Identity and Access Management
Technical Oversight Committee

April 16, 2015
Thursday
1:00-2:00 p.m.
6 Story Conference Room
Agenda

• Meeting Purpose and Intended Outcomes

• Approval of Previous Minutes (5 min)

• Chair’s Report & Executive Committee Summary (10 min)

• Shared Topics of Interest: POI Sponsored Affiliation (10 min)

• Shared Topics of Interest: HarvardKey (20 min)
  • Onboarding Workflow
  • Responsive Design
  • Walk-Through: HarvardKey Design Assets
  • UX Consistency Across HUIT

• General Discussion (15 min)
Purpose

• Present the latest status of the IAM Program Plan
• Provide update on POI sponsored affiliation process
• Discuss HarvardKey responsive design
• Examine UX consistency across HUIT strategic initiatives

Intended Outcomes

• Bring everyone up to date on processes for POI sponsored affiliations
• Demonstrate HarvardKey’s responsive design
• Better knowledge of how HarvardKey, SIS, and TLT demonstrate design consistency
March 12 Meeting

Topics

• Multifactor Authentication
• Email as Login Name
• Cloud Migrations

Action Items

• Refine communications strategy
• Investigate how Lync will interact with HarvardKey (since still on ICEMail)
Previous Minutes: Action Items

Research how Lync will work with HarvardKey (still on Icemail and use ADID to login at present)

- HUIT Unified Communications has a project underway to convert Lync to a cloud-based service using the same O365 credential pair
- The legacy Lync service will continue to use the University AD password, which will match to HarvardKey; the login name in this scenario is unique

Refine communications strategy

- In progress: ability for “production support” emails to go to technical staff prior to business owners
- In progress: methods for reaching out to various populations across the University about HarvardKey
Chair’s Report: Executive Committee

See the latest dashboard at iam.harvard.edu/executive-dashboard

- Program Status: Green
- Key points: Collapsing instances of IAM databases; HarvardKey design; lower environment cloud migration underway
Shared Topics: POI Sponsored Affiliation

Issue: Guest accounts contribute to identity proliferation

- FAS sponsored accounts in Waveset are local identities only without broader capabilities in the University
- We want to include these identities in IdDB (centralized identity registry)
- Establish smooth transitions as role changes occur over time
- Recognize existing University roles to avoid duplicate accounts

Solution: Integrate with simplified POI (person of interest) in MIDAS

- Add personae/roles to clearly define the person’s need for access and who they are — add the sponsored affiliation on the POI
- Use MIDAS to administer these identities
- Require DOB for better identity-proofing against existing records
- Move closer to the “one identity for life” paradigm
- Maps more closely to Internet2.edu and InCommon standards
- Integrate self-claiming of identity via HarvardKey
Shared Topics: POI Sponsored Affiliation

Same identity - evolving roles

• Once an identity is established, it will evolve with the addition of various roles
• This approach provides consistency and reduces the number of accounts issued

Example

• An employee sponsors the creation of an account for a contractor; contractor claims their account and is issued credentials
• Contractor is offered employment and has a new role added to the same identity
• The contractor role should be expired by the sponsor, but can coexist with employee role
• Adding other roles is also possible — for example, that one identity may also include DCE enrollment or multiple jobs
Expanding POI role types will provide a better match with how the identities are actually used.

- Clear definition of roles to be provided to sponsors/administrators
- Expanded roles may be tied to default service provisioning packages
- Sponsored roles will expire (but can be renewed)
Shared Topics: HarvardKey Onboarding Workflow

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 affiliation 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.

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.
Shared Topics: HarvardKey Responsive Design

HarvardKey will support desktop and mobile with equal fluency.

- Width-based, not device-based
- Multiple width “breakpoints”
- Content items follow a modular mental model
- Allows for greatest possible flexibility and future-proofing
Shared Topics: HarvardKey Responsive Design

Modular design will automatically adjust to fit the needs of the user’s device.

A = Header      B = Page Content      C = Footer

On both desktop and tablet in landscape, the page structure will follow the format outlined above. The header will span across the top of the page. Content will be displayed in a multi-column format the width of the page. A standard footer will be included at the bottom of the page.

Page content will primarily live in either a single or double column and the footer will remain at the bottom of the page.

For the smallest screen size, mobile in portrait orientation, the page structure will fall into a single column format. Page content will be displayed in a single column format.
Shared Topics: HarvardKey Responsive Design

Content in these modules can be combined or rearranged as needed, but together create a cohesive pattern with which users will become familiar.
Shared Topics: HarvardKey Responsive Design

Let’s try it out!

Welcome/Options Screen:
http://tinyurl.com/harvardkey-welcome

Login Screen:
http://tinyurl.com/harvardkey-login

Setup (User Type):
http://tinyurl.com/harvardkey-usertype

Set Password:
http://tinyurl.com/harvardkey-setpassword
Walk-Through: HarvardKey Design Assets

Major use cases for HarvardKey:

• Claim an account (new users)
• Manage an existing account (existing users)
• Sign in to protected applications (existing users)
HarvardKey Walk-Through: Claim an Account
HarvardKey Walk-Through: Claim an Account

Enter Your Alumni Identity Information

HAA ID: What is my HAA ID?
12345678

Last Name

First Name

Year of Graduation

Quit Registration Process Continue
HarvardKey Walk-Through: Claim an Account

Identity Confirmed

Your record has been successfully identified.

Check your [type] email address for an email with a validation passcode and instructions to complete your account registration process.

If you do not use your passcode within the next 24 hours, it will become invalid. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Enter Your Passcode

Copy stating to enter the passcode that was received in the email. Nulla ut mauris at diam tempor cursus nec ot noque.

Passcode

12345978

Submit
HarvardKey Walk-Through: Claim an Account
HarvardKey Walk-Through: Claim an Account
HarvardKey Walk-Through: Claim an Account

Password Rules
Copy about making sure your password is strong enough.

No Personal Information:
Your password should not contain any of your personal information such as email address, your first, middle or last name, or the parts of your address like street name, city, or state name.

No common words with 4 or more letters:
There should not be common words in forward or backward order (i.e. ‘Tree’ or ‘eert’). Common words can also be words found within dictionary.

No number sequences with 4 or more numbers:
There should not be a sequences of numbers in forward or backward order (i.e. 1234, 9876)

Still need password assistance?
Please contact HarvardKey at harvardkeyhelp@harvard.edu
All other inquiries should be directed to the Online Help Desk at helpdesk@harvardkey.com or 800-000-0000

Close
HarvardKey Walk-Through: Manage Existing Account
HarvardKey Walk-Through: Manage Existing Account

Account Management

Copy instruction providing details around account management. Aenean eget pulvinar odio, et aliquet quam.

I need to...

Update my password
Change Password >

Update my recovery Primary email, Alternative email or Mobile Phone Number
Change Recovery Information >

Change my Login ID (Preferred Email)
Change Preferred Login Name >
HarvardKey Walk-Through: Application Sign-In
HUIT Guiding Principles for User Experience

1. Perform similar tasks in similar ways
2. Navigate seamlessly across applications
3. Apply common branding, look, and feel
4. Leverage a common mental model
HUIT Cross-Program UX Review

Perform similar tasks in similar ways
• Manage distinctions between app functions by focusing on shared UX components

Navigate seamlessly across applications
• Transition from authentication screen to a protected application minimizes differences between the two interfaces

Apply common branding, look, and feel
• Create continuity across applications by using unified branding
• Harmonize design wherever possible

Leverage a common mental model
• Use shared user personas and industry conventions

For IAM
• Present a minimal interface with few major UX elements
Guiding Principle: Focus on Shared UX Components

Navigation and wayfinding

• All user options should be visible on page load
• No “hidden” menus
Guiding Principle: Focus on Shared UX Components

The user input form is the common component used in all applications.

- User inputs presented using similar layout choices
- Inline validation of form inputs
- Layering of UI with internal windows
- Use of color for call-to-action elements
Guiding Principle: Focus on Shared UX Components
Guiding Principle: Focus on Shared UX Components

Welcome to HarvardKey

Copy instruction providing details around login details for users who currently exist in Harvard community.

<table>
<thead>
<tr>
<th>HarvardKey</th>
<th>HUID</th>
<th>FAS / Central</th>
<th>XID / Login</th>
<th>eCommons</th>
</tr>
</thead>
</table>

Login Name

Password

✔ Stay signed in

LOGIN

I Forgot My Login Name
I Forgot My Password
Guiding Principle: Navigate Seamlessly Across Apps
Guiding Principle: Apply Common Branding
Guiding Principle: Apply Common Look and Feel

Harmonize design choices to create a consistent look and feel

Consistent typography

• Serif typefaces used only in branding contexts
• Sans serif for body text

Consistent color usage

• Color palette limited to Harvard’s preferred web-safe colors
• Exception: Standard red and green for alert feedback messaging
Guiding Principle: Apply Common Look and Feel
Guiding Principle: Leverage a Common Mental Model

Break with design and usability norms only when use cases require it

- All applications make use of “web-common” page layout and structure
- Iconography and call-to-action signals are familiar to the user
- Use patterns drive implementation choices
Thank you!
Appendix A
Technical Oversight Committee Members
# Technical Oversight Committee Members

**Chair:** Magnus Bjorkman, Director of IAM Engineering

<table>
<thead>
<tr>
<th>Name</th>
<th>School/Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indir Avdagic</td>
<td>SEAS</td>
</tr>
<tr>
<td>Carolyn Brzezinski</td>
<td>SIS</td>
</tr>
<tr>
<td>Steve Duncan</td>
<td>Harvard Kennedy School</td>
</tr>
<tr>
<td>David Faux</td>
<td>HUIT Admin Tech/FAS &amp; College</td>
</tr>
<tr>
<td>Dan Fitzpatrick</td>
<td>Partners</td>
</tr>
<tr>
<td>Eileen Flood</td>
<td>Campus Services</td>
</tr>
<tr>
<td>Tim Gleason</td>
<td>HUIT IAM/AD</td>
</tr>
<tr>
<td>Sherif Hashem</td>
<td>Harvard Law School</td>
</tr>
<tr>
<td>Ken Ho</td>
<td>GSE</td>
</tr>
<tr>
<td>Yadhav Jayaraman</td>
<td>Harvard Business School</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>School/Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tyson Kamikawa</td>
<td>Harvard Medical School</td>
</tr>
<tr>
<td>Colin Murtaugh</td>
<td>HUIT Academic/TLT</td>
</tr>
<tr>
<td>Micah Nelson</td>
<td>HUIT Security</td>
</tr>
<tr>
<td>Rich Ohlsten</td>
<td>HUIT Admin Tech/Alumni</td>
</tr>
<tr>
<td>Brian Pedranti</td>
<td>HSPH</td>
</tr>
<tr>
<td>Jonah Pollard</td>
<td>Unified Communication/Cloud</td>
</tr>
<tr>
<td>Sara Sclaroff</td>
<td>HUIT Admin Tech/HR</td>
</tr>
<tr>
<td>Randy Stern</td>
<td>Library IT</td>
</tr>
</tbody>
</table>