HARVARD UNIVERSITY
Information Technology

Identity and Access Management

IAM Lifecycle Committee

Jan. 12, 2015 | Monday | 10:30 a.m.-12 p.m. | 561 Smith Center

Agenda

- Short Program Status Update
- User Name Progress
- Discussion Topics:
  - Sponsored people tool will be MIDAS
  - New “deceased” status at person level
  - Onboarding and role of HR office
- Close

IAM Program: Quick Update

Current Focus: Delivery of Program Increment 2

BO1 Advance Alumni release by implementing methods for migration and consumption of alumni data, and allow migrated users to authenticate and manage credentials

- **F1** Deploy Identity APIs needed by Alumni in production so they can import people data *(Alumni Identity APIs)*
- **F2** Develop and prove a credential capturing functionality to re-board an Alumni with an appropriate user name, password and recovery info *(Alumni re-boarding: Account Management)*
- **F3** Implement Alumni provisioning into LDAP to enable PIN to authenticate Alumni *(Alumni Provisioning into Harvard LDAP)*

IAM Program: Quick Update

Current Focus: Delivery of Program Increment 2

- **BO2** Meet externally-driven program commitments for InCommon, FAS/Collaboration, IIQ Audit
  - **F1** Support cloud services for FAS so end users will not have disruption in service for Google Apps *(Support Cloud Services for FAS — Google Apps)*
  - **F2** Respond to findings in audit to close open findings *(IIQ Audit)*
  - **F3** Upgrade algorithm in IdP so we can maintain InCommon Bronze Certification *(InCommon Bronze)* — DONE
  - **F4** As-needed dev support for owners needing to move off PIN3 webgates *(PIN3 Decommission)* — should be complete as of 2/1/15

IAM Program: Quick Update

Current Focus: Delivery of Program Increment 2

- **BO3** Aggressively retire tech to speed future development (platform investment)
  - **F1** Rationalize our databases to allow for easier expansion of future populations *(Database Rationalization)*
  - **F2** Keep PIN application current with other IAM systems *(PIN to Cloud)*

IAM Program: Quick Update

Current Focus: Delivery of Program Increment 2

- **B04** Capture HMS functional and technical requirements so we can plan HMS implementation project
  - **F1** Discovery Phase: Knowledge transfer and requirements gathering
  - **F2** Analysis & Design Phase: Technical design and architecture, implementation decision-making

IAM Program: Quick Update

Current Focus: Delivery of Program Increment 2

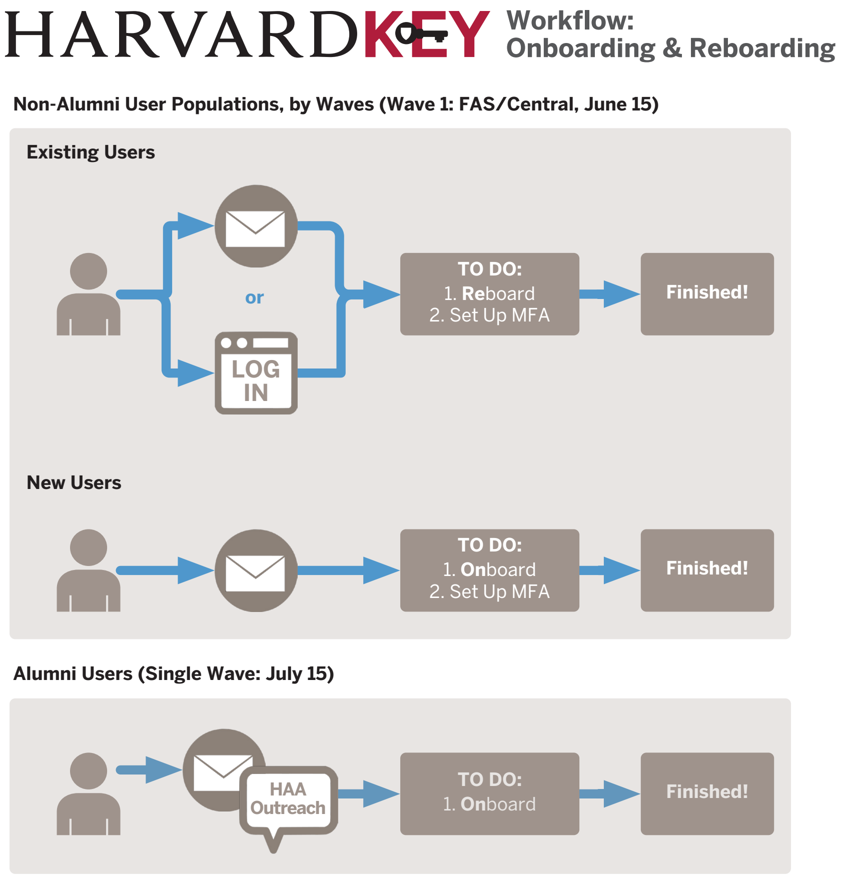
- **BO5**: Replace FAS Account Management and Provisioning currently so that we can decommission Waveset, enhancing the user experience.
  - **F1** Implement Account Management so users can change or reset passwords
  - **F2:** Service Desk functions that allow for assisting users with Account Management functions
  - **F3:** Replace connectors to FAS targets
  - **F4:** Replace existing reports that enable FAS to update email addresses to IDMRW and update the software downloads page
  - **F5:** Migrate FAS sponsored accounts into the IdDB schema
  - **F6:** Redesign the IIQ cube as required for FAS

Changes of Interest

- One user account for email, network and web access for University
- Self-service user account claiming
- Enable login using email
- As part of onboarding, enable eligible users to select email
- Alumni user authentication brought in-house
- Let students keep same account for transition to alumni status
- New universal sponsored account process
  - Assign all users HUIDs as part of identity registration (collect date of birth)
- Assign user IDs to individuals for their lifetime of affiliation

HarvardKey

- New brand name for the primary University credential
  - Gradually replaces PIN
- Works for network, email, **and** web applications



HARVARDKEY **Workflow: Onboarding & Reboarding**

Non-Alumni User Populations, by Waves (Wave 1: FAS/Central, June 15)

Existing Users

or

LOG IN

TO DO:
1. **Re**board
2. Set Up MFA

Finished!

New Users

TO DO:
1. **On**board
2. Set Up MFA

Finished!

Alumni Users (Single Wave: July 15)

HAA Outreach

TO DO:
1. **On**board

Finished!

Notes:

1. Order of HarvardKey migration is keyed to user populations, *not* individual apps. FAS/Central will roll out in the first wave in June, with additional Schools and units to follow in the next 18 months.
2. Within 18 months, every Harvard Community user will be prompted to onboard/reboard
3. UI and branding changes will be applied to the login screen in two stages:
   June 2015: New UI elements and core HarvardKey logo/visual branding
   6 months after final user population is enabled: Implement any lessons learned from UI changes, remove redundant login type options
4. *To be addressed:* Do we allow users to abstain from or postpone setup of MFA?

IAM Vocabulary Quiz

Term	How Used	Examples	Notes
Login Name (Login Email)	• Used as login ID • Expected to be an email, but could technically be another value	• Email-eligible user: *jay_hill@sph.harvard.edu* • Sponsored collaborator: *jayhill@stanford.edu* • Alumna/us: *coolguyjay@comcast.net*	HarvardKey will expect the user to provide their login email and password User Principal Name (UPN with 0365) = email
User ID	• System-assigned identifier	• Sam Account: ADID=*jeh454* • Unix LDAP: UID=*jeh454*	Permanently assigned value enables prestaging
Username	• User-selected email address component (left side of @ sign)	• *jay_hill*	User picks this as part of self-service account claim and onboarding
Harvard Email Address	• Harvard-assigned email	• *username@optionalsubdomain.harvard.edu*	Email address is assigned and written back to directory
(School) name	• Local user name(s)		Local usernames will be mapped to identity as additional attributes

Positive Change for Users

- Transition to using email to login rather than HUID or Active Directory usernames
- Self-service account management including more flexible password reset options
- Smoother onboarding by allowing “early” access for incoming employees via sponsorship mechanism
- Assign HUIDs to POIs and other sponsored people to smooth the way if there is a transition to employee or student later

Discussion: Follow-up on POI Processing

- For the initial expansion release (FAS/CA) in June, FAS sponsored account process now in Waveset will be replaced using MIDAS
  - Scope: People Only (“Affiliates” in FAS language)
  - Today: Helpdesk enters requests that are submitted on paper using Waveset
  - Future: MIDAS will be used

Discussion: Terminology

- FAS uses “affiliates,” but other schools are bothered by that terminology

Discussion: Onboarding New Users

- Lifecycle of account assignment: new employee, with “early access”
  - Recap the process flow (next series of slides)
- Getting the onboarding email into the system
  - SIS feed to IdDB
  - HR and Academic Affairs roles in getting email entered

Lifecycle: New Faculty (Bob) Onboards in the FAS

- Bob accepts Harvard’s offer of employment (9/1/15 appointment start)
- Department admin sponsors an account immediately (April 2015)
  - Name, birthdate, onboard email, start/end dates, type of affiliation, reason
- Identity is created in Identity Registry with HUID assigned
- HR sends Bob an email inviting him to claim an account
- Bob goes to start.harvard.edu to begin the account claiming process
  1. Provides his name, date of birth, and code from his onboarding email
  2. System emails him a temporary password he uses to continue the claiming process
  3. Since he is email-eligible as an incoming faculty member, Bob selects his username from a list of predefined options
  4. Provides recovery email (for future password reset)
  5. Sets his permanent password

Bob is Provisioned (as a Sponsored Incoming Employee)

- Account Management flips Bob’s status in SailPoint IIQ to “Claimed”
- Accounts are provisioned in appropriate targets based on role as “Incoming Faculty”:
  - Harvard LDAP (HarvardKey LDAP)
  - University AD
  - 0365
  - FAS AD
  - FAS LDAP
  - Kerberos
  - Google

Bob's Appointment Officially Begins 9/1

- In August, HR job data is fully complete in PeopleSoft, and is submitted to the identity registry (IdDB) by PS
- A future-effective dated employee role update results in some provisioning to downstream systems
- On 9/1/15, when his Incoming Employee role ends and his Employee role starts, additional attributes are updated in LDAP
    - His data have "aged" and mere passage of time results in additional provisioning
- Now, when Bob accesses the Athletic Office site to buy a sticker to use the pool, he is recognized as a full employee

Discussion: New Status for Deceased

- Addition of a deceased flag at person level effective December 2014
- PeopleSoft is the first system to modify its import to set this flag
- Alumni system will update it as well

Discussion:

- What are the IAM lifecycle ramifications?

Discussion: New Status for Deceased

Issues we have today:

- Overlaying the identity of an employee with the image of the deceased's person's spouse results in:
  - Untenable confusion for physical access systems
  - Very confusing for MIDAS user (example: seeing female photo against male identity)
- Now in conflict with the deceased flag at the person level
  - If we get an update a person is deceased, we should not keep the identity going to enable a spouse to have access?
- Why are we doing it that way?

Thank you!

Supporting Materials

Appendix A: IAM Accomplishments to Date

Simplify the User Experience

- Selected and purchased an identity creation toolset that will lead to improved onboarding for all users.
- Implemented a new Central Authentication Service for faster, flexible deployment of applications across Harvard.
- Implemented one-way federation with the Harvard Medical School as proof of concept of credential self-selection by users in order to access services.
- Implemented provisioning improvements that set a foundation for expanded cloud services, support for Active Directory consolidation, and support for email migration.
- Integrated a new ID card application that enables large-scale replacement of expired cards.
- Implemented a new external-facing IAM website for regularly updated information on project purpose and status.
- Migrated University AD users to the SailPoint IdentityIQ provisioning solution.

Enable Research and Collaboration

- Joined the InCommon Federation, enabling authorized Harvard users to access protected material at HathiTrust.
- Enabled access to a planning tool used by Harvard researchers to assist with compliance of funding requirements specific to grants (e.g. NSF, NIH, Gordon and Betty Moore Foundation).

Protect University Resources

- Proposed a new University-wide password policy to the HUIT Security Organization in order to standardize password strength and expiration requirements.
- Drafted a cloud security architecture with the HUIT Security Organization to provide Level 4 security assurance for application deployments using Amazon Web Services.
- Refreshed the AUTH and HU LDAP software and infrastructure to current, supported versions.
- Certified as an InCommon Bronze Identity Provider.

Facilitate Technology Innovation

- Created a conceptual architecture for IAM services to be deployed within the Amazon's offsite hosting facilities.
- Deployed the Connections directory to the AWS cloud.

Appendix B: Project Description Summary

The IAM program will be implemented according to the four strategic objectives, and work will be managed as a portfolio of 11 projects:

Project	Description
Provisioning	Improves user account management processes by replacing outdated tools with a new, feature-rich solution that can be expanded for local use by interested Schools across the University.
Federation	Enables Harvard and non- Harvard users to collaborate and easily gain access to both internal and external applications and tools.
Directory Services	Reduces the number of user-information systems of record while expanding data model and user attributes stored in the central IAM identity repository — enabling quick, consistent, appropriate access across LDAP, AD, and web authentication protocols.
App Owner Support	Enables Harvard application owners to learn about and easily integrate applications and software services with central IAM services.
One-Way Federation	A series of authentication releases and school onboarding efforts that provide Harvard users the flexibility to access applications and services using the credential of their choice.
Identity & Access Governance	Delivers visibility into IAM program metrics — including in time business intelligence capabilities such as advanced reporting and trend analysis — in support of security requirements.
Authentication Enhancements	Provides users with a simplified login experience, as well as enhanced security options for sensitive data and applications.
Authorization Enhancements	Provide application owners and administrators with the ability to manage users via access groups, as well as the ability to manage authorization rules for access to applications or software services.
External Directories	Securely exposes user identity information inside and outside of the University.
Expanded Provisioning	Enables identity creation and proofing for non-person users.
Cloud Migration	Provides the University with a cloud reference architecture for Harvard application deployments, including migrating IAM services from on-premise hosting to Amazon Web Services.