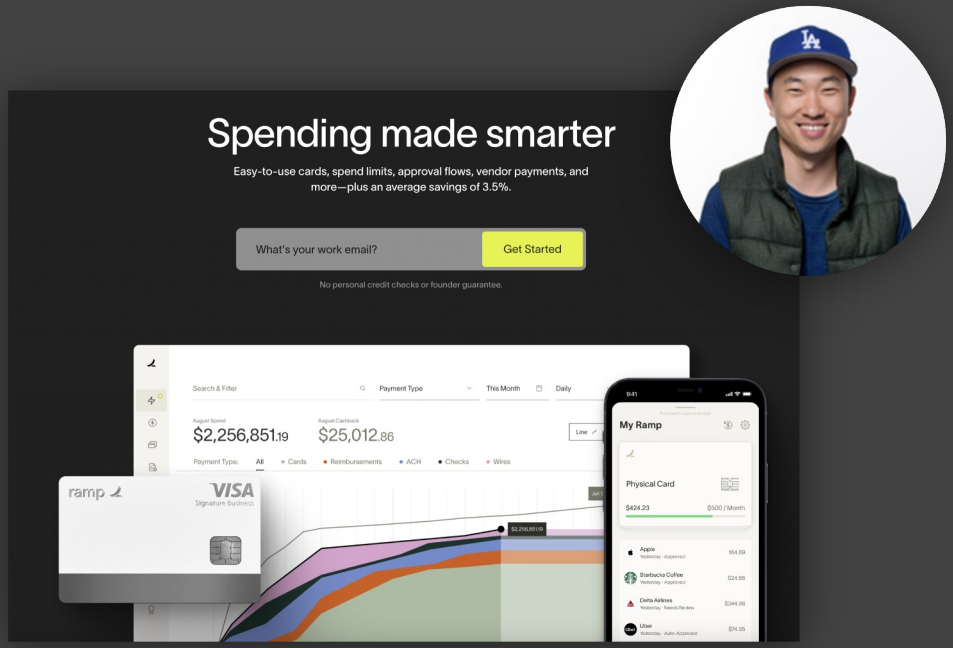
Passkeys

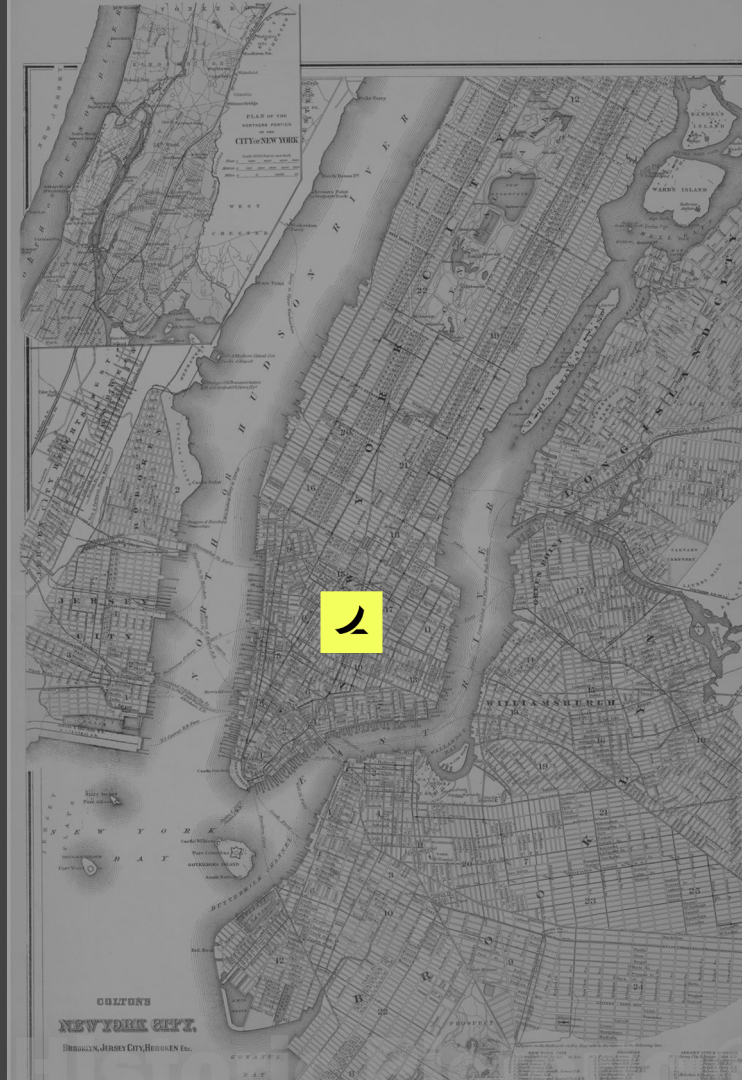
Considerations for (mobile) Enterprise Deployments

John Yang, Ramp | July 2023

Who am I?

- John Yang - Director of Corporate IT @Ramp
- Find me at Macadmins Slack





Why Passkeys?


PASSKEYS
+ DYNAMIC
AUTH POLICIES
IT +
SECURITY
PASSWORDS
WITH MFA*


PASSWORDS
AS ONLY FACTOR

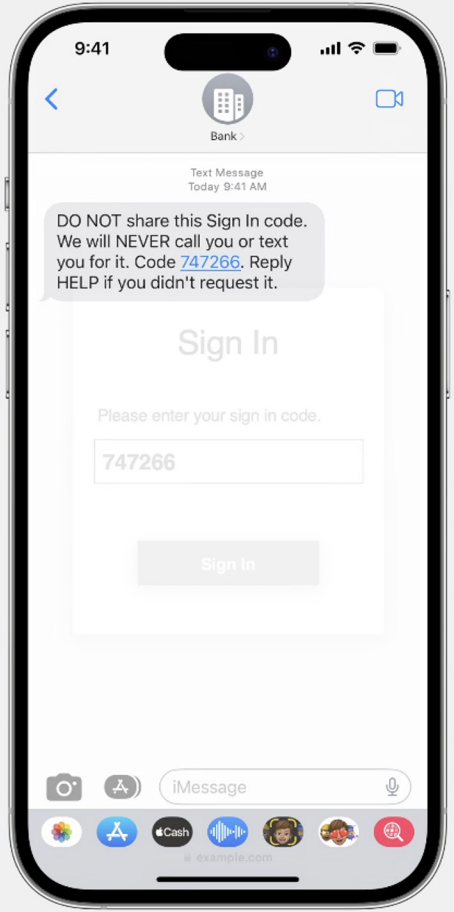
Passwords + Traditional 2FA alone are no longer account takeover or phishing resistant.

okta

Authenticator Type	Deployability	Usability	Phishing Resistance	Real-Time AiTM Resistance
Password	Good	Moderate	No	Very weak
Security Question	Good	Moderate	No	Very weak
SMS, Voice, Email OTP	Good	Strong	No	Weak
Mobile/Desktop OTP apps	Moderate	Moderate	No	Weak
Physical token OTP	Weak	Moderate	No	Weak
PIV smart card	Weak	Moderate	Yes	Strong
Mobile app push notifications	Good	Strong	No	Moderate
FIDO2.0 / WebAuthn + CTAP2	Moderate	Strong	Yes	Strong
Okta FastPass	Good	Strong	Yes	Moderate

Tricking users to bypass 2FA

Type of 2FA	Attack
SMS	Phishing
TOTP	Phishing
Push notifications	Push fatigue



Goal: Phishing resistance across desktop + mobile... quickly, and cheaply


yubico

security

adoption

cost/complexity

How can Passkeys solve this?

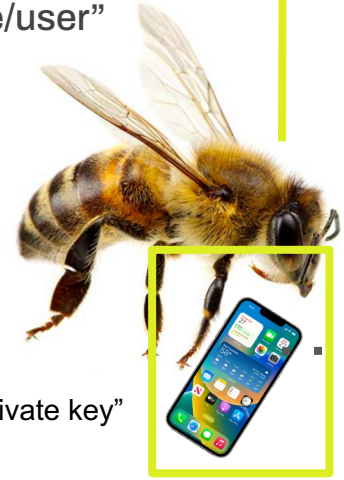
Also what is a passkey?

Passkeys can qualify as two factors in one

Something you have

Something you are

“bee/user”



“private key”

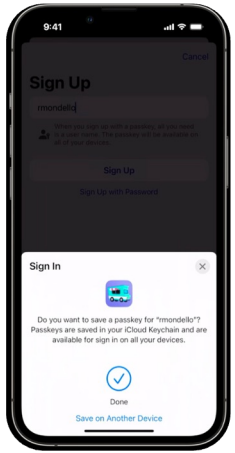
“(roaming authenticators)”

“public key”

onelogin

“relying party” or RP

“biometric factor”



Passkeys Adoption

This can be done in one week

- Testing for just IT
- Update New Hire onboarding to include
- All Hands to entire company about Passkeys
- Hit the button (configure your IDP for webauthn/FIDO2 MFA as required)

How to enroll a Passkey

Requirements

In order to use passkeys, ensure that your mobile device is on iOS 16+ and Android 9+.

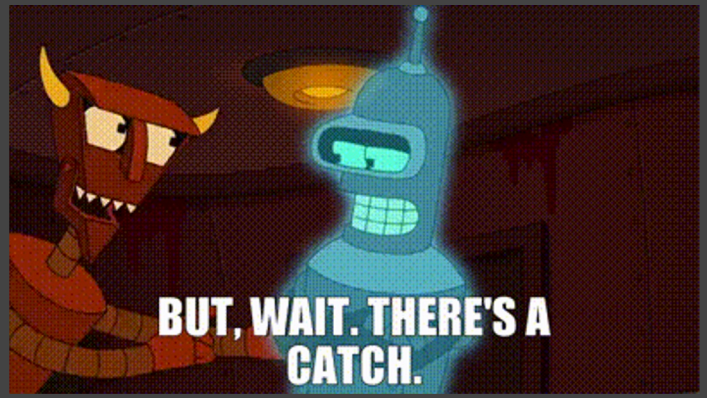
MacOS enrollment

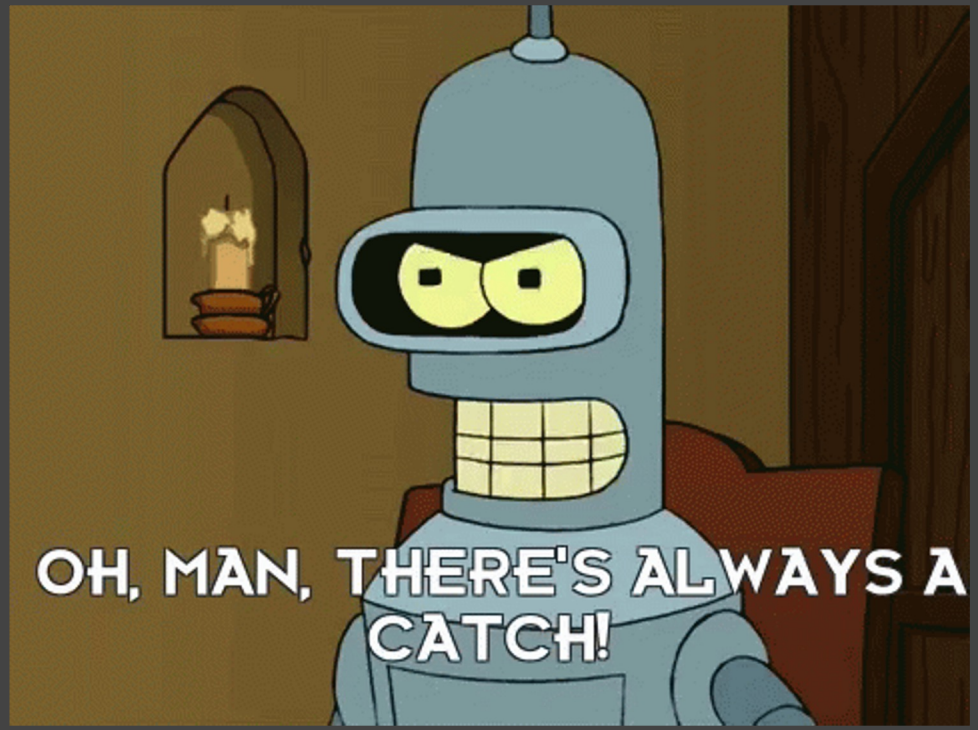
1. Go to your Okta profile settings - go/okta-profile
2. On the top right click `Edit Profile`

Simon
Ramp

Go on…

- We saved lots of money $50K 5ci = $75 + logistical headache (lost/stolen/new hire setup etc)
- 100% Adoption rate for 550 users in < 1 week
- Reduce average time to login for organization from 63 hours in to 15 hours per month
- Most users have a compatible roaming authenticator already (their phone)


BUT, WAIT. THERE'S A CATCH.


OH, MAN, THERE'S ALWAYS A CATCH!

But what are some disadvantages to the current implementation for passkeys?

NIST BEE

Multi-factor cryptographic software authenticators SHOULD discourage and SHALL NOT facilitate the cloning of the secret key onto multiple devices.

- Compromised user Google Workspace account / Apple ID can cause a passkey to be compromised
- Roaming authenticators implementation forces you to live in walled ecosystem, e.g. iCloud Keychain Sync/Google Password Manager
- Lack of full support from 3rd Party Password Managers (for now!)
- Not AAL3 compliant under current implementation, due to lack of adoption of device bound keys

Go on…

- Apple and Google Workspace have many chances for use to be notified and account recovery is strong:
  - Both require Pin code of a previously setup mobile device to setup password sync.
- Compromising a user's Workspace/Apple ID is not impossible, but raises level of difficulty vs buying credentials + MFA attack.
- Deprecates need for hardware tokens, while maintaining *similar* level of authentication assurance levels
- Most users have a compatible roaming authenticator already (their phone)

The biggest problem with Passkeys:

What if someone gets a passkey who shouldn’t?

Passkeys + Dynamic Authentication policies can be a path to mitigate this problem.

PASS BEE

Even if you don’t use Passkeys, you should still have risk based authentication policies!

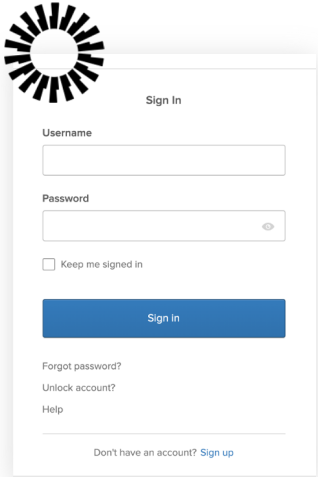
Let’s see how…

The “evil bee” scenario

“evil bee”

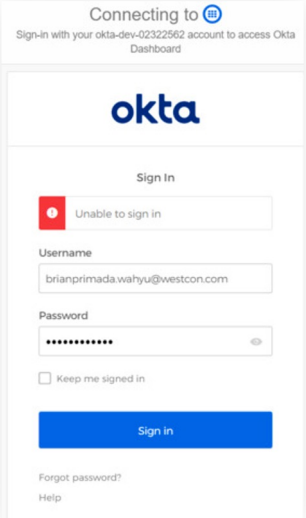
“Different device, synced with iCloud Keychain, has passkey”

“relying party” or RP



“I don’t recognize this device, based on the last 20 successful authentications. Let’s see some ID”

“dynamic risk auth policy”



By stepping up, and forcing a user to provide additional factors, when a new device is detected at login, this mitigates the biggest risk of passkeys.

Most IDPs support Risk based login approach, Okta, Ping.

A brief history of Apple Passkeys

I've been talking about it for years!

Apple on Passkeys in 2021

Authentication methods

	Memorized passwords	Password manager	Password + OTP	Security key	Passkeys in iCloud Keychain
Easy to use	✓	✓	✓	✓	✓
Works on all your Apple devices	✓	✓	✓	✓	✓
Works on non-Apple devices	✓	✓	✓	!	!
Always with you	✓	✓	✓	✗	✓
Security level	✗	!	!	✓	✓
Recoverable	✗	!	!	✗	✓
Phishing resistant	✗	!	!	✓	✓
Doesn't require shared secrets	✗	✗	✗	✓	✓

Apple on Passkeys in 2022

Protects against	Memorized password	Password manager	Password manager + SMS/TOTP	Passkey
Guessing	✗	✓	✓	✓+
Credential reuse	✗	✓	✓	✓
Device theft	✓	!	!	✓
Phishing	✗	!	!	✓
Server leaks	✗	✗	✗	✓

Apple on Passkeys in 2023

- Manage the Apple IDs used with iCloud Keychain and passkeys
- Ensure passkeys only sync to managed devices
- Store passkeys created for work in iCloud Keychain of managed accounts
- Prove to relying parties that passkey creation happens on managed devices
- Turn off sharing of passkeys between employees

Apple Update

- All updates have major asterisks.
  - Controls for which devices Passkeys are synced to
    - Requires Managed Apple ID
  - Controls on Passkey Creation
    - Only works if Relying Parties support it
    - Likely will take some time

Google Update

- Note: Starting from Android 14, users will be able to opt to use third-party credential management apps to store their passkeys.
- As of May 2023, Chrome on macOS and Windows stores passkeys on the local device only.

3rd Party Coming Soon!

bitwarden

DASHLANE

DUO

1Password

	WebAuthn based	Supports multiple devices	Supports multiple platforms	Cross-platform sync	Sharing passkeys	Data portability
Passkeys in 1Password	✓	✓	✓	✓	✓	✓
Other platform passkeys	✓	?	?	?	?	✗

Bitwarden Roadmap 2023

Timelines listed are for beginning product research and development (R&D) unless otherwise noted.
Ongoing Research: Overlay popup interface, Auto-type/Autofill for logging into other desktop apps

	1st half of 2023 - R&D priorities		Future initiatives	
Vault Experience and Community	Passwordless Login Options	Vault Item Sharing	Passkey Support	Offline Editing
	Custom Item Types	Enhanced Localization	Referrals	Desktop App Updates
	Vault Item Labels	Account Switching - browser	Notification Center	

Manage passkeys with Dashlane

Dashlane is preparing to help you manage your online life with sites using passkeys. For the moment, only a few websites and platforms have the technology to do so. For sites set up for passkey login, you can manage and use your passkeys with Dashlane in these ways.

What you can do	Web app	Android	iOS (Apple)
Save and store passkeys	✓	Available with Android 14 Beta Program	Coming soon (iOS 17)
Log in to your accounts with passkeys	✓	Available with Android 14 Beta Program	Coming soon (iOS 17)
View, edit, and delete passkeys	Coming soon	Available with Android 14 Beta Program	Coming soon (iOS 17)

Should I deploy passkeys?

security

adoption

cost/complexity

Resources

- Lastpass Sec Incident Write Up
- Security update | Uber Newsroom
- Deploy passkeys at work - WWDC23 - Videos - Apple Developer
- Now in beta: Save and sign in with passkeys using 1Password in the browser
- Passwordless Authentication: Step into the Future with NordPass
- Take Your Security to the Next Level with Context-Based Authentication | Okta
- FIDO Alliance
- Passkeys.directory
- Risk-based Authentication | Ping Identity
- Risk-Based Authentication: What You Need to Consider | Okta
- Not All MFA Is Created Equal
- 2023 Data Breach Investigations Report | Verizon
- About the security of passkeys - Apple Support
- Factor Types and Authenticator Assurance Levels - an overview
- NIST Special Publication 800-63B
- Passkeys (Passkey Authentication)
- Say goodbye to passwords: The rise of Passkeys | OneLogin

Thank you

June 2023 @johnyang linkedin/johnkyang