effort certification)
- API (Time & Attendance)
Administrative Systems / IDMS Architecture
Hire Process Overview

- Position requisition created/approved in MSS
- Open position posted in Candidate Selection
- Candidate selected, data transferred to MSS hire form
- Identity created/verified
- Hire approved, personnel record created
- Identity updated with organizational attributes
- Administrative systems accounts provisioned
- Roles updated in administrative systems
Requisition to Hire

**ECC/EP MSS**
- Create Requisition
- Approve?
- Hire Form
- Approve

**Candidate Selection**
- Open Requisition
- Select Candidate

**IDMS**
- Create/verify Duke UniqueID
- Create “Affiliate” entry in LDAP
Hire into Position

<table>
<thead>
<tr>
<th>ECC/EP MSS</th>
<th>IDMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approve</td>
<td>Update LDAP with org attributes for perrr</td>
</tr>
<tr>
<td>Create Personnel Record (P-S-O-O exists)</td>
<td>NetID created in KRB5, LDAP updated</td>
</tr>
<tr>
<td>Web Service</td>
<td>OIM retrieves org attributes from ECC (P-S-O-O)</td>
</tr>
<tr>
<td>Update InfoType 0105</td>
<td>Grouper, Active Directory updated</td>
</tr>
</tbody>
</table>
Administrative Systems Role Update

| ECC | Evaluate Org Structure (RHPROFLO) | Update ECC users/roles | Evaluate Users/Roles | BI | Update BI users/roles | CRM | Update CRM users/roles | SRM | Update SRM users/roles | Other | Update EP users/groups | Update BI Java users/groups | Update ECRT users/roles | Update Brass Ring users/roles |
IDMS is continuously updated with ECC organizational data.

Roles, services, applications, access, etc. move as a person changes positions or leaves the organization.

ESS, MSS applications change data that propagates through the Administrative, IDMS systems.

- MSS: Name, Campus address, faculty appointments, titles, job transfers
- ESS: Home address, telephone, etc.

Active Directory information synchronized with Health System AD for separate purposes (HIPAA, clinical applications, etc.).

IDMS-initiated changes are replicated in Administrative Systems.

- Email aliases
Key development objects

- Copied and modified RHPROFL0 to update roles in all ABAP systems based on naming convention and position/user assignment
- Built a portal component to perform UME actions. (see http://www.sdn.sap.com/irj/scn/weblogs?blog=/pub/wlg/3052)
- ABAP program to build portal user/group assignments and call UME component above
- ABAP program to extract role data and transmit xml update files to ECRT, Brass Ring
- ABAP call to stored procedure in Duke UniqueID database to verify/create external pernr
- Extract of people and organizational master data for daily interface to IDMS
- Import of daily IDMS data into ECC
- Web service called by OIM for organizational hierarchy information
- Custom webdynpro application for ongoing departmental maintenance
Questions?