HARVARD UNIVERSITY
Information Technology

Identity and Access Management
Technical Oversight Committee

March 12, 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: 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

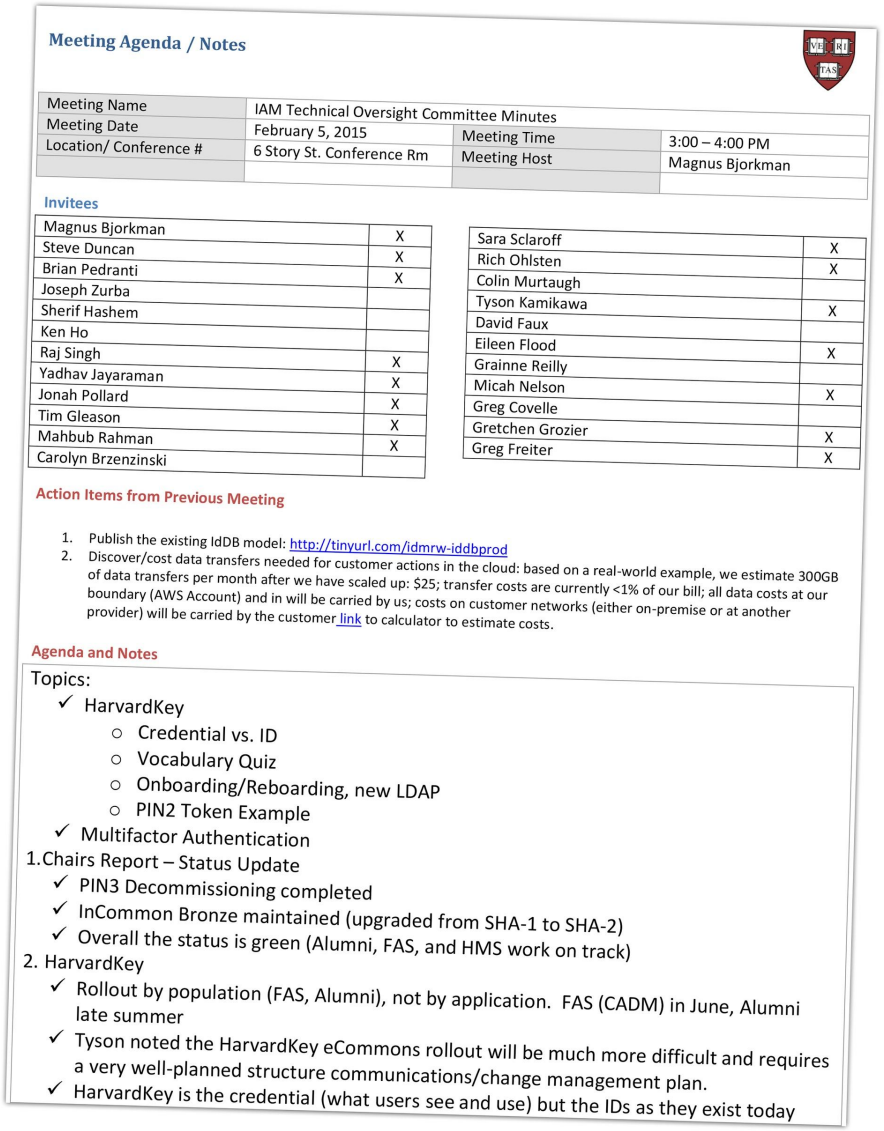
Intended Outcomes

- 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



Meeting Agenda / Notes

Meeting Name	IAM Technical Oversight Committee Minutes		
Meeting Date	February 5, 2015	Meeting Time	3:00 – 4:00 PM
Location/ Conference #	6 Story St. Conference Rm	Meeting Host	Magnus Bjorkman

Invitees

Magnus Bjorkman	X	Sara Sclaroff	X
Steve Duncan	X	Rich Ohlsten	X
Brian Pedranti	X	Colin Murtaugh	
Joseph Zurba		Tyson Kamikawa	X
Sherif Hashem		David Faux	
Ken Ho		Eileen Flood	X
Raj Singh	X	Grainne Reilly	
Yadhav Jayaraman	X	Micah Nelson	X
Jonah Pollard	X	Greg Covelle	
Tim Gleason	X	Gretchen Grozier	X
Mahbub Rahman	X	Greg Freiter	X
Carolyn Brzenzinski			

Action Items from Previous Meeting

1. Publish the existing IdDB model: http://tinyurl.com/idmrw-iddbprod
2. 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 link to calculator to estimate costs.

Agenda and Notes

Topics:
- ✓ HarvardKey
  - Credential vs. ID
  - Vocabulary Quiz
  - Onboarding/Reboarding, new LDAP
  - PIN2 Token Example
- ✓ Multifactor Authentication

1.Chairs Report – Status Update
- ✓ PIN3 Decommissioning completed
- ✓ InCommon Bronze maintained (upgraded from SHA-1 to SHA-2)
- ✓ Overall the status is green (Alumni, FAS, and HMS work on track)

2. HarvardKey
- ✓ Rollout by population (FAS, Alumni), not by application. FAS (CADM) in June, Alumni late summer
- ✓ Tyson noted the HarvardKey eCommons rollout will be much more difficult and requires a very well-planned structure communications/change management plan.
- ✓ HarvardKey is the credential (what users see and use) but the IDs as they exist today

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

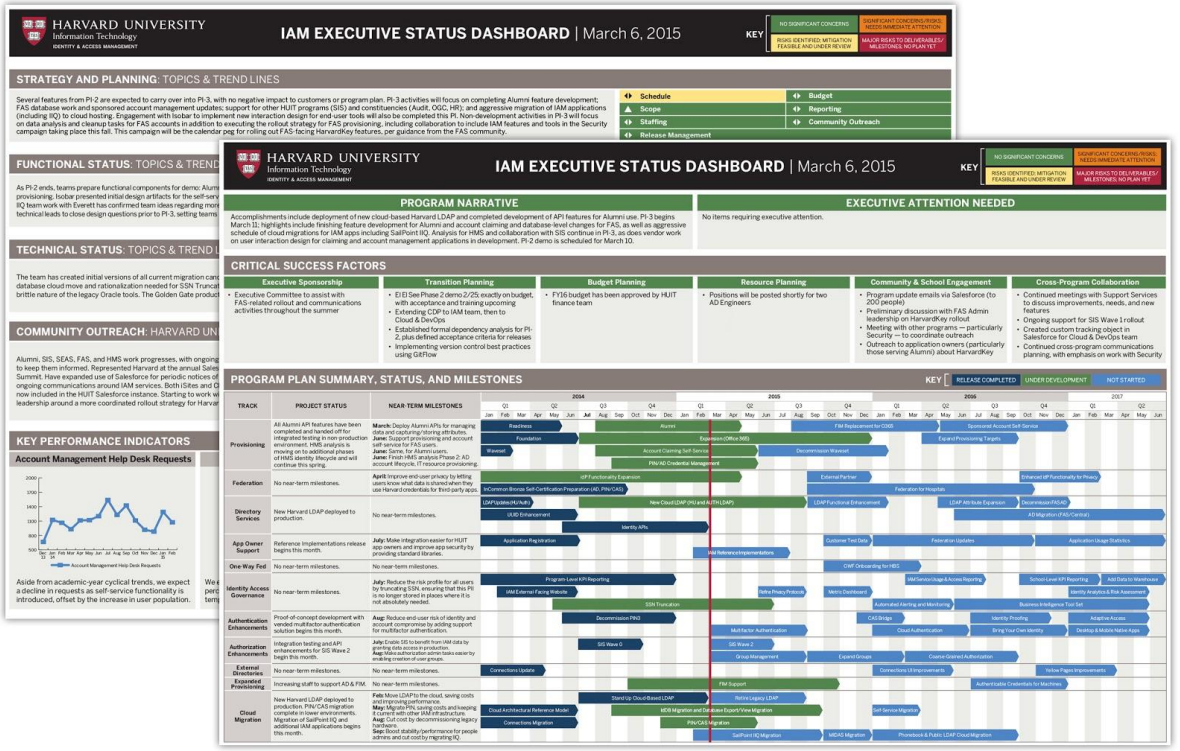
- Addressed as a discussion topic in today's meeting

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

Shared Topics: MFA Update

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).

Shared Topics: Login Name and SaaS

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

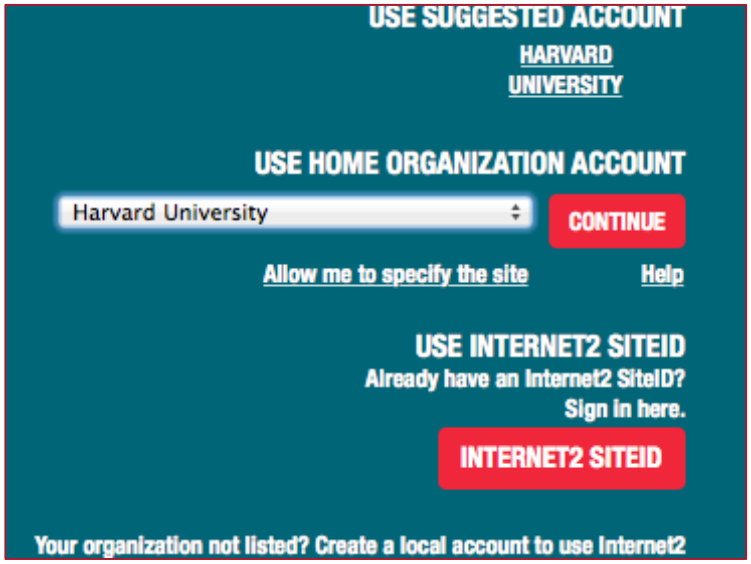
Example of a HarvardKey login name:

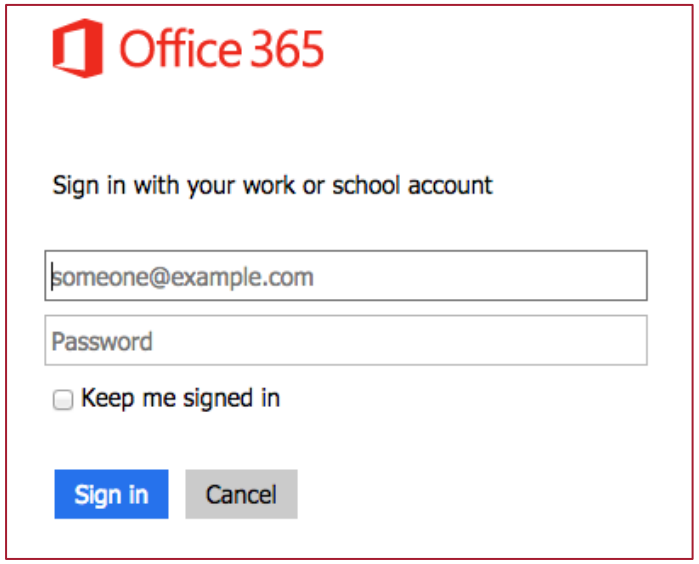
- *tim_gleason@harvard.edu*
- *tdg396* is the assigned UID alternative

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:

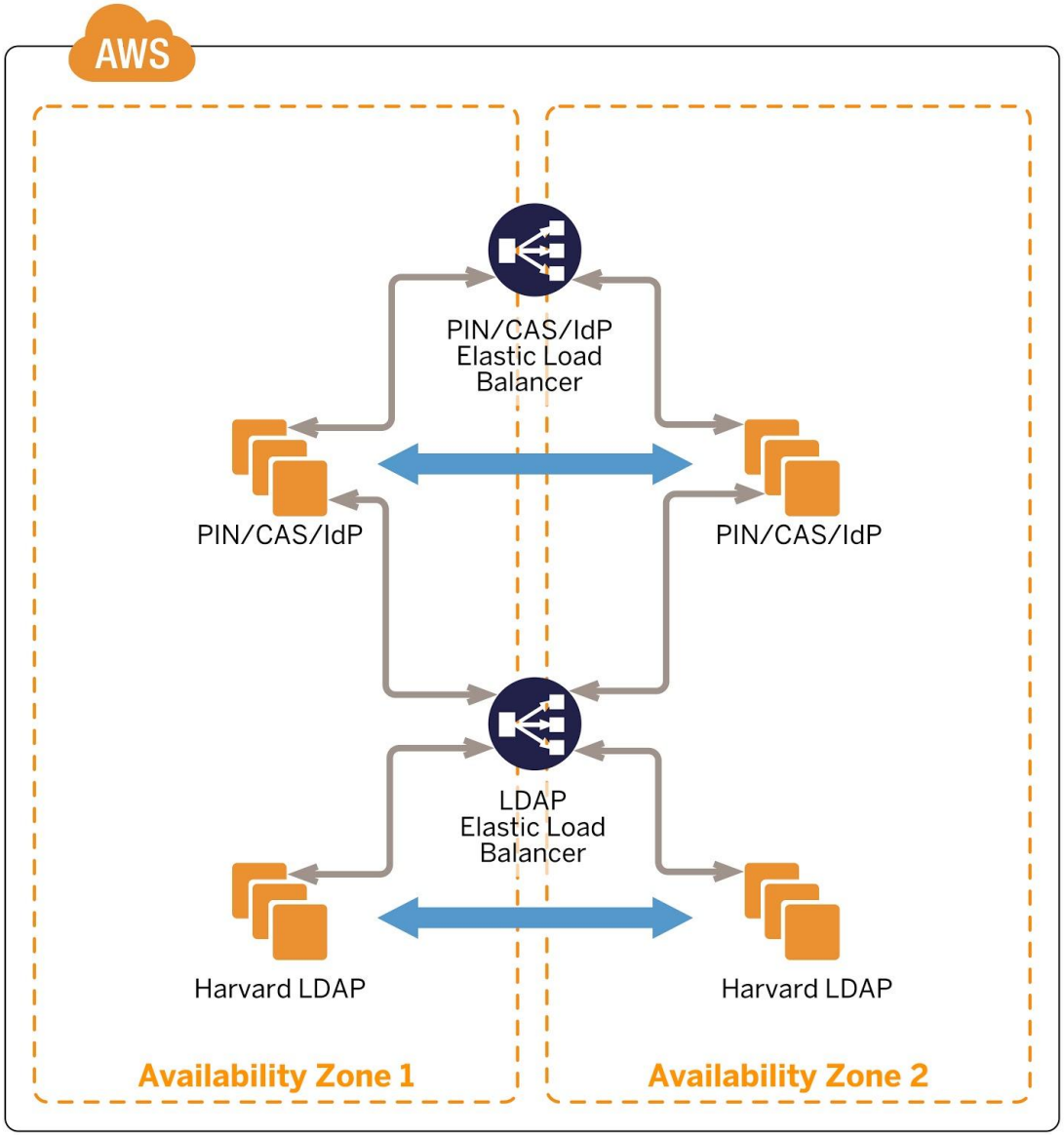
- **HarvardKey login name with an @harvard and associated subdomains function as expected**
- Without the domain selection option, non-Harvard email domains in the HarvardKey are not valid in many SaaS applications:
  - *user@gmail.com* cannot be made to resolve to Harvard
- An alternative Harvard-assigned 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

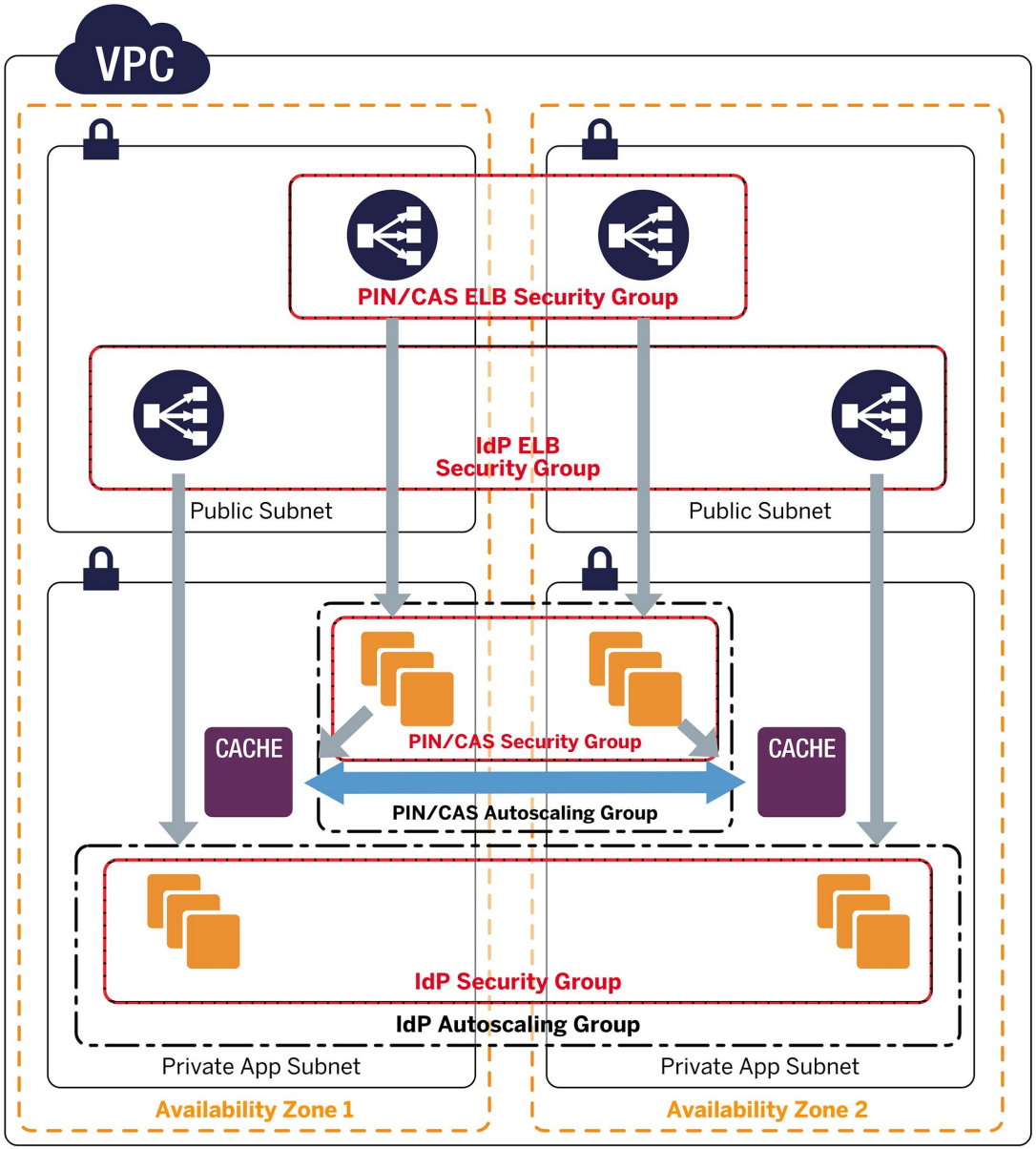
Moving the new AuthN/CAS/IdP and HLDAP (consolidated LDAP for HarvardKey) to the cloud has a number of benefits:

- 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

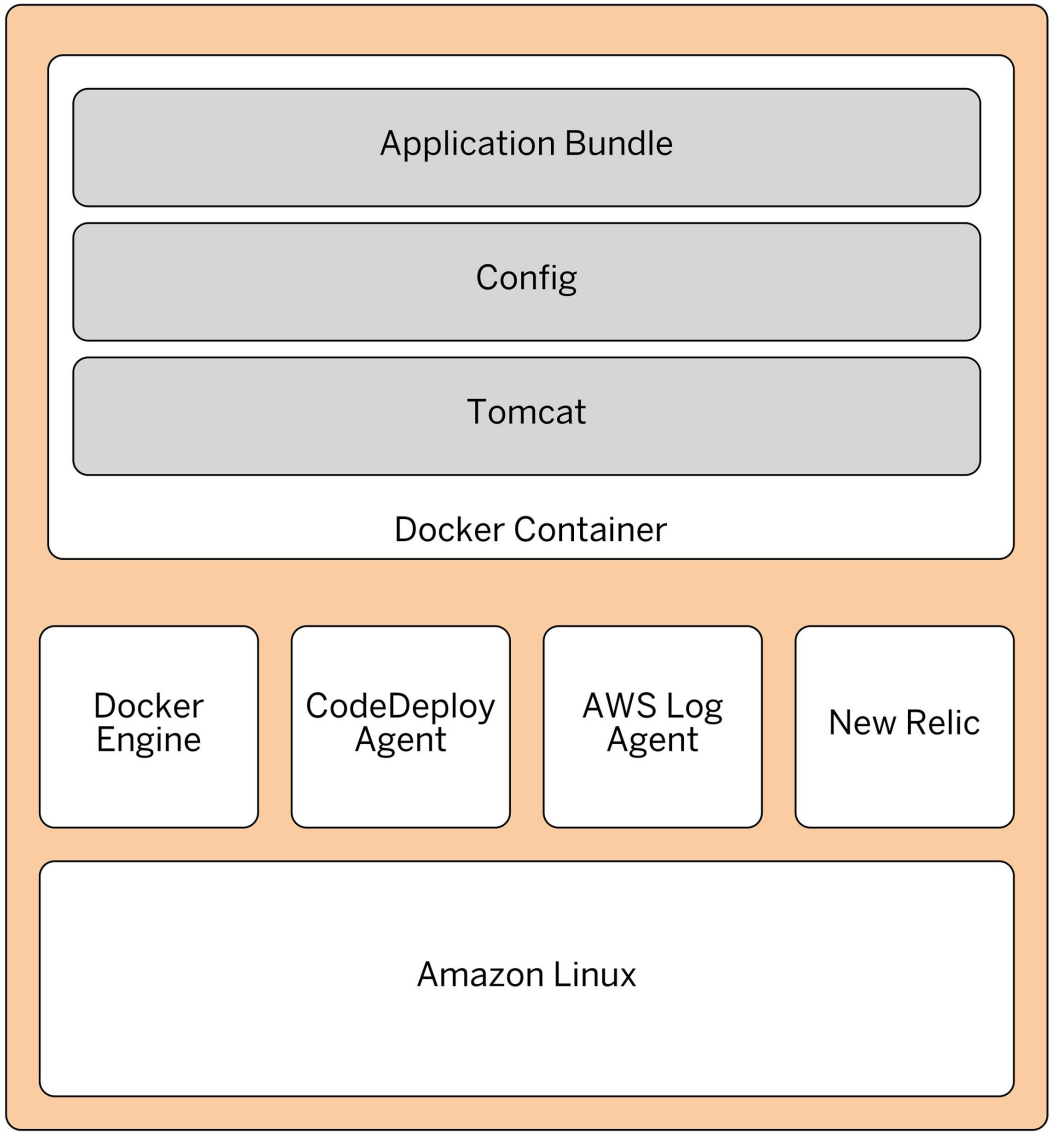
High-Level System Context



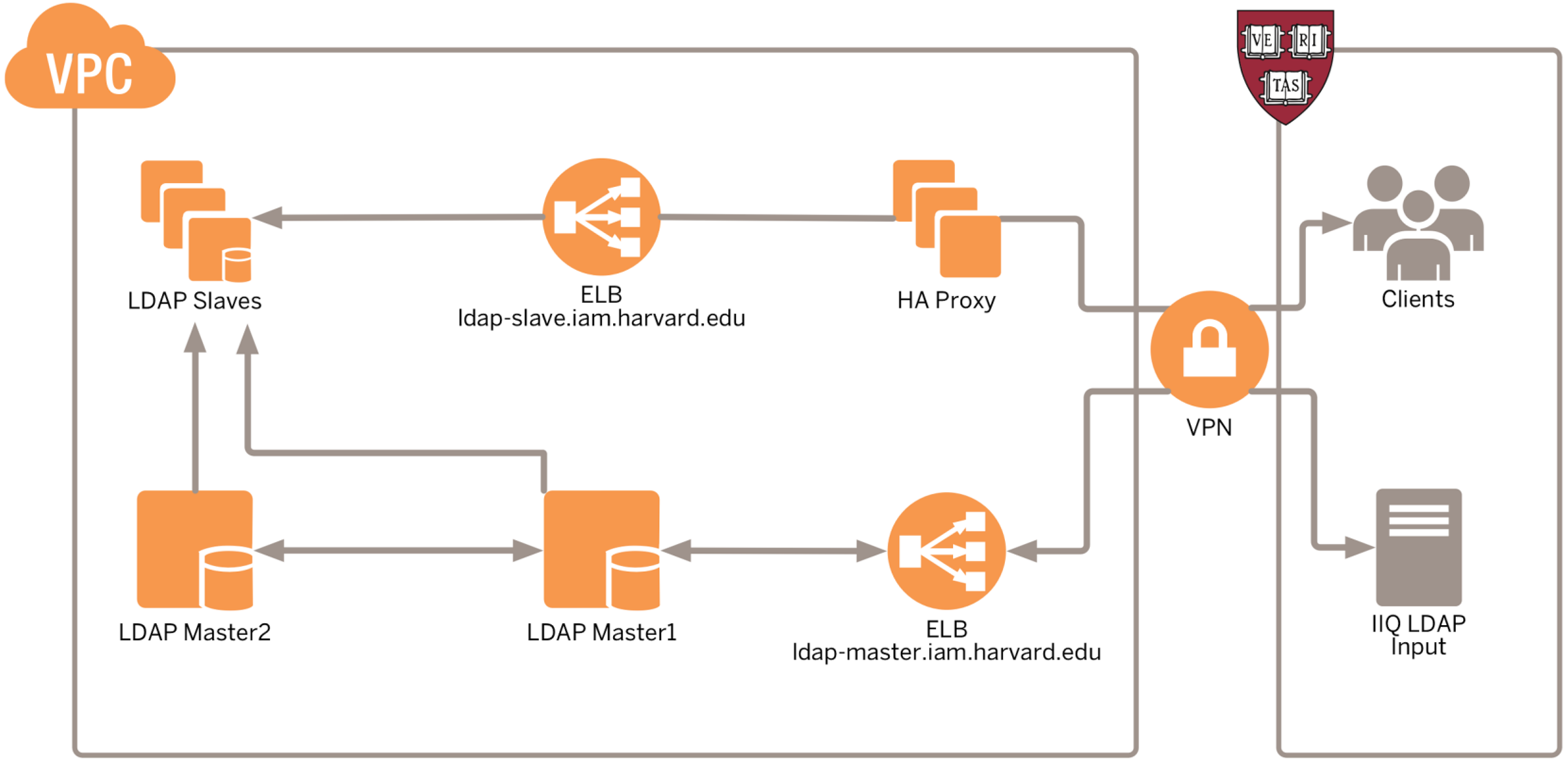
AuthN/CAS/IdP System Context



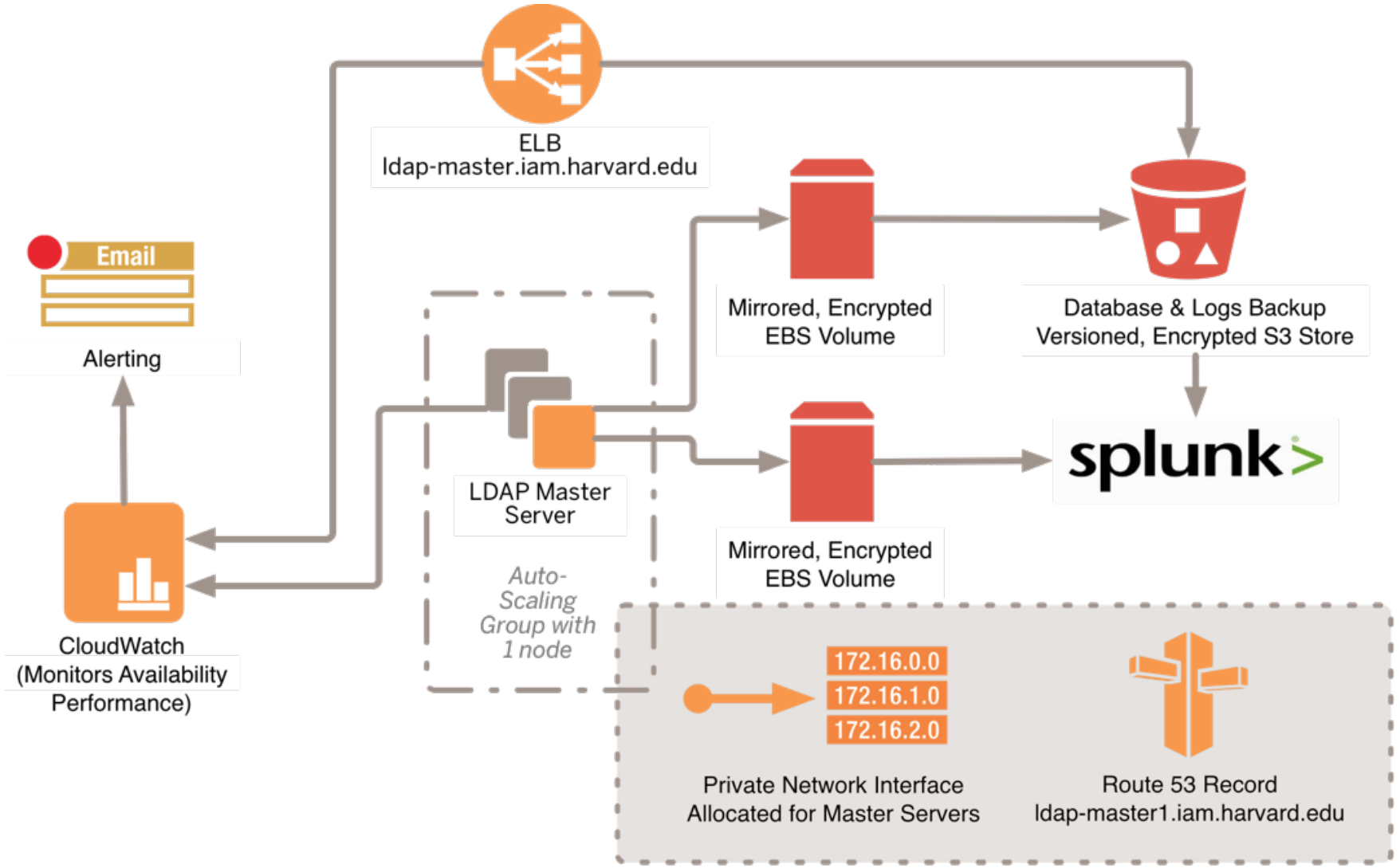
AuthN/CAS/IdP Instance Setup



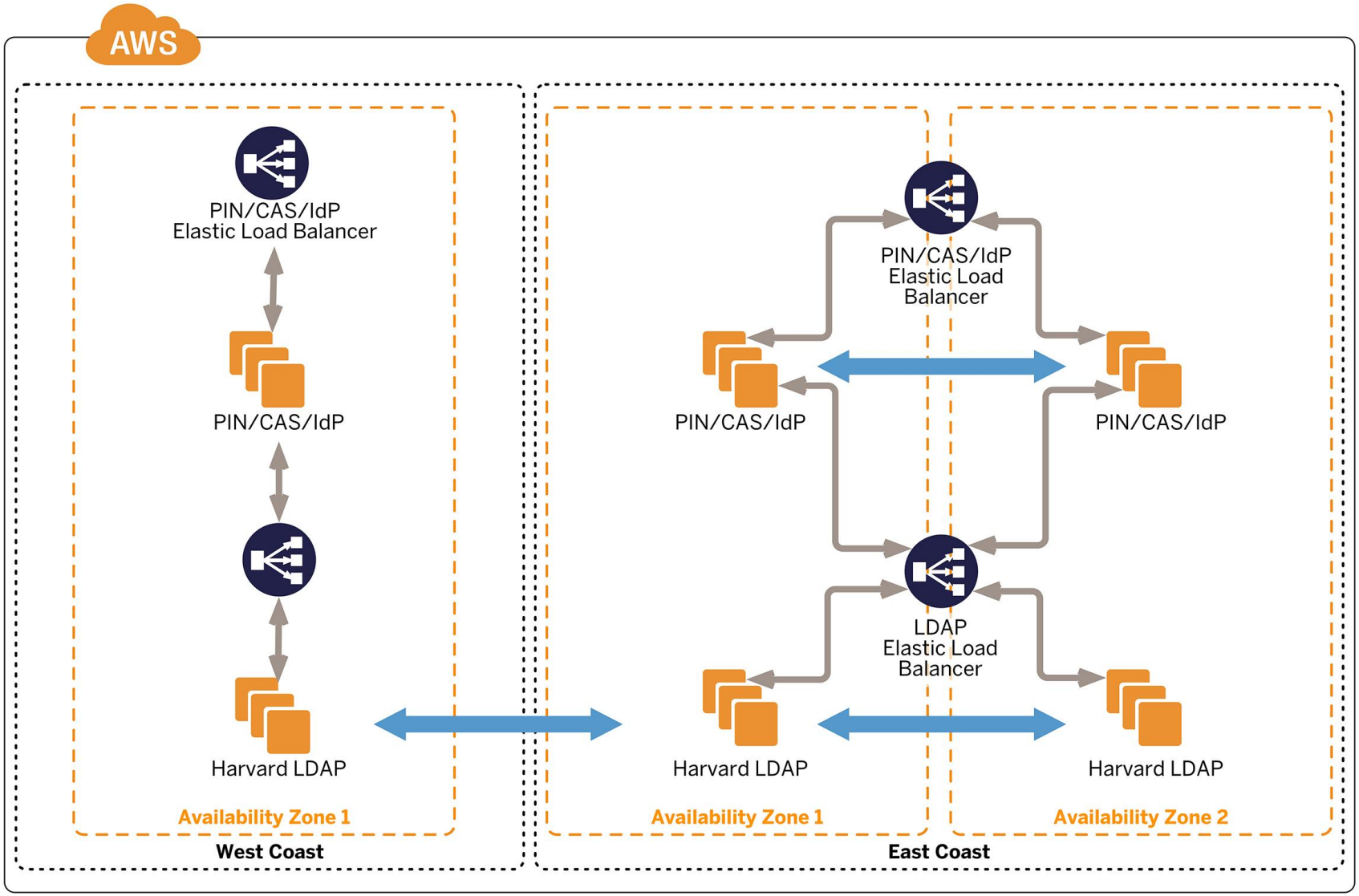
HLDAP System Context



HLDAP Master System Context



Across Region DR



Thank you!

HARVARD UNIVERSITY
Information Technology

Appendix A

Technical Oversight Committee Members

Technical Oversight Committee Members

Chair: Magnus Bjorkman, Director of IAM Engineering

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

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