Identity and Access Management
Technical Oversight Committee
Agenda

• Meeting Purpose and Intended Outcomes
• Approval of Previous Minutes (5 min)
• Chair’s Report & Executive Committee Summary (10 min)
• Shared Topics of Interest: MFA Update (5 min)
• Shared Topics of Interest: Login Name and SaaS (5 min)
• Shared Topics of Interest: PIN/CAS/IdP & Cloud HU-LDAP (20 min)
• General Discussion (15 min)
Meeting Purpose and Intended Outcomes

Purpose

• Present the latest status of the IAM Program Plan
• Provide update on MFA vendor selection and implementation
• Discuss login name and SaaS
• Talk about PIN/CAS/IdP and cloud Harvard LDAP

Intended Outcomes

• Bring everyone up to date on progress of IAM’s MFA work
• Better knowledge of interaction between login name and SaaS applications
• Clarify relationship between PIN/CAS/IdP and the cloud Harvard LDAP
Approval of Previous Minutes

February 5 Meeting

- PIN3 Decommissioning
- InCommon Bronze
- HarvardKey
- Multifactor Authentication
- **Action Item:** Distribute communications strategy
- **Action Item:** Investigate how third-party service providers work using non-Harvard domains for login
- **Action Item:** Look into MFA vendor for federation in Schools
Previous Minutes: Action Items

Distribute communications strategy (including for application owners and different business owners)

- Developing general steps to be used, but strategy will be tailored to each rollout population
- Starting outreach to all PIN app owners — Town Hall meeting is in late March

Think about how third-party service providers would work with using non-Harvard domains for login, e.g. O365

- Addressed as a discussion topic in today’s meeting

Look into MFA vendor ability to use federation in schools, so same app on phone does all

- Addressed as a discussion topic in today’s meeting
Chair’s Report: Executive Committee

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

- Program Status: Green
- Key points: Cloud Harvard LDAP deployed, Alumni API completed, HMS analysis continues, PI-2 demo March 10
MFA vendor selection criteria:

- Must be deployable in our own infrastructure
- Flexible provisioning and deprovisioning of users
- Integrates with multiple platforms — especially the ones in which we are interested

Why not use Google Authenticator?

- Can’t be deployed in our own infrastructure
- Many campuses were burned by “lost key” and switched vendors

ADFS support:

We are considering two vendors for POC:

- Toopher supports ADFS
- Callsign is working on ADFS support

MFA POC will be completed in PI-3 (June), and should be available in production in PI-4 (Fall).
Benefits of using an email address as the login name:

- Easy to remember — it’s your Harvard email address
- Provides a degree of personalization
- Common practice in many consumer applications today

An overall improved experience, even considering challenges:

- Longer to type
- Not compatible with all systems, such as UNIX command-line
- Assumptions on user scoping may be made by some applications, such as Office 365 and Windows Azure

Example of a HarvardKey login name:

- tim_gleason@harvard.edu
- tdg396 is the assigned UID alternative
Shared Topics: Login Name and SaaS

HarvardKey support for external federation

- InCommon and other federations refer the user to the HarvardKey login page based on a user selection
- The Office 365 generic login screen attempts to determine the “home” authentication system by the email domain; domains are scoped to the Harvard authentication provider
Shared Topics: Login Name and SaaS

HarvardKey support for external federation:

- HarvardKey login name with an @harvard and associated subdomains function as expected
- Without the domain selection option, non-Harvard email domains in the HarvardKey are not valid in many SaaS applications:
  - user@gmail.com cannot be made to resolve to Harvard
- An alternative Harvard-assigned address will be issued based on the unique UID value:
  - abc1234@harvard.edu is an alternative address
- Ideally, a current Harvard user should be using a Harvard email address as his or her HarvardKey login name
Shared Topics: AuthN/CAS/IdP & HLDAP to Cloud

Moving the new AuthN/CAS/IdP and HLDAP (consolidated LDAP for HarvardKey) to the cloud has a number of benefits:

• Improved availability
  • #1: Active-active HA across two data centers
  • #2: DR across regions
• Improved security
  • Key management services
  • Improved encryption of disks and configuration
  • Additional best practices for storing passwords in LDAP
  • Working with Security group for additional cloud firewalls and outgoing proxies for active monitoring for malicious traffic
High-Level System Context

Availability Zone 1
- PIN/CAS/IdP
  - Elastic Load Balancer
  - PIN/CAS/IdP
- LDAP
  - Elastic Load Balancer
  - Harvard LDAP

Availability Zone 2
- PIN/CAS/IdP
  - Elastic Load Balancer
  - PIN/CAS/IdP
- LDAP
  - Elastic Load Balancer
  - Harvard LDAP
AuthN/CAS/IdP System Context

VPC

PIN/CAS ELB Security Group

Public Subnet

IdP ELB Security Group

Public Subnet

CACHE

PIN/CAS Security Group

PIN/CAS Autoscaling Group

CACHE

IdP Security Group

IdP Autoscaling Group

Private App Subnet

Availability Zone 1

Private App Subnet

Availability Zone 2
AuthN/CAS/IdP Instance Setup
HLDAP System Context
HLDAP Master System Context

1. ELB
   ldap-master.iam.harvard.edu

2. LDAP Master Server
   Auto-Scaling Group with 1 node
   CloudWatch
   (Monitors Availability Performance)

3. Mirrored, Encrypted EBS Volume
4. Splunk
   Database & Logs Backup
   Versioned, Encrypted S3 Store

Private Network Interface
Allocated for Master Servers

Route 53 Record
ldap-master1.iam.harvard.edu

Email
Alerting
Across Region DR

AWS

PIN/CAS/IdP Elastic Load Balancer

PIN/CAS/IdP

Harvard LDAP

Availability Zone 1
West Coast

Availability Zone 1
East Coast

PIN/CAS/IdP

LDAP Elastic Load Balancer

PIN/CAS/IdP

Harvard LDAP

Availability Zone 2
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>
<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>