

Practical Identity Access Management

Lessons From the Field
John Benninghoff

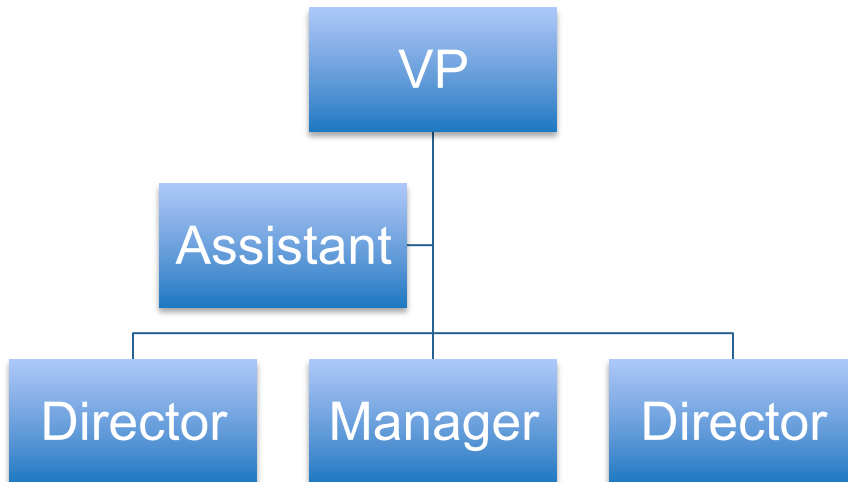
Introduction

- My background
- Lessons learned from designing & building IAM/SSO solutions
- Reflects my personal experience only
- Working with government organizations
- Focus on getting access to the system

Why do you need an IAM system?

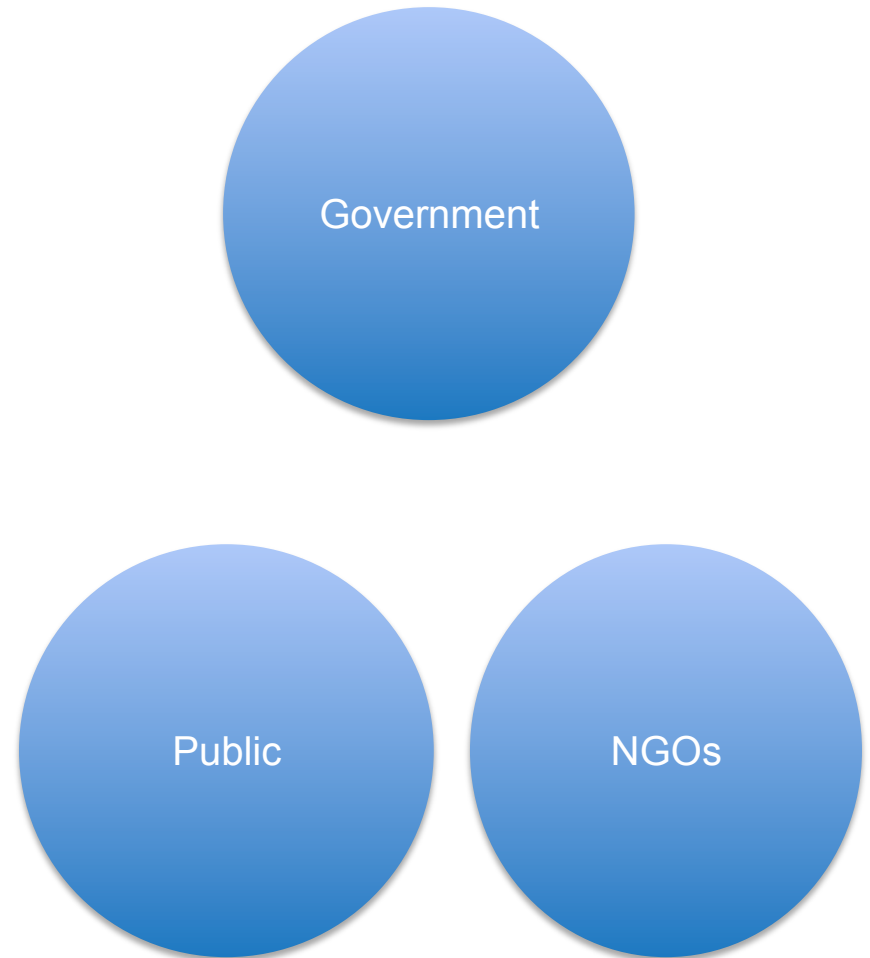
Traditional IAM

- One Constituency
 - Join
 - Change Jobs
 - Reviewed
 - Leave



Government IAM

- Three Constituencies:
 - Government
 - Public
 - NGOs



Buying an IAM Product

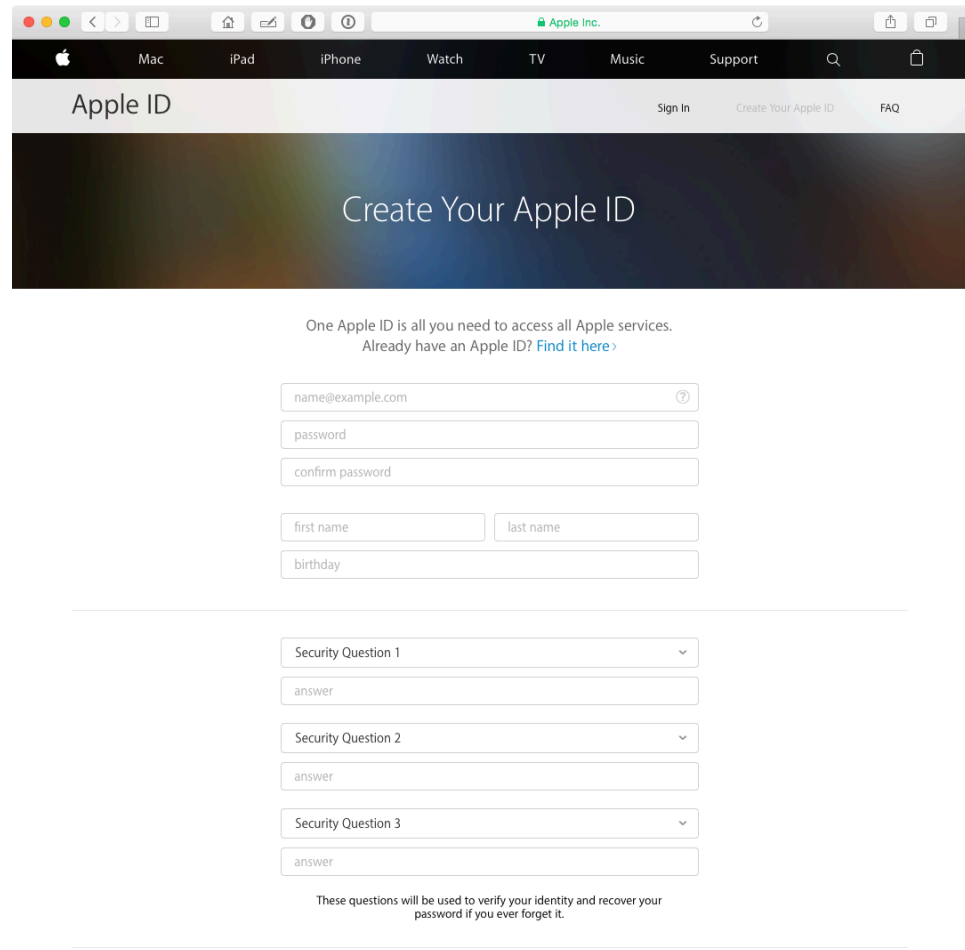
IAM Products

- **They're all expensive**
- **They're all platforms**
- **They all require professional services**

- **Lesson: choose one you can support. Have the professional services team picked out when you buy.**

The User Experience

Getting a User ID



The image shows a browser window displaying the Apple ID creation page. The browser's address bar shows "Apple Inc." and the page title is "Apple ID". The navigation bar includes links for "Mac", "iPad", "iPhone", "Watch", "TV", "Music", and "Support". The main heading is "Create Your Apple ID". Below the heading, there is a sub-heading "One Apple ID is all you need to access all Apple services." and a link "Already have an Apple ID? Find it here >". The form consists of several input fields: "name@example.com" (with a help icon), "password", "confirm password", "first name", "last name", and "birthday". Below these are three security questions, each with a dropdown menu and an "answer" input field. A note at the bottom states: "These questions will be used to verify your identity and recover your password if you ever forget it."

Apple ID

Sign In Create Your Apple ID FAQ

Create Your Apple ID

One Apple ID is all you need to access all Apple services.
Already have an Apple ID? [Find it here >](#)

name@example.com ⓘ

password

confirm password

first name last name

birthday

Security Question 1 ▾

answer

Security Question 2 ▾

answer

Security Question 3 ▾

answer

These questions will be used to verify your identity and recover your password if you ever forget it.

Enrollment

- Getting a User ID
- Identity Matching
- Identity Verification

Enrollment: Getting a User ID

- Public: self-service enrollment
- Government: use existing IDs
- NGOs: requesting an ID OR through federation

Login Screen: Single ID

Who do you use today?

- Case
- Ben App
- Assi



Enrollment: Getting a User ID

- Public: self-service enrollment
- Government: use existing IDs
- NGOs: requesting an ID OR through federation

- Lesson: a person could have 3 or more User accounts
- Lesson: a user account is not a person

Enrollment: Identity Matching

- Identity Matching: comparing 2 or more records to determine if they represent the same person
- Problem for public only (generally) to link a user to “their” data
- Even harder problem than IAM
- Identity matching in banking

Enrollment: Identity Matching



[View My Profile](#) Your information is secure

[Home](#)

[My Mortgage Summary](#)

[Buying a Home](#)

[Refinancing a Home](#)

[Homeowner Support](#)

Link Your Mortgage Accounts

Access your Citi mortgage accounts all in one place.

Already Linked to My Profile

Account Number:	XXXXXX	Nickname:	Home	» remove this link
-----------------	--------	-----------	------	------------------------------------

Link to My Profile

*Required fields

Citi mortgage account:

* Account Number: - X [» View a Sample Statement](#)

* State: * Zip Code:

[Return to View My Profile](#)

[» Continue](#)

† Calls are randomly monitored and recorded to ensure quality service.

TTY Services available: Dial 711 from the United States; Dial 1-866-280-2050 from Puerto Rico.



First mortgage loans are originated by Citibank, N.A. NMLS ID 412915

[Contact Us](#)

Enrollment: Identity Matching

- Identity Matching: comparing 2 or more records to determine if they represent the same person
- Problem for public only (generally) to link a user to “their” data
- Even harder problem than IAM
- Identity matching in banking
- Lesson: IAM shouldn't do identity matching but should record results of ID matching

Enrollment: Identity Verification

- Verifying a user's claimed identity
- Government users are verified at time of hire
- NGO users are verified through a process
- Public users must prove who they are

Enrollment: Identity Verification

Which of the following vehicles have you owned?

- A. 2005 Ford Taurus
- B. 2014 Chevrolet Malibu
- C. 2010 Toyota Prius
- D. 1998 Audi TT
- E. None of the above



Enrollment: Identity Verification

- NIST 800-63-2 discusses in detail
- Lesson: verify identity after granting a User ID but before granting access
- Lesson: provide a manual identity verification process

Enrollment: 3 phase approach

1. Getting a User ID
2. Identity Matching
3. Identity Verification

Logging In (finally!)

Special page

Log in

Username

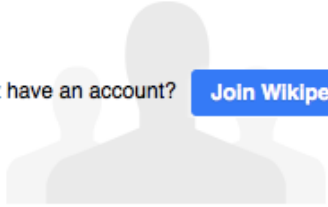
Password [Forgot your password?](#)

Keep me logged in (for up to 30 days)

Log in

[Help with logging in](#)

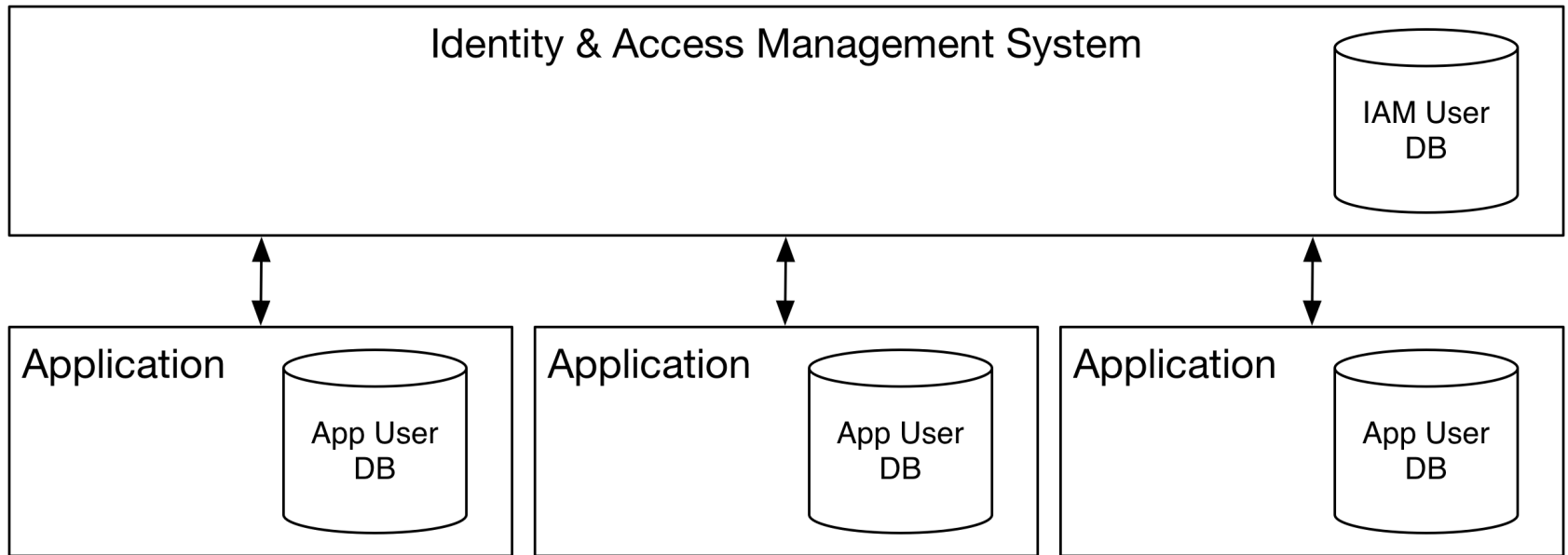
Don't have an account? [Join Wikipedia](#)

A faint background image of three stylized human silhouettes representing user avatars, positioned behind the 'Join Wikipedia' button.

Logging In

- User ID for logging in
- User accounts may span multiple systems

Logging In



Logging In

- User ID for logging in
- User accounts may span multiple systems
- Unique ID for user account
- Single Sign-on:
 - Traditional
 - SAML
 - OAuth

Logging In

- Lesson: don't use case-sensitive usernames!
- Lesson: each constituency needs a unique user ID namespace
- Lesson: Use an IAM-specific unique identifier for user IDs
- Lesson: Use SAML today, also consider OAuth

Managing Access

Getting Access: Role Mapping

IAM Role	Applicant			Case Worker		
Application Role	External User	Applicant	N/A	Internal User	Case Worker	View Only

Getting Access

- Lesson: manage coarse-grained authorization in IAM, fine-grained authorization in the applications
- Lesson: start with fewer roles

Removing Access

- Public: user IDs are “never” disabled
- Government: disable upon termination
- NGOs: disable by process

- Lesson: Manage costs of public users by disabling inactive or abandoned user accounts

Changing & Reviewing Access

- Vision: automated, end-user driven request process
- Request – Notify – Approve – Grant

Questions?

email: john@transvasive.com

twitter: [@transvasive](https://twitter.com/transvasive)