HARVARD UNIVERSITY
Information Technology

Identity and Access Management
Technical Oversight Committee

June 18, 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: HarvardKey Authentication (10 min)
- Shared Topics of Interest: Grouper (20 min)
- General Discussion (15 min)

Meeting Purpose and Intended Outcomes

Purpose

- Present the latest status of the IAM Program Plan
- Provide update on refinement of HarvardKey authentication scope
- Provide update on Grouper implementation

Intended Outcomes

- Describe essential updates to HarvardKey authentication
- Bring everyone up to date on intended implementation of Grouper

Approval of Previous Minutes

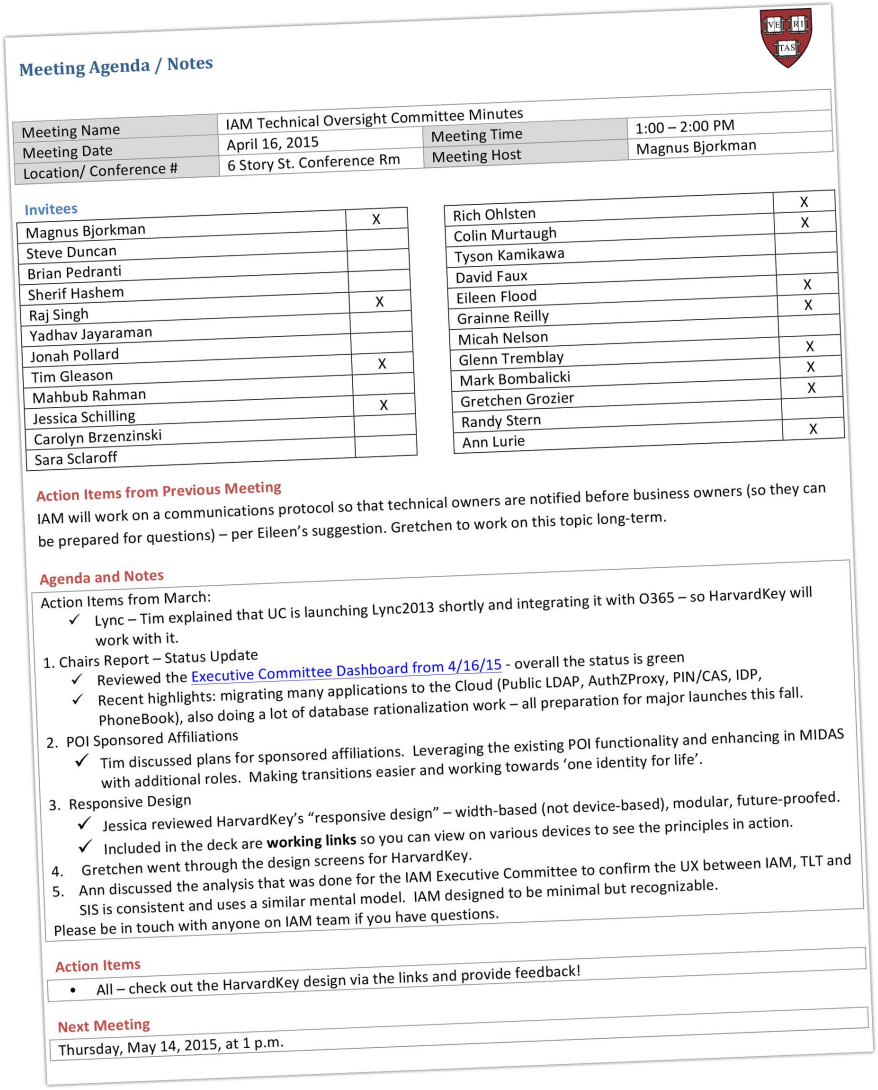
April 16 Meeting

Topics

- POI Sponsored Affiliations
- HarvardKey Design
- User Experience

Action Items

- Committee members to use HarvardKey UX links and provide feedback on design



Meeting Agenda / Notes

Meeting Name	IAM Technical Oversight Committee Minutes		
Meeting Date	April 16, 2015	Meeting Time	1:00 – 2:00 PM
Location/ Conference #	6 Story St. Conference Rm	Meeting Host	Magnus Bjorkman

Invitees

Magnus Bjorkman	X	Rich Ohlsten	X
Steve Duncan		Colin Murtaugh	X
Brian Pedranti		Tyson Kamikawa	
Sherif Hashem		David Faux	
Raj Singh	X	Eileen Flood	X
Yadhav Jayaraman		Grainne Reilly	X
Jonah Pollard		Micah Nelson	
Tim Gleason	X	Glenn Tremblay	X
Mahbub Rahman		Mark Bombalicki	X
Jessica Schilling	X	Gretchen Grozier	X
Carolyn Brzenzinski		Randy Stern	
Sara Sclaroff		Ann Lurie	X

Action Items from Previous Meeting

IAM will work on a communications protocol so that technical owners are notified before business owners (so they can be prepared for questions) – per Eileen's suggestion. Gretchen to work on this topic long-term.

Agenda and Notes

Action Items from March:
- ✓ Lync – Tim explained that UC is launching Lync2013 shortly and integrating it with O365 – so HarvardKey will work with it.

1. Chairs Report – Status Update
   - ✓ Reviewed the Executive Committee Dashboard from 4/16/15 - overall the status is green
   - ✓ Recent highlights: migrating many applications to the Cloud (Public LDAP, AuthZProxy, PIN/CAS, IDP, PhoneBook), also doing a lot of database rationalization work – all preparation for major launches this fall.
2. POI Sponsored Affiliations
   - ✓ Tim discussed plans for sponsored affiliations. Leveraging the existing POI functionality and enhancing in MIDAS with additional roles. Making transitions easier and working towards 'one identity for life'.
3. Responsive Design
   - ✓ Jessica reviewed HarvardKey's "responsive design" – width-based (not device-based), modular, future-proofed.
   - ✓ Included in the deck are **working links** so you can view on various devices to see the principles in action.
4. Gretchen went through the design screens for HarvardKey.
5. Ann discussed the analysis that was done for the IAM Executive Committee to confirm the UX between IAM, TLT and SIS is consistent and uses a similar mental model. IAM designed to be minimal but recognizable.

Please be in touch with anyone on IAM team if you have questions.

Action Items

- All – check out the HarvardKey design via the links and provide feedback!

Next Meeting

Thursday, May 14, 2015, at 1 p.m.

Previous Minutes: Action Items

Any feedback on the new HarvardKey design and UX?

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

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

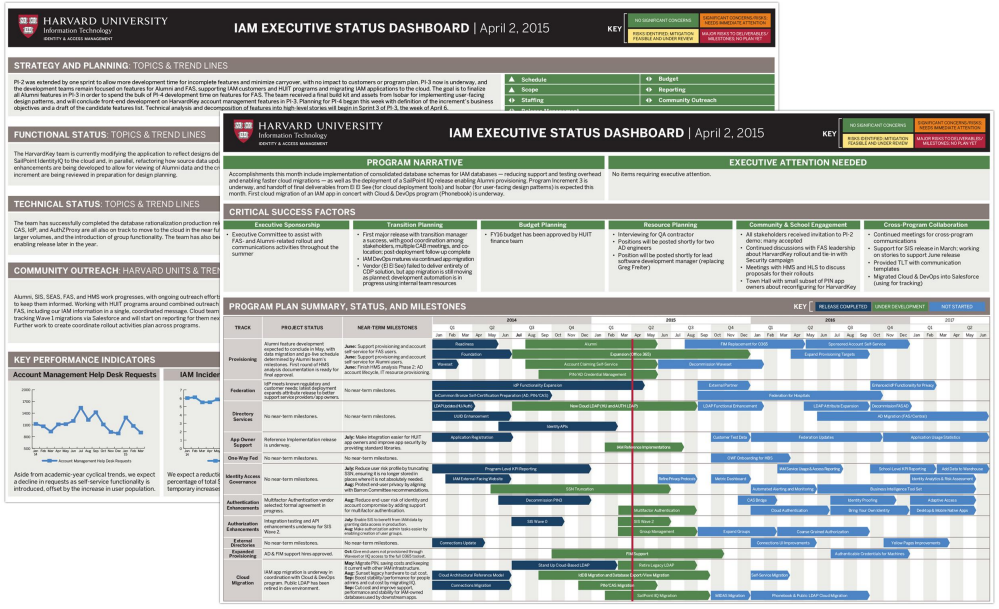
Setup (User Type):
http://tinyurl.com/harvardkey-usertype

Set Password:
http://tinyurl.com/harvardkey-setpassword

Chair's Report: Executive Committee

Welcome to Tim Vaverchak, our new chair!

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

Shared Topics: HarvardKey Authentication

Passphrase implementation will be delayed

- Passphrase implementation introduced complexity in local system implementations; if improperly implemented, could result in weak password management practices
- Security review and possible future inclusion

Multifactor authentication

- Selected Duo Security for web authentication enhancements

PIN applications move to HarvardKey

- Outreach to application owners: The vast majority of applications will not need any alterations, and we have already contacted systems that need work
- HarvardKey test platform available this summer

Shared Topics: Grouper

Access Management: Current State

- Some web applications use AuthZProxy, a centrally managed access management service that works in conjunction with the PIN2 authentication protocol
- Some web applications take care of access management by getting attributes about authenticated users from HU-LDAP or other sources
- Currently, we do not have a comprehensive access management strategy that works for all/most web applications and other systems

Shared Topics: Grouper

Access Management: Challenges

- Harvard has a highly distributed management environment, making it extremely difficult to manage access control by a single central team
- Harvard has a heterogeneous technology environment, so a common service like access management must support multiple integration schemes in order to be useful
- Unlike the corporate world, access management does not follow any organizational rules — ad-hoc teams are quite common (such as a research team where members do not follow any statically defined rules to be part of the team), and an access management framework must be flexible enough to support this

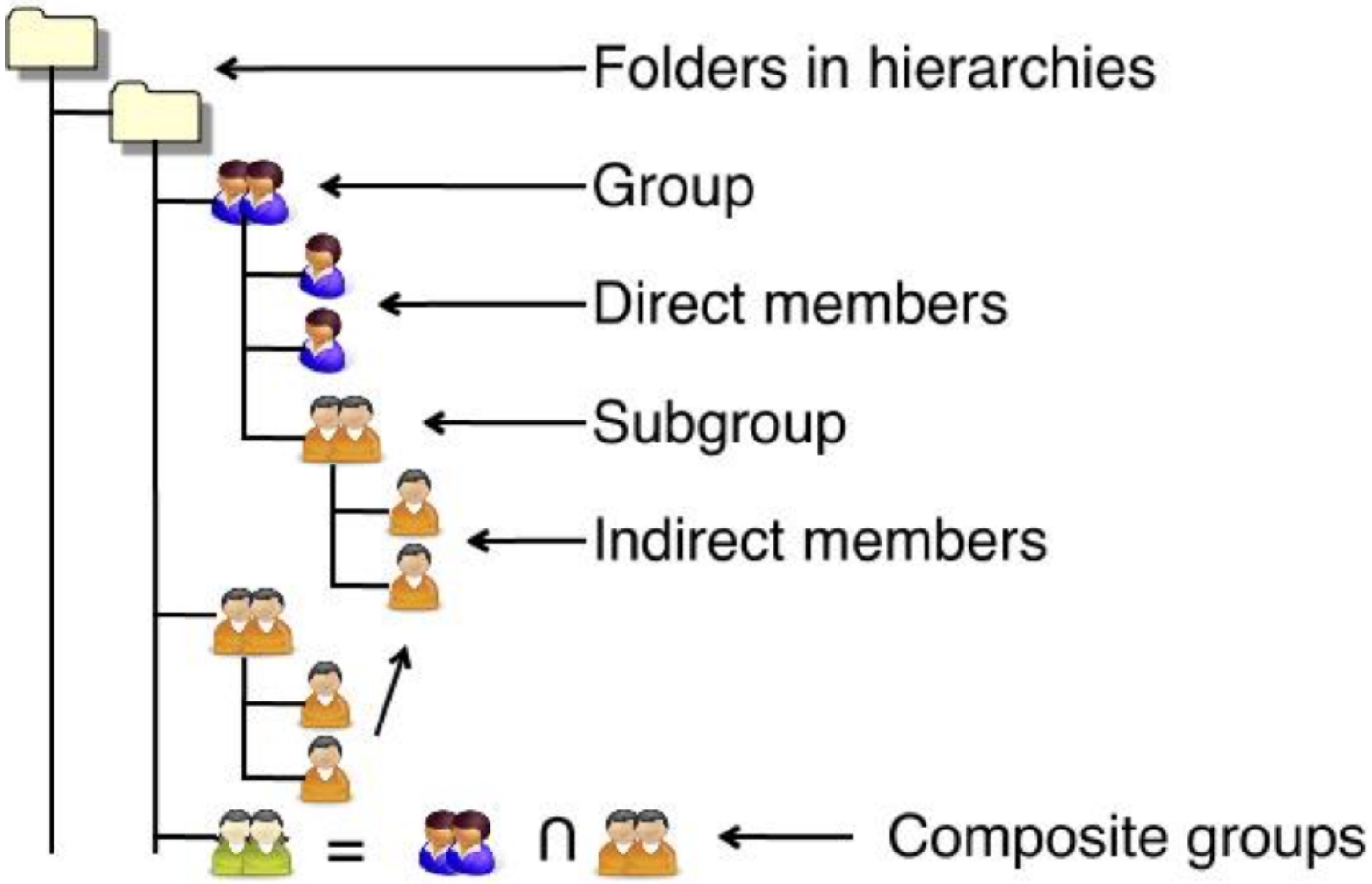
Shared Topics: Grouper

Access Management System: Internet2's Grouper

- An enterprise-scale access management system that manages groups and group memberships
- Built by the higher education community for higher-ed institutions
- Best suited for a highly distributed management environment and heterogeneous technology environment
- Supports delegated administration of groups — departments or teams can manage access control for their applications/resources, eliminating the need for central IT team to be involved in everyday group and group membership management
- Many successful deployments in higher-education institutions around the globe

Shared Topics: Grouper

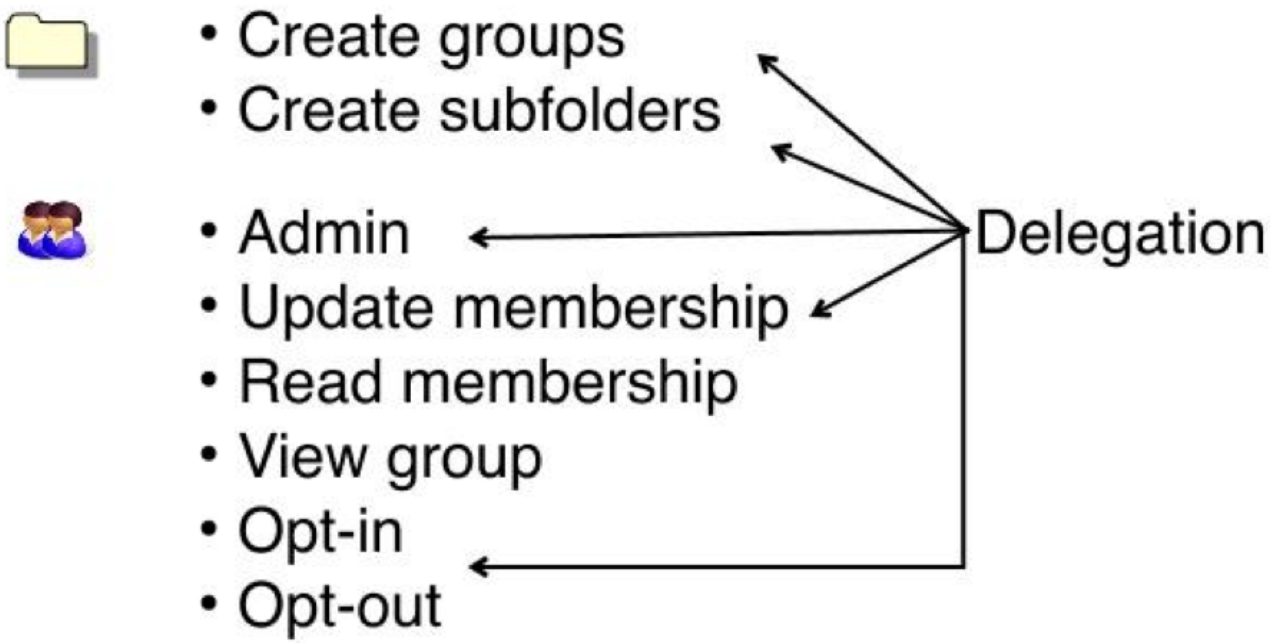
Grouper's core concept:



Diagrams courtesy Internet2's Grouper team

Shared Topics: Grouper

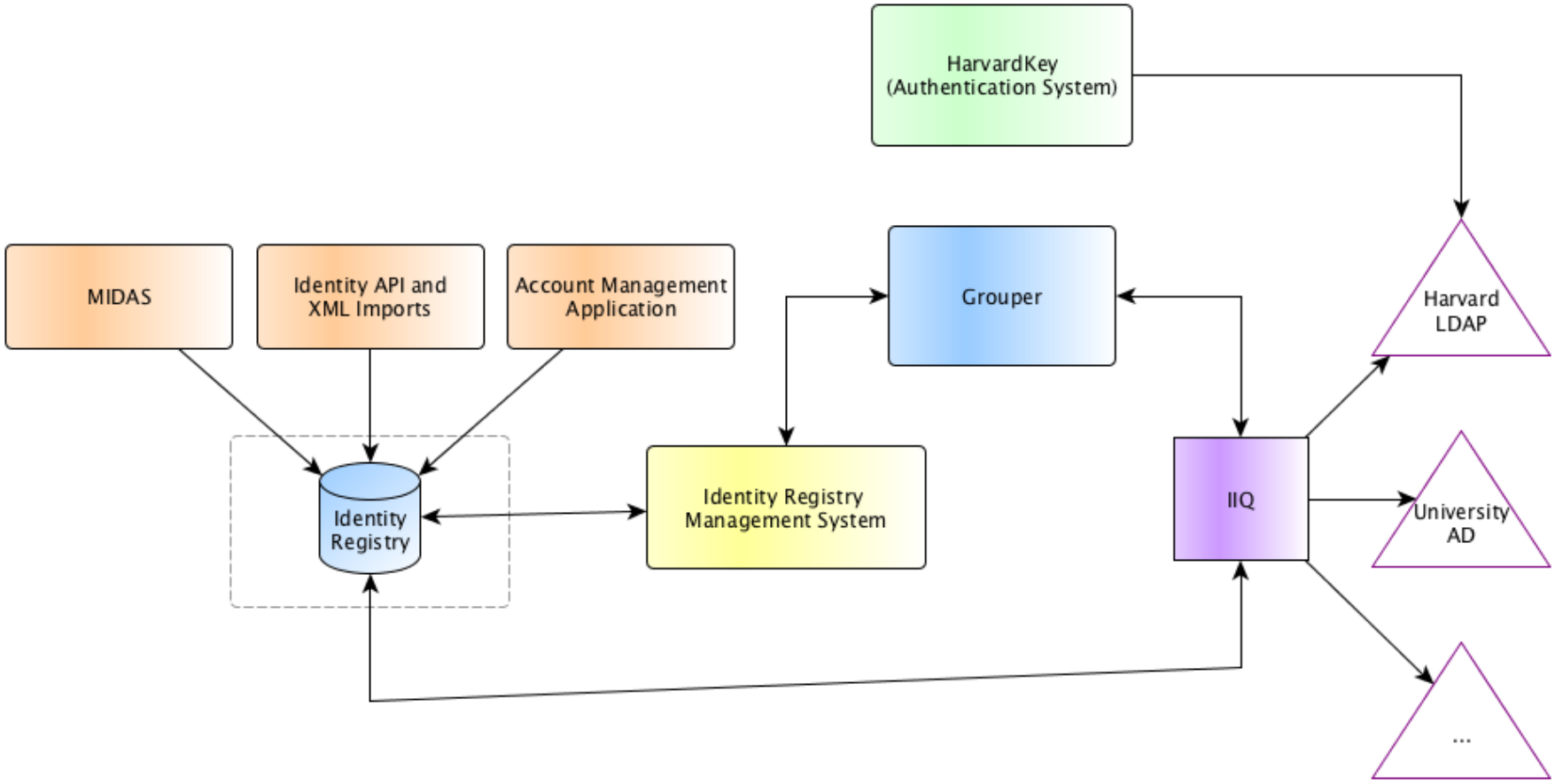
How delegation works:



Diagrams courtesy Internet2's Grouper team

Shared Topics: Grouper

Grouper integration:



Shared Topics: Grouper

Grouper Integration Highlights

- The identity registry is Grouper's identity source; group membership will be created by applying business rules in identity attributes
- A IIQ connector will be configured for Grouper to get the groups
- IIQ will use the groups for provisioning, as well as provision the groups to Harvard LDAP
- Other systems or applications can access groups in different ways:
  - As part of a SAML or CAS authentication assertion
  - As a multivalued attribute in LDAP (*memberOf* or *eduPersonEntitlement*)
  - As a service (using REST API)

Thank you!

HARVARD UNIVERSITY
Information Technology

Appendix A

Technical Oversight Committee Members

Technical Oversight Committee Members

Chair: Tim Vaverchak, 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