Identity and Access Management
PIN App Owner Town Hall

July 28, 2015  Tuesday  1:00 – 2:00 p.m.  6 Story, First Floor
Agenda

- Meeting Purpose and Intended Outcomes
- HarvardKey Rollout Briefing
- Testing Process and Timeframes
- Follow-Up and Next Steps
- Q & A
Meeting Purpose and Intended Outcomes

Purpose
Provide applications registered with PIN2, AuthProxy, CAS or SAML information on HarvardKey and guidance on optional testing

Intended Outcomes
• Discuss HarvardKey rollout strategy and timeline
• Provide steps on how to test with HarvardKey
• Verify timeline for testing and next steps
Introduction: Video
The Benefits

HarvardKey is a unifying credential that enables access to the Harvard Web resources you use every day using 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!)
- Secure password (which never changes unless you decide to change it)
- Authentication and authorization work as before for registered apps
- 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.
- Continued credential management after separation from Harvard
UI Preview: Login Screen

Note: These sample designs do not contain final language.
Rollout Timeline

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

• **September 22**: New HarvardKey self-service account management functions available to all Alumni users

• **November 12**: HarvardKey available to FAS and Central Administration users in conjunction with Harvard’s IT Security Campaign

• **Within 18 months**, every Harvard Community user will be invited to onboard
As always, the IAM QA team extensively tests all protocols: PIN2, Authorization Proxy (AuthZProxy), CAS, and SAML.

• Testing for your applications is not required, but we can register your P-1 instances with our P-1 authentication service if you request

• Note that many of your existing P-1 environments are probably integrated with production ‘PIN’

• The transition from PIN to HarvardKey on 9/22 will continue to result in a HUID or XID being returned in the authentication assertion:
  – If an application is registered for a Alumni and HUID, the assertion will contain an HUID; the HAA ID can be requested as an additional attribute (NEW)
  – If registered for eCommons, you get an eCommons ID if that is how the user authenticated
Testing Process: Step 1

First, validate your non-production environment is registered:

• Copy your production URL from the PIN login page and also the URL from your non-production environment

• Put both URLs into an email addressed to iam_help@harvard.edu — this will generate a ticket assigned to us

• The IAM Production Support group will verify your non-production application is registered with our stage authentication environment

• Depending on your protocol, you will get metadata/SAML (or you’ll need to download a public key/PIN) so that your non-production environment will be integrated

TARGET DATE = end of August (if you are testing)
Testing Process: Step 2

We will provide appropriate data for testing:

- IAM will provide you with test users for the HarvardKey environment (you’ll need to add them into your application)
- Then, validate that those users can log in using HarvardKey and authenticate to your application
- Report any concerns to iam_help@harvard.edu

TARGET DATE = 9/4 (confirm authentication with HarvardKey)
IAM Summer Lunch & Learn Series

Multifactor Authentication
• July 29
• August 19

HarvardKey
• August 12

POI Sponsored Affiliations
• August 5

Provisioning
• August 26

Sign up online for other sessions — and encourage your colleagues to attend, too!
iam.harvard.edu/lunch-and-learn
Questions?
Thank you!