HARVARD UNIVERSITY
Information Technology

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

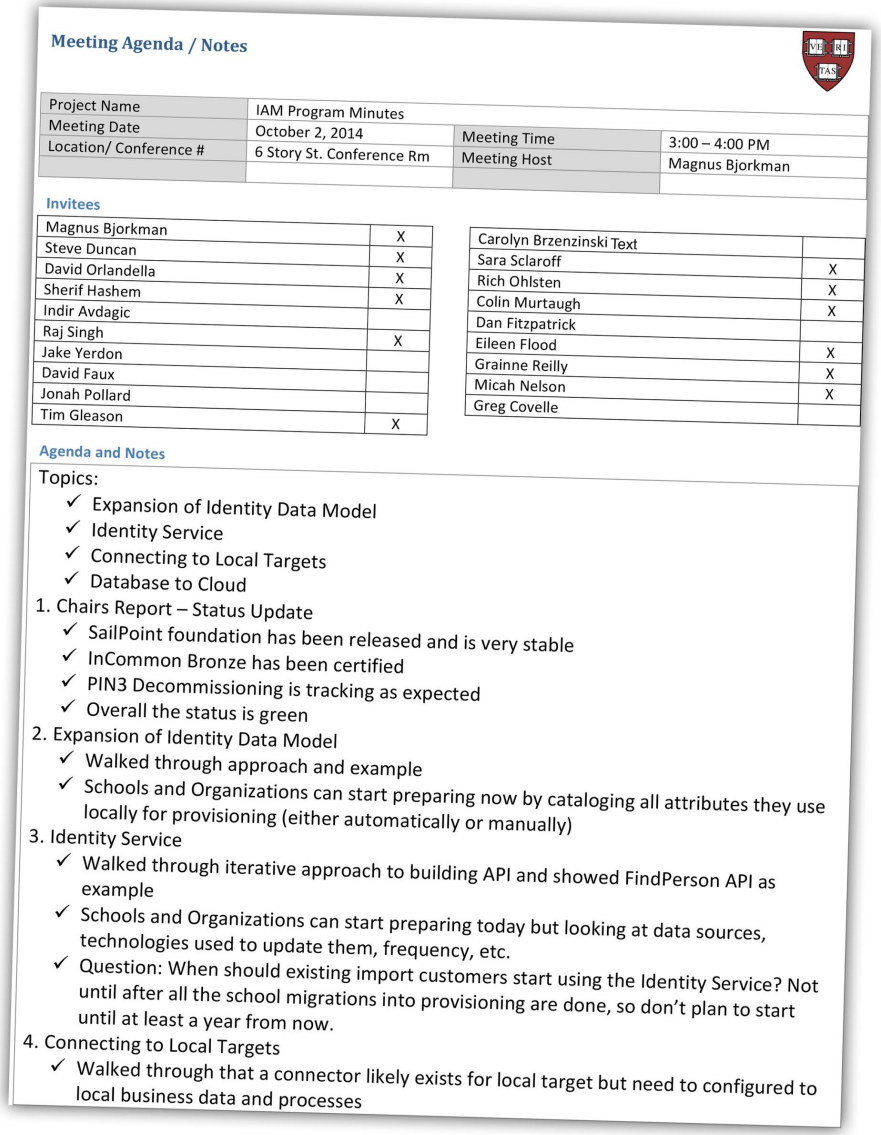
Intended Outcomes

- Greater clarity on proceeding with HarvardKey rollout, plus discovery of any local technical issues
- Better knowledge of Harvard's MFA implementation

Approval of Previous Minutes

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



Meeting Agenda / Notes

Project Name	IAM Program Minutes		
Meeting Date	October 2, 2014	Meeting Time	3:00 – 4:00 PM
Location/ Conference #	6 Story St. Conference Rm	Meeting Host	Magnus Bjorkman

Invitees

Magnus Bjorkman	X	Carolyn Brzenzinski Text	
Steve Duncan	X	Sara Sclaroff	X
David Orlandella	X	Rich Ohlsten	X
Sherif Hashem	X	Colin Murtaugh	X
Indir Avdagic		Dan Fitzpatrick	
Raj Singh	X	Eileen Flood	X
Jake Yerdon		Grainne Reilly	X
David Faux		Micah Nelson	X
Jonah Pollard		Greg Covelle	
Tim Gleason	X		

Agenda and Notes

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

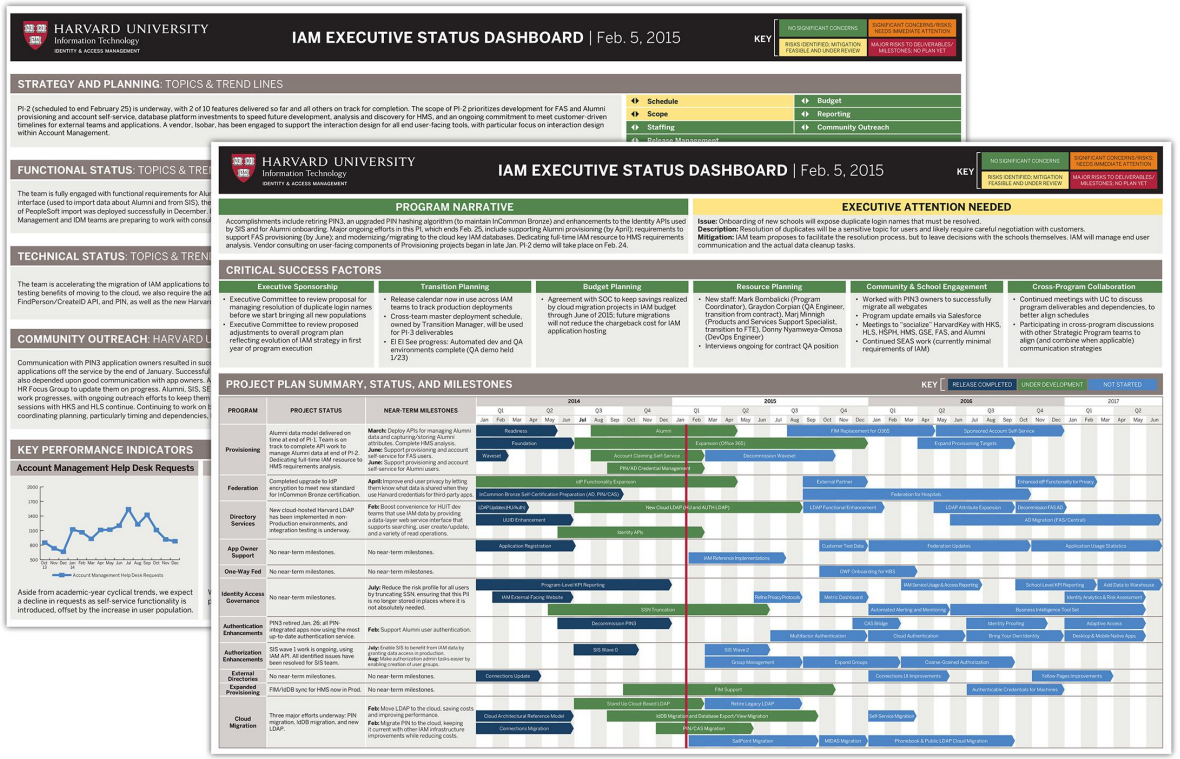
1. Chairs Report – Status Update
   - ✓ SailPoint foundation has been released and is very stable
   - ✓ InCommon Bronze has been certified
   - ✓ PIN3 Decommissioning is tracking as expected
   - ✓ Overall the status is green
2. Expansion of Identity Data Model
   - ✓ Walked through approach and example
   - ✓ Schools and Organizations can start preparing now by cataloging all attributes they use locally for provisioning (either automatically or manually)
3. Identity Service
   - ✓ Walked through iterative approach to building API and showed FindPerson API as example
   - ✓ Schools and Organizations can start preparing today but looking at data sources, technologies used to update them, frequency, etc.
   - ✓ Question: When should existing import customers start using the Identity Service? Not until after all the school migrations into provisioning are done, so don't plan to start until at least a year from now.
4. Connecting to Local Targets
   - ✓ Walked through that a connector likely exists for local target but need to configured to local business data and processes

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

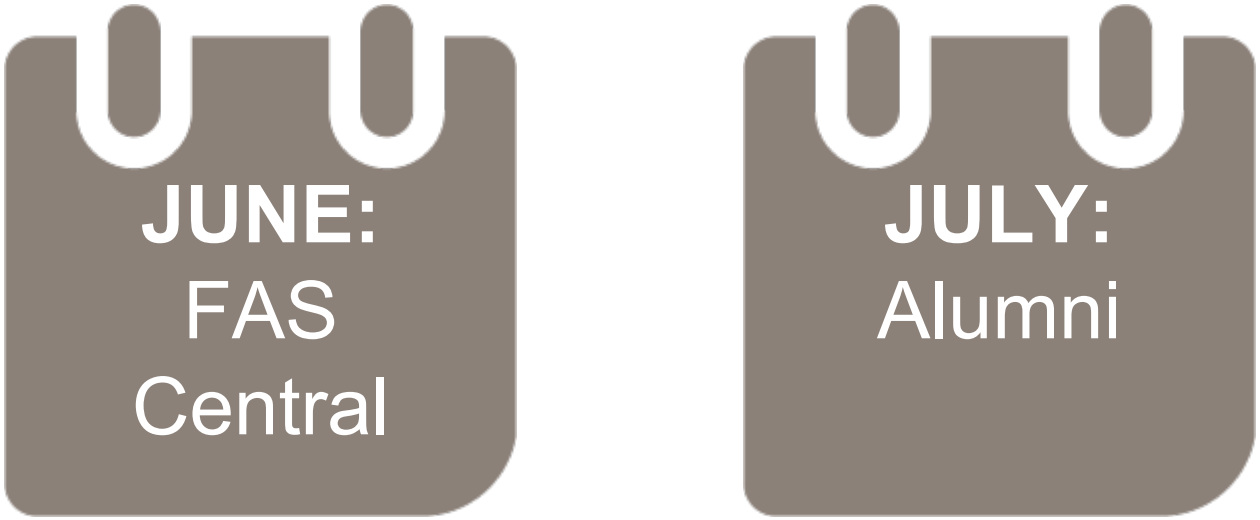


- Program Status: Green
- Key points: PIN3 decommissioned, SHA-2 upgrade, Alumni/FAS/HMS work continues apace

Shared Topics of Interest

HARVARDKEY

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

HARVARDKEY

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

HARVARDKEY

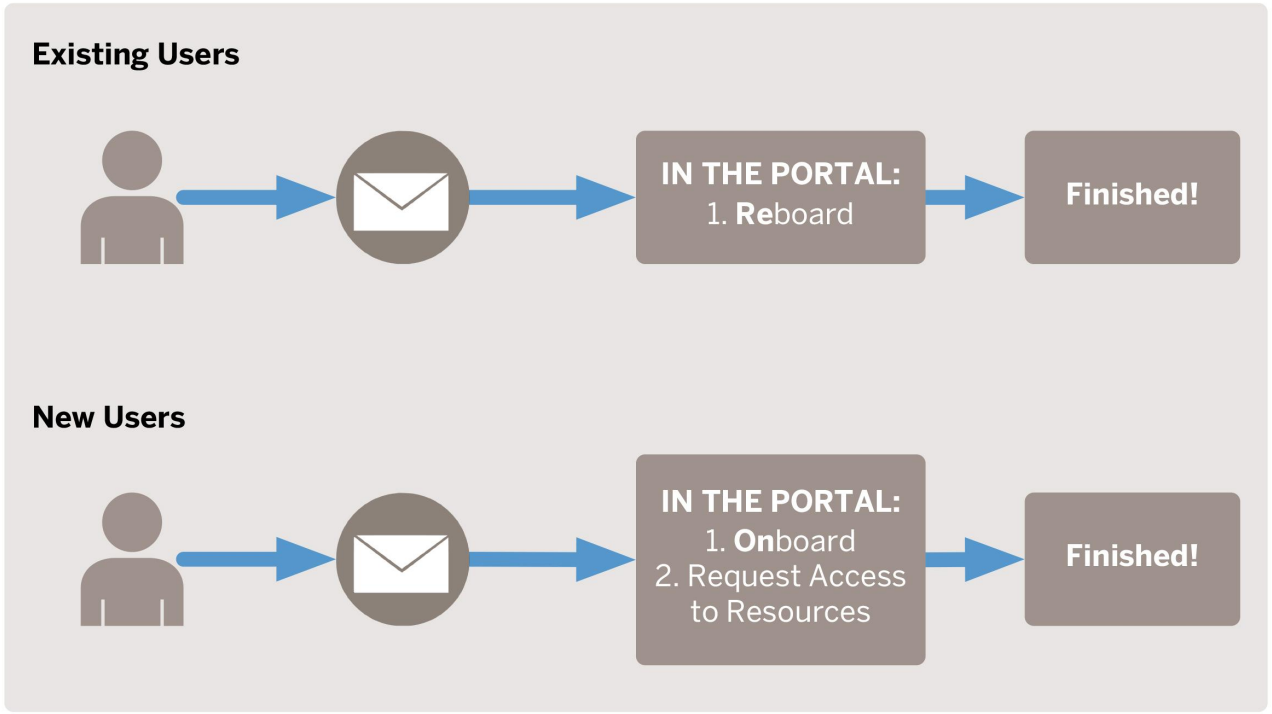
Understanding how we are using the terms below

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

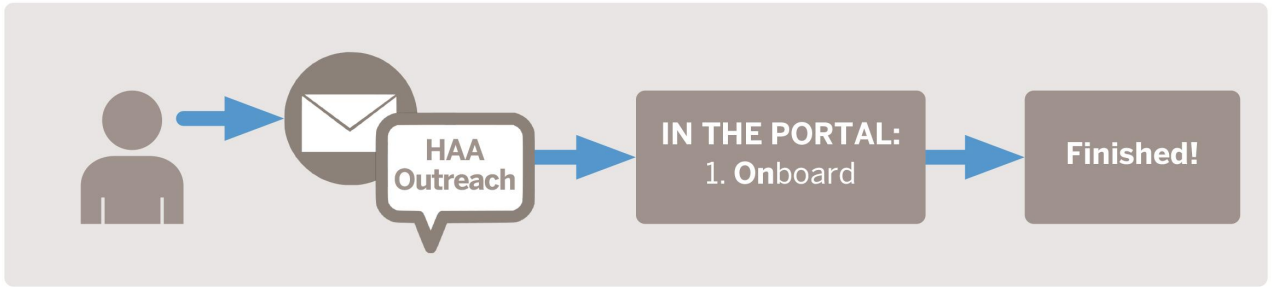
Onboarding/Reboarding

HARVARDKEY

Non-Alumni User Populations, by Waves (Wave 1: FAS/Central, June 15)



Alumni Users (Single Wave: July 15)



Onboarding/Reboarding

HARVARDKEY

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

Reboarding & New LDAP

HARVARDKEY

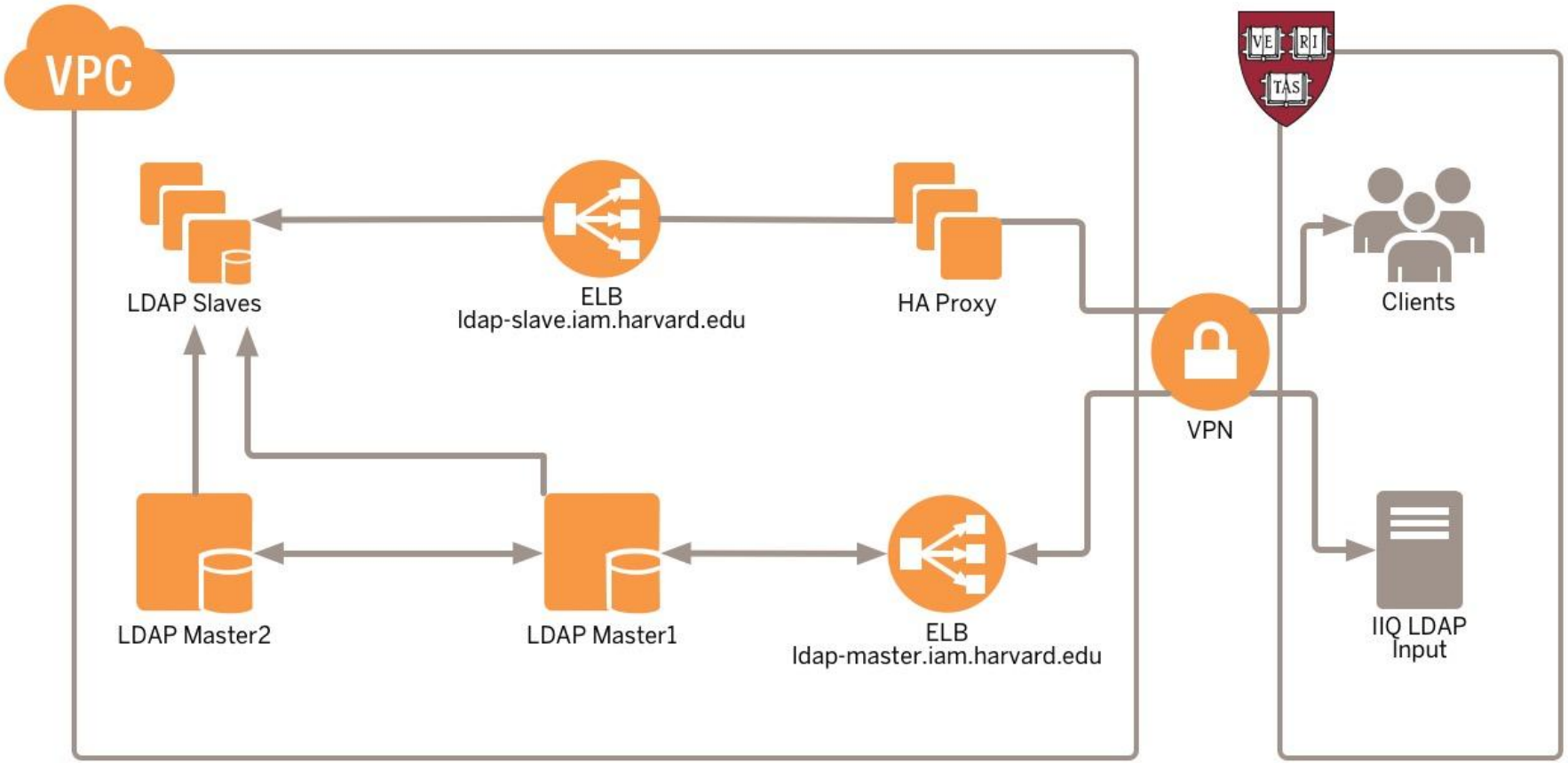
New Harvard LDAP (HLDAP) deployed in the cloud

- 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

HARVARDKEY

Harvard LDAP on AWS:



More details: http://tinyurl.com/hldap-aws

PIN2 Token Example

HARVARDKEY

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

Shared Topics of Interest: Multifactor Authentication

Multifactor Authentication (MFA) is a type of authentication that requires a user's identity to be verified by more than one independent factor.

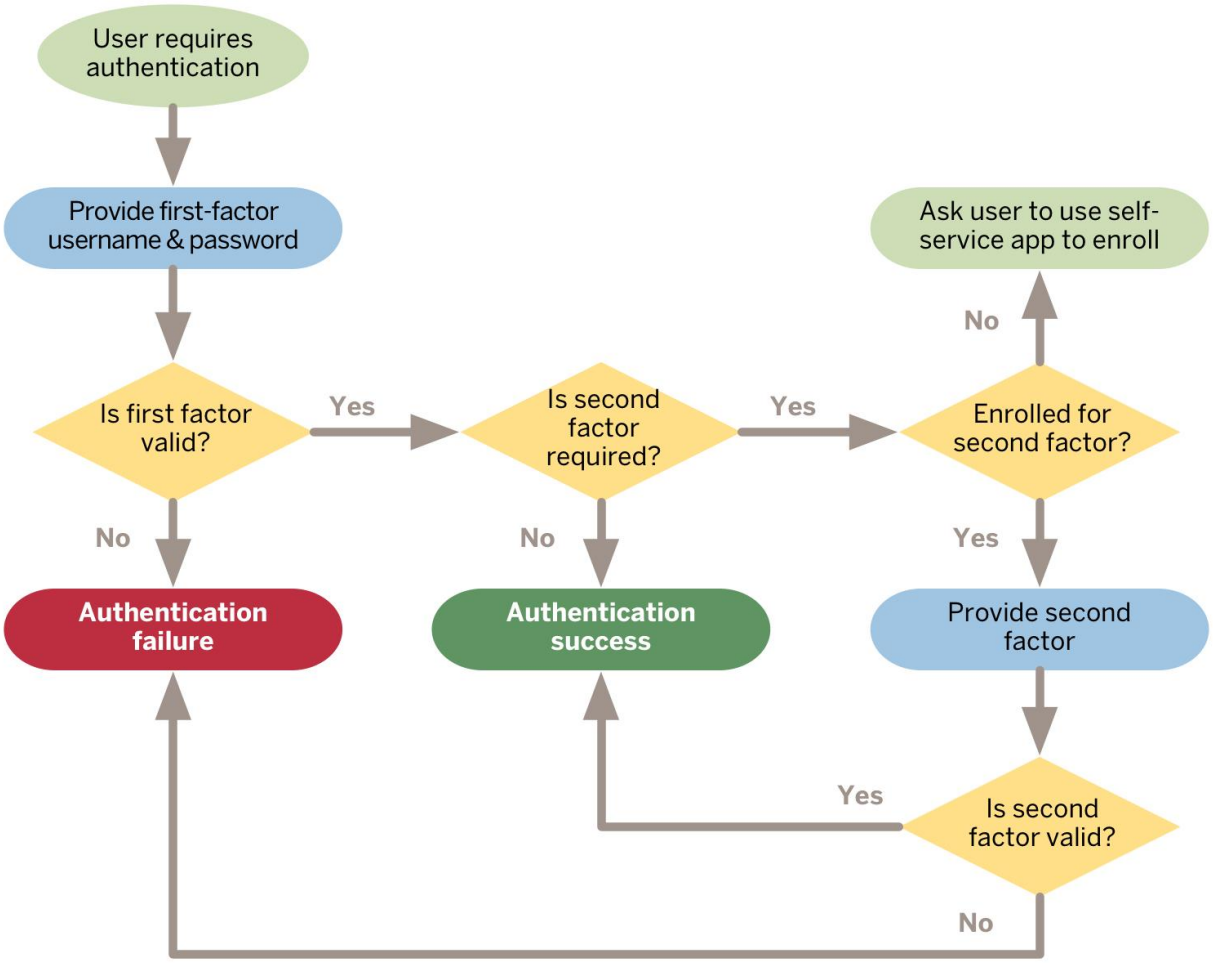
Types of factors:

- 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.

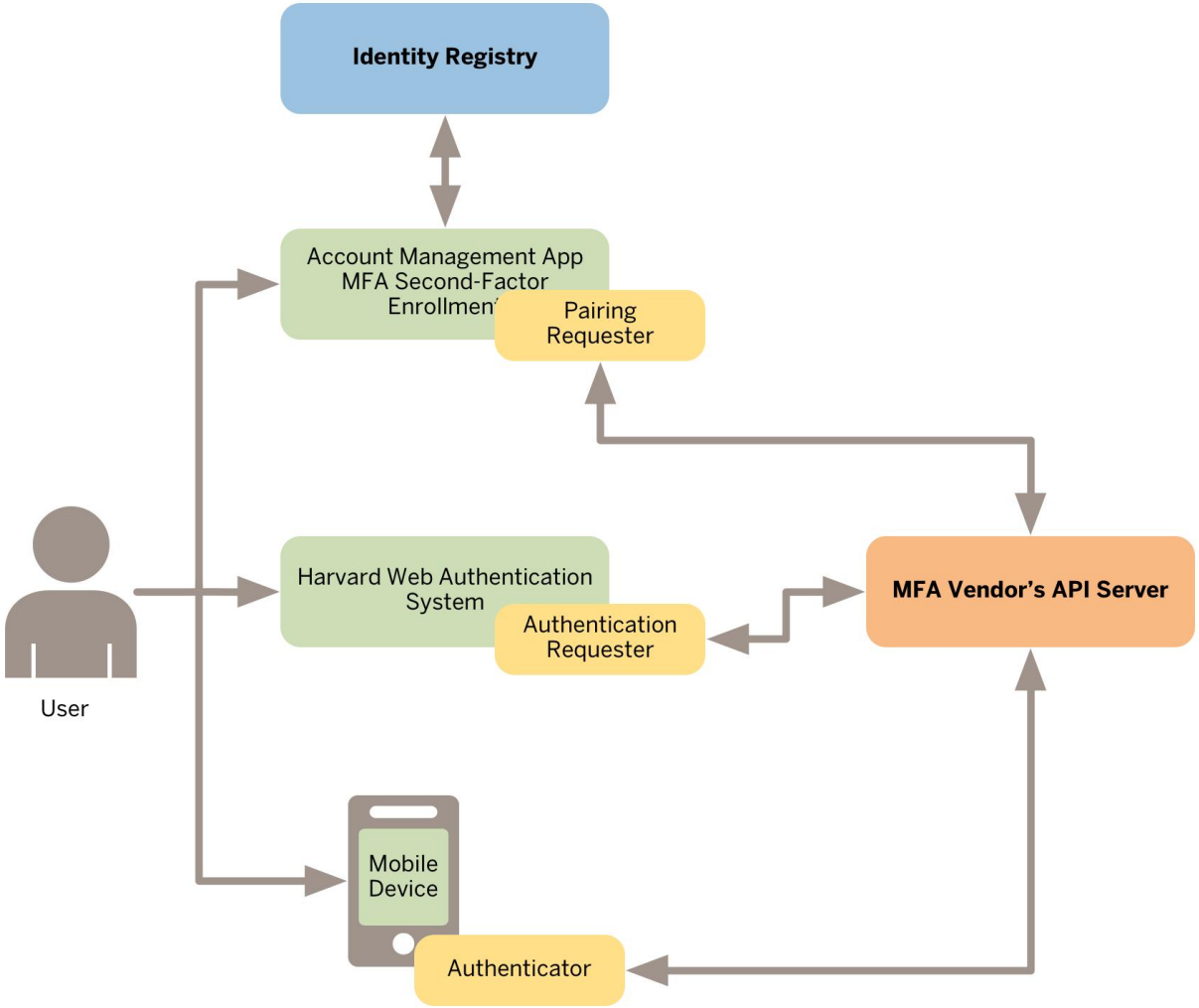
Shared Topics of Interest: Multifactor Authentication

Multifactor authentication flow



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!

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