HARVARD UNIVERSITY
Information Technology

Identity & Access Management:
Changes for FAS and Beyond

May 6, 2015	12 p.m.	FAS Standing Committee on IT	Barker Center Plimpton Room

Agenda

- The Vision for Harvard Identity & Access Management
- Business Needs
- HarvardKey
  - Overview
  - Benefits
  - Why Claim Your HarvardKey?
  - Rollout Calendar
  - UI Preview
- Onboarding Workflow for New Users
- Sponsored Affiliations
- For PIN Application Owners

The Vision for Harvard IAM

The Vision for Identity and Access Management (IAM)

Our vision is to provide users, application owners, and IT administrative staff with secure, easy access to applications; solutions that require fewer login credentials; the ability to collaborate across and beyond Harvard; and improved security and auditing.

Strategic Objectives

Simplify User Experience
Simplify and improve access to applications and information inside and outside of the University

Enable Research & Collaboration
Make it easier for faculty, staff, and students to research and collaborate within the University and with other institutions

Protect University Resources
Improve the security stature of the University via a standard approach

Facilitate Technology Innovation
Establish a strong foundation for IAM to enable user access regardless of new and/or disruptive technologies

Guiding Principles

Harvard Community needs will drive our technology

Tactical project planning will remain aligned with the program's strategic objectives

Solution design should allow for other Schools to use foundational services to communicate with the IAM system in a consistent, federated fashion

Communication and socialization are critical to our success

Key Performance Indicators

Monthly number of help desk requests relating to account management

Monthly number of registered production applications using IAM systems

Monthly number of user logins and access requests through IAM systems

Monthly number of production systems to which IAM provisions

Business Needs

Stakeholder	Experience Today	Imagine If….	Program Benefit
End Users	• End users have different usernames and credentials for accessing applications and data both internal and external to Harvard • End users rely on manual, paper-based processes for creating and managing accounts • Users have no access or are forced to register for accounts to use external sites • A user's identity is not consistent throughout the identity lifecycle, resulting in interrupted access to services and resources	• End users could access information and perform research across schools and with other institutions without having to use multiple credentials • Users could manage their own accounts and sponsor others through a centralized web application • Users could use Harvard credentials to access common external sites • End users could keep using the same credentials despite changes in status, role, or affiliation	• **Simplify Account Management** • **Increase Self-Service** • **Expand Access to Resources** • **Allow Choice of Credentials** • **Ensure Continuity of Identity**
Application Owners	• Application owners have difficulty integrating access management, creating long implementation timelines and higher costs • Application owners must grant access to users with the same access rights for each user separately	• Application owners could easily integrate Harvard users with internal and external applications via a portal • Application owners could easily manage groups for controlling access to their applications	• **Simplify Application Setup** • **Simplify Application Administration**
People Admins	• People administrators manually create sponsored guest identities, resulting in delays in end-user productivity • People administrators cannot streamline de-provisioning of users' access privileges across multiple systems	• Sponsors could create and manage external persons' identity and access • Automated provisioning would reduce the burden on people admins of disparate systems and increase the security posture of the University	• **Reduce Manual Process for Guest Membership** • **Reduce Local Administrative Overhead**

Overview

HARVARDKEY

As one of the primary IAM program initiatives, HarvardKey …

- Provides a unifying credential enabling access to email, desktop, and Web resources with a single login name and password
- Successor to the PIN system
- New user experience for account management and login screen
- "One Identity for Life"
  - Consistent from Incoming Student all the way through Alumni
  - Consistent from Incoming Employee through to Retiree
  - Seamlessly supports changes between schools and departments
- Supports additional onboarding (and off-boarding) scenarios
- More robust support for collaboration with sponsored affiliates

Benefits

HARVARDKEY

What HarvardKey means for you:

- Just a single login name and password for nearly everything
  - Your login name is your FAS email, so it's easy to remember
- Works on any device — desktop, tablet or mobile! Simply claim your HarvardKey to login to web apps easily from anywhere
- A more secure password (in compliance with Harvard's new IT security policy) — plus no requirement to change it annually
- HarvardKey works consistently throughout your lifetime of Harvard affiliation, even if you change roles
- Self-service password reset works even if you leave Harvard

Why Claim Your HarvardKey?

HARVARDKEY

Claiming your HarvardKey gets you a wealth of benefits in both security and convenience.

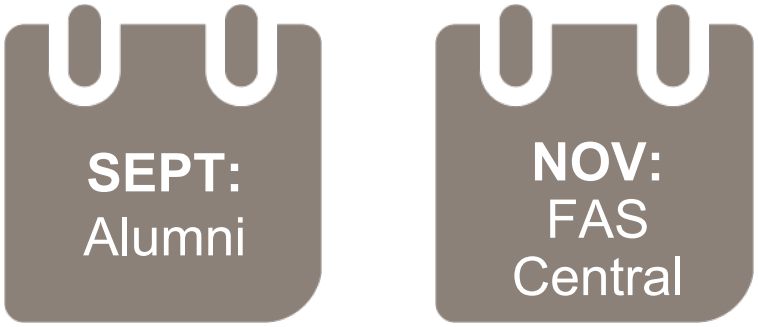
- Ensures you comply with Harvard's new password security policy
- Enables you to access advanced features of the new Harvard Phone system
- Enables you to use the new ACE Alumni system (launching in Sept.)
- Provides you with a better login experience and greater degree of accessibility on your tablet or other mobile device
- Gives you the option to add multi-factor ("two-step") authentication if you wish, boosting your security even further
- Avoid an extra click to change to a non-HarvardKey login type

But, you can continue using your PIN or FAS login until you are ready to transition.

Rollout Timeline

HARVARDKEY

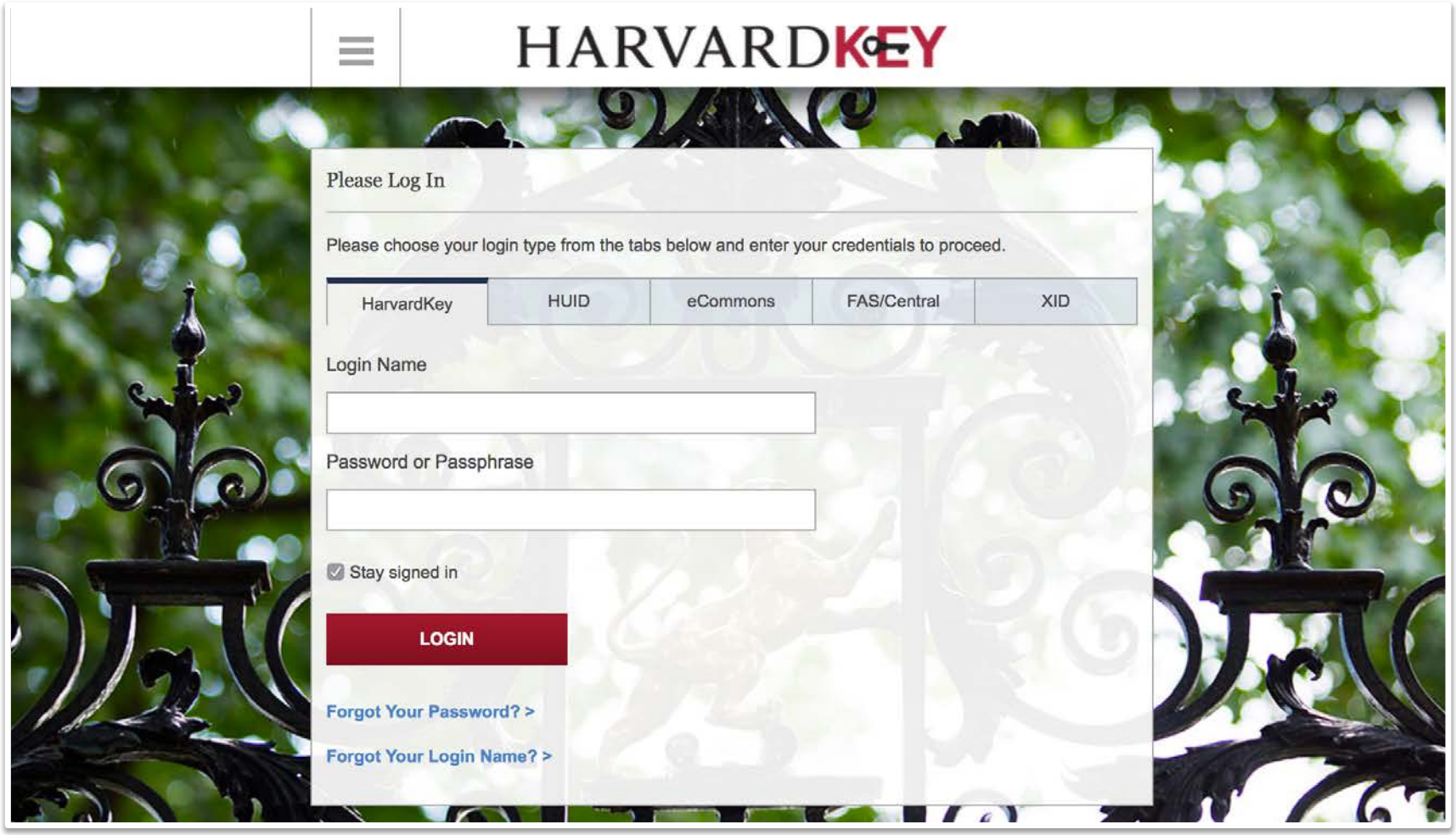
We are poised for an initial rollout in September in waves by *user population*, not application.



- Within 18 months, every Harvard Community user (except HBS) will be invited to onboard
- You'll see some design and branding changes to the login screen:
  - *Sept.-Nov. 2015:* In conjunction with Harvard's IT Security campaign, Alumni and FAS/Central users will see core HarvardKey branding and get new account management tools
  - *Six months after final rollout wave:* Implement lessons learned and remove legacy login types

UI Preview: Welcome

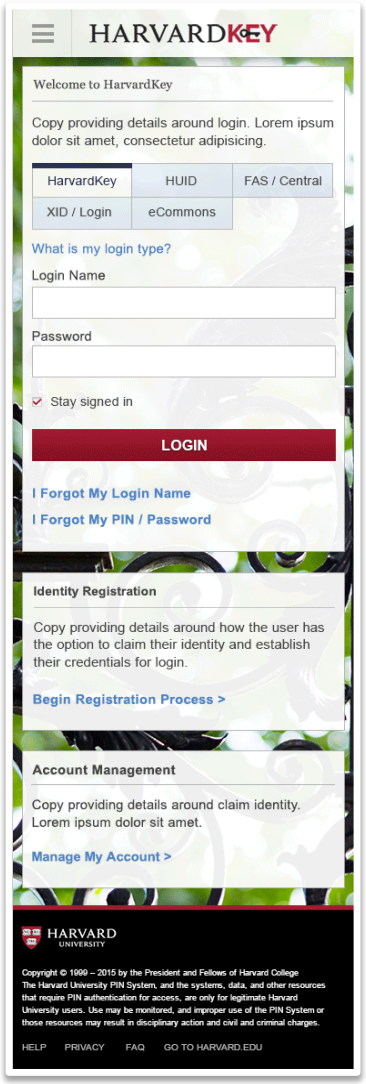
HARVARDKEY

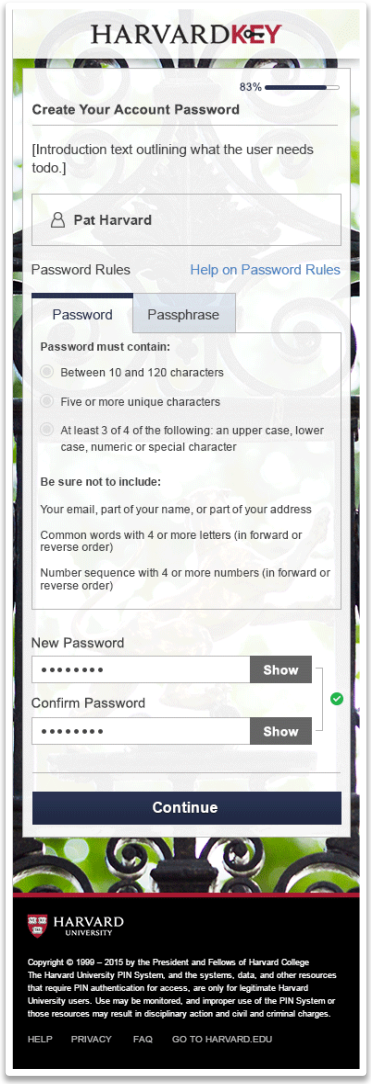


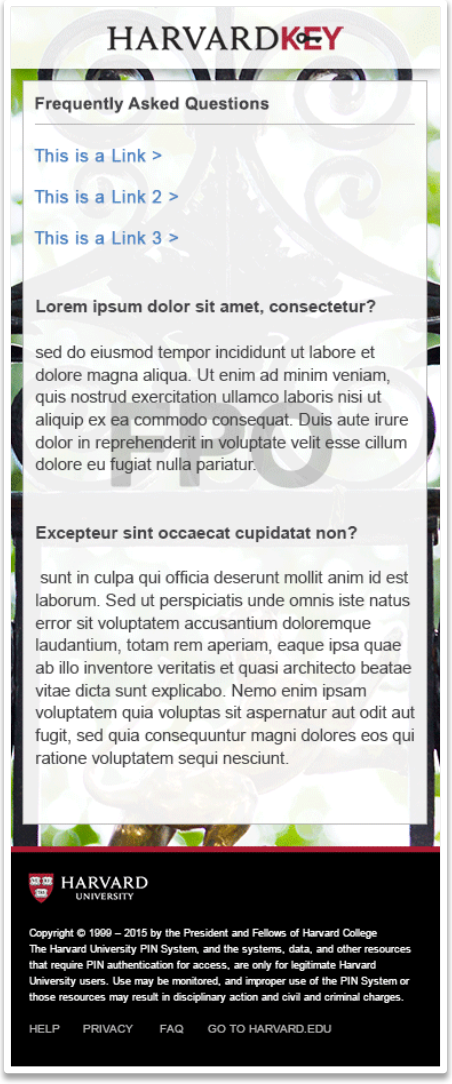
Note: These sample designs do not contain final language.

UI Preview: Mobile

HARVARDKEY







Note: These sample designs do not contain final language.

Onboarding New Users

HARVARDKEY

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 affliation 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 a 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.

PeopleSoft.

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.

Sponsored Affiliations = Sponsored POI Roles

Changes coming this fall also include a new, improved approach to sponsored accounts!

- Nimble, locally managed process for onboarding collaborators
- Sponsors may delegate administration of a sponsorship to a designated sponsor administrator
- Sponsored POI roles must still be renewed on a periodic basis — but convenient online tools will make the renewal process easier
- If a sponsored affiliate later becomes an employee, our “one identity for life” paradigm means there is no change to their HarvardKey and their user experience is consistent

For PIN Application Owners

For owners and administrators of Harvard apps that currently use PIN to log in, the transition to HarvardKey will be easy.

- Seamless transition — no work required on the application side
- Plus, new options for authorization, including attribute release using the CAS and SAML2 protocols

Thank you!

HARVARD UNIVERSITY
Information Technology

Appendix

Vocabulary Quiz

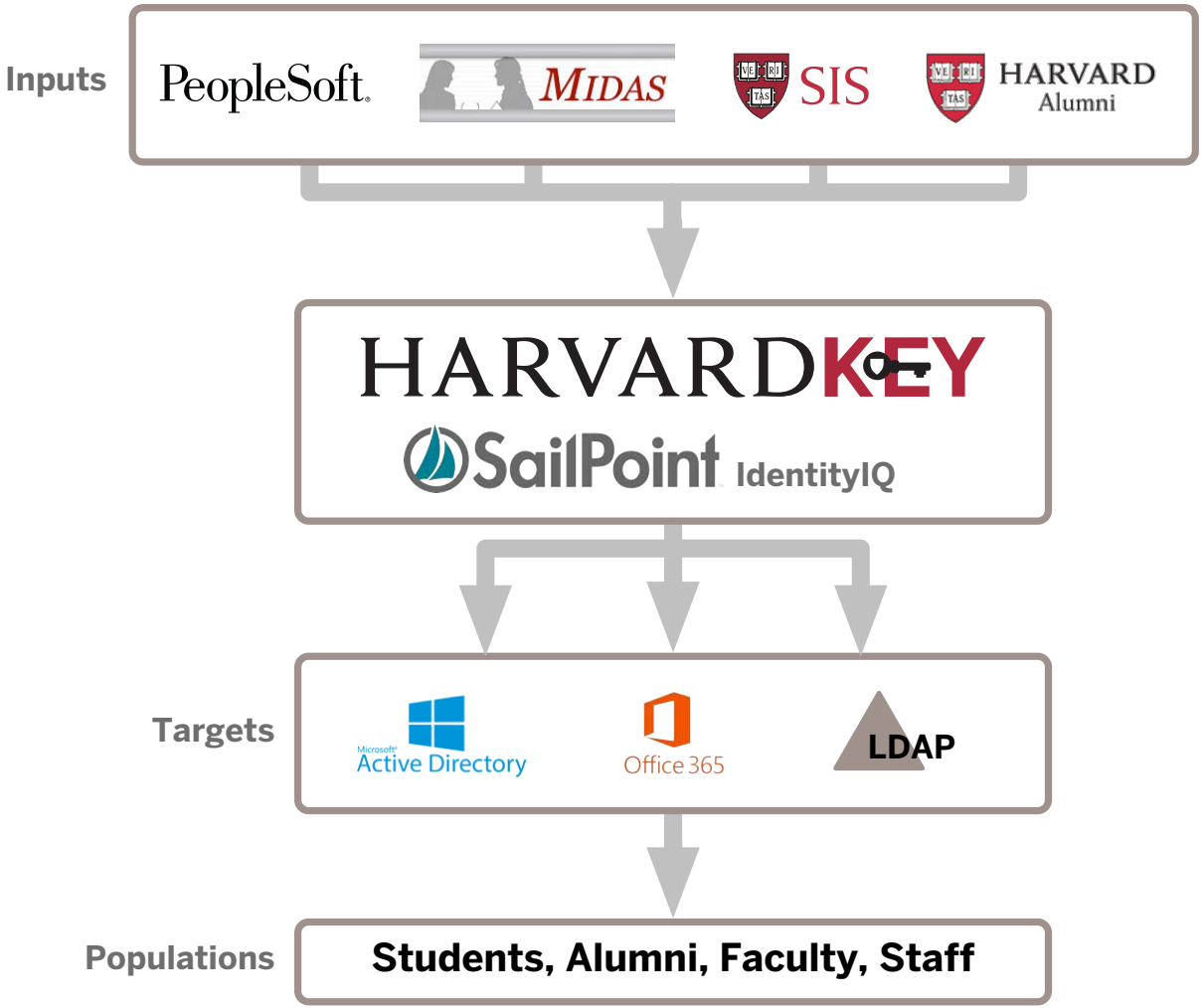
HARVARDKEY

Do you know the differences between the key terms below?

Term	How Used	Examples	Notes
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	Sam Account: ADID = *jeh454* UNIX LDAP: UID = *jeh454*	Permanently assigned value enables presaging
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

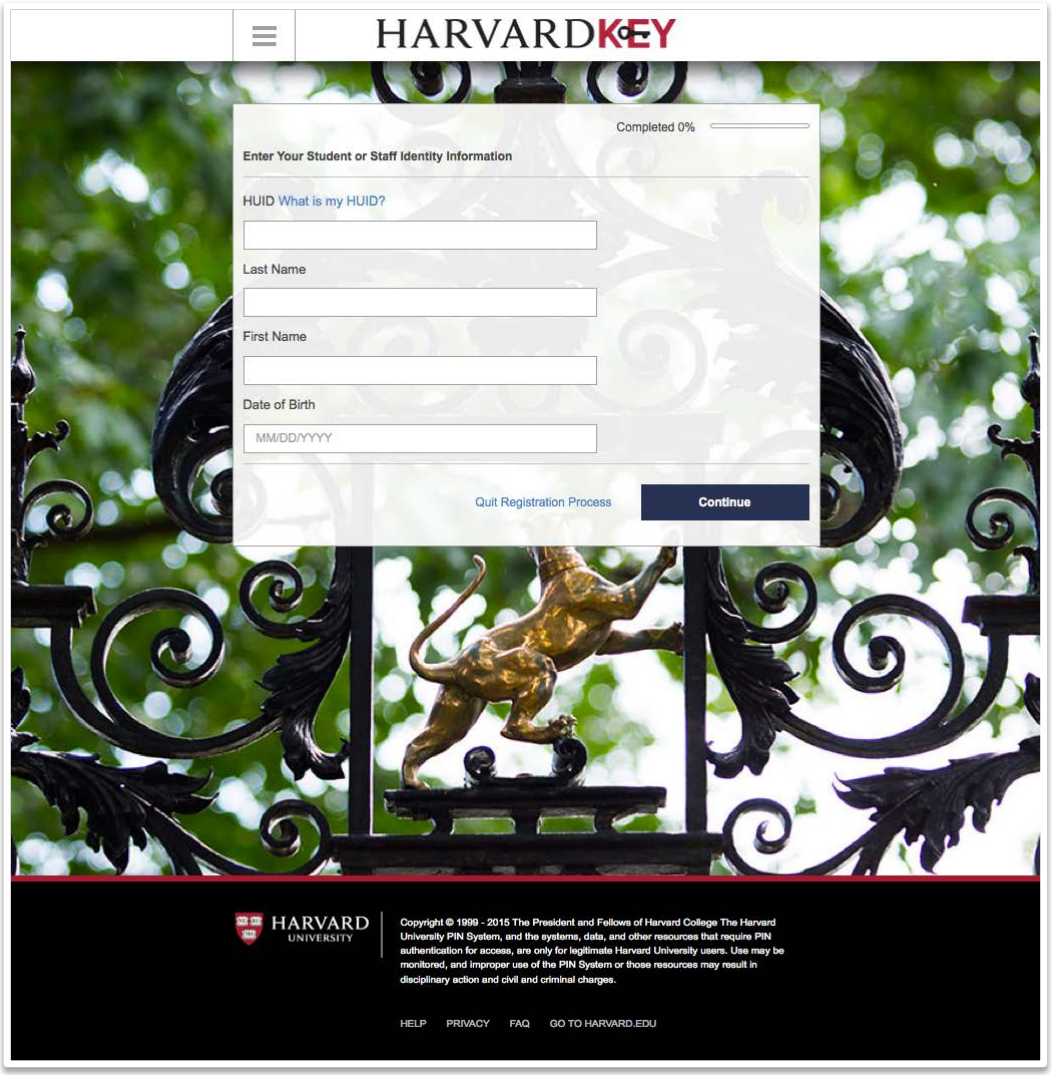
Quick Guide to Data Flow

HARVARDKEY



UI Preview: Verify

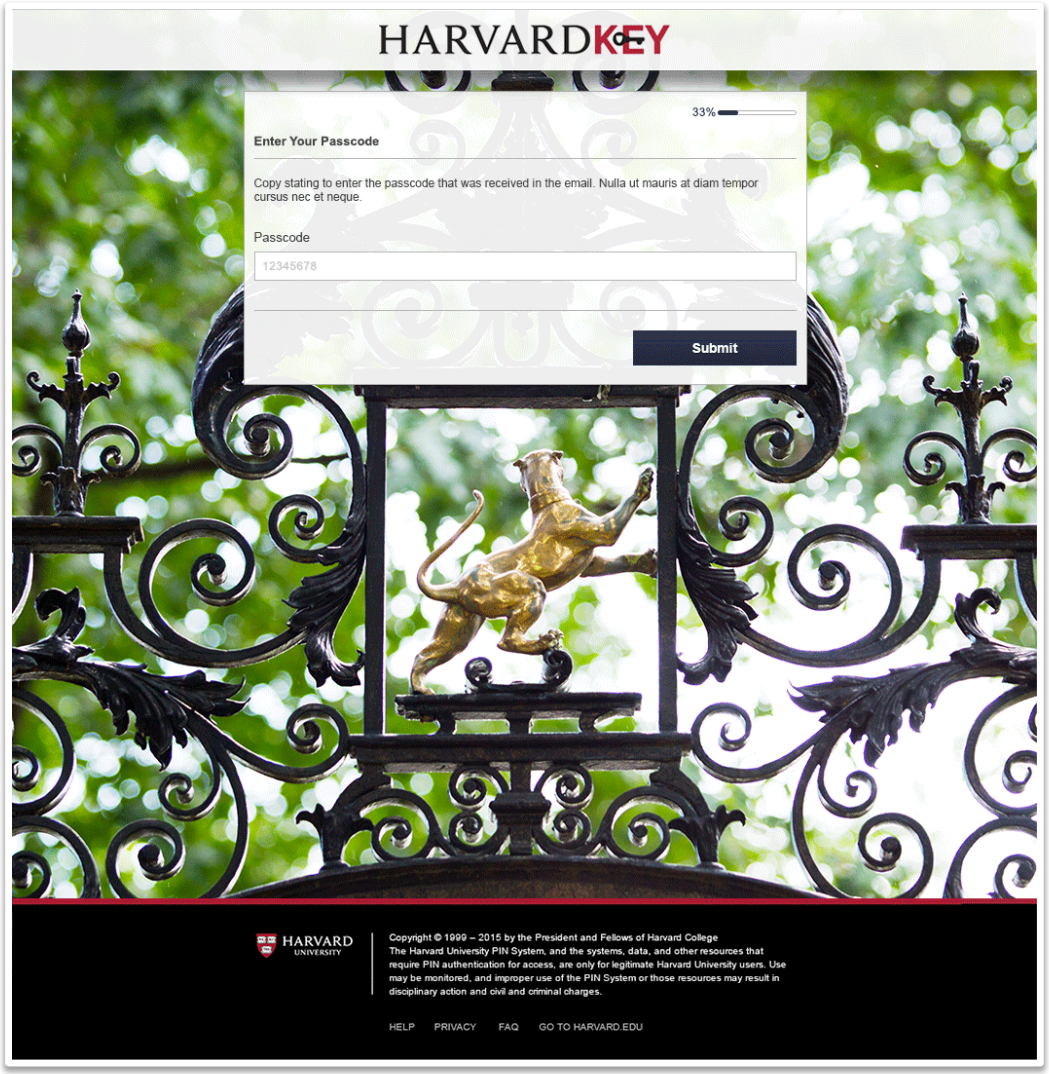
HARVARDKEY



Note: These sample designs do not contain final language.

UI Preview: Passcode

HARVARDKEY



Note: These sample designs do not contain final language.

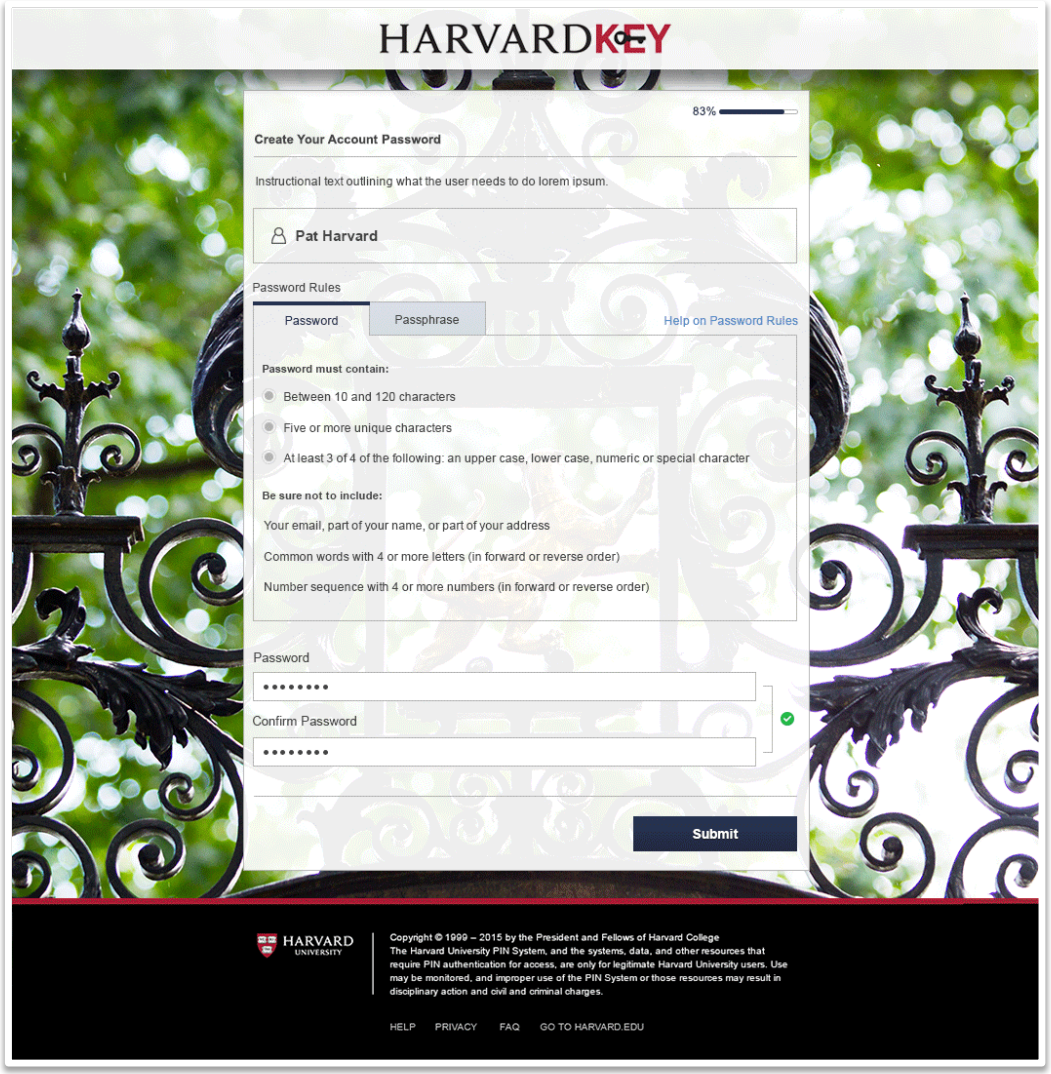
UI Preview: Recovery

HARVARDKEY

Note: These sample designs do not contain final language.

UI Preview: Password

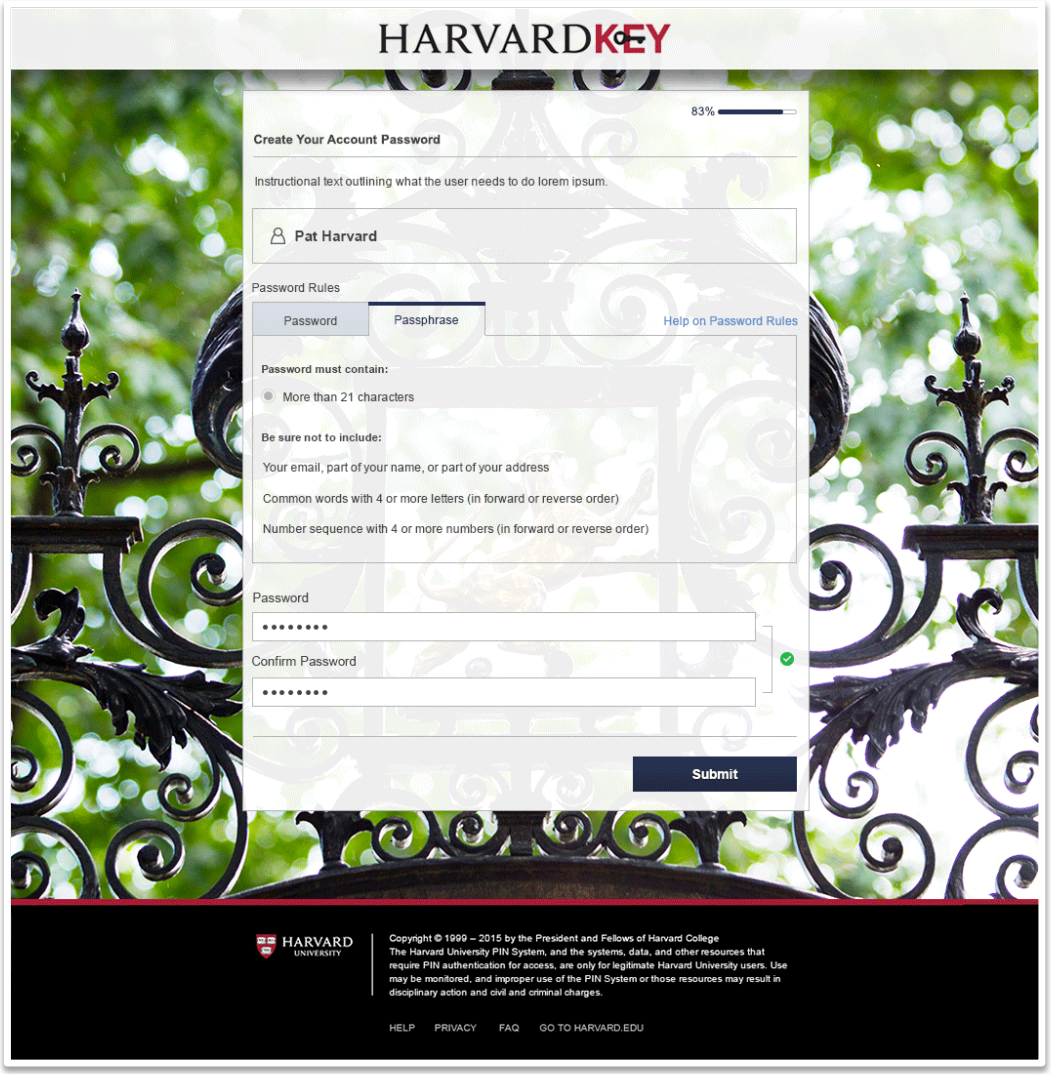
HARVARDKEY



Note: These sample designs do not contain final language.

UI Preview: Passphrase

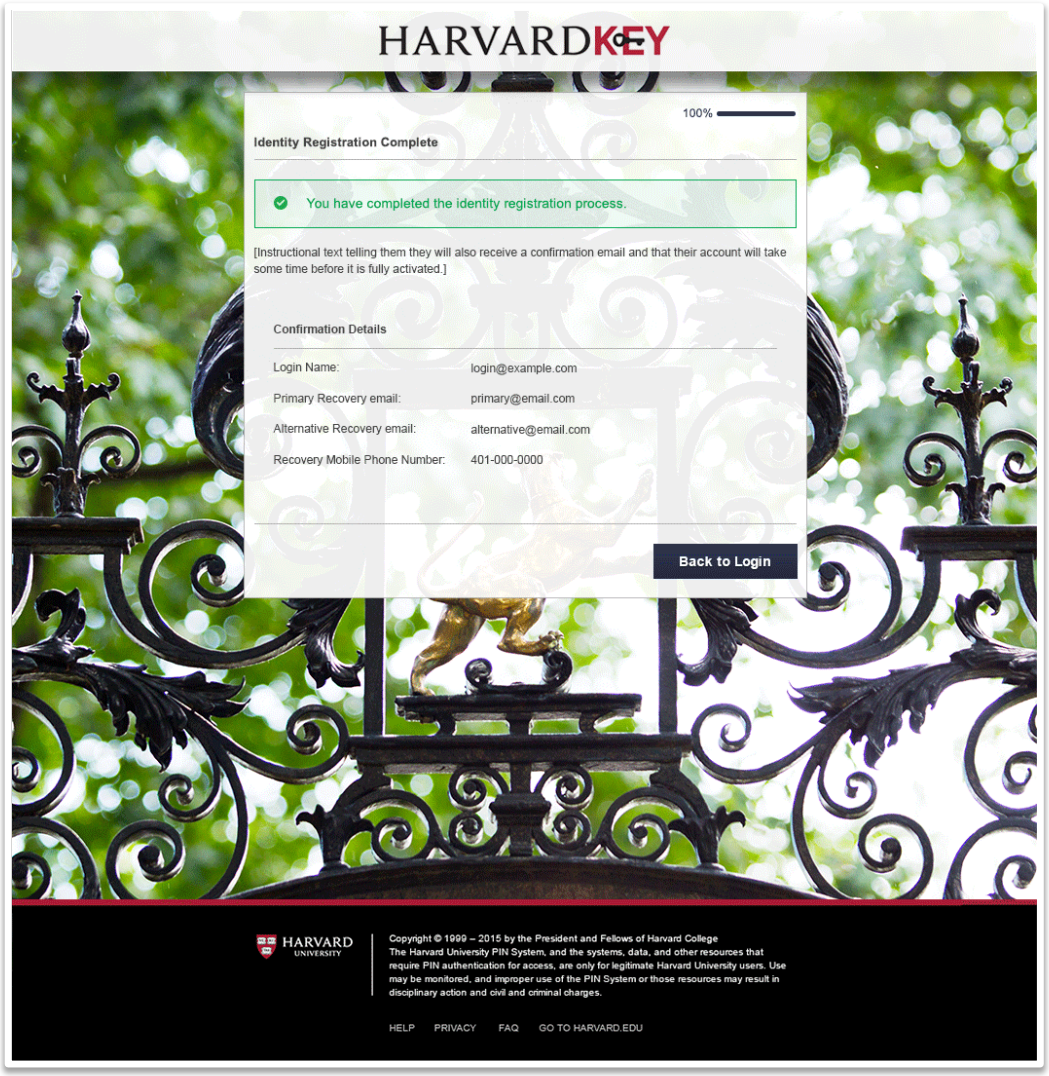
HARVARDKEY



Note: These sample designs do not contain final language.

UI Preview: Complete

HARVARDKEY



Note: These sample designs do not contain final language.

Sponsored Affiliations and 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

Proposed Additions to POI Role Types

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