Identity and Access Management
Technical Oversight Committee

February 5, 2015
Thursday
3:00-4:00 p.m.
6 Story Conference Room
Agenda

• Meeting Purpose and Intended Outcomes
• Approval of Previous Minutes (5 min)

Chair’s Report & Executive Committee Summary (15 min)

• Shared Topics of Interest: HarvardKey (15 min)
  • Credential vs. ID
  • Vocabulary Quiz
  • Onboarding/Reboarding, New LDAP
  • PIN2 Token Example

• Shared Topics of Interest: Multifactor Authentication (15 min)
  • Flow, Components, Integration Strategies

• General Discussion (10 min)
Meeting Purpose and Intended Outcomes

Purpose

• Present the latest status of the IAM Program Plan
• Discuss details of HarvardKey rollout
• Examine implementation of multifactor authentication

Intended Outcomes

• Greater clarity on proceeding with HarvardKey rollout, plus discovery of any local technical issues
• Better knowledge of Harvard’s MFA implementation
October 2 Meeting

- Expansion of Identity Data Model
- Identity Service
- Connecting to Local Targets
- Database to Cloud

**Action Item**: Publish the existing IdDB model

**Action Item**: Discover/cost the data transfers needed for customer actions in the cloud

Approval of Previous Minutes
Previous Minutes: Action Items

• Publish the existing IdDB model
  • http://tinyurl.com/idmrw-iddbprod

• Discover/cost data transfers needed for customer actions in the cloud
  • Based on a real-world example, we estimate 300GB of data transfers per month after we have scaled up: $25
  • Transfer costs are currently <1% of our bill
  • All data costs at our boundary (AWS Account) and in will be carried by us
  • Costs on customer networks (either on-premise or at another provider) will be carried by the customer
  • You can go to the following calculator to estimate costs: http://calculator.s3.amazonaws.com/index.html
Chair’s Report: Executive Committee

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

- Program Status: Green
- Key points: PIN3 decommissioned, SHA-2 upgrade, Alumni/FAS/HMS work continues apace
We are poised for an initial rollout in June with waves by *user population*, not application.

Additional user populations will follow, with full rollout anticipated within an 18-month window.
Credential vs. ID

Credential:
• What the users see and use
• Login name, password, and potential second factor
• In time, HarvardKey will be the single credential in use by end users

ID:
• What the applications use
• In the past, sometimes the credential and the ID have been the same — but we are separating them going forward
• We will keep (and keep supplying as needed) old IDs for backward compatibility with some applications
• HUID, ADID, XID, eCommons, Post, etc.
• Going forward, UUID will be the preferred ID
## Vocabulary Quiz

Understanding how we are using the terms below

<table>
<thead>
<tr>
<th>Term</th>
<th>How Used</th>
<th>Examples</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login name</td>
<td>Used as the login ID</td>
<td>Email-eligible user: <a href="mailto:jay_hill@sph.harvard.edu">jay_hill@sph.harvard.edu</a></td>
<td>When a user logs in using HarvardKey, the system will expect the user to enter this login name and its related password</td>
</tr>
<tr>
<td></td>
<td>Expected to be the Harvard email address, can be another for Alumni or sponsored accounts</td>
<td>Sponsored collaborator: <a href="mailto:jayhill@stanford.edu">jayhill@stanford.edu</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alumnus/alumna: <a href="mailto:coolguyjay@comcast.net">coolguyjay@comcast.net</a></td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>System-assigned identifier</td>
<td>Sam Account: ADID = jeh454</td>
<td>Permanently assigned value enables prestaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UNIX LDAP: UID = jeh454</td>
<td></td>
</tr>
<tr>
<td>Harvard email address</td>
<td>Harvard-assigned email</td>
<td><a href="mailto:username@optionalsubdomain.harvard.edu">username@optionalsubdomain.harvard.edu</a></td>
<td>Users chooses value on left of @ sign as part of self-service account claim &amp; onboarding process</td>
</tr>
<tr>
<td>FAS name</td>
<td>Legacy username for FAS person</td>
<td>jayhill</td>
<td>Former names will exist as mapped attributes</td>
</tr>
<tr>
<td>Google name</td>
<td>Google username</td>
<td><a href="mailto:jayhill@g.harvard.edu">jayhill@g.harvard.edu</a> (always scoped)</td>
<td>Since Google accounts can’t be changed without content loss, some will keep accessing via old names</td>
</tr>
<tr>
<td>{School} name</td>
<td>Local username(s)</td>
<td>[we want to accomodate values when necessary]</td>
<td>Local usernames are mapped to identity as additional attributes</td>
</tr>
</tbody>
</table>
Non-Alumni User Populations, by Waves (Wave 1: FAS/Central, June 15)

Existing Users

1. Reboard

 Finished!

New Users

1. Onboard
2. Request Access to Resources

 Finished!

Alumni Users (Single Wave: July 15)

1. Onboard

 Finished!
Notes on the HarvardKey onboarding/reboarding workflow:

• Order of HarvardKey migration is keyed to user populations, *not* individual applications

• Within 18 months, every Harvard Community user will be prompted to onboard or reboard

• Design and branding changes will be applied to the login screen in two stages:
  • *June 2015*: New Account Management functions and core HarvardKey branding
  • *6 months after final user population enabled*: Implement lessons learned from design and branding changes, remove redundant login types
New Harvard LDAP (HLDAP) deployed in the cloud

• HLDAP schema containing both identity data and credentials within the same branch

• Credentials and identity data contained in HLDAP are updated incrementally via IIQ

• HLDAP will contain new credentials for SSO access to Harvard applications

• HLDAP will not be used for the old HUID-based access; existing HU and AUTH LDAPs will be slowly phased out

• New HLDAP utilizes cloud features:
  • Fully automated creation, such that a new version can be built and deployed without worry of configuration consistency, etc.
  • Automated scaling depending on access load
  • Built-in health checking and self-healing
Reboarding & New LDAP

Harvard LDAP on AWS:

More details: [http://tinyurl.com/hldap-aws](http://tinyurl.com/hldap-aws)
PIN2 token contains authenticated user’s identifier (e.g. HUID) and login type (e.g. PIN), which directly map login type used for login.

How to construct PIN2 token when using HarvardKey?

• Read all identity attributes (HUID, eCommons ID, Alumni Advance ID, etc.) of login user, and map these attributes to login types

• Read login types supported by application user is accessing

• Find intersection between attribute-mapped and application-supported login types

• Determine effective PIN2 token login ID and type from intersection:
  • If intersection is empty, then authentication will fail
  • If intersection is just one login type, then that login type will be used in PIN2 token
  • If more than one type found, then one login type will be used in PIN2 token based on predefined rules
Multifactor Authentication (MFA) is a type of authentication that requires a 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 username/password authentication.
Shared Topics of Interest: Multifactor Authentication

Multifactor authentication flow

User requires authentication

Provide first-factor username & password

Is first factor valid?

Yes

Is second factor required?

Yes

Enrolled for second factor?

Yes

Provide second factor

No

Authentication success

Is second factor valid?

Yes

Authentication failure

No

Ask user to use self-service app to enroll
Shared Topics of Interest: Multifactor Authentication

Components involved in MFA
Shared Topics of Interest: Multifactor Authentication

MFA integration strategies:

• Application requires MFA
  • Application registration will be extended to support this

• User prefers MFA
  • User will use our self-service app to set the preference

• Application requires MFA for some users (e.g. Admin User)
  • A group management tool will be used to support this requirement

We will introduce MFA to a selective small set of users first before releasing it to the larger user base.
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>