

A Quick Flashback

Last year, at MacAD...


What Apple Said in 2023:

- Separating a managed keystore from the user keystore is a challenge on a deep technical level
- Use cases for that keystore are certainly interesting
- There are “deeper architectural issues” at play
- This is a complicated subject

What We Heard:

-  This isn't happening right now.

What They Actually Meant:

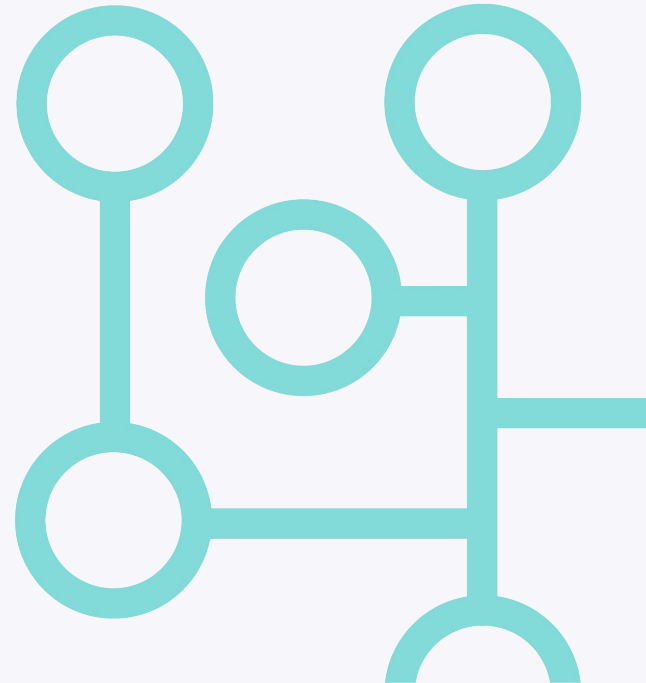
-  This is happening in exactly three weeks.

Listen to what's being said out loud, but...

...recognize that what you take away from a conversation may not be what was intended.

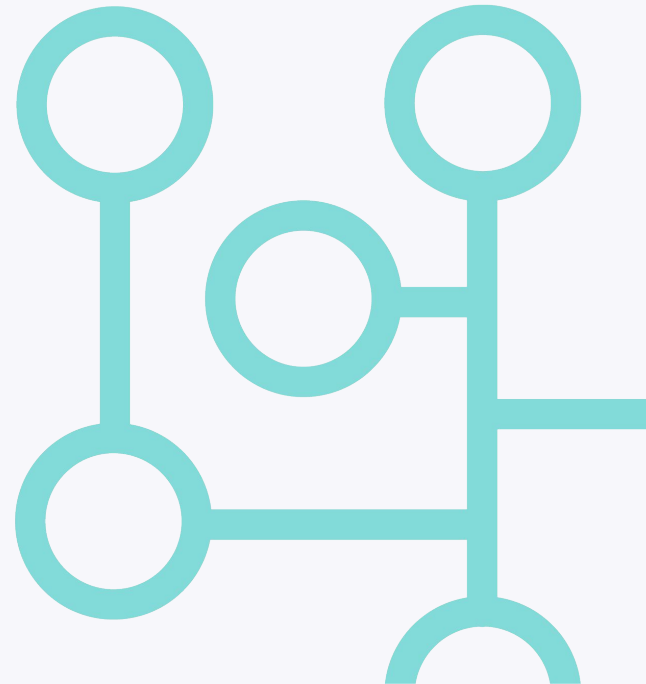
Managed AppleIDs

Threat or Menace?



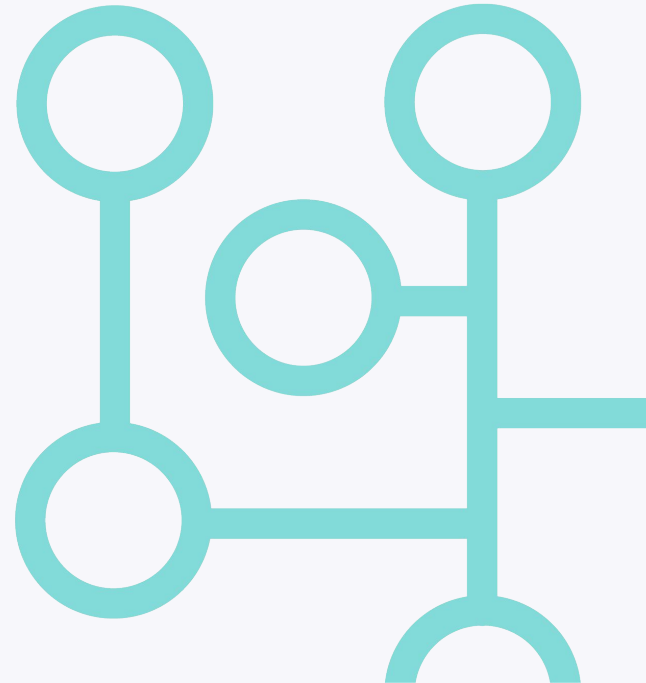
Managed AppleIDs

Will I need a Psychiatrist?



Managed AppleIDs

How Much Faffing About
Will There Be?



Managed AppleIDs

Federation, Challenges, & Opportunities

Tom Bridge, Director of Product Management, Devices



Agenda

- What are Managed Apple IDs?
- Why should I federate authentication?
- Who can I federate to?
- When should I consider this?
- Where is all of this going?

What's a Managed Apple ID?

Apple Business

- Activity
- Locations
- Users**
- User Groups
- Roles
- Devices
- Assignment History
- Apps and Books
- Custom Apps

Search Add

Your Users Filter Sort

All Users
227 Users at Jumpcloud Inc.

Alejandro Abad-Kelly
Device Enrollment Manager - Jumpcloud Inc.

melhem abourjeily
3 Roles - Jumpcloud Inc.

JumpCloud Admin
Administrator - Jumpcloud Inc.

Sam Aduamah
3 Roles - Jumpcloud Inc.

Andres Aguilar
2 Roles - 2 Locations

Cristopher Aguilar
Device Enrollment Manager - Jumpcloud Inc.

Angelica Aguirre
Device Enrollment Manager - Jumpcloud Inc.

Omar Al Fil New

Tom
Jumpcloud Inc.

9:41 Signal Wi-Fi Battery

< Apple ID **iCloud**

iCloud+ 20 GB of 50 GB Used

Backups Photos Docs Others

Manage Account Storage >

Recommended For You
Share iCloud+ with Family, and 3 more >

APPS USING ICLOUD

- Photos On >
- iCloud Drive On >
- iCloud Mail On >
- Passwords and Keychain On >

Show All >

DEVICE BACKUPS

- iCloud Backup On >

ICLOUD+

- Private Relay Off

WED
28

iCloud

Sign In

User iOS Configuration ⓘ

You can control if a user's personal Apple iOS Device can enroll in JumpCloud's MDM to access company resources. Select Allow users to enroll mobile devices, and instruct the user to log into the User Portal and go to Security > Enroll Your iOS device. After the user scans a QR code to enroll the phone in MDM, the enrolled iOS device is visible in the Admin Portal.

Allow users to enroll personal mobile devices and access **Enroll Your iOS Device** in the User Portal.

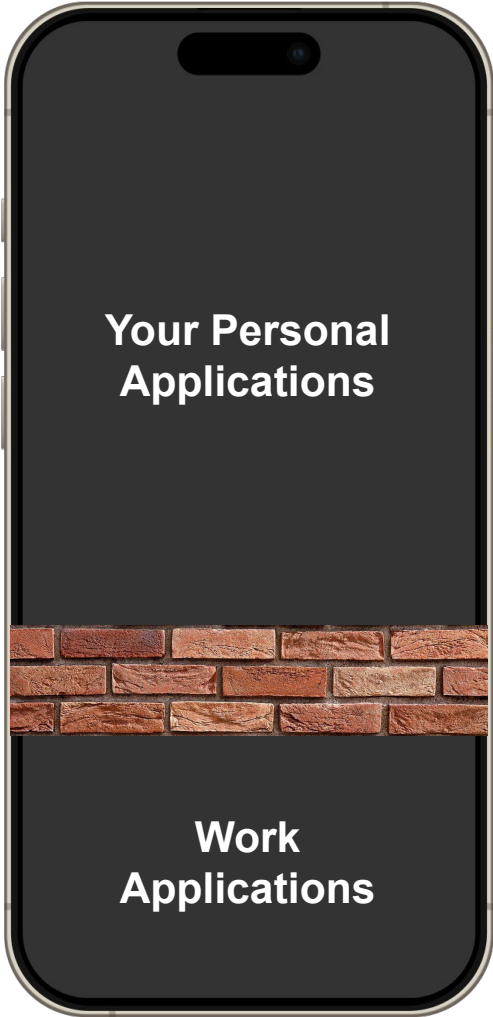
Select the Device Group to automatically add enrolled devices to:

Device Group: **BYOD iOS Devices** ▾

Enroll Your iOS Device

You can enroll your personal iOS device in JumpCloud's Mobile Device Management (MDM) so that you can access company resources, such as email, calendar, contacts, and documents. Click "View QR Code" to scan a QR code to enroll your device. Ensure that you are in a private, secure environment before you scan the code.

[View QR Code](#)



Your Personal
Applications

Work
Applications

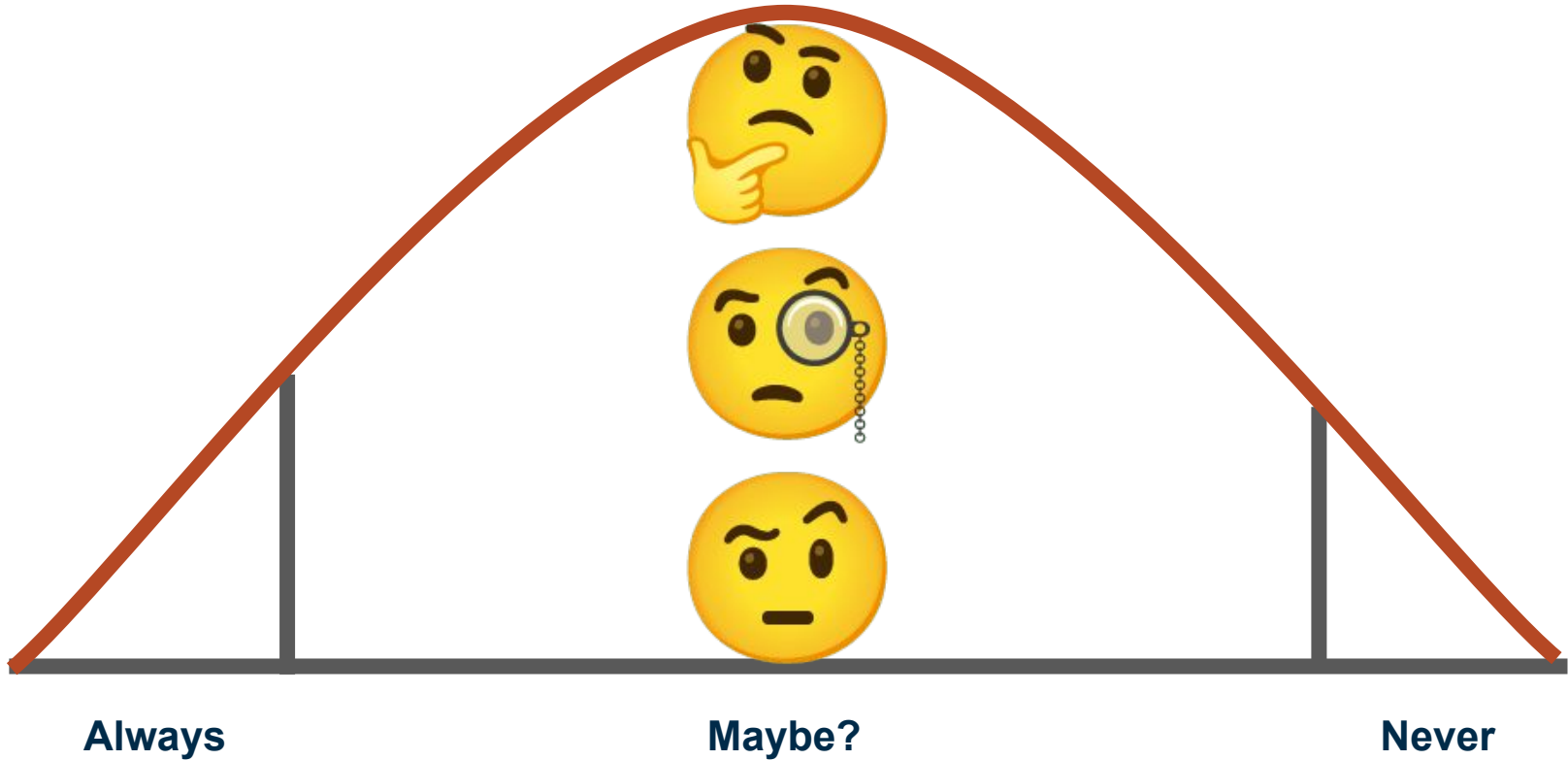
What Can They Do?

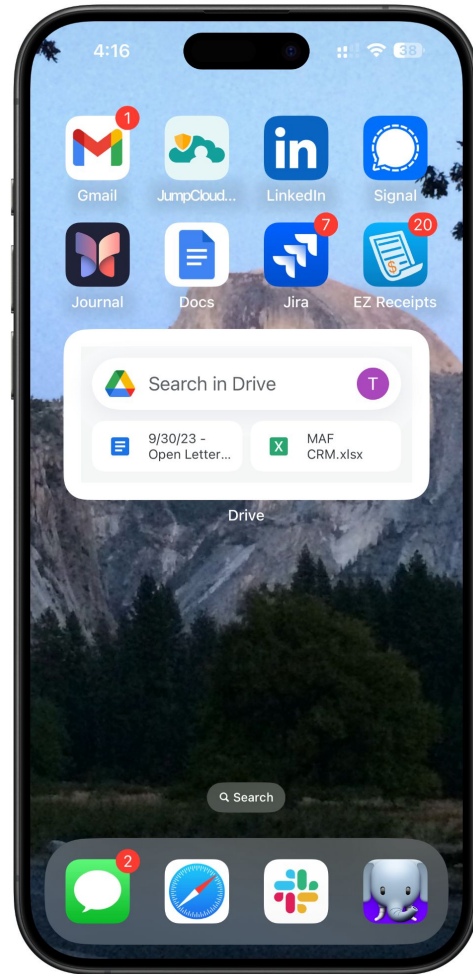
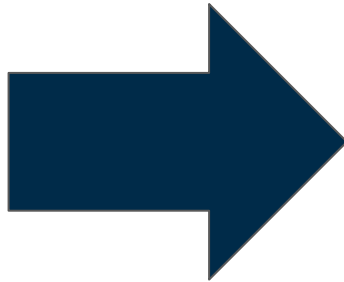
- Sign-in to Apple services
 - **Anchor an iCloud Keychain, with Passkeys**
 - **Support Continuity Features like Handoff**
- Sign-in to third party services
 - [Sign in with Apple](#)
- Perform a User Enrollment for BYOD iOS Devices
- Backup iOS Devices (up to 5GB)
- Use iCloud Drive (up to 5GB)
- **Gate Access to Developer Tools**
- **Hold Identities and Cards in Wallet**

Why Should I Actually Deploy These?

Managed Apps on Unmanaged Devices

- User-Enrolled MDM is **privacy-preserving** without **compromising management**.
- Both sides hold some **trust** in the other party without giving up **privacy**.
- Enrollment gates access, and preserves ownership.





What You Know

SN: XHFJ1289FJ0

Phone: +1.571.243.3555

MAC: 02:03:40:cb:bc:01

Apps: Instagram,
Facebook, WhatsApp,
Whova, Airbnb,
1Password



What Your MDM Knows

EID: 010204104050892

Apps: Google Drive,
JumpCloud Protect,
Jira, Confluence, EZ
Receipts, Expensify



What Your MDM Can Do in User Enrollment

Policy:

- Work Apps Separate
- 6-digit non-simple PIN
- No Screenshots
- No Pasteboard across Management boundary
- Delete Managed Things at Unenroll
- Apply Accounts in Managed Containers

Apps:

- Send, but not replace, Managed Applications
- Patch Managed Apps

Comms Strategy

- Make People Comfortable Early
- Demonstrate What You Can See, So They Can See and Believe
- Clarify Your Apple ID Plan
- Provide Utility and Usefulness

Why Federate?

A Primer on OpenID Connect, System for Cross-Identity Management,
and Shared Signals Framework

In the beginning...

...there was the Password.

Site	Password
Netflix.com	Hunter2
ParamountPlus	Hunter22!
Peacock	hunter2!
HBO Max	hUnter22!12
Hulu	hunter2
Disney+	Hunter222

Authentication vs. Authorization

Who Are You? Do You Belong Here?

AuthN

- Password
- Passkey
- Identity Certificate
- PIN
- Hardware Token

AuthZ

- Group Membership
- Application Permissions
- Time of Access Evaluation
- Contextual Awareness

Federation is all about Context and Control

Most importantly, **Centralizing** those things

- A single user and authentication source for all your apps*
- Grouping those users and providing richer data for decision-making
- Allow or Deny access based on rules (who/what/when/where)

* That support use of external identity providers, and hopefully don't make you pay the [SSO Tax](#).

When should you federate?

Federating a Domain for Managed Apple ID

Keeping Control for the Business



Accounts

Domains

[Edit](#)

Only verified domains can be used to create Managed Apple IDs.

- demonimpcloud.com
- jumpcloudlabs.appleid.com

Federated Authentication

[Edit](#)

Federated authentication allows your users to sign in to their Managed Apple ID by signing into their Identity Provider.

- ✔ Custom Identity Provider Configured

To enable automatic creation of Managed Apple IDs, turn on [Directory Sync](#).

Benefits for You for Federating

- Account creation using your domain is limited to Apple Business Manager
- Create accounts using an external directory
- Know who has a company domain Apple ID
- Password Resets can flow through your Helpdesk or Directory

Stuff You Have to Deal With During Federation

- Apple IDs created before federating have a time they can hang around.
- They will have to change their identity, but you still have no control over them.
- This takes 60 days to complete.
- You have no way to know who has these accounts before you start.

The Federation Timeline

1. Verify Your Domain via DNS Record Changes
2. Begin Federation Process
3. **Resolve Apple ID Conflicts**
Up To 60 Days Required...
4. Finalize Federation
5. Configure Provisioning
6. Begin Program

Who can I federate to?

**Until this past January:
Google
Azure AD / Entra ID**

**Now: Google, Azure AD and
anyone who does
OpenID Connect and Shared
Signals Framework!**

How Does Federation Work?

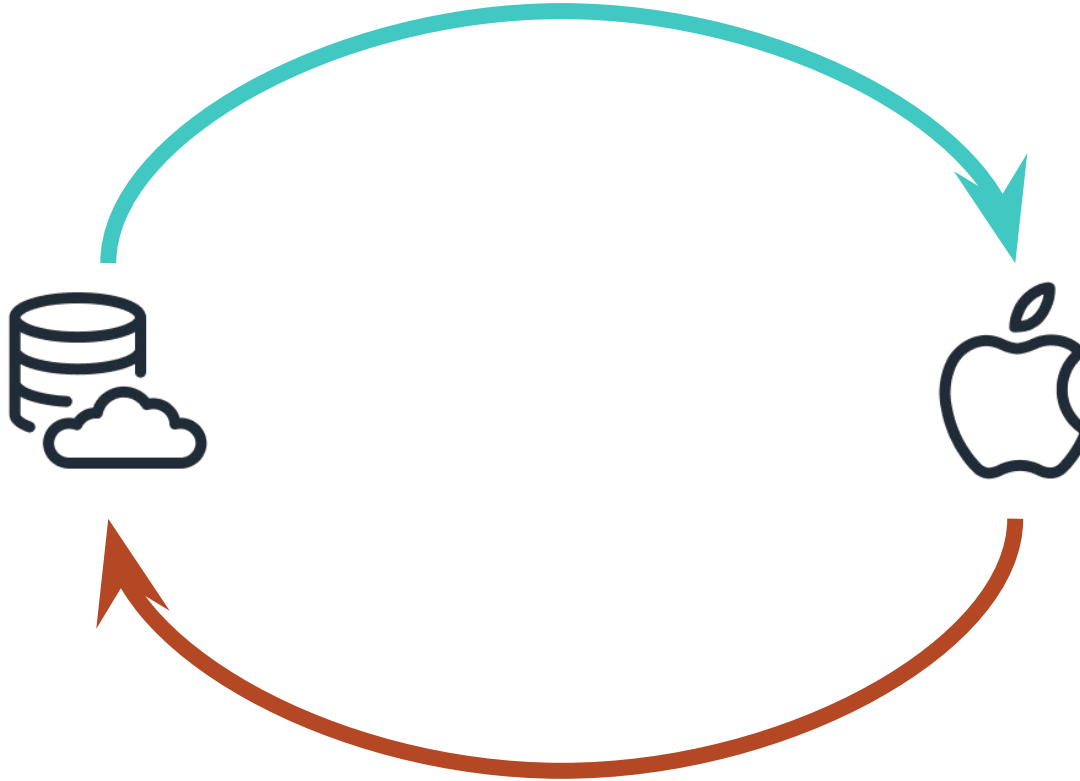
Open ID Connect

What if I just wanted to use one
identity everywhere?

- Begun in 2005 by Brad Fitzpatrick as a way to authenticate users from outside LiveJournal to allow commenting.
- Yes. LiveJournal.

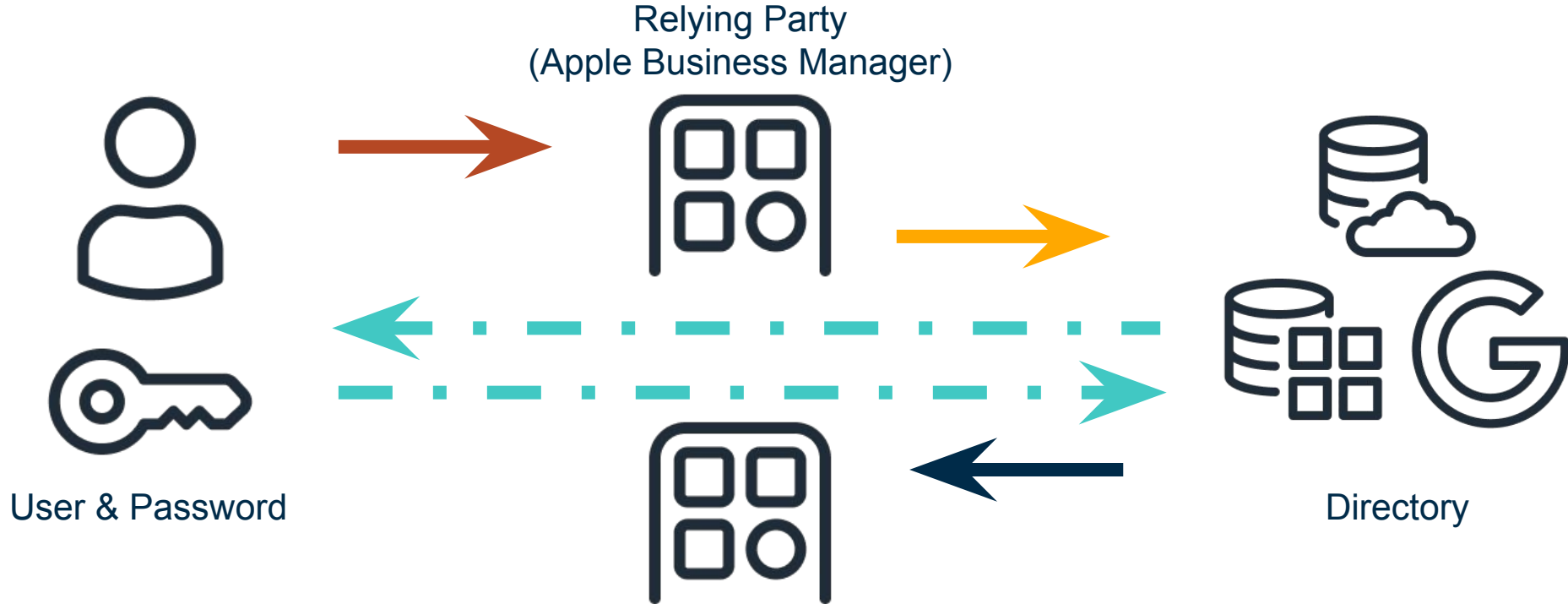


User Accounts, via SCIM



User Access, via OpenID Connect

Access to Applications via OpenID Connect



Wait.

Isn't this just more passwords?

Not quite! It's Tokens.

OpenID Tokens

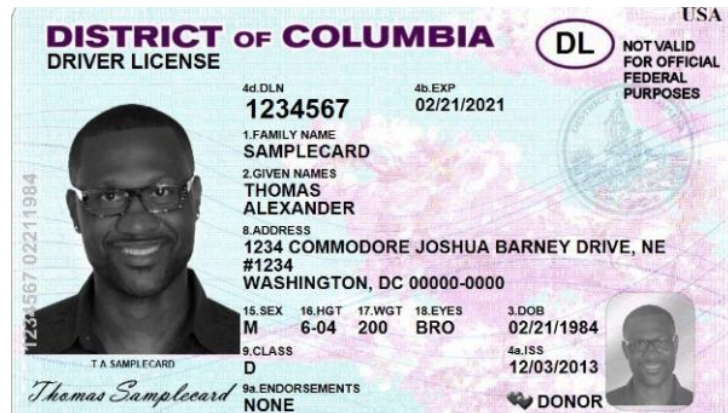
They're not **exactly** passwords.

On successful AuthN, you often get:

- An ID Token, signed
- An Access Token, encrypted

ID Tokens say who you actually are

Access Tokens let you through the streetcar turnstyle.



OpenID Tokens

They're not **exactly** passwords.

On successful AuthZ with an Access Token, you get:

- A Session cookie, or similar
- Another Access Token, encrypted

Most Access Tokens are only ever good ONCE.
Most Access Tokens get you another Access Token for Next time.



An ID Token's Payload

```
{  
  "iss": "https://console.jumpcloud.com",  
  "sub": "jc-012031054591925cd23057f",  
  "aud": "my_federated_AppleID",  
  "exp": 1716459371,  
  "iat": 1716457371,  
  "name": "Thomas Samplecard",  
  "given_name": "Thomas",  
  "family_name": "Samplecard",  
  "birthdate": "1984-02-21",  
  "email": "t.samplecard@pretendco.com"  
}
```

Issuer of ID Token
GUID of this Identity
Who This Token is For
Expiry Datestamp
Issued Datestamp
Full Name for Identity
Given Name for Identity
Family Name for Identity
Birthdate for Identity
Email for Identity

ID Tokens also contain headers and cryptographic signatures

Thomas.

**I just got over my overwhelming
fear of Kerberos.**

Those look like TGTs.

I am triggered right now.

**Since You Don't Have To Do
Your Own DNS For This,
It's Not Scary.**

Shared Signals Framework

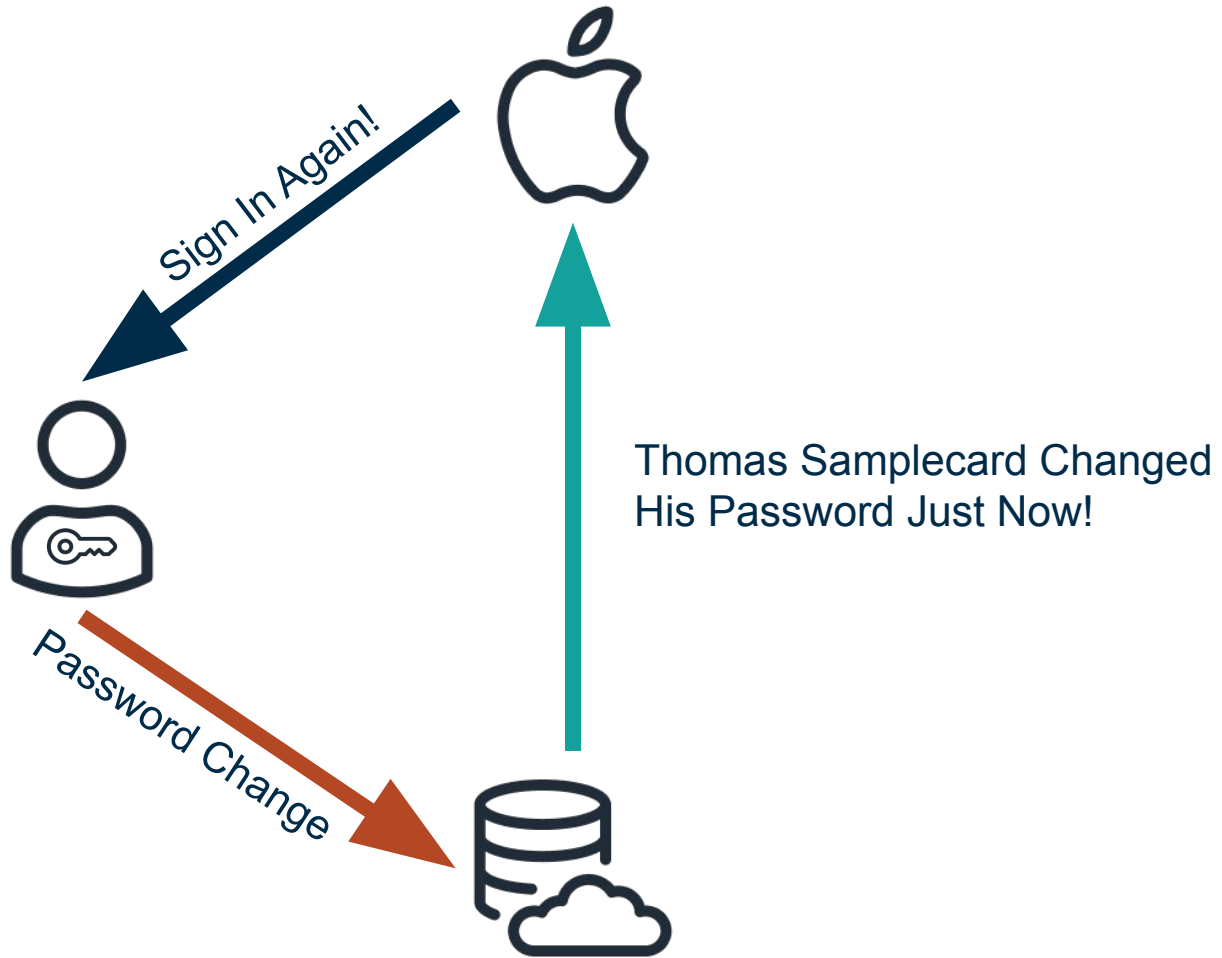
What if I wanted to tell someone about account changes?

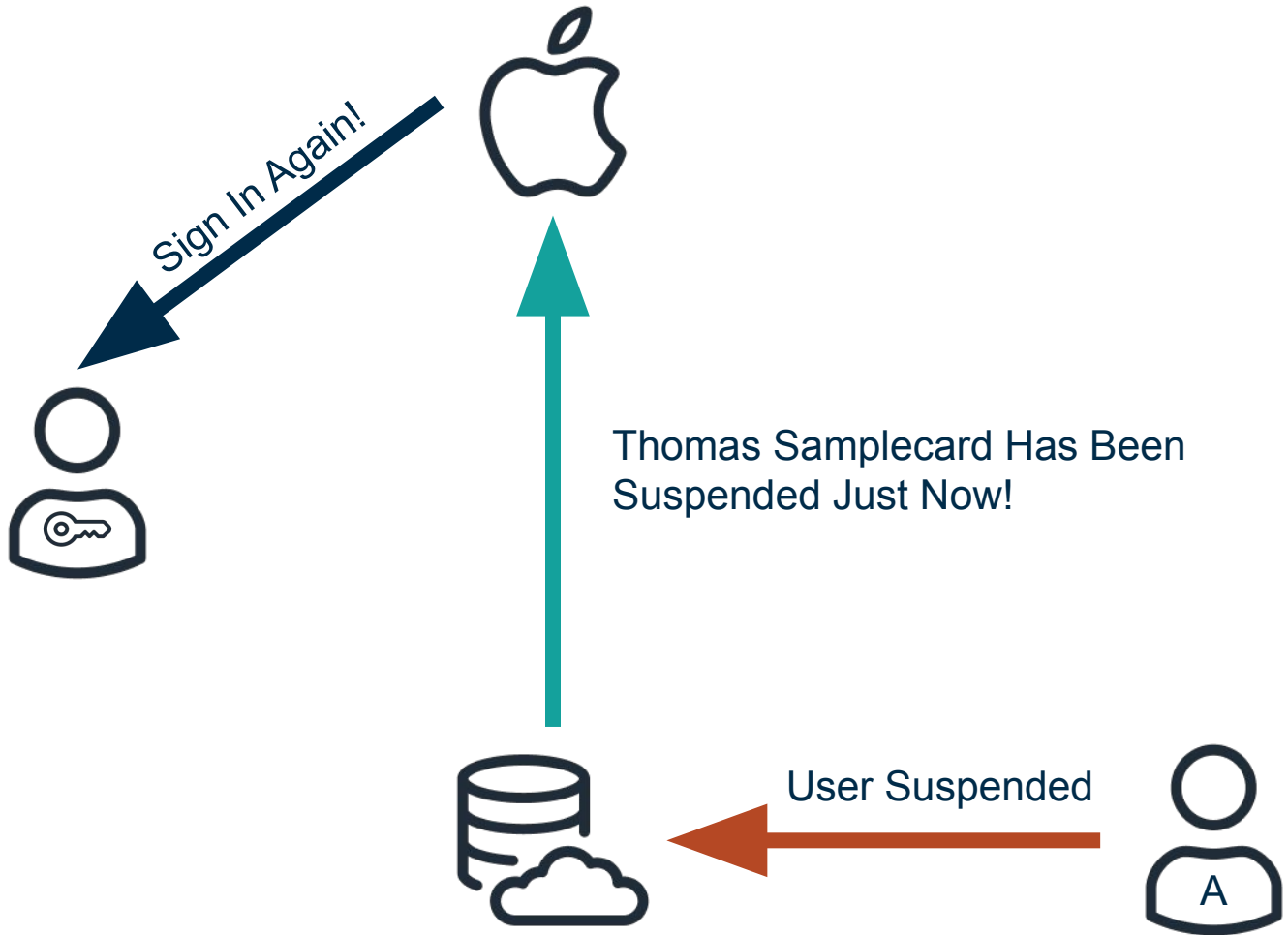
- Still a Draft Specification of the OpenID Group
- Latest updates in mid-2023
- Ratification...?





Photo by [70023venus2009](#) on Flickr, used under CC License





What Do You Need To Federate with OIDC?

And where do you need to get it from?

Get From IDP for ABM:

- Client Secret for OIDC
- Client Identifier for OIDC
- OpenID Connect Well-Known URL
- Shared Signals URL

Get From ABM for IDP:

- Redirect URL for ABM

But What About Provisioning?

OIDC without SCIM is like...



Relying Party
(JumpCloud)



Identity Party
(Apple Business Manager)



What Do You Need To Use SCIM with ABM?

And where do you need to get it from?

Get For IDP From ABM:

- Client Secret for OIDC
- Client Identifier for OIDC

Get For ABM From IDP:

- Redirect URL for ABM

Takeaways on Apple IDs

Managed Apple IDs & Your Business

- This Isn't Something You Do By Accident. Or Quickly.
- There are GREAT reasons to deploy Managed Apple IDs
- When you do it, Federate it.
- If you don't have a test domain, now's the time to make one.
- File Feedback to make use-cases better.

