HARVARD UNIVERSITY
Information Technology

Identity & Access Management

IAM Lifecycle Committee

Feb. 29, 2016	Monday	10:00-11:30 a.m.	561 Smith Center

Agenda

- Introductions
- Meeting Purposes and Intended Outcomes
- Status Update
- Discussion: SSN Remediation Plans
- Discussion: HarvardKey Process Challenges
    - IAM Summit
- Update: Special Library Borrowers (Steven, Terry)

Meeting Purpose and Intended Outcomes

Purpose

Bring the group up to date, and kick-off the group for 2016

Intended Outcomes

- Answer questions about status of HarvardKey
- Get input from the group on policy regarding SSNs and the Registry
- Discuss the challenges surrounding status transitions and HarvardKey that are arising
- Explain our intended approach with Library Borrowers
- Identify topics for our upcoming meetings

Current HarvardKey Status

Since go-live on Nov. 11, 2015 ...

72,000+ HarvardKeys claimed

Claim is a process step for O365, Harvard Phone, HAA, security remediation

5,600 HarvardKey service desk tickets opened

This means ...

- Graduating class of 2016 will not need to claim another identity
- Improved mobile experience and overall accessibility
- Alumni access to Library resources
- Duo multifactor authentication offers option for more secure login
- 100% Plan for security remediation underway
- Password resets implemented across identity lifecycle

HarvardKey Adoption Phases

PIN replacement: Replacement of enterprise web authentication

- Approximately 1,200 web applications

Standard business processes: Definition and use of central processes for students, faculty, staff, Alumni, and sponsored affiliates

- Onboarding
- Transitions (multi-role)
- Start and end dates, grace periods, deprovisioning

Onramp to O365 and Harvard Phone: Required login for new enterprise services such as Office 365, Enterprise SharePoint, and Harvard Phone

Application provisioning: Provisioning to School directories

- Same username and password at both University and Schools
- Active Directory, LDAP, web applications

SSN Remediation in Registry

SSN: OGC / Security Request

OGC has asked IAM to eliminate the SSN from the Registry. IT Security has recently issued a new policy, as well.

- Identity Registry (IAMDB) contains all the HUID holders (current and past)
- SSN has historically been collected and managed as follows:

Previously Approved HRCI (Current State)	Remediation Recommendation
IDGEN batch creation, web service, web applications (ID Assign, ID Resolve)	• ID generation and identity disambiguation can be accomplished with last 4 digits of SSN
MIDAS (see document) to confirm identity	• Same as above
Export data to qualified internal service providers (UHS) who have a valid business need	Options: • Provide SSN to UHS, then drop the data from IAMDB • Have HR and SIS feed UHS directly
Export data to core source systems of record of employee and student data to keep identity data in synch between core systems. (PeopleSoft, Central Term Bill System)	Not normally an identity registry function • HR and SIS interact directly already; can this be added to scope?

DISCUSSION

SSN Policy: (Proposed?) IT Security Policy

The goals of this policy are

- To restrict the use of SSN databases to specific legal or business requirements that cannot otherwise be met
- To enhance the security of SSN databases
- To encourage truncation or removal of SSNs when there is no longer an active need for full SSNs

Plans:

- Modify the database and tools
- Relatively complex series of remediation tasks that are mapped out for next few months for IAM team

SSN Remediation: Next Steps

Capture the discussion

HarvardKey Process Challenges

Recap HarvardKey Benefits

Phased adoption results in benefits in two key areas.

Improved user experience and security:

- Replace PIN credential with stronger password/multifactor authentication
- Account and password management during and after active affiliation
- Password consolidation between web and desktop, simplifying login
- Enhanced experience on mobile devices
- Provisioning logic that handles multiple roles and entitlement differences

We are here -->

Opportunities for process improvement for users, business, and IT

- Self-service onboarding with better fit to business needs
- Standard processes that streamline transitions
- User passwords aligned for most user logins
- Automated creation and removal of accounts and access
- Replacement of local identity stores and provisioning systems

Critical HarvardKey Challenges

HR Processes: Standardization

- Need: Reduce reliance on the POI workaround for HUID creation during onboarding
- Challenges: Can we provide improve process for users and HR professionals?

HR Processes: Multiple Roles

- Need: A defined methodology to support employees being multi-homed or moving from one School to another
- Challenges: HarvardKey requires one login name (email address) per user, but users can be affiliated with multiple Schools and get multiple emails

Managing Login Name (provisioning expansion, transitions between units)

- Need: A defined cross-University plan for managing login names across Schools and at the enterprise level
- Challenges:
  - Default login name for most apps will be email address, but some applications require a short name (8 characters or fewer)
  - Schools have local implementations that may not align
  - Login names must match O365 email addresses

IAM and CIOs from Schools Held an IAM Summit

In response to feedback from Schools, the IAM Summit meeting was held on 2/24/16

- CIO Council agreed to work with IAM to support solving some process challenges that were hindering adoption of HarvardKey
  - Objective: By working together, processes could be improved for users and administrators
- IAM Summit included representatives from the CIO area and technical staff responsible for Identity and Access Management

IAM Summit: Breakout Session Topics

HR Processes: Multiple Roles

- Need: A defined methodology to support employees being multi-homed or moving from one School to another
- Challenges: HarvardKey requires one login name (email address) per user

Login Name Creation and Update

- Need: A defined cross-University plan for managing login names across Schools and at the enterprise level
- Challenges:
  - Default login name for most apps will be email address, but some applications require a short name (8 characters or fewer)
  - Schools have local implementations that may not align
  - Login names must match O365 email addresses

IAM Summit: Challenges of Multiple Roles

Multiple-persona roles are prevalent in higher education

- Student employees; dual-degree or jointly appointed academics; parents who are also alumni and employees; etc.

Constraints:

- HarvardKey supports a single login name
- No accepted business rule for declaring one role primary over the others
- ExO/O365 design forces alignment of *userPrincipalName* with mailbox name

Challenges:

- Administrators who onboard newcomers have limited awareness of other roles or pre-existing access; they just want to follow a standard process
- Self-service is a goal, but can the process be designed to protect a user from confusion or worse?
- Transfers are complicated by policy differences between departments
  - Grace periods on email might suggest the former email account should remain for a time, but what are the ramifications?
  - Can such transitions actually be automated?

IAM Summit: Login Name

Provides shared login experience across the University:

- Provides a consistent password (paired with HarvardKey login name) for the majority of login experiences
- HarvardKey uses email address as an easy-to-remember login name
  - Becomes primary method for HarvardKey login
  - Can change over time due to internal transfers or changes in last name
  - Unique across the University
- Other legacy apps require alternative format (short username)
  - Short length and static format
  - Does not have to be contained in the longer login name
  - Unique across the University

Challenges:

- Maintaining and updating login name alignment with real email service
- Assigning the NetID format at scale, maintaining uniqueness
- Reducing impact on local applications with existing local usernames

Process Improvements: Next Steps

At IAM Summitt, top priority was to reach out and working with HR Community

- IAM - HR Summit being scheduled

Special Borrower Update

Library - IAM Meeting Report

Special borrowers present challenges for Identity Management and HarvardKey

- The fact that separate numbers are used for same individual to track borrowing on the functional equivalent of a library card create problems for claiming because everyone needs a unique Email, Login Name, and Recovery Email

Next Steps:

1. Library Donor will be a new Widener Library role type to track a new type of user they are tracking with a special card
2. Determine when we will require Special Borrowers to claim HarvardKey (tied to PIN phase-out)
3. Longer Term:
    a. Ability to put a library borrower role on a permanent HUID will reduce the number of people with duplicate numbers
    b. Due diligence required for MIDAS and Exports
    c. Library working with other libraries to make sure the processes are aligned

Future Meetings:

What topics should we cover in the future?

As we discussed today, these are some topics:

1. IAM - HR Summit
2. Interest of Local Units and access to IIQ and the account creation process is painful
3. Review the self-service email onboarding process
4. XID, eCommons(?), Identities where we don't have a date of birth, Executive Education use cases
5. Early access to library resources? Remember last year's issues?
6. SIS Class Participants, and other new populations we are IDing; there is some overlap with the library borrowers...
7. Identity Registry 2.0
    a. What is the wishlist?
    b. What about MIDAS?
    c. Revisit the authoritative data flows
8. Identity Data and the emerging University Data Services
9. Groups

Thank you!