HARVARD UNIVERSITY
Information Technology

Identity and Access Management

PIN App Owner Town Hall Meeting

March 31, 2015	Tuesday	3:00 – 4:30 p.m.	Taubman, T-520 (HKS)

Agenda

- Meeting Purpose and Intended Outcomes
- Rollout of HarvardKey
  - Explanation of the new unified credential (15 min)
- Explanation of Current State (30 min)
  - Authentication, Authorization, and Attributes
  - Potential Scenarios and Considerations
- Options for HarvardKey Integration (20 min)
- Discussion, Questions, Concerns (20 min)
- Follow-Up and Next Steps (5 min)

Meeting Purpose and Intended Outcomes

Purpose

To provide Application Owners (of apps using the PIN2 service and allowing multiple credentials) information on HarvardKey and potential integration scenarios

Intended Outcomes

- Understand the current configuration of all applications
- Discuss HarvardKey rollout strategy and its technical aspects
- Provide options on how best to integrate with the HarvardKey
- Determine best path for each application and next steps

HarvardKey for the End User

The new HarvardKey will offer a single credential for access to most applications across the University

- Log in to your desktop, check your email, use your Web apps … all using the same login name and password
- Easier-to-use self-service features for common tasks like changing your password
- Options for two-step verification via phone for even greater security
- Rollout begins in September for Alumni and for others in October. This rollout will be done in conjunction with the Security Outreach Campaign in order to optimize communication with users

HARVARDKEY

HarvardKey for People Administrators

Improvements in onboarding, account management, and sponsored affiliation processes make work easier for people administrators.

- Easier onboarding, including self-service account claiming and some automatic provisioning
- Account management will be easier for both users and people administrators
- Sponsored affiliations will fit within the POI user classification, with simpler, more streamlined setup

Current State: Authentication, Authorization, Attributes

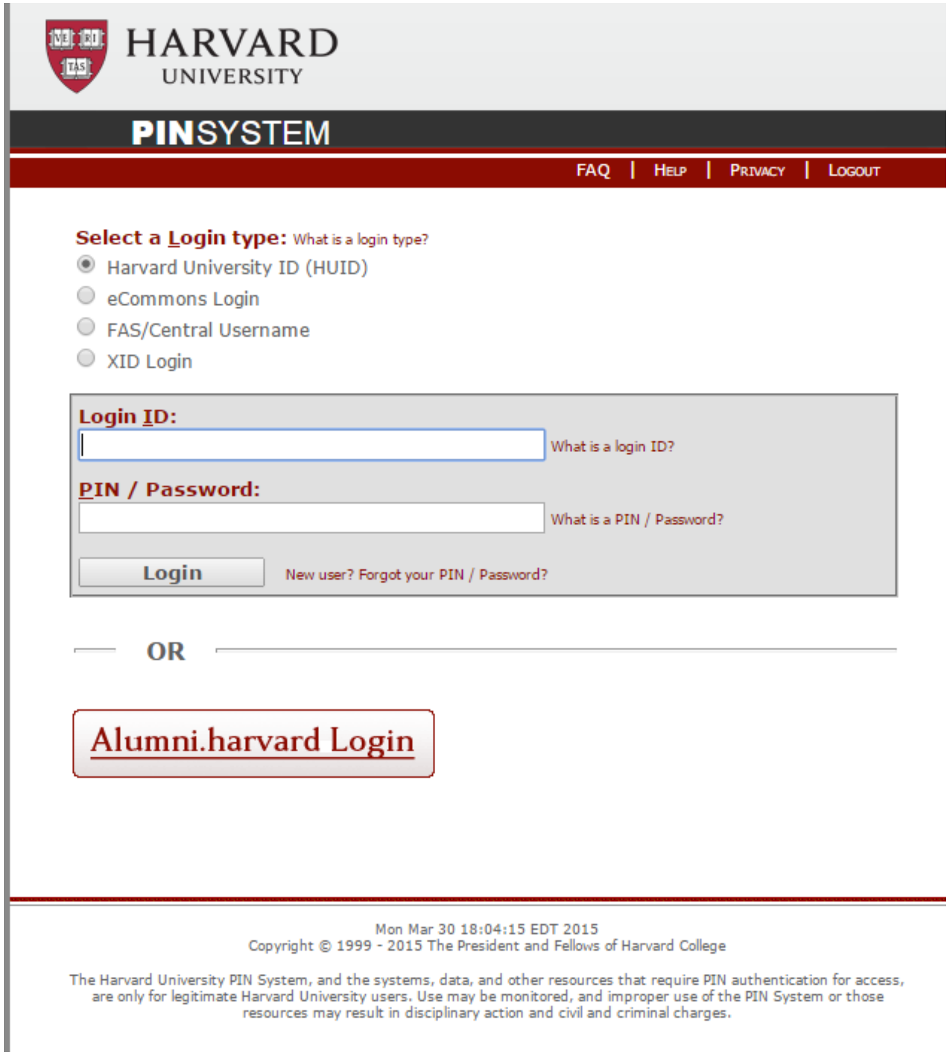
Authentication (PIN system handles)

- User successfully supplied the password

Authorization (application responsibility)

- The application compares the user name that is provided in the authentication response to a local list of named users
- An authorization proxy 'rule' can be used (PIN with an authorization filter)
  (e.g. 'active employee' OR 'active temporary employee')
- Attributes included within the authentication response are used by the application to analyze each user as they are passed on to the application
  (e.g. 'student or class participant at FAS' OR 'student at DCE')
- Attributes are queried from HU-LDAP (or another local authoritative repository) using the unique user name that was provided in the authentication response
- No authorization used (anyone who successfully supplies the correct password can access the resource)

Why are you here? What is the concern?



HARVARD
UNIVERSITY

PINSYSTEM

FAQ | HELP | PRIVACY | LOGOUT

Select a Login type: What is a login type?

● Harvard University ID (HUID)
○ eCommons Login
○ FAS/Central Username
○ XID Login

Login ID: What is a login ID?

PIN / Password: What is a PIN / Password?

Login New user? Forgot your PIN / Password?

OR

Alumni.harvard Login

Mon Mar 30 18:04:15 EDT 2015
Copyright © 1999 - 2015 The President and Fellows of Harvard College

The Harvard University PIN System, and the systems, data, and other resources that require PIN authentication for access, are only for legitimate Harvard University users. Use may be monitored, and improper use of the PIN System or those resources may result in disciplinary action and civil and criminal charges.

Currently, the authentication response contains different information depending on what type of user authenticated (which radio button was selected)

With use of the HarvardKey, login options begin to consolidate:

Alumni login = HarvardKey
HUID holder = HarvardKey
FAS/Central = HarvardKey

When the someone uses HarvardKey, there is no way to determine if they are an Alumni, an Employee or Student or have a FAS sponsored affiliation/POI, etc.

So depending on what the authorization approach is, your application may not be able to differentiate between types of users adequately.

Discussion of Integration with HARVARDKEY

Login Option	Today	Future:HarvardKey	Solution
HUID +	Contains an id type indicator If the HUID radio button was selected, value contains a HUID If Alumni option selected, value contains a HAA ID (Advance ID)	No id type for differentiation (all HarvardKey) Value will always be = HUID To figure out id type of Alum or eCommons holder requires requesting and using additional attributes	If the type of user who is authenticating into the application is irrelevant, then there is no issue. However, this implies the application is not using authorization (and will not be migrating to use HUID-based authorization).
Solution?	id_type indicators: 'P' for Harvard's HUID 'M' for the HMS eCommons 'A' for the Alumni 'X' for XID system	NameID = HUID Attributes: 'harvardEduAlumniId' 'harvardEduHMSId'	Always send all the login types Look-up all the user's identifiers, and include them. Authorization model must be reevaluated

Options for Integration With HARVARDKEY

Adapt your application to expect HUIDs for all populations, regardless of whether they are Alumni or not:

Considerations:
The applications local named-users list may be expressed in HAA IDs, these would need to be converted to HUIDs
eCommons system does not have HUIDs for the self-registered population

Migrate to CAS or SAML which can provide attributes (but no authorization rule):

Considerations:
There is no eCommons attribute service (yet)
CAADS/Alumni attribute service exists, but is being integrated with PIN/CAS and PIN/SAML

Migrate to use the AuthProxy token in order to get attributes for various user login types; potentially use an authorization rule?

Considerations:
AuthProxy token format is proprietary format; using it requires development (by applications)
Create new AuthProxy token format to support multiple login types - IAM Development

Use multiple registrations?

Important Points To Consider

- Are all the registrations with PIN system that exist today still needed? (If no longer needed, please email iam_help@harvard.edu)
- What does the application do with the authentication response today?
- What authorization look-up method is used to determine who should get access to the resources?
- Does the application rely only on ID type to for its authorization logic? If yes, this situation is the most affected by HarvardKey (multiple identifiers will be sent for some users).
- Is the option to use multiple registrations for a single login type viable? PIN registration name can give additional information.
- If using PIN2 service today, and attributes are required, can the application migrate to PIN/CAS or SAML?

Open Discussion

- What are your questions and concerns?
- What additional information do you need?
- Dependencies?

Follow-Up and Next Steps

- Inform IAM of any applications that are no longer active (April 15)
- Determine which approach will work for each of your applications (May 15)
- If none of the approaches works, start a conversation with IAM to figure out how best to proceed (May 15)
- IAM to confirm availability of eCommons attribute service (May 15)
- What else?

Thank you!

Supporting Materials

PIN2 Applications

harvardeduapplicationname	harvardeduredirecturl	official_email
	https://www.countway.harvard.edu/harvard_pin	Douglas_MacFadden@hms.harvard.edu
Webdash Registration	https://cbmi.med.harvard.edu/webdash/register.cgi	Douglas_MacFadden@hms.harvard.edu
Countway Legacy Site	https://legacy.countway.harvard.edu/login.html	Douglas_MacFadden@hms.harvard.edu
HMS Countway Website	https://new.www.countway.harvard.edu/harvard_pin	Douglas_MacFadden@hms.harvard.edu
Harvard Faculty Finder	http://facultyfinder.harvard.edu/login/default.aspx?pin=receive	Douglas_MacFadden@hms.harvard.edu
Harvard Catalyst Apply Hub	https://apply.catalyst.harvard.edu/login	Gregory_Polumbo@hms.harvard.edu
Pathway	http://pathfinder.catalyst.harvard.edu/login	Gregory_Polumbo@hms.harvard.edu
Harvard Catalyst Education Video Library	http://catalyst.harvard.edu/educationvideolibrary/	Gregory_Polumbo@hms.harvard.edu
iPS Core	https://authzproxy.harvard.edu/authzproxy/authorize.do	halip_saifi@hms.harvard.edu
Harvard Catalyst Profiles	http://connects.catalyst.harvard.edu/Profiles/login/default.aspx?pin=receive	James_Norman@hms.harvard.edu
Harvard Catalyst Profiles 2	http://connects.catalyst.harvard.edu/Profiles/login/default.aspx?pin=receive	James_Norman@hms.harvard.edu
harvard Catalyst Profiles 2 New	http://new.connects.catalyst.harvard.edu/profiles/login/default.aspx?pin=receive	James_Norman@hms.harvard.edu
Departmental Dell Computer Purchase	https://authzproxy.harvard.edu/authzproxy/authorize.do	jane_sulkin@harvard.edu
Personal Dell Computer Purchase	https://authzproxy.harvard.edu/authzproxy/authorize.do	jane_sulkin@harvard.edu
Message Me	https://authzproxy.harvard.edu/authzproxy/authorize.do	katie_kilroy@harvard.edu
Message Me	https://authzproxy.harvard.edu/authzproxy/authorize.do	katie_kilroy@harvard.edu

PIN2 Applications, continued

harvardeduapplicationname	harvarderedirecturl	official_email
AAD Web Content Administration	https://authzproxy.harvard.edu/authzproxy/authorize.do	kenton_doyle@harvard.edu
HUIT Site Content Owners	https://authzproxy.harvard.edu/authzproxy/authorize.do	kenton_doyle@harvard.edu
Web Content Management	http://itis-wcmprd.cadm.harvard.edu:8080/Alfresco	kenton_doyle@harvard.edu
Web Content Management	http://itis-wcmpub.cadm.harvard.edu:9080/Alfresco	kenton_doyle@harvard.edu
Alumni	http://alumni.harvard.edu/pinserver/auth	kenton_doyle@harvard.edu
checkin.harvard.edu	https://authzproxy.harvard.edu/authzproxy/authorize.do	kenton_doyle@harvard.edu
UIS Web Site	http://www.uis.harvard.edu/ldap/index.php	kenton_doyle@harvard.edu
IIC	http://www.iic.harvard.edu/ldap/index.php	kenton_doyle@harvard.edu
Computer Science 50	https://authzproxy.harvard.edu/authzproxy/authorize.do	malan@harvard.edu
JACK - Jobs and Careers at Harvard's Kennedy School of Government	https://authzproxy.harvard.edu/authzproxy/authorize.do	michael_humphrys@harvard.edu
Harvard Immunology Website	https://immunology.hms.harvard.edu/harvard_pin	William_Murphy@hms.harvard.edu
HIBIE Wiki	http://wiki.hibie.harvard.edu	
Harvard Center for Jewish Studies Application Review	https://www.fas.harvard.edu/~cjs/fellowships/apply/review/index.cgi	

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 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 IAM website for regularly updated information on project purpose and status
- Migrated University AD users to the SailPoint IdentityIQ provisioning solution
- Deployed identity APIs for SIS strategic initiative

Enable Research and Collaboration

- Joined 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 HUIT Security 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 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 app 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