Identity & Access Management: Changes Are Coming!

April 13, 2015

FAS IT Stakeholders Meeting

Lamont Forum Room
Agenda

• HarvardKey
  – Benefits
  – Rollout Calendar
  – UI Preview
  – Onboarding Workflow

• Person-of-Interest (POI) Affiliations
  – Sponsored Affiliations and Sponsored POI Roles
  – POI Role Types
HarvardKey Benefits

HarvardKey is a step forward because:

• Unified credential enabling access to email, desktop, and Web resources

• More people will have it
  – Alumni
  – FAS
  – Most other schools over the next year

• User experience is significantly superior to PIN

• System is much more nimble for authentication and authorization

• Includes better levels of assurance (identity-proofing)

• Easier onboarding (and offboarding)
We are poised for an initial rollout in September in waves by user population, not application.

- Within 18 months, every Harvard Community user (except HBS) will be prompted to onboard.
- Design and branding changes will be applied in two stages:
  - Nov. 2015: New Account Management functions and core HarvardKey branding
  - 6 months after final user population added: Implement lessons learned, remove redundant login types
UI Preview: Welcome

Note:
These sample designs do not contain final language.
UI Preview: Passphrase
Onboarding Workflow

1. Dr. Pat Patrick accepts an offer for an assistant professorship. Pat’s start date is Sept. 1.

2. Pat’s department admin sponsors an account for Pat — even though it’s only April. This includes details like birthdate, personal email, start/end dates, and affiliation type.

3. An identity for Pat — including a HUID — is created in the Harvard Identity Registry (IdDB).

4. HR sends Pat an email with an invitation to claim a new Harvard account.

5. Pat claims an account using name, date of birth, and the code from the email. Then, Pat chooses a username from a list of options, sets a strong password, and adds a recovery email in case a password reset is ever necessary.

6. Account Management flips Pat’s status in SailPoint iIQ to “Claimed.”

7. Accounts are provisioned for Pat in the appropriate targets for an Incoming Faculty role — in this case, HarvardKey LDAP, University AD, 0365, FAS AD, FAS LDAP, Kerberos, and Google.

8. By August, HR job data for Pat is fully complete in PeopleSoft, and PeopleSoft submits this data to IdDB.

9. A future-effective dated employee role update results in some provisioning to downstream systems.

10. On Sept. 1, when Pat’s Incoming Employee role ends and the Employee role starts, additional attributes are updated in LDAP — Pat’s data have “aged,” and the passage of time automatically results in additional provisioning.

11. Pat comes to campus to start the new appointment! Pat already has access to all the apps and services needed for day-to-day life at Harvard — including the Athletic Office site, where Pat buys a pool sticker for a workout after a great first day on the job.
Person-of-Interest (POI) Affiliation

The POI category includes all affiliations which are *not* classified as student, faculty, staff, library borrower or alumni.

- Has the most variation of uses
- Potential for misunderstanding and misuse
- Important to understand the reason, know the person, and control their access
- Most POIs require a sponsor
- Implemented and managed through HUIT’s MIDAS system
Sponsored Affiliations = Sponsored POI Roles

Sponsored affiliations allow Harvard faculty and staff to give individuals outside of their School or organization — or outside of Harvard itself — temporary access to resources.

- Sponsored affiliations are implemented via POI roles that require a Harvard sponsor (“sponsored POI roles”)
- Sponsors may be held accountable for how resources are used
- Sponsors may delegate administration of the sponsorship to a Sponsor Admin
- Sponsored POI roles must be renewed on a periodic basis
- If the person being sponsored doesn’t already exist in the identity registry, the system will create an identity record for them — this requires a minimum of first name, last name, and date of birth
Affiliations = Roles

Roles are the means within the HUIT identity registry of defining an individual’s affiliation(s) with Harvard.

- Included as part of a person’s HarvardKey
- A person may have multiple roles (e.g. student and employee)
- Role *types* are generic (e.g. student), but a person’s instance of a particular role also relates to a specific School or organization (e.g. FAS Student)
- Roles control access to a School or organization’s resources
# POI Role Types

<table>
<thead>
<tr>
<th>Current</th>
<th>Proposed Additional</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sponsored Affiliations</strong></td>
<td><strong>Sponsored Affiliations</strong></td>
</tr>
<tr>
<td>- Consultant</td>
<td>- Incoming Employee/Transfer</td>
</tr>
<tr>
<td>- Contractor</td>
<td>- Collaborator</td>
</tr>
<tr>
<td>- Vendor</td>
<td>- Inter-school Affiliated</td>
</tr>
<tr>
<td>- Security</td>
<td>- Short-Term Visitor or Guest</td>
</tr>
<tr>
<td>- Family Member</td>
<td>- Volunteer</td>
</tr>
<tr>
<td>- Tenant</td>
<td>- Hospital Employee</td>
</tr>
<tr>
<td>- Smithsonian Employee</td>
<td>- Field Education Supervisor</td>
</tr>
<tr>
<td>- Harvard Management Co. Employee</td>
<td>- Academic Advisor</td>
</tr>
<tr>
<td>- Other</td>
<td></td>
</tr>
<tr>
<td><strong>Non-sponsored Affiliations</strong></td>
<td></td>
</tr>
<tr>
<td>- Overseer</td>
<td></td>
</tr>
<tr>
<td>- Retiree</td>
<td></td>
</tr>
<tr>
<td>- Spouse of Deceased Retiree</td>
<td></td>
</tr>
<tr>
<td>- Retired Hospital Affiliate</td>
<td></td>
</tr>
<tr>
<td>- Spouse of Deceased Hospital Affiliate</td>
<td></td>
</tr>
</tbody>
</table>
Any questions?
Thank you!
## Vocabulary Quiz

Do you know the difference between the key terms below?

<table>
<thead>
<tr>
<th>Term</th>
<th>How Used</th>
<th>Examples</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Login name            | Used as the login ID  
Expected to be the Harvard email address, can be another for Alumni or sponsored accounts | Email-eligible user: jay_hill@sph.harvard.edu  
Sponsored collaborator: jayhill@stanford.edu  
Alumnus/alumna: coolguyjay@comcast.net | When a user logs in using HarvardKey, the system will expect the user to enter this login name and its related password |
| User ID               | System-assigned identifier  
Harvard-assigned email | Sam Account: ADID = jeh454  
UNIX LDAP: UID = jeh454 | Permanently assigned value enables prestaging                                                     |
| Harvard email address | Harvard-assigned email  
username@optionalsubdomain.harvard.edu |                                                                                                   | Users chooses value on left of @ sign as part of self-service account claim & onboarding process |
| FAS name              | Legacy username for FAS person  
jayhill |                                                                                                   | Former names will exist as mapped attributes                                                   |
| Google name           | Google username  
jayhill@g.harvard.edu (always scoped) |                                                                                                   | Since Google accounts can’t be changed without content loss, some will keep accessing via old names |
| {School} name         | Local username(s)  
[we want to accommodate values when necessary] |                                                                                                   | Local usernames are mapped to identity as additional attributes                              |