HARVARD UNIVERSITY
Information Technology

Identity and Access Management

Technical Oversight Committee

May 15, 2014 | Thursday | 3:00PM-4:00PM | 6 Story Street

Agenda

- Approval of Prior Minutes
- Chairs Report
- Get Started with an IAM Service
- Shared Topics of Interest
- Proposal Review and Recommendations to Approve
- General Discussion

Meeting Purpose and Intended Outcome

Purpose

- Provide a status update
- Introduce “Get Started” for authentication
- Present and discuss “Find Person” and “Create/Reuse ID” services

Intended Outcome

- Enable people to bring back “Get Started” for authentication back to their organizations.
- Validate approach for “Find Person” and “Create/Reuse ID” services and that they meet the needs of organizations

Approvals of Minutes

Project Name	IAM Program – IAM Technical Oversight Committee		
Meeting Date	April 3, 2014	Meeting Time	2:00 – 3:00
Location/ Conference #	Smith Campus Center 869	Meeting Host	Magnus Bjorkman

Invitees

Steve Duncan	X	Carolyn Brzezinski	X
Tyson Kamikawa	X	Sara Sclaroff	X
Sherif Hashem		Rich Ohlsten	
Indir Avdagic	X	Colin Murtaugh	X
Ken Ho	X	Dan Fitzpatrick	
Jake Yerdon	X	Eileen Flood	X
David Faux		Grainne Reilly	X
Jonah Pollard	X	Joe Zurba	X
Tim Gleason	X	Micah Nelson	X
Gretchen Grozier	X		

Agenda and Notes

1. **Why are we here? – IAM Program Governance**
   a. Reviewed the purpose of the committee and the general IAM Program Governance.
   b. There was a request for the list of representatives of the overall IAM governance groups (the Executive and Identity Lifecycle Committees), as people wanted to make sure there is adequate representation.
2. **IAM Program Overview**
   a. Discussed importance of service to work for organizations that want to use services in replacement of local solution as well as working with a local solution.
   b. Requested input on potential KPIs as we have not yet settled on those.
   c. There was a question if each project would result into a capability/service. It will depend on the project. Some will build a service, e.g. SailPoint, and others will be geared toward standards and collaborations, e.g. Federation.
   d. Confirmed that AD and FIM is part of this program.
   e. The Identity and Access Governance project is different from the actual governance of the program. It includes defining policies, processes and systems to manage the identities and visibility into access risks.
3. **IAM Technical Oversight Committee**
   a. There was a question if the example policy approval process would be the exact sequence followed. The example is more schematic than exact, as the order of the initial steps might be in a different order and may have additional feedback loops.
   b. There was consensus on having the meeting on Thursday afternoon, preferable in the same week as the Executive Committee, but after the Executive Committee.
   c. Additional Topics Suggested:

IAM Executive Committee - Membership

- Anne Margulies, UCIO, *Co-Chair*
- Rainer Fuchs, CIO HMS, *Co-Chair*

- Mary Ann Bradley, Associate Dean, FAS
- Mike Burke, Registrar, FAS
- Ben Gaucherin, Deputy UCIO
- Prasanna Gopalakrishnan, Director, Campus Services IT
- John Jurus, CIO, UHS
- Jason Snyder, Program Director, IAM
- Jim Waldo, CTO
- Bob Wittstein, Managing Director, HUIT ATS

Chairs Report: Progress Against the Plan – Key Accomplishments

The following table outlines the key program accomplishments achieved since the March IAM Executive Committee meeting :

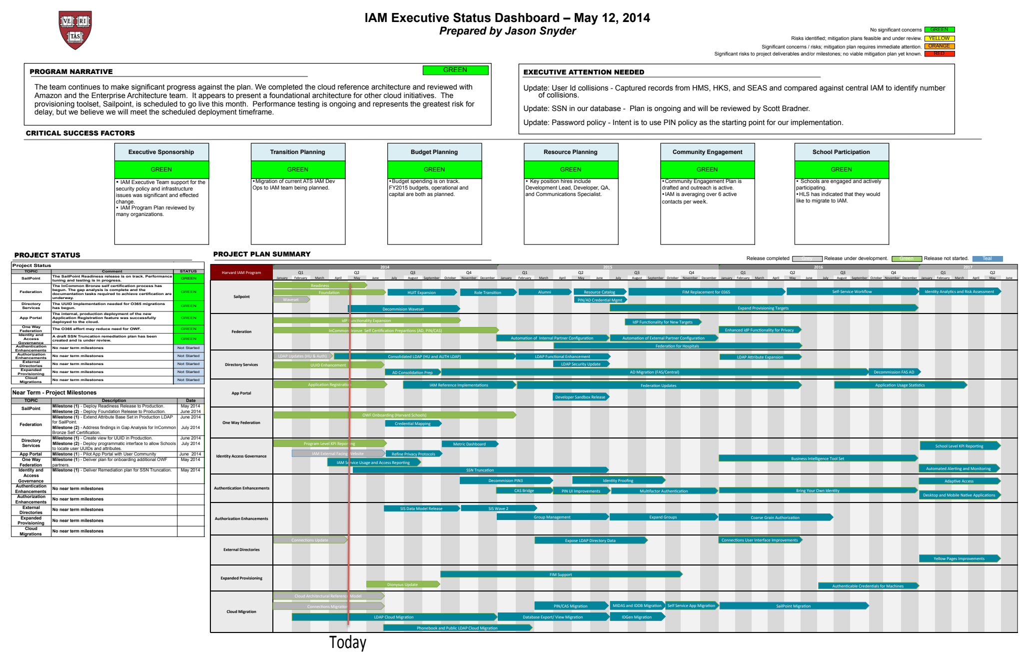
Project	Release	Description	Plan Date	Actual Date	Impact
App Portal	Application Registration (Internal)	Deploy a new application to to streamline application integration with IAM services.	April 2014	April 2014	✓ Reduce the complexity of IAM integration for application team. ✓ Deploy second IAM application to to AWS.
Federation	InCommon Bronze Self Certification Preparation	Complete the Gap Analysis for InCommon Bronze Self Certification	June 2014	**May 2014**	✓ Position IAM Services to be InCommon Bronze Self Certified by end of July 2014.
Cloud Migration	Cloud Architectural Reference Model	Create a document that provides an overview of the IAM AWS cloud architecture and continuous integration environment.	July 2014	**May 2014**	✓ Deliver cloud architecture document that describes design, technology, processes, and operations of an application within AWS. ✓ Share findings and lessons learned with other HUIT application teams.

Chairs Report – Program Status

- Latest detailed status uploaded at http://iam.harvard.edu

- Program Status: Green

- Office 365 Shared Tenant. Increased focus on provisioning.



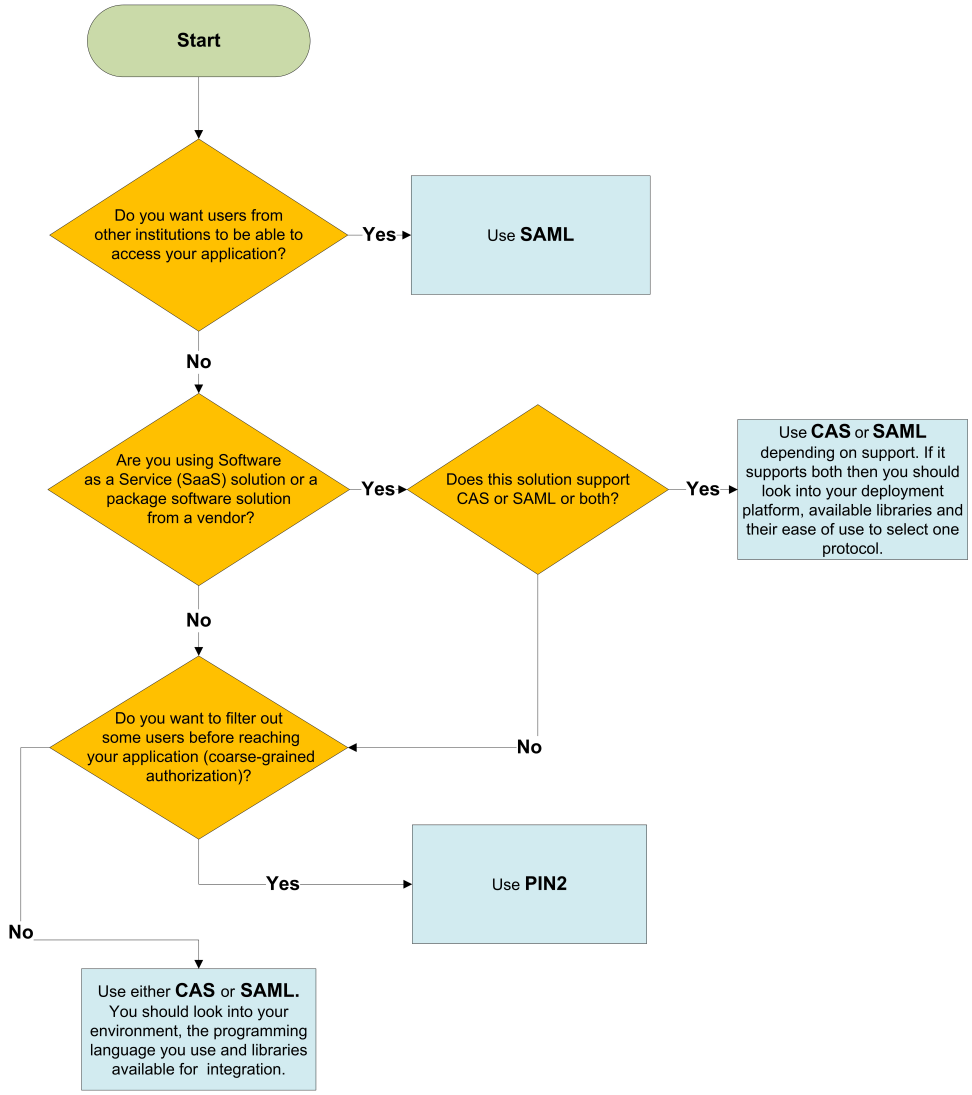
Get Started with an IAM Service: Authentication

- There is a new web site available for IAM that gives information about the program and our services:
  - http://iam.harvard.edu
- The web site contains a section to help people to use our services that we call “Get Started:
  - Introduction to Service
  - Guide on what service or what part of service to use
  - Technical information and how-to’s
  - Links to additional resources
- The first part of the “Get Started” section is for Authentication.

Get Started with an IAM Service: Authentication (cont.)

- Introduction
- Selecting an Authentication Protocol
- Using CAS as your authentication protocol
  - How CAS works
  - Why CAS is helpful
  - Application configuration in order to use the CAS protocol
- Using SAML as your authentication protocol
  - How SAML works
  - Why SAML is helpful
  - Application configuration in order to use the SAML protocol
- Using PIN2 as your authentication protocol
  - How PIN2 works
  - Why PIN2 is helpful
  - Application configuration in order to use the PIN2 protocol

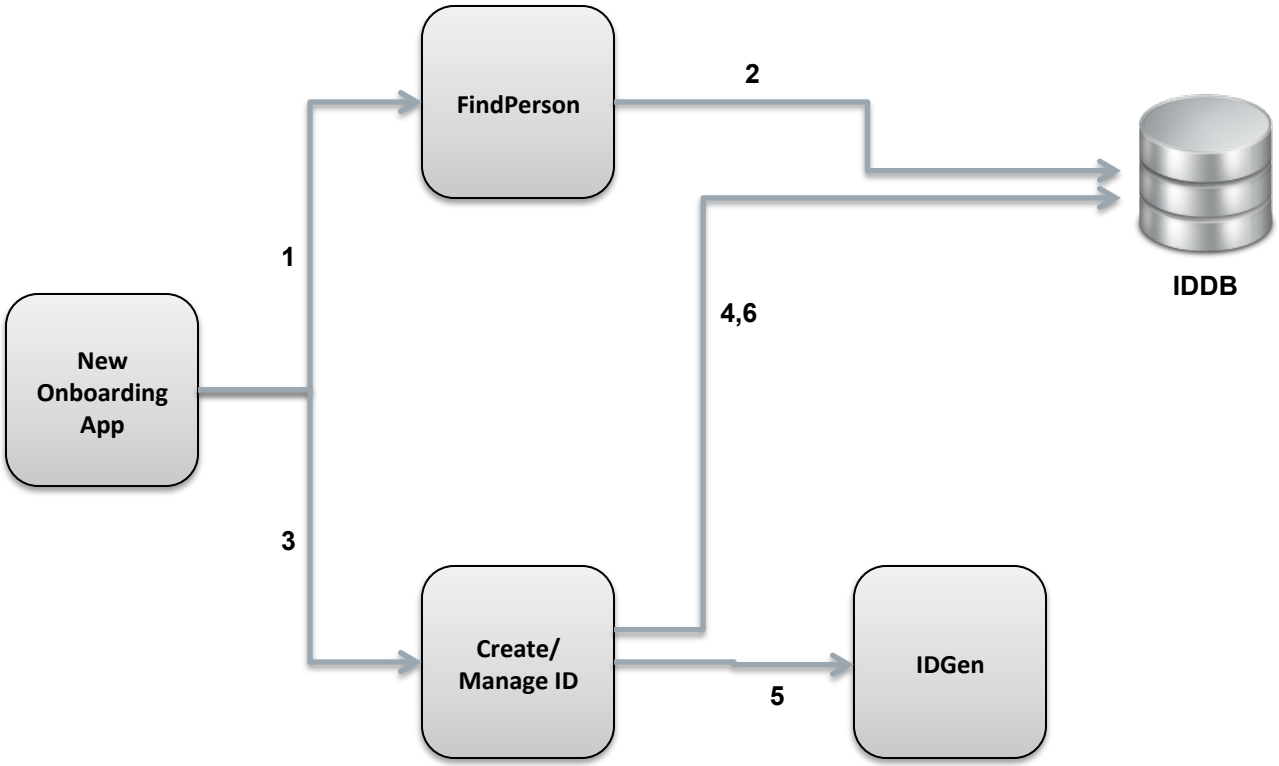
Get Started with an IAM Service: Authentication (cont.)



Shared Topics of Interest: “Find Person” and ”Create/Manage ID”

- The UUID provides the unique identifier that will allow us to correlate and join users across schools and systems. Provides the following benefits among others:
  - Avoid giving multiple accounts to the same user.
  - Enable our systems to give access based on the identity of the user not the credential they use. In turn allowing people to use the credential they know.
- Apart from the definition of the UUID itself, we need a process to assign a person the same UUID across Harvard to realize the benefits of this.
- We are looking at providing services to address this:
  - **“Find Person”** Allows systems to find people with already existing identifiers.
  - **“Create/Manage ID”** Allows people to create new identifiers, storing essential information about a person so people can later find them using “Find Person”. It also allows for that information to be later updated.
- There will also be an additional service, “**Insert Role”**, that will allow onboarding applications to add roles needed for provisioning. The main intent for this is to capture sponsored roles that do not flow through HR and SIS systems.

Using the APIs: New Onboarding Application



1. Onboarding app calls FindPerson to see if person already exists
2. FindPerson checks in IDDB for information about existing people
3. If the person does not exist, Create/Manage ID is called to generate a new identifier (HUID, UUID)
4. Create/Manage ID generates UUID and ADID (if needed) and stores it in IDDB
5. If a HUID is needed. Create/Manage ID will call IDGen to get a HUID generated.
6. Create/Manage ID also calls IDDB to create a skeleton record for the person, allowing for immediate provisioning if needed and appropriate

“Find Person” API

- Fuzzy Matching
  - FindPerson_byEPI(name, dob, last four of SSN, e-mail, etc.)
- Exact Matching
  - FindPerson_byUUID()
  - FindPerson_byHUID()
  - FindPerson_byEmailAddr()
  - FindPerson_byPhoneNumber()

“Create/Manage ID” API

- CreatePersonRecord(In EPI, OUT UUID, HUID)
- CreatePersonRecordGivenUUID(In EPI, UUID; OUT HUID)
- CreatePersonRecordGivenHUID(In EPI, HUID; OUT UUID)
- UpdatePersonRecordByUUID(In EPI, UUID; OUT HUID)

“Batch” API

- Provides a method for onboarding applications to provide a list of people to create identifiers for
  - Uses the previous APIs to implement the batch functionality
  - Looping through the list, trying to match people in the list with existing people in IDDB
    - For an exact match, return the ID of that person (HUID, UUID, etc.)
    - For partial match, or multiple matches, return a list of potential matches, so onboarding application can make a determination
    - For a confident non-match, create a new ID/Record for the person and return the ID
- When a list of potential matches is returned, the onboarding application can use the Create/Manage ID for individual people, or send a list back for people to explicitly create IDs for (batch)

General Discussion

Appendix

Technical Oversight Committee Members

Chair: Magnus Bjorkman, HUIT IAM

Name	School/Group
Steve Duncan	Harvard Kennedy School
Tyson Kamikawa	Harvard Medical School
Sherif Hashem	Harvard Law School
Indir Avdagic	SEAS
Ken Ho	GSE
Jake Yerdon	HSPH
David Faux	HUIT Admin Tech/FAS & College
Jonah Pollard	Unified Communication/ Cloud
Tim Gleason	HUIT IAM/AD

Name	School/Group
Carolyn Brzezinski	SIS
Sara Sclaroff	HUIT Admin Tech/HR
Rich Ohlsten	HUIT Admin Tech/Alumni
Colin Murtaugh	HUIT Academic
Dan Fitzpatrick	Partners
Eileen Flood	Campus Services
Randy Stern	Library IT
Joe Zurba	HUIT Security