HARVARD UNIVERSITY
Information Technology

IAM Lunch & Learn:
HarvardKey Provisioning

August 26, 2015	Wednesday	12:00-1:00 p.m.	6 Story St CR

Today's Agenda

- Today's Objectives
- Provisioning Concepts
- Basic Provisioning Flows
- Source Data
- Provisioning Targets
- Service Entitlements and Lifecycle of Affiliation
- Q&A

Today's Objectives

Our goals for this presentation: Explain HarvardKey provisioning in non-technical terms, and answer your questions.

- These terms from identity and access management can be loaded with buzzwords
- We're trying to avoid jargon, but please don't hesitate to ask for clarification if anything doesn't make sense!

User Provisioning: The Key Concepts

User provisioning is about creating and managing end-user accounts and attributes so that users can gain access to resources. This includes:

- Creating accounts
- Updating attributes in “downstream” systems that are used for authentication and authorizing access
  - Business processes
  - Technical processes for actually updating the data in downstream target systems
- Processes may involve gaining approval in advance, or be directly automated from source data
- No matter how attributes are added or updated, user access, rights, and privileges will all depend on the data that target systems have about the user

Provisioning: Just One Aspect of Identity Management

In the identity ecosystem, unique individuals are assigned *digital identities* and tracked in an *identity registry*.

- The registry contains identifiers and attributes such as personal data, contact data, privacy preferences, and — importantly — roles
- These "persona roles" capture an individual's relationship with Harvard in several different categories: student, alumnus/alumna, employee, or POI (non-student, non-employee "person of interest")
- Roles and other attributes are a (mini) master data record of an individual that provides a foundation for provisioning access to applications
- This data is a "source of truth" that is the basis for provisioning driven by business rules — extracting, transforming, and loading data into downstream systems

Source Data for Provisioning Action

Clean, authoritative source data are critical to success.

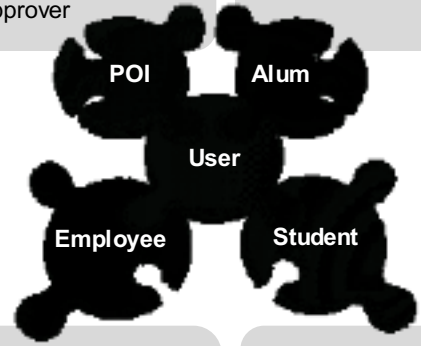
- Authoritative repository of people, with unique identifiers
- Duplicate identities are resolved
- Common data model helps standardize data from multiple sources

POI Role(s), Including Library

- Start date
- End date
- Prime role indicator
- Tub affiliation (faculty code)
- Description/company
- Authorized approver

Alumni Role(s)

- Start date
- End date
- School
- Degree
- Year
- More..



Primary Identity

- ID numbers: HUID, Alumni ID, etc. (i.e. NetID)
- Names: listing/preferred, official
- Date of birth
- National ID
- Images
- Ethnicity, gender
- Longer service, EPE status

Email & Directory Listing

- Official email address
- Directory listings: title, phone number/type, location-related, office/home, dorm (mail center, dorm location)

Directory Privacy

- Name
- Student role
- Employee role
- Special role
- Email (official, onboard, alumni)
- Image
- Address (home, office, dorm, alumni)
- Phone (home, office, mobile)
- FERPA

Addresses

- Address
- Office/home/dorm

Employee Role(s)

- Job start date
- Job end date
- Prime role indicator
- Job status
- Employee class
- Job code
- Job location
- HR department
- Tub affiliation (Faculty code)
- Job title
- Hire date, termination date
- Union code
- Paygroup, paid indicator

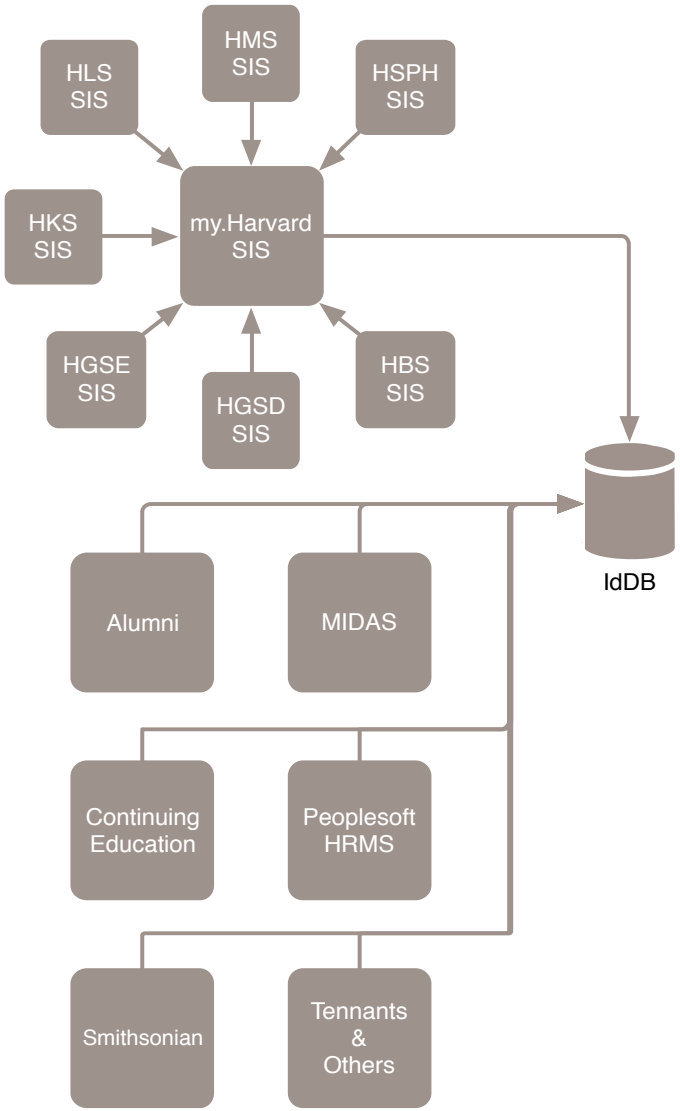
Student Role(s)

- Student status
- Role start date
- Role end date
- Prime role indicator
- School
- Optionally: academic department, special status, House (College), Board House (College)

IdDB: The Main Source for HarvardKey People

IdDB is the identity registry for all Harvard ID holders.

- MIDAS shows you the data in IdDB
- Data originate locally and flow to central systems like HR and SIS
- Feeds from the SORs are consolidated into a common structure that uses roles



IdentityIQ: Harvard's Provisioning Platform

As part of HarvardKey implementation, we are reshaping the process by which users obtain their accounts and access resources in FAS and CA+.

- New provisioning solution, SailPoint IdentityIQ (IIQ), replaces existing Oracle Waveset product
- IIQ reads source data from IdDB, stores user attributes, and performs provisioning and deprovisioning actions on downstream systems
- HUIT Service Desk (and some other helpdesks around campus) will use IIQ to assist users with account and access issues

Other Provisioning of Directory Objects

Accounts are also provisioned for "non-carbon life forms" to enable authentication to protected resources using strong passwords. Accounts are owned by departments, and are needed year to year, but regular reviews must take place to determine if needs are still justified.

Type of Directory Object	Description
Course Account	Account used by administrative staff to email course participants, manage other online content
Department Account	Same as above, but on behalf of a department
Application Account	Used to allow an application to login to online resource such as a database or application interface

Source Data for Provisioning: FAQs

Some commonly asked questions about provisioning source data …

- Where did this IdDB data come from?
- Why is IdDB the “source of truth” for user provisioning?
- What about users who don’t have HUID numbers?
- Is there other information that is required in order to make provisioning decisions?

About Target Systems

Target systems are downstream directories or other data stores that receive user data and enable the credential (login and password).

Target	Used For	User Population
H-LDAP	Authenticating HarvardKey users; attributes	All
University Active Directory	Authenticating to network and email for HUIT-managed services; applications	All but some Alumni and POIs
Auth-LDAP (PIN)	Authenticating PIN users with HUID, XID	Everyone with a PIN
FAS AD	FAS account auth for some FAS-specific apps	All FAS affiliates
FASMail AD	FAS account auth for FAS email (MS Exchange)	@fas email users not yet on 0365
FAS LDAP	FAS account authentication	All FAS affiliates
Kerberos, Homedir	FAS accounts for specific technical type of auth	Most FAS affiliates, but not always used
Google (multiple domains)	Google accounts for @college, @g used by FAS undergrads and University affiliates	Some FAS and other University affiliates

Entitlement for Services

All HUID holders are eligible to claim a HarvardKey — but depending on community of eligibility, access to services will be provisioned accordingly (some automatically, some on an opt-in basis).

Community	Automatically Provisioned	Opt-In
FAS Faculty	FAS AD account, @fas email, @g Google, Unix account	SharePoint
FAS Staff	FAS AD account, @fas email, @g Google, Unix account	SharePoint
Central Employee	@harvard.edu email	SharePoint; @ g google
DCE Student	FAS AD account	@g Google
DCE Non-Degree Student	FAS AD account	@g Google
FAS Consultant	FAS AD account	SharePoint, @g Google
Alumnus/Alumna	No Harvard email or Active Directory account	None

Types of Entitlements

Entitlements fall into two categories: automatic and optional.

Birthright (automatic):

- Assigned when a user becomes eligible (qualifying role)
- Note that not all users qualify for the same services; the provisioning system must be modified as services' eligibility requirements evolve

Permitted (optional):

- Self-service opt-in (i.e. a DCE student who can opt in to an @Google account)
- Assisted by the Service Desk (i.e. an employee who requests SharePoint access)

The User Provisioning Lifecycle

When users are "born into" the IdDB (fed for the first time by a source system of record such as HR or SIS), IdentityIQ creates an *identity cube* for them.

Some accounts are provisioned immediately for all users, and are permanent accounts:

- H-LDAP, for HarvardKey
- University Active Directory, for a subset of populations

Communities of Eligibility

IT services that are dependent on downstream directories tend to organize and offer services to groups of similar users, enabling a business approach that's consistent across populations.

Variations in how services are delivered may include:

- A grace period after formal affiliation terminates
- If there is a grace period, how long?

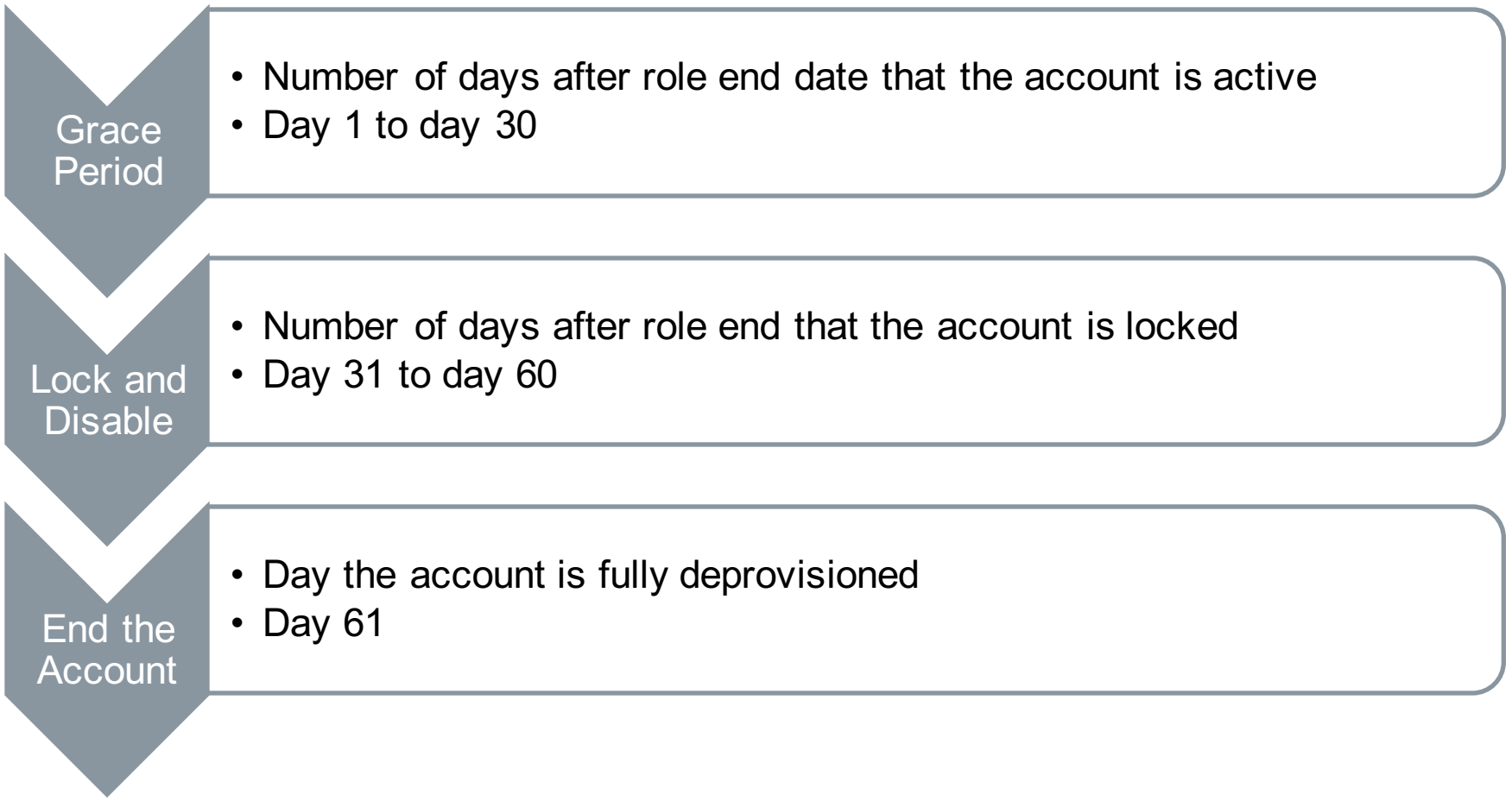
User Provisioning Lifecycle: End of Affiliation

***Deprovisioning* is as important as provisioning.**

- As affiliations end, users may lose eligibility for services such as Harvard email or SharePoint access
- However, eligibility to hold a HarvardKey and maintain its associated password continues indefinitely
- Even though a person may no longer hold an active, current student or employee role, they hold an active, “separated” role
- Users with impending changes in their account status receive automated notifications

User Provisioning Lifecycle: Deprovisioning

Here's an example of a deprovisioning lifecycle.



Lifecycle of Community Membership

By combining the lifecycle and community membership concepts, we supply the provisioning system with attribute data (community membership tags on individual users) that can drive provisioning actions.

- Community definitions are calculated in the source data
- Memberships map to business roles, and IT roles in IIQ
- As users enter or leave communities, their entitlements to services are automatically recalculated to ensure that only eligible users have access to services

Manual Provisioning of Services

Not all provisioning automatically takes place when the source data causes an update to IIQ.

- Some services are requested through Helpdesk and manually added to user accounts
- Others are requested via self-service opt-in, provided the user is eligible

Common Business Scenarios

In all these scenarios, the user will still be seen as one identity in the provisioning system.

- Onboarding
- Request to add an optional service
- Transfers that result in changes to service eligibility
- Dual roles can create a choice of where to create the one email account for a user who is in two different Schools
- Termination of services when affiliation ends

IAM Summer Lunch & Learn Series

Presentations are online now for recaps of this summer's Lunch & Learn sessions!

iam.harvard.edu/lunch-and-learn

- Provisioning (today's presentation!)
- HarvardKey
- POI Sponsored Affiliations
- Multifactor Authentication

Identity & Access Management

SUMMER
Lunch & Learn
BROWN BAG SERIES

Questions?

What other information would be helpful for us to present or publish about provisioning?

Thank you!

HARVARD UNIVERSITY
Information Technology