Identity and Access Management
PI-2 Demo

March 10, 2015
Tuesday
11:00a.m.-12:00 p.m.
Lamont Forum Room
Agenda

• Meeting Purpose and Intended Outcomes (5 min)
• PI-2 Business Objectives (5 min)
• Demo: Alumni Imported from Advance to Identity Registry (5 min)
• Demo: Alumni Registration Using HarvardKey Application (10 min)
• Demo: Alumni Authentication to Manage HarvardKey (10 min)
• Summary and Close
Demonstration: Program Increment Accomplishments

Purpose
To provide the team and invited guests a summary and demonstration of key work accomplished during our second Program Planning Increment (PI-2).

Intended Outcomes

• Share our work in PI-2 and provide a forum for stakeholder feedback
• Continue to build an understanding of the IAM program
# PI-2 Business Objectives

Teams accomplished the following objectives:

<table>
<thead>
<tr>
<th>Objective</th>
<th>Demonstration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement data migration method for Alumni data</td>
<td>• Import Alumni data into Identity Registry (IdDB) using Identity API</td>
</tr>
<tr>
<td>Allow migrated Alumni users to claim and manage their HarvardKey credentials</td>
<td>• Self-service alumni registration for a new HarvardKey</td>
</tr>
<tr>
<td></td>
<td>• Provision an account and password to credential repository (H-LDAP)</td>
</tr>
<tr>
<td>Support Alumni authentication using HarvardKey</td>
<td>• Authenticate Alumni user via HarvardKey</td>
</tr>
</tbody>
</table>
## PI-2 Business Objectives

### Teams accomplished the following objectives:

<table>
<thead>
<tr>
<th>Objective</th>
<th>Accomplishment</th>
</tr>
</thead>
</table>
| Replace FAS account management and provisioning so that we can decommission Oracle Waveset | Self-service …  
• Password change  
• Password reset  
• Update password recovery email |
| Retire technical debt to speed future development | • PIN/CAS to the cloud |
## PI-2 Business Objectives

### Teams also met these additional commitments:

<table>
<thead>
<tr>
<th>Objective</th>
<th>Accomplishment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade SHA algorithm to remain compliant with InCommon Bronze standards</td>
<td>• Upgrade to SHA-2 without any interruption to customer applications</td>
</tr>
<tr>
<td>Migrate off Oracle Access Manager (PIN3)</td>
<td>• Decommissioned servers in order to save $100K</td>
</tr>
<tr>
<td>Implement new Google API before new students onboard</td>
<td>• Deployed Waveset changes for new Google API design</td>
</tr>
<tr>
<td>Capture HMS functional and technical requirements to facilitate further planning of the School’s migration to SailPoint IIQ</td>
<td>• Extensive requirements-gathering work from Marlena Erdos</td>
</tr>
</tbody>
</table>
Refresher: Identity Registry is the Foundation

- Data are generated by source systems of record and fed to the Identity Database (IdDB), which is an identity registry.
- IdDB has a master data record of the Harvard user — a source of truth.
- SailPoint IdentityIQ (IIQ) aggregates source data on a continuous basis.
- Based on eligibility rules determined by the service owner, the provisioning system automatically activates and deactivates individual users and their entitlements.
- This streamlines onboarding — and, even more importantly, turns off access when a person separates from Harvard or otherwise loses eligibility.

The right access, for the right people, in a timely manner.
Various Alumni Populations Comprise the User Base

Associate Members

Students and Degree Recipients

Executive Education Programs

More than 380,000 Alumni
Alumni data are managed in HAA’s Advance database

Alumni data will be fed to the identity registry (IdDB) to enable Alumni to get a HarvardKey for login to Harvard resources

New API-based approach to implementing business rules for data creation in the IdDB identity registry will be employed for import of Alumni data (instead of batch XML imports)

- Only the data needed to manage access and support users will be transferred to the registry
- The transition from graduating student to Alumni should be seamless
- API enables a more near-real-time data transfer if required
Demo: Scripted Update from Advance to IdDB

Mike Thomas, HUIT/Administrative Systems
Recap: Scripted Update from Advance to IdDB

- Scripted submission allows control over submission rate and automates error thresholds
- Messages returned through API provide feedback on transactions
Next: Alumni Online Access Will Require HarvardKey

• Access to many Harvard resources is protected and requires login (authentication)

• The current vendor-based solution for issuing Alumni credentials is being sunsetted, and Harvard is building all the components needed to bring this process “in house”

• As part of this major transition, we need to register Alumni again so they can set secure passwords and provide information to support self-service password management

• The new HarvardKey self-service application will support Alumni registration
Demo: Alumni Registration for HarvardKey

Joe Hardin, HUIT/IAM Team
We saw:

• New self-service registration process for Alumni to claim HarvardKey credentials

Benefits:

• In the future, students with a HarvardKey will no longer need to re-register as Alumni

• No more confusing security questions for Alumni – simple password reset over email
Recap: Registering for an Alumni Account

HARVARD UNIVERSITY

Alumni Identity Information

Please enter your personal information so we can verify you in our system.

- HAA ID
- Last Name
- First Name
- Year of Graduation

Clear Submit

HARVARD UNIVERSITY

Create Login Name

Please enter your desired login name. The login name you entered should be in an email address like format.

Login Name: example1@example.com

Clear Submit
Recap: Login Name Provisioned by IIQ

We saw:

• Login name assigned by or entered with HarvardKey application
  – IIQ automatically provisions the password to back-end systems
    (Harvard LDAP in the case of HarvardKey)

Benefits:

• Best of both worlds — a customer-facing user interface integrated
  with a powerful provisioning solution
Recap: IIQ Updated Based on Alumni Registration

![IIQ Updated Based on Alumni Registration Image]

---

**View Identity iamalumsixfn iamalumsix**

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Entitlements</th>
<th>Application Accounts</th>
<th>Policy</th>
<th>History</th>
<th>Risk</th>
<th>Activity</th>
<th>User Rights</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Name</td>
<td><a href="mailto:test.account@mail.com">test.account@mail.com</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AD ID</td>
<td>ia431</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Name</td>
<td>iamalumsixfn iamalumsix</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAS User Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Name Prefix</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Name First</td>
<td>iamalumsixfn</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Name Middle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Name Last</td>
<td>iamalumsix</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Name Suffix</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Official Name</td>
<td>iamalumsixfn iamalumsix</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Birth Date</td>
<td>02/26/1990 00:00 AM EDT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOB Month</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOB Day</td>
<td>29</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOB Year</td>
<td>1990</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claim Status</td>
<td>CLAIMED</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Primary Email</td>
<td><a href="mailto:iamalumv.test@gmail.com">iamalumv.test@gmail.com</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Alternate Email</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Primary Phone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Alternate Phone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Recap: H-LDAP Updated with New Password

- mail: test-account@mail.com
- userPassword: SSHA512 hashed password
- harvardEduClaimStatus: CLAIMED (2015-03-09T14:00:50.642 EDT)
Next: HarvardKey - A Better Self-Service Experience

The HAA Helpdesk fields thousands of calls a year for forgotten user names and passwords.

The HarvardKey application supports self-service for these routine interactions:

- I want to update my recovery email or phone number
- I need to change my password
- I have forgotten my login name
- I have forgotten my password and need to reset it
Demo: Login to Manage HarvardKey

Joe Hardin, HUIT/IAM Team
Recap: Alumni Managing HarvardKey (Self-Service)

We saw:

• Logging into HarvardKey application to manage a HarvardKey
  – Authentication with HarvardKey integrated with PIN/CAS

Benefits:

• Self-service that doesn’t rely on security questions or defunct Harvard email addresses
Recap: Alumni One Option in HarvardKey App
Recap: Entering an Additional Recovery Email

In case you ever forget the user name and/or password, the information you provide will be used to recover your Harvard University account.

You must provide at least your primary email address for recovering your Harvard University account.

**EMAIL ACCOUNTS**

Primary: l****@gmail.com

Alternate: add_alternate@example.com
Recap: Viewing the Updates in IIQ and H-LDAP
Functionality Completed … Facelift Pending

• Team has completed the core functionality
• Isobar will be delivering a build kit to Harvard at end of March, which will enable us to align the look and feel of the application with Harvard standards
  – Responsive design (works with different formats/devices)
  – Familiar navigation
  – Level A accessible
  – Nicer looking!
Wrap-Up: Status of PI-2 Business Objectives

Today’s demonstrations illustrated the following objectives:

• Data migration method for Alumni data being used by HAA
• Alumni registration process
• Authentication with HarvardKey using PIN/CAS
• Self-service HarvardKey features
Other Accomplishments During PI-2

Cloud:
• New Harvard LDAP (H-LDAP) deployed to the cloud
• PIN/CAS migrated to the cloud, ready for testing during PI-3

Platform Investment:
• Database rationalization project
• PIN3 decommissioned
• SHA2 upgrades
• Upgrade for Google API

Preparing for Future Development:
• Sponsored Account requirements analysis
• HMS system and requirements analysis
Discussion

Questions? Feedback?
Thank you!