HARVARD UNIVERSITY
Information Technology

CIO Council:
IAM Update

June 15, 2015	Monday	4:25-5:00 p.m.	561 Smith Center

Agenda

- HarvardKey:
  - The Benefits
  - Rollout Timeline
  - A Sneak Peek
- Multifactor Authentication
  - How Does MFA Work?
  - The Components
  - Integration Strategies

HarvardKey: The Benefits

HARVARDKEY

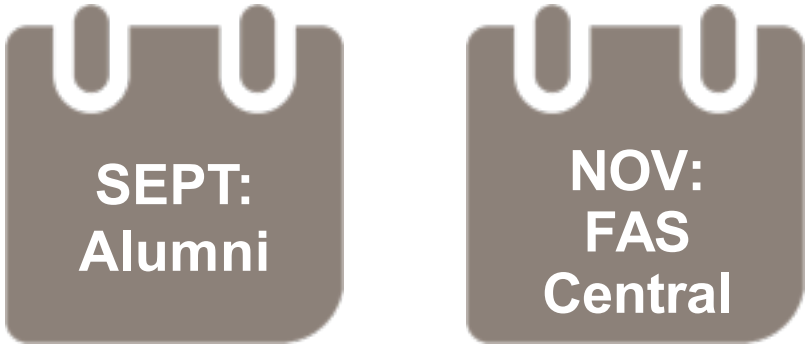
HarvardKey is a unifying credential that enables access to email, desktop, and Web resources with a *single* login name and password.

- 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

HARVARDKEY

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, 2015: New HarvardKey self-service account management functions available to all Alumni users
- Nov. 12, 2015: 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

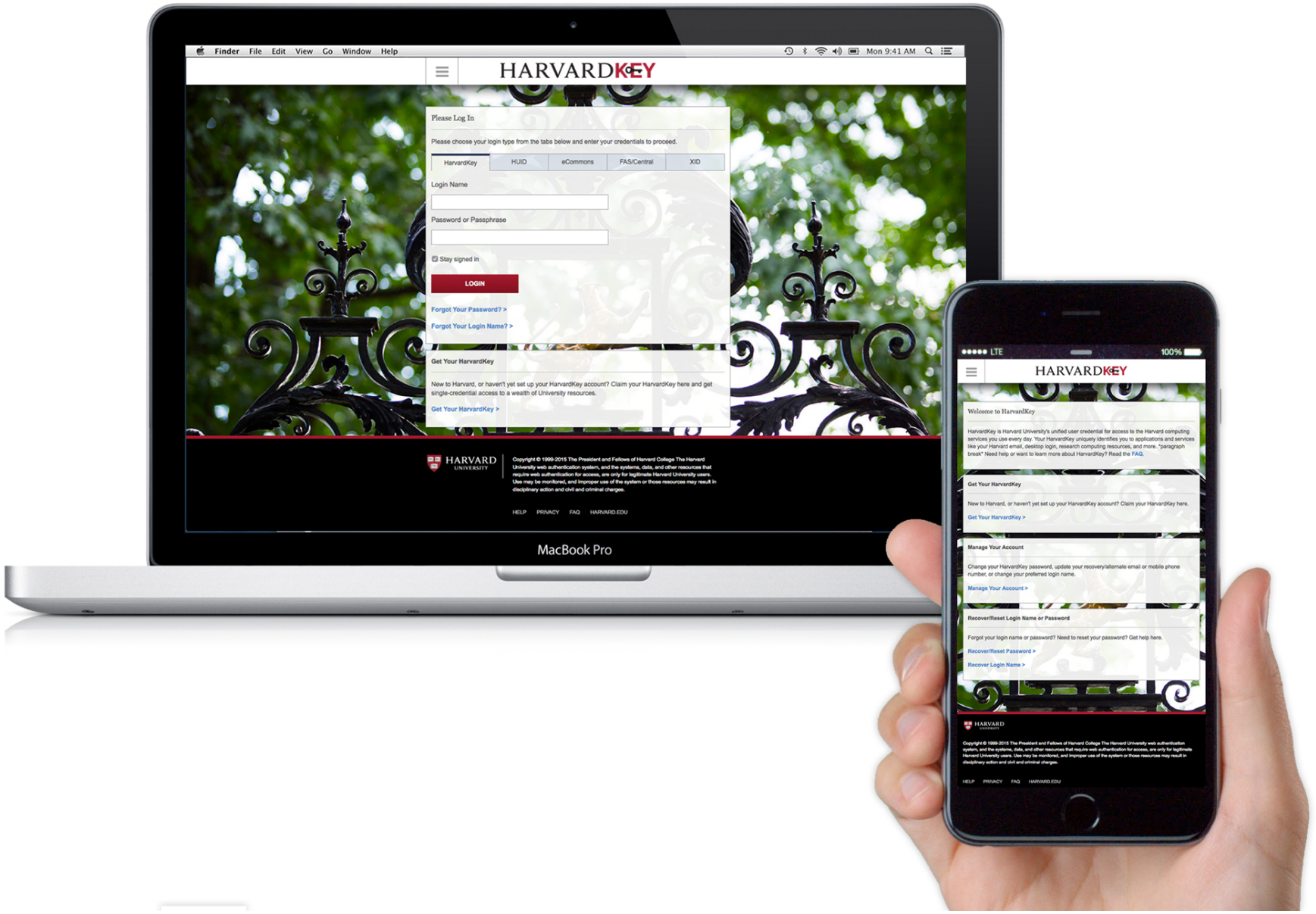
HARVARDKEY

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 Nov, 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

HARVARDKEY



Multifactor Authentication

Multifactor authentication (MFA) is an authentication method that requires the user's identity to be verified by more than one independent factor.

Types of factors:

- Something you **know**: Password
- Something you **have**: Security token or smartphone app push notification response
- Something you **are**: Fingerprint

We will use the user's smartphone as a primary second-factor device in addition to standard username/password authentication. (Users without smartphones will have other phone-based options.)

- User enables MFA for selected app(s) using HarvardKey self-service
- User downloads app to smartphone
- When user goes to log in, he/she acknowledges a push notification on his/her phone and login proceeds as normal

Multifactor Authentication Integration Strategies

An application requires use of MFA:

- Application registration with HarvardKey will be extended to support this option

User prefers MFA on all his/her access points:

- User can use the self-service functionality within HarvardKey to set this preference

Application requires MFA for some users (e.g. admin users):

- Grouper, IAM's group management tool, will be used to support this requirement

Questions?

Thank you!

HARVARD UNIVERSITY
Information Technology