HARVARD UNIVERSITY
Information Technology

Identity and Access Management

IAM Lifecycle Committee

July Meeting: Early Access

July 21, 2014 | Monday | 10:30 – 12:00 | Holyoke 561

Agenda

- Welcome
- Status Update
- Discussion: Early Access Policy
- Discussion: Sponsored Accounts and Guest Access
- Wrap-up

Status Report

- Released:
  - POIs now created on IDGEN numbers
- Releases – Coming up soon
  - Sailpoint Foundation Release
    - Provisioning of University AD (supports CADM, GSE, GSD, DIV, SPH) for network and email. Release delayed from mid July to mid August
- News
  - Office 365 driving an accelerated schedule for school-specific provisioning.
  - Program schedule and budget adjusted accordingly
- Active topics
  - SIS and Alumni
  - Planning / developing next phase of Sailpoint
  - Migrating customers off of PIN3 to the other new PIN system protocols
  - Developing new APIs for identity (FindPerson, Create/Update ID holder,…more)

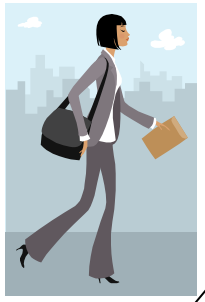
Near Term Milestones:

- Provisioning:
  - Deploy HMS FIM bridge solutions (HMS Office 365 Provisioning interim strategy)
  - Complete FAS and Central HMS Sailpoint Provisioning Requirements
  - Finish Alumni requirements for provisioning, sponsored accounts
- Federation
  - Self-certify for InCommon Bronze
- Data Services
  - Deliver FindPerson Identity API (Similar to IDGEN for identifier assignment, matching, etc.)

Discussion: Early Access

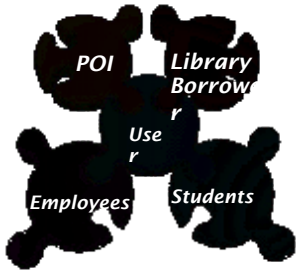
- Follow-up On:
  - Lack of clear policies on when early access is or is not okay
- Sponsored Account Process versus POI: What is the difference?
- First dive into Sponsored Accounts

POI and LB Departments in IdM



POI Role(s)
- Start Date
- End Date
- Prime role indicator
- Tub Affiliation (Faculty code)
- Description/Company
- Authorized Approver

Library Borrower Role(s)
- Start Date
- End Date
- Prime role indicator
- Library affiliation
- Borrower Code
- Authorized Approver



Each **POI Role** has an associated **Faculty Code**

This is the only 'department' information we have.

Each **Library Borrower** has a borrower code that can be mapped to the School that owns the Library.

Not all library borrowers are captured in IDM.

Address(es)
- Address information
- Address Type:
  - **Office**
  - **Location**

POI and Library Borrower Addresses are rarely in the system

They originate with local department

Email & Phone(s)
- Official Email Address
- Directory Listings
  - Listing Title
  - Phone #/ type
  - **Listing Location**
  - **Home**

POI's may have an office phone

Typically entered by the Directory Contact for the local department.

6

Early Access: Guidelines

- Concerns around potential for abuse and how to mitigate?

- Guidelines for appropriate Use
  - How many days prior to employment?
  - Does it vary depending on type of employee?
  - Who should authorize the entry?
  - To what extent are we comfortable with distributed data entry?

Sponsored Accounts vs. Guests

Background:

- Most schools are creating sponsored accounts / guest accounts using local tools
- Drive towards centralizing provisioning of email resulting in emerging set of global "guest" requirements that are being gathered as part of the analysis of school requirements

FAS Sponsored Account details:

Today: Paper process that is not making anyone happy

Future: Online process with great convenience, and accountability for sponsors

- On-boarded by a sponsor (or a requester acting on behalf of sponsor)
- Onboarded with relatively full demographic data: Full Name, DOB, last four of SSN.
- Sponsored Account Holder will claim their account via self-service
- Discussion around Self-Registered Guests (anonymous users) still in nascent stage

Sponsored Account Use Cases:

- Early Access for incoming employee
- Consultant, Contractor
- Collaborator in Academic Context
- Mechanism used for cross-registered student
- Visitors for conferences
- More…?

- How is a “GUEST” use case different?
  - Length of time of approval?
  - Level of services?

Guest Use Cases

Today:

- Managed Guests
  - Executive Education
  - Course / Classroom Collaborators (Icommons)
  - Conferences (for wireless network, web site access)
  - Groups of Research or other Academic Collaborators
  - Vendor access via shared credentials (e.g. to test PIN-enables web sites)
- Self-Registered Anonymous Guests
  - Sites that require anonymity (e.g. discussion forums for sensitive issues)
  - Applications for Fellowships
  - Mechanism to expedite allowing a user to be added to a website (User gets the account, then presents it to the web master)
  - Wireless access

Sponsored Account Survey: Likes

- Process is quick
- HUIT staff is responsive
- Can submit requests in bulk
- Doesn't require sensitive information
- Accounts are not deleted, allowing for responsorship
- No official Harvard affiliation required
- Advance notification given prior to account disablement
- Email forwarding
- Some users can select user name
- PIN validation for those accounts with HUIDs

Sponsored Account: Dislikes

- Must manually track responsorship dates
- Request process is manual
- Department related aliases are not captured
- Difficult to issue XIDs
- Long delay between account creation and publication to applications and directories
- Managers can’t assign for each other
- Poorly documented self-service process

Sponsored Account Survey: Conclusion

- Automated emails to sponsor and others upon account creation and prior to account expiration
- Accounts not deleted if not responsored within given timeframe
- Different sets of criteria/restrictions regarding responsorship for different account types
- Quicker, online system
- Automated account creation based on course enrollment
- Ability to transition from one type of sponsored account to another, and from sponsored from to non-sponsored and vice versa
- Automatically prevent the issuance of a new HUID when a POI account is converted to an employee/faculty/staff account
- Ability to see/update all accounts sponsored for renewal\disablement\add & remove access and services
- Add some notes on the account
- Control who can actually sponsor an account with a system of checks and balances

Wrap-Up

- Topic for next meeting
- Recap any action items