HARVARD UNIVERSITY
Information Technology

Enabling Cross-University Collaboration with Harvard IAM:
TIER, InCommon, and Grouper

IT Summit 2015	June 4, 2015	Thursday	1:10-2:00 p.m.

Agenda

- What is Identity & Access Management at Harvard?
- IAM in Higher Education is Different
- Requirements and Concerns for IAM in Higher Education
- Internet2: InCommon, Shibboleth, Identity Federation, and More
- TIER: Trust and Identity in Education and Research
- Harvard's Role in TIER
- Major IAM Projects at Harvard: HarvardKey and Grouper
- Summary: Supporting the Teaching & Research Mission

Who We Are

- **Jason Snyder**
  Managing Director, Architecture and Engineering, HUIT
- **Jane Hill**
  Director, IAM Product Management, HUIT
- **Scott Bradner**
  Senior Technology Consultant, HUIT

What is Identity & Access Management at Harvard?

The Vision for the Identity & Access Management Program

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.

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

IAM in Higher Education is Different

Our users are different from those in industry, and their needs are different, too.

- Users are frequently affiliated with more than one institution, whether simply through multi-institution research conducted at "home" or something as multivariate as a temporary guest lecturer assignment at another university
- Inter- and intra-university partnerships continue to expand
- People often hold multiple rules – with multiple privileges – concurrently
- Affiliations often don't have clear start or end dates — faculty need early access to set up course sites, and many users continue to collaborate after formal appointments end
- Privacy is of greater importance in higher education than within many corporate environments
- Faculty and researchers depend upon continuity and accuracy in their publishing records and academic biographies, and therefore have their own unique needs

Scholarly Identity and Collaboration

- Increasingly, academic users need to maintain an accurate profile of their publication history and academic biography
- Since IAM already involves a large amount of attribute and identifier exchange, adding scholarly identifiers to the attribute repository is a way to include this information in an existing data flow
- Identifiers enable integration around an individual's scholarly record, such as LTI, VIVO, etc.
- ORCID (Open Researcher & Contributor ID) identifiers are being added to Internet2's standardized eduPerson schema, as well as various data repositories around the academic community
- Items linked to an ORCID record can have multiple external identifiers, and these can connect to other identifiers: DOIs, ISBNs, ISNIs, PubMed IDs, grant numbers, etc.

Learn more about ORCID at orcid.org.

Identity and Privacy in Higher Education

"The rise of Internet identity began in earnest ten years ago, as academic, government and corporate and social deployments started and began to influence each other. Government initiatives have come and gone and come anew. Research and education deployments worldwide have pushed the envelope but are now challenged to inter-federate. **Social providers evolve business models that leverage the user as product.**

"There are impressive successes now in many instances and key integrations have been achieved. The extent of usage has grown dramatically. At the same time, there are obvious stress points, where the conflict of economic motives compound issues of privacy, where the international differences in cultures and legal systems create a swamp of issues, and helping the institution and the user manage the complexity of privacy."

— Ken Klingenstein, Internet2, December 2014

IAM in Higher Education: Common Requirements

Commonly accepted requirements for IAM solutions across the academic community include the following:

- Services must support complex authorization models to grant individuals the right levels of access to licensed resources (all roads lead to groups!)
- Solutions must support federation to enable inter- and intra-institution access — not feasible to rely on centralized control of all users
- Solutions must allow for the fact that users will need to access some resources on the public Internet
- With interest in cloud services exploding, solutions should be able to work in the cloud if desired
- Preference for open source, standards-based solutions
- Services and solutions should be built with the financial constraints of higher education in mind

IAM in Higher Education: Building Our Own Solutions

Since higher-education users have their own special needs, out-of-the-box vendor solutions often aren't satisfactory. Why build our own solution?

- Commercial products are designed for corporate intranet environments
- Vendor solutions are often a poor fit with our identity data and the requirements it poses (multiple roles, fuzzy lifecycle, increased privacy)
- If support for federation even exists in vended solutions, it tends to be bi-lateral
- Vendors discount software, but often look to sell expensive professional services
- Use cases are often the same across institutions, regardless of their size:
  - Extended identity lifecycles
  - Context-sensitive privacy management
  - An identity registry that supports multiple personae
  - Group management

Addressing These Issues: Internet2

Internet2 is a not-for-profit organization started as a U.S. higher education consortium in 1996.

- 252 U.S. universities
- 82 corporations
- 68 affiliates, including government agencies
- 41 regional and state education networks
- More than 65 national research and education networking partners, representing more than 100 countries

Internet2 projects include:

- National network (100 Gbps links, Harvard is a member)
- Trust and Identity in Education and Research (TIER)
- Grouper
- Shibboleth
- InCommon Federation

Internet2: InCommon

- **Certificate service**
  Flat-rate certificates

- **Identity management federation**
  Use your Harvard identity elsewhere

- **Assurance program**
  Standard for quality of authentication

- **Multifactor authentication**
  Discount for Duo multifactor service

Internet2: Shibboleth

As a technology enabling identity federation, Shibboleth defines the interaction between the two key players in authentication:

- **Identity provider (IdP)**
  An authentication and attribute service
- **Service provider (SP)**
  An Internet-based website that uses an IdP to authenticate a user

Shibboleth®

Shibboleth Identity Federation at Harvard

Identity federation at Harvard is a cooperative system that supports the interconnection between SPs and IdPs, resulting in the following user experience:

1. User connects to a service and clicks a “log in” button or link
2. The service presents the user with a list of universities
3. The user selects “Harvard University”
4. The user’s browser is redirected to the Harvard web authentication system (PIN or HarvardKey)
5. The user inputs his or her credentials
6. If credentials are accepted, the user’s browser is redirected to the original service
7. The service is told that the user is authenticated

Identity Federation at Harvard: Security & Privacy

Harvard's federated identity system has a number of security and privacy benefits:

- The actual act of authentication is done at Harvard
- The service never gets the user's credentials
- All interactions are cryptographically protected
- Harvard controls what user attributes are given to the service
  - Usually *eduPersonPrinicpalName* (*eppn*), a random-appearing unique identifier
  - May also get a user's login name and email

Identity Federation: The Scope

- According to InCommon, 8 million people are supported by their affiliated federated identity providers
  - 397 IdPs
  - 2,275 SPs
- Harvard supports referrals from more than 30 InCommon and other SPs
- Harvard also runs one SP — the Loeb Classical Library

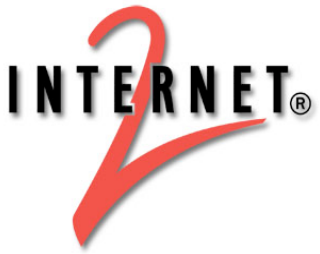
Identity Federation: InCommon Assurance

Harvard is certified as an InCommon Bronze-level identity provider.

- This means that we have met the extensive requirements in InCommon's Bronze certification requirements document
- See more details at http://iam.harvard.edu/resources/incommon, including our Bronze self-certification documentation
- The only user impact to this certification is that users will be asked to change their passwords the first time they try to access an InCommon Bronze SP
- We have also completed nearly all the requirements for Gold-level certification

TIER: Wrapping Them All Up

How can Harvard and other higher-education institutions effectively share and standardize the results of their IAM efforts? Through TIER — Trust and Identity in Education and Research.



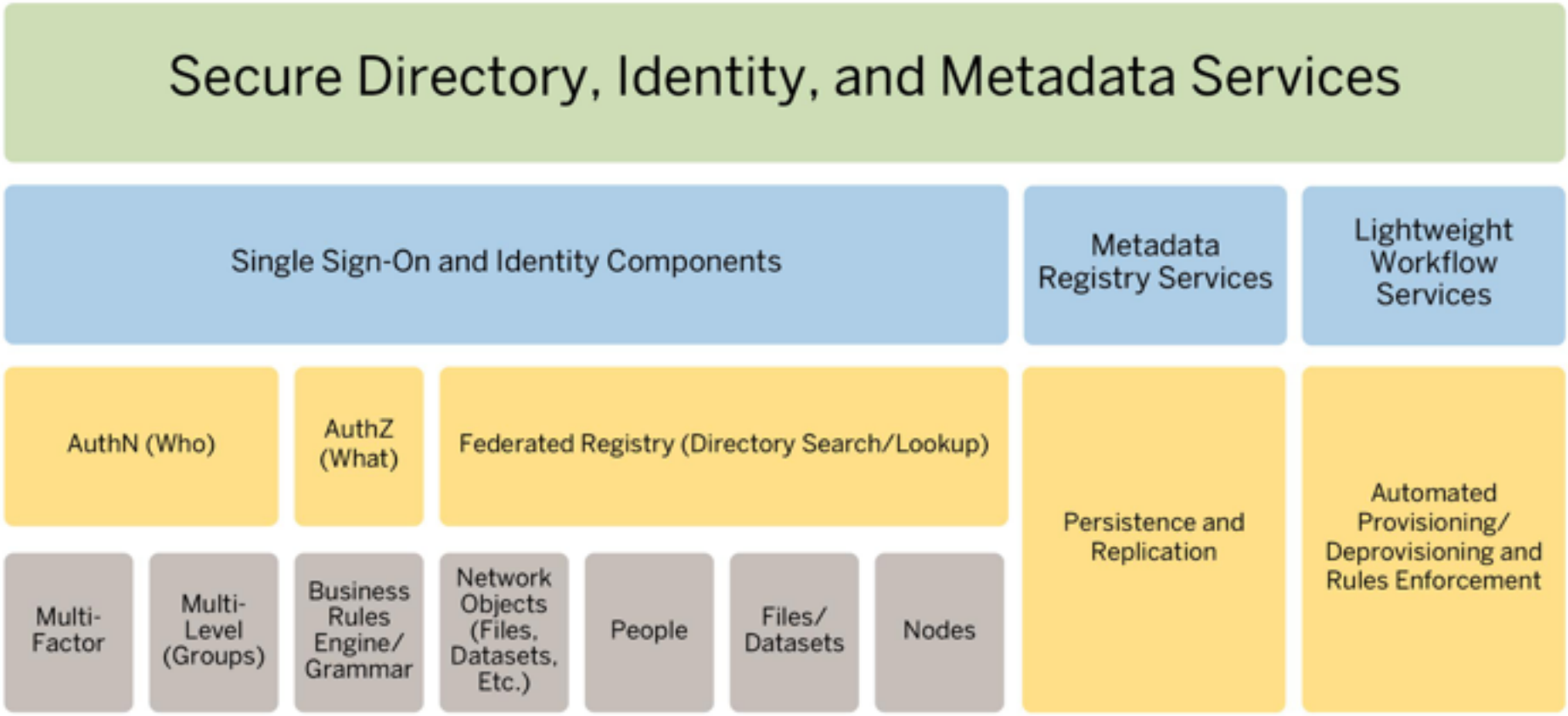
- Higher-education community created to accelerate maturity and broad adoption of IAM best practices
- The creation of TIER formally recognizes needs for IAM standards and practices in higher education
- TIER will aid in the creation of a sustainable support model for producing and maintaining tools needed to support the unique requirements of the higher-education identity ecosystem

Benefits of Harvard's membership in TIER include:

- Opportunities to help develop direction for standards and design
- Advance knowledge of components that TIER exists to sustain (including Shibboleth, InCommon, Grouper, and others key to Harvard's IAM mission)

The TIER Unified Model

TIER operates under a unified model of IAM services corresponding to the structure below.



TIER and Harvard's IAM Effort

Many of the IAM program's key projects relate directly to domains within TIER's unified model — for example:

- Authentication 

- Federated Registry 

- Automated Provisioning and Deprovisioning
- Groups 

- Multifactor Authentication 

This means not only that our mission-critical projects rely on services and technologies under TIER's purview, but also that the processes, workflows, and technologies we develop for IAM at Harvard can inform other TIER universities working on similar problems.

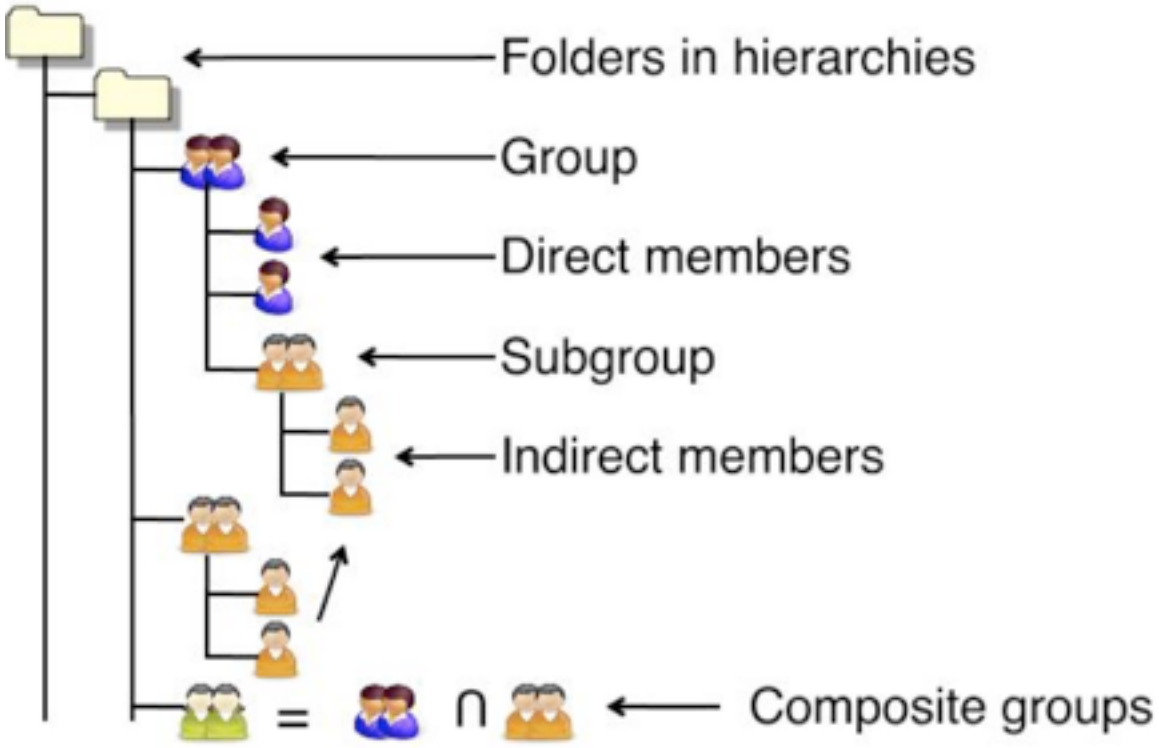
Major Projects for Harvard IAM: Grouper

IAM is implementing a new access management system using Internet2's Grouper, with rollout in tandem with the HarvardKey launch this autumn.

- Enterprise-scale access management that manages groups and group memberships
- The most suitable option for Harvard's highly distributed management environment, as well as our heterogenous technology environment
- Supports delegated group administration — meaning that because departments and teams can manage their own access control, HUIT will not need to be involved in everyday group and membership management
- As an Internet2 product supported by TIER, Grouper was built by the higher education community with our needs in mind — and is backed up by successful deployments in institutions worldwide

Major Projects for Harvard IAM: Grouper

Grouper's core concept includes hierarchies of groups, subgroups, and composite groups, with delegation of rights for group administration.



Grouper's Benefits for Harvard

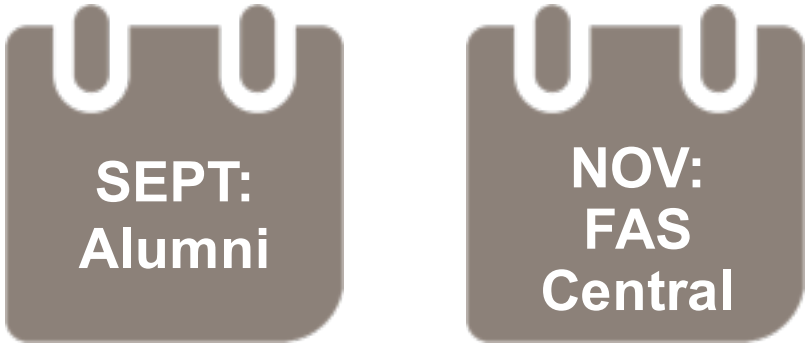
You can use groups created and maintained by Harvard IAM to support your own local groups.

- Because Grouper is integrated with the main IAM identity registry, IAM will build and maintain a set of fundamental groups
- IAM will also provide maintenance for locally defined and managed groups such as courses or collaboration groups
- Other systems and applications that need to access groups will be able to do so easily using a variety of methods:
  - A SAML or CAS authentication assertion
  - A multivalued attribute in LDAP
  - A RESTful API

Major Projects for Harvard IAM: HarvardKey

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

HARVARDKEY



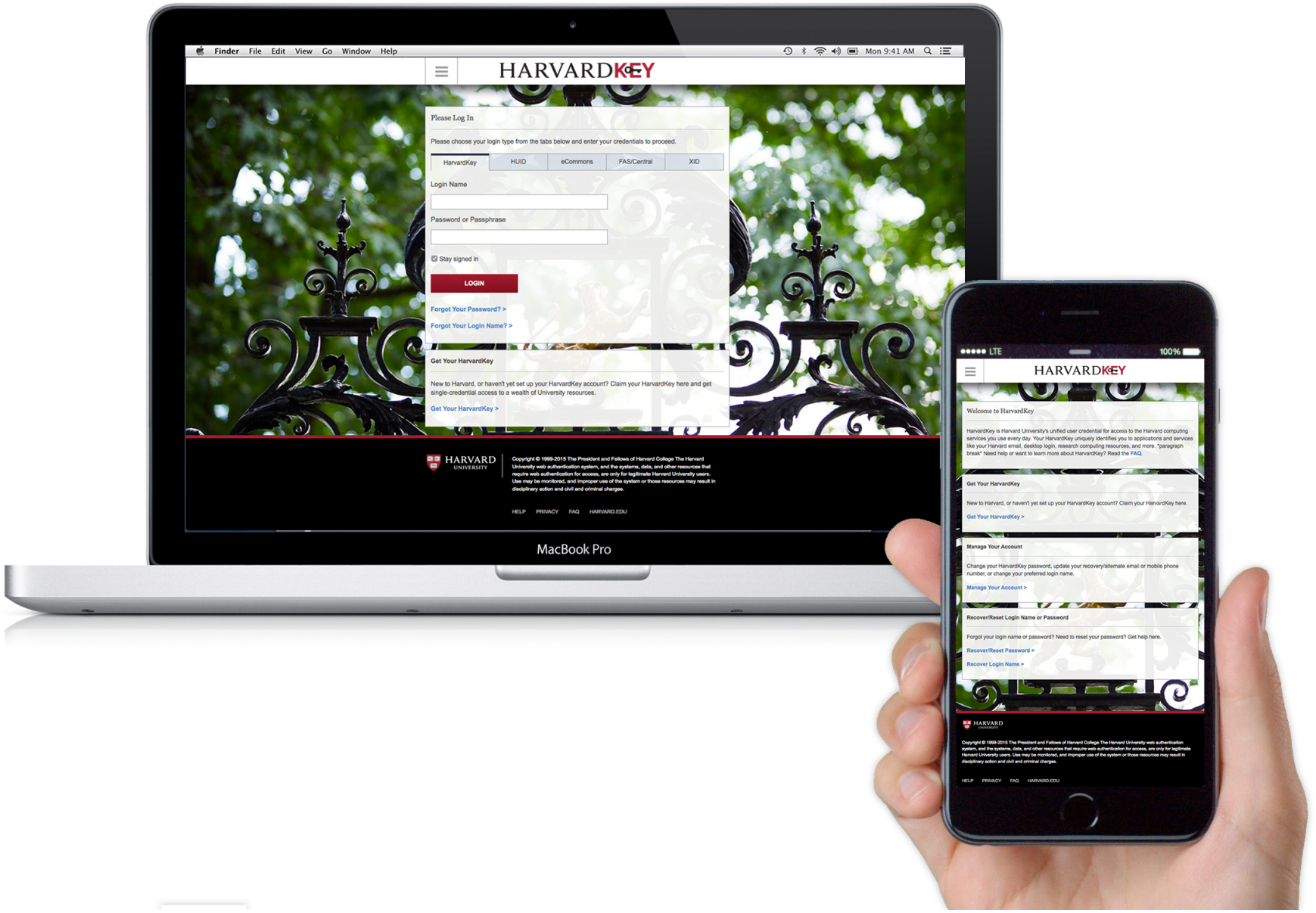
You'll see changes to the old PIN login screen beginning in September, with waves of user populations invited to activate a HarvardKey soon after:

- September 22, 2015: New HarvardKey self-service account management functions available to all Alumni users
- November 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

HarvardKey: The Benefits

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

HarvardKey: A Sneak Peek



In Summary: Supporting the Harvard Mission

- At times, Harvard on its own can feel like multiple institutions … but solutions such as HarvardKey, Grouper, InCommon federation and ORCID are addressing this:
  - One user credential
  - Attribute consolidation
  - Facilitating interoperability with external institutions
- Our users can work across organizational as well as institutional boundaries thanks to IAM solutions
- Our users' ability to assert their identities and attributes from anywhere in the world, at any time, facilitates collaboration — that's one thing that makes IAM in higher education unique
- Our membership in TIER supports collaboration in higher education as a whole as the community identifies and addresses important IAM needs and opportunities for standardization

Thank you!

HARVARD UNIVERSITY
Information Technology

Appendix

In Summary: Supporting the Harvard Mission

The IAM toolset — both custom solutions and tools supported by TIER — supports the critical goals supporting Harvard's teaching and research mission.

What Goal?	What Tool?
Give a credential to everyone who needs it	HarvardKey
Enable identities to work wherever researchers and scholars need to go	InCommon Federated Identity
Effective group management, including a distributed permissions manager meeting the needs of teachers, scholars, and researchers	Grouper
Provide users with added security beginning at the login screen	Multifactor Authentication (Duo)