HR Deans & Directors Meeting: IAM Update

July 14, 2015  Tuesday  2:00-2:30 p.m.  Mass Hall, Perkins Room
Agenda

• HarvardKey
  – The Benefits
  – Rollout Timeline
  – A Sneak Peek

• POI Sponsored Affiliations
  – Enhanced Functions
  – Onboarding Example

• Multifactor Authentication
  – How Does MFA Work?
  – The Components
  – Integration Strategies
HarvardKey: The Benefits

HarvardKey is a unifying credential that can enable access to email, desktop, and Web resources with a *single* login name and password.

- Successor to Harvard’s current PIN System
- New, mobile-responsive user experience for the login screen and account management suite (looks great on tablets, too!)
- Authentication and authorization are much more nimble
- Supports optional multifactor authentication
- Easier onboarding and off-boarding
- Supports the HUIT goal of “*One Identity for Life*” for any person — regardless of role — including seamless support for changes between roles, schools, etc.
Rollout Timeline

You’ll see changes to the old PIN login screen beginning in September, with waves of user populations invited to activate a HarvardKey soon after.

• September 22: New HarvardKey self-service account management functions available to all Alumni users
• October 6: HarvardKey available to FAS and Central users in conjunction with Harvard’s IT Security Campaign
• Within 18 months, every Harvard Community user will be invited to onboard
Rollout Timeline

As we rebrand, all screens that currently contain PIN branding will be converted to HarvardKey.

- Alumni (Post.Harvard) credential goes away (this includes all active students)
- In October, for FAS and CADM+:
  - New Harvard users will claim a HarvardKey during onboarding
  - All password reset requests will go through HarvardKey
  - Existing users may claim a HarvardKey if they wish
  - Harvard Phone users will require HarvardKey
  - One-year cycle for CADM+, since those users will need to reset password on anniversary

- Rollout will be coordinated with Security Campaign to reinforce strong-password requirement (including reminder that strong passwords don’t need to be periodically reset) and ensure that users will recognize the “claim your HarvardKey” email

- No changes to applications anticipated
A Sneak Peek
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
Onboarding Workflow

1. Dr. Pat Patricks 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 I1Q to “Claimed.”

7. Accounts are provisioned for Pat in the appropriate targets for an Incoming Faculty role — in this case, HarvardKey LDAP, University AD, G365, 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.
### POI Role Types

<table>
<thead>
<tr>
<th>Current</th>
<th>Proposed Additional</th>
</tr>
</thead>
</table>
| **Sponsored Affiliations**  
  - Consultant  
  - Contractor  
  - Vendor  
  - Security  
  - Family Member  
  - Tenant  
  - Smithsonian Employee  
  - Harvard Management Co. Employee  
  - Other | **Sponsored Affiliations**  
  - Incoming Employee/Transfer  
  - Collaborator  
  - Inter-school Affiliated  
  - Short-Term Visitor or Guest  
  - Volunteer  
  - Hospital Employee  
  - Field Education Supervisor  
  - Academic Advisor |
| **Non-sponsored Affiliations**  
  - Overseer  
  - Retiree  
  - Spouse of Deceased Retiree  
  - Retired Hospital Affiliate  
  - Spouse of Deceased Hospital Affiliate |
Multifactor Authentication

Multifactor authentication (MFA) is an authentication method that requires the user’s identity to be verified by more than one of these independent factors:

- Something you **know** (such as a password)
- Something you **have** (such as a physical security token or a response to a smartphone app ‘push notification’ )
- Something you **are** (such as a fingerprint)

For multifactor authentication, we will use the user’s smartphone as the second factor in addition to standard login name/password authentication. (Users without smartphones will have other phone-based options.)

1. User enables MFA in the HarvardKey self-service admin portal
2. User downloads the app to his/her smartphone
3. After logging in to a requested service, user must acknowledge the push notification on his/her phone and is then granted access as normal
Multifactor Authentication Integration Strategies

An application requires the use of MFA for all users:
• Application registration with HarvardKey will be extended to support this option

User prefers to use MFA on all his/her access points:
• Users can use HarvardKey’s self-service functionality to set this preference for themselves

Application requires MFA for some users (e.g. admin users):
• Grouper, IAM’s group management tool, will be used to support this requirement (*rollout anticipated in 2015*)
Questions?
Thank you!