What to consider when adopting Passkey and how to build a great Passkey user experience

Huan Liu

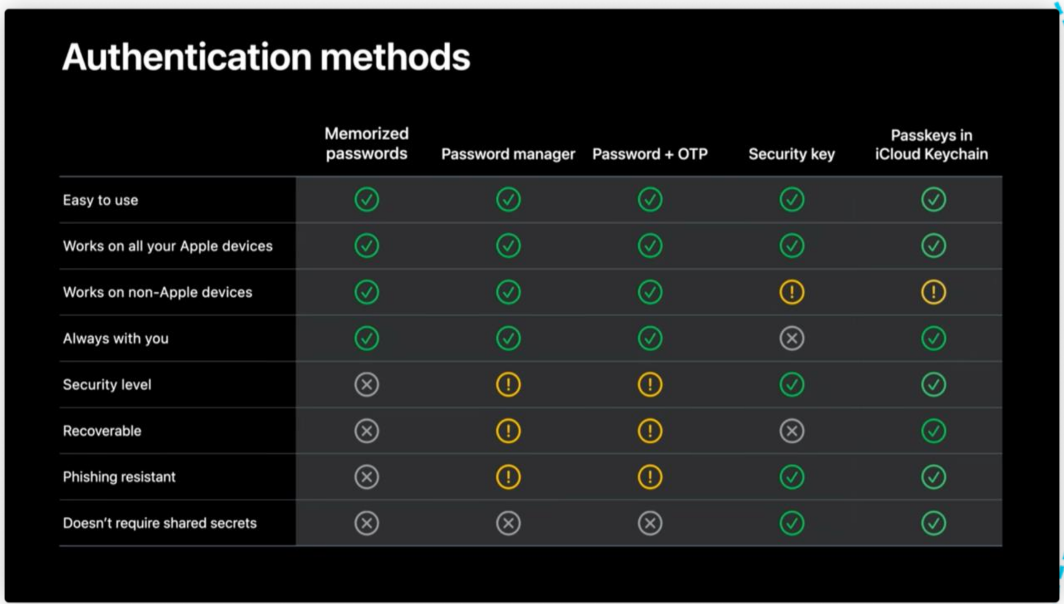
Head of Access Management

Cash App, Block

Passkey

- Lots of benefits

- But adoption is not straightforward



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	✗	✗	✗	✓	✓

This talk is about understanding the constraints and how to accommodate their limitations

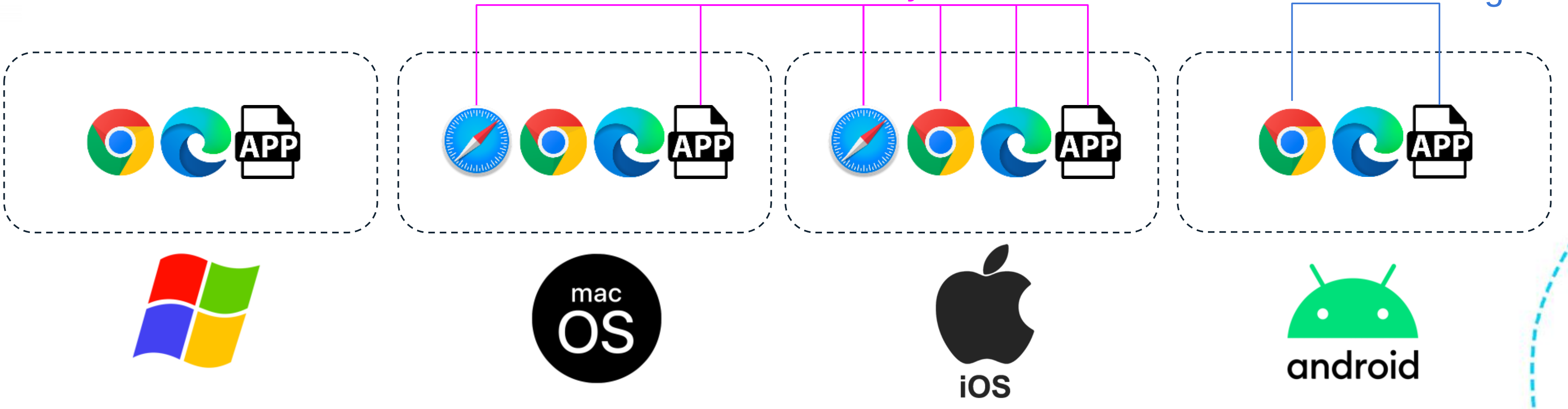
Agenda

What you need to consider when adopting Passkey?

1. Platform variation
2. Managing security guarantee
3. Difference from password
4. Gradual transition

Platform variation

Syncing is fragmented



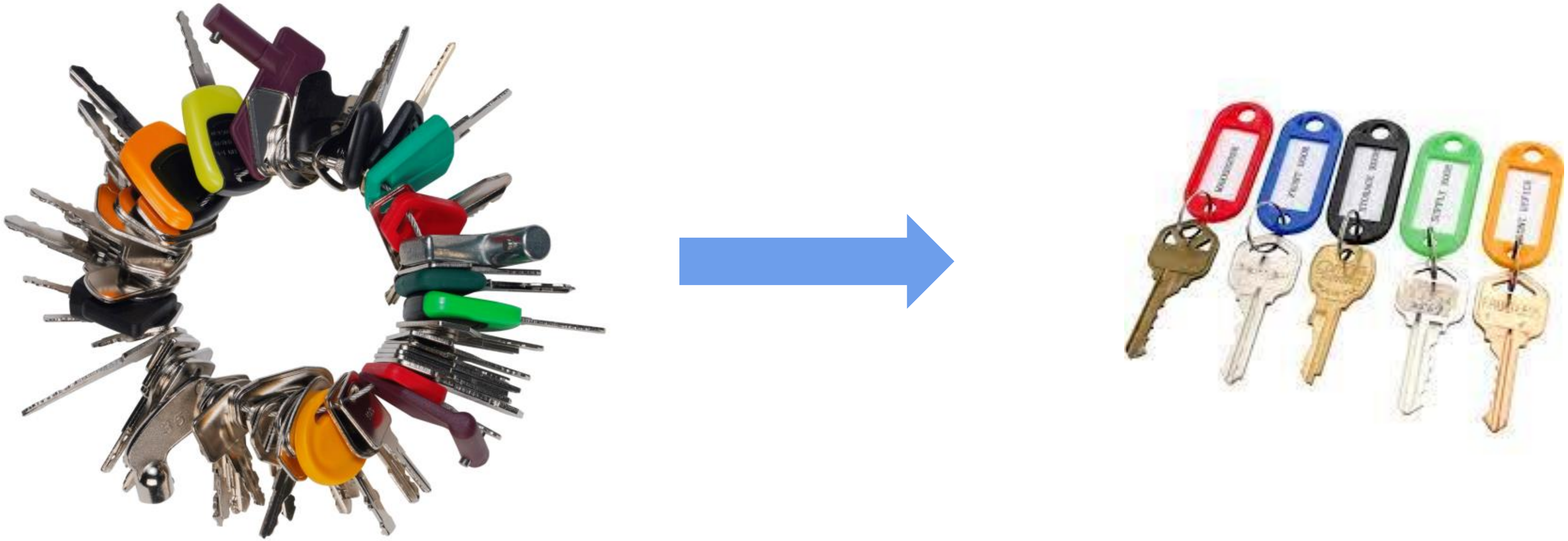
Shared via iOS Keychain

Shared via Google Password Manager

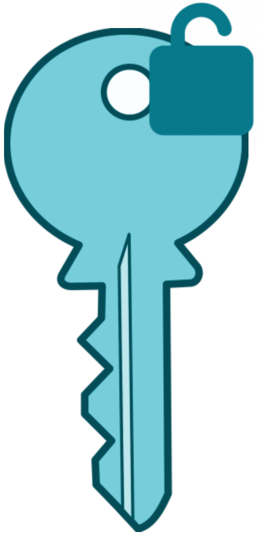
Pass~~Word~~Key Manager will make the problem worse due to the lack of passkey exporting capabilities

Implication

	One password	Multiple passkeys
Client		
Server		


FRONT DOOR
STORAGE ROOM
SUPPLY ROOM

Contexts to capture



1. User Agent (platform + browser)
   `Mozilla/5.0 (Macintosh; Intel Mac OS X 13_3_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36`

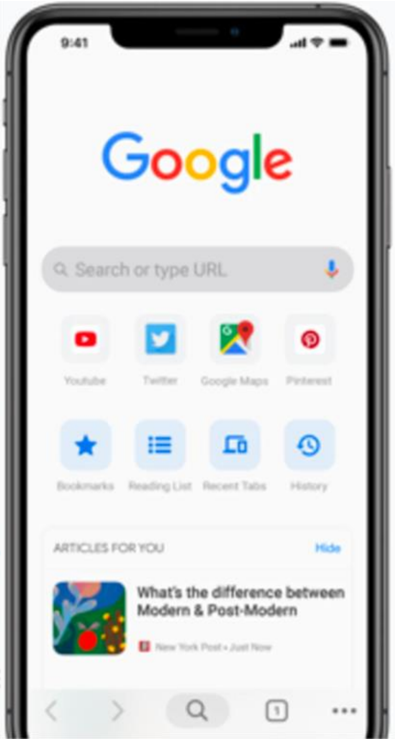
2. Device Name
   `Joe’s iPhone`

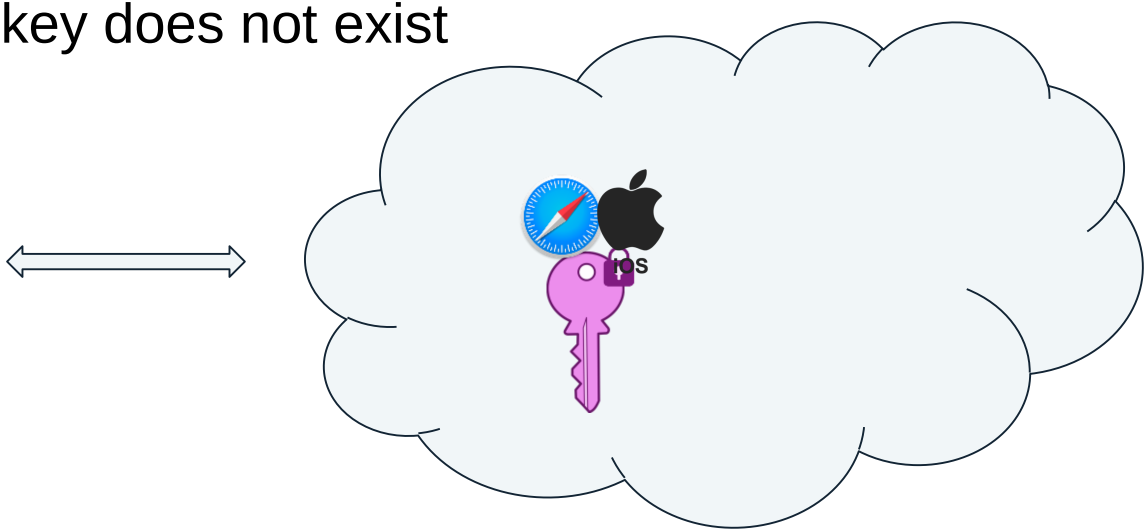
3. Creation time
   `2023-5-29 12:00:00`

4. User input
   `My first key`

Enable platform detection

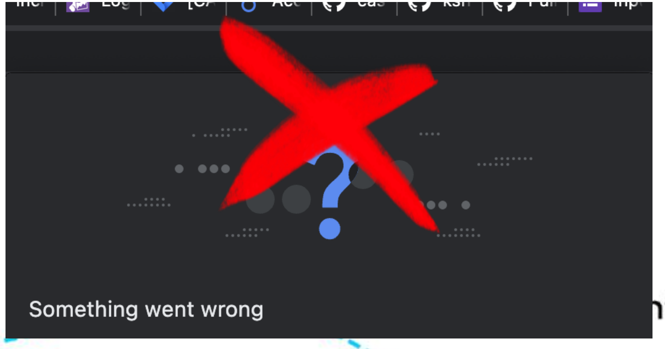
Example: fall back if key does not exist





Silently fail if possible

- Currently feasible on iOS



Something went wrong

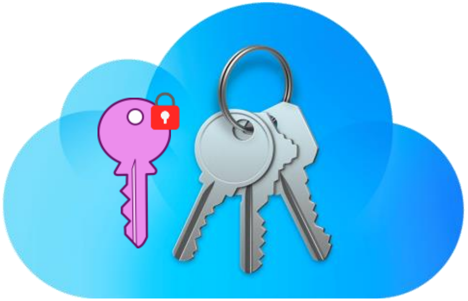
Lowered Security Guarantee

Private key is in software, not in hardware TPM

Before
(single-device credential)

In hardware
Key can never be exported

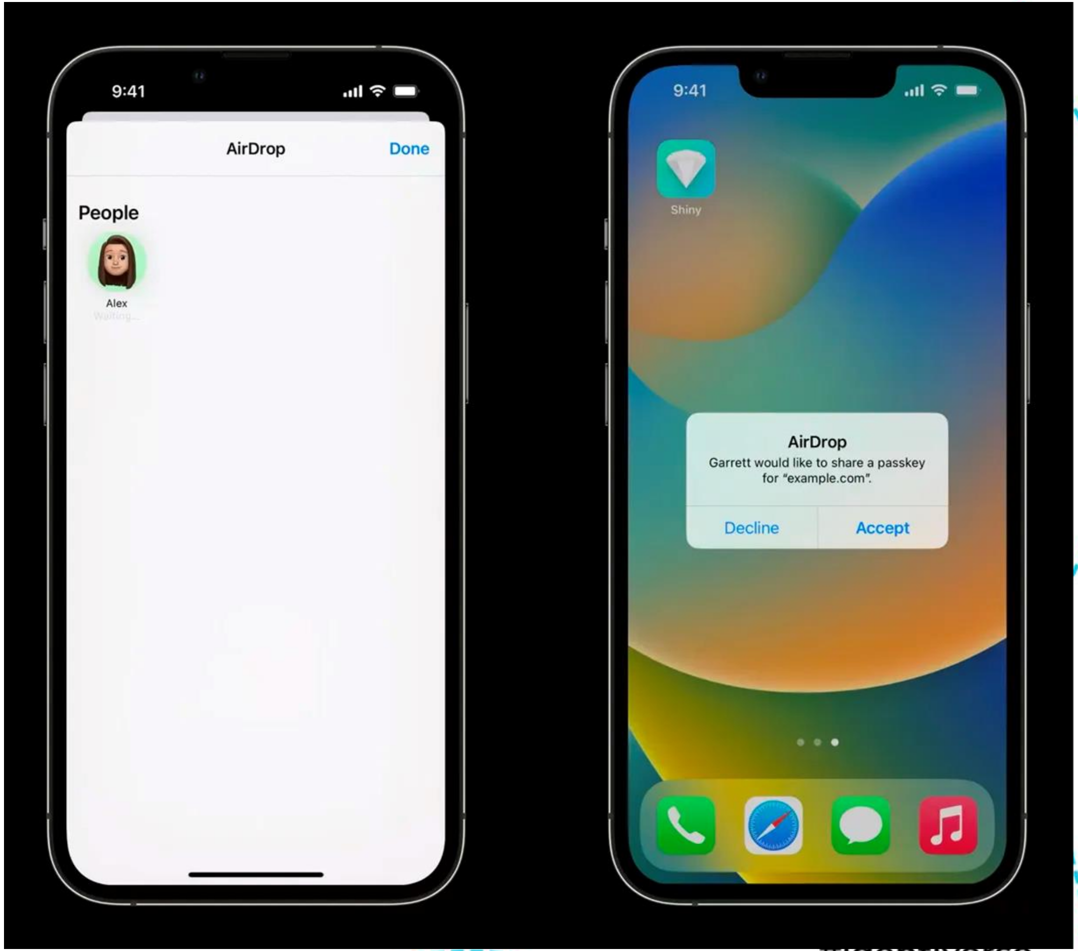
After
(passkey)



In software
Key could potentially be cloned

Airdrop-able

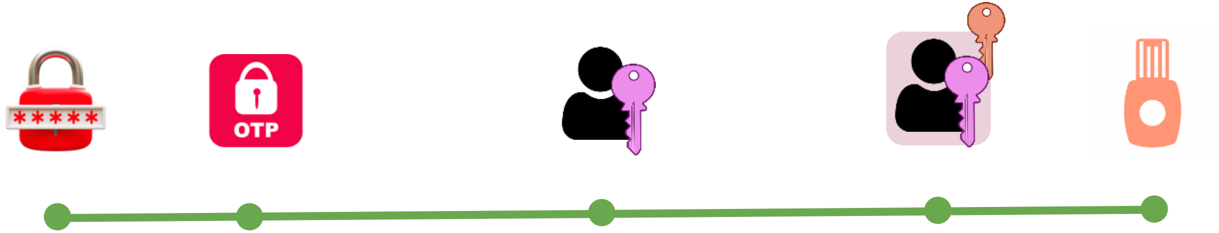
- Human will make mistakes



AirDrop

Garrett would like to share a passkey for "example.com".

Security spectrum



Password

X + OTP

Passkey (Multi-device credential)

Passkey + DPK

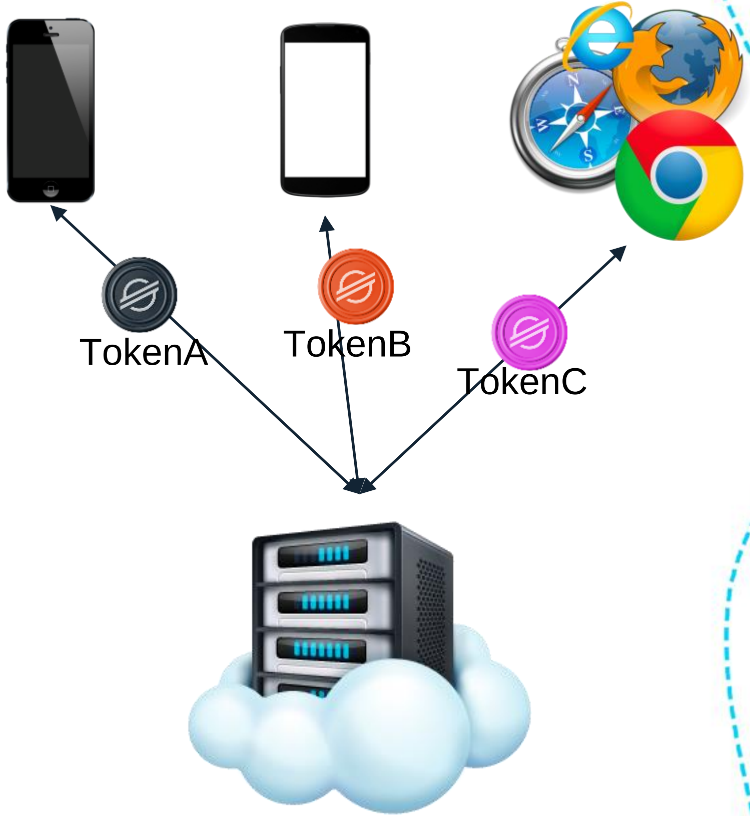
Single-device Credential

Device Public Key (DPK) is still in draft
Apple will unlikely implement it

Solution (step 1)

Track installations per “device”

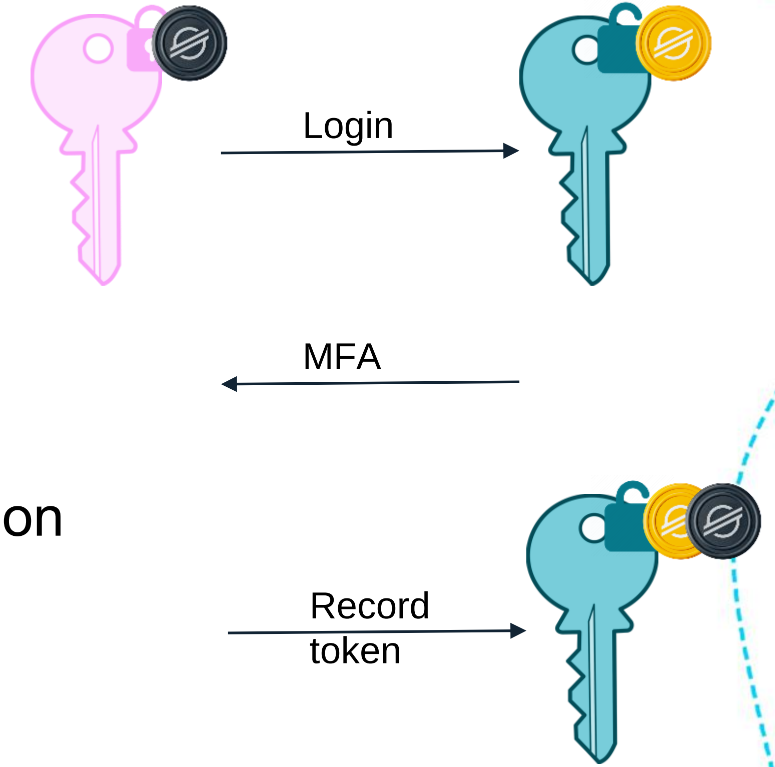
- Issue token on a new “device”
- Attach in future requests



Solution (step 2)

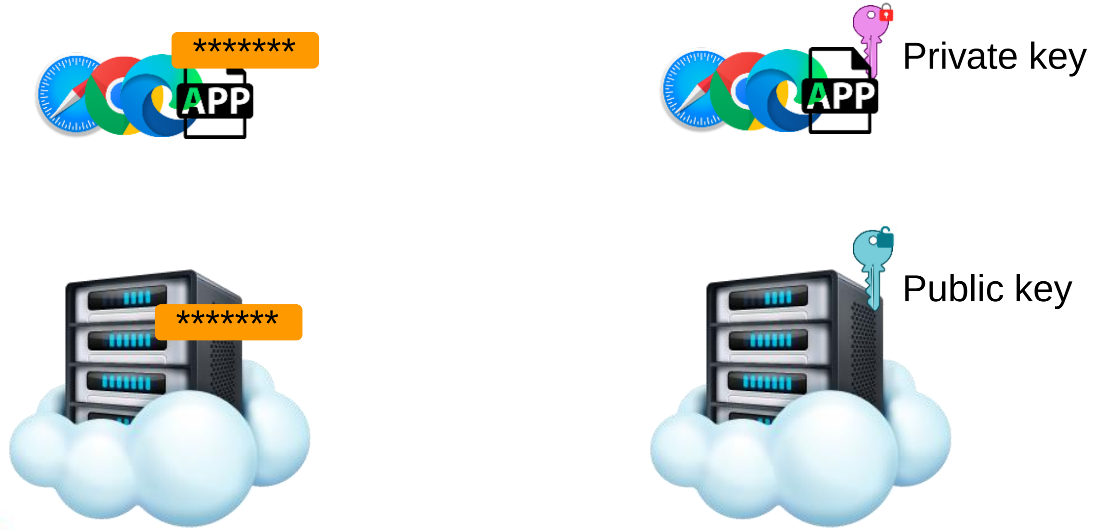
1. MFA on new device
   a. Prompt MFA if
      i. New “device”, or
      ii. Token does not match

1. Record key←→ device association on success



Difference from password

One vs two



One artifact

Two artifacts
(private and public keys)

Client

Server

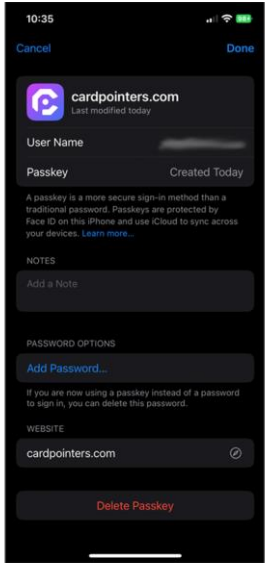
Private / Public key

Private key

- Managed by client platform
- App has no access

Public Key

- Managed on server



10:35

cardpointers.com
Last modified today

User Name [redacted]

Passkey Created Today

A passkey is a more secure sign-in method than a traditional password. Passkeys are protected by Face ID on this iPhone and use iCloud to sync across your devices. Learn more...

NOTES

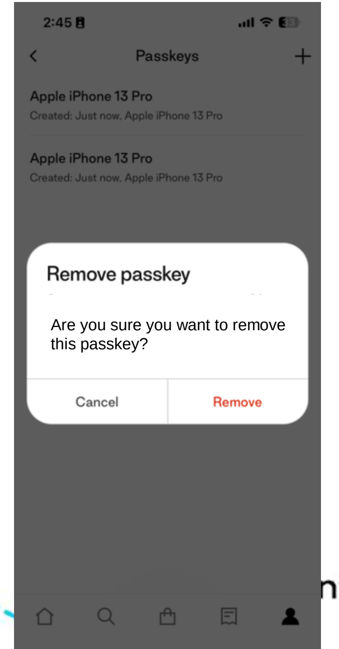
Add a Note

PASSWORD OPTIONS

If you are now using a passkey instead of a password to sign in, you can delete this password.

WEBSITE

cardpointers.com



2:45

Apple iPhone 13 Pro
Created: Just now, Apple iPhone 13 Pro

Apple iPhone 13 Pro
Created: Just now, Apple iPhone 13 Pro

Remove passkey

Are you sure you want to remove this passkey?

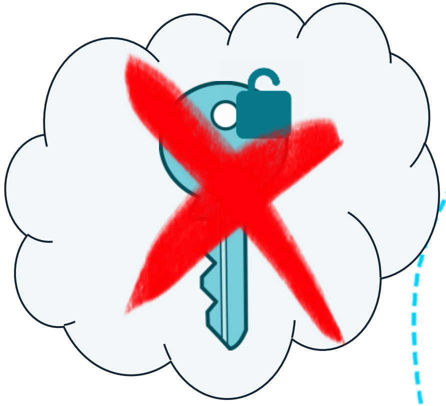
What happens when they get out of sync?

Case 1: Private key is deleted

What happens when they get out of sync?

Case 2: Public key is deleted

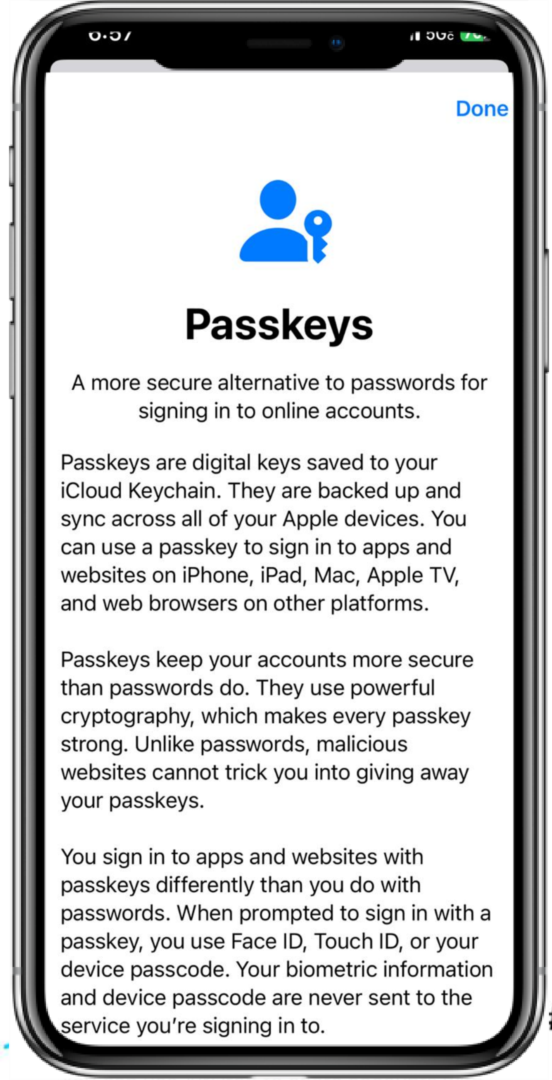
a. Use `allowCredentials`
b. Mark public key as deleted, when private key is matched, tell user to delete



It is a transition (not a flip of switch)

User education

- Most users have not heard of passkeys
- Take many years to get users on board
  - Many still turn off biometrics today



Passkeys

A more secure alternative to passwords for signing in to online accounts.

Passkeys are digital keys saved to your iCloud Keychain. They are backed up and sync across all of your Apple devices. You can use a passkey to sign in to apps and websites on iPhone, iPad, Mac, Apple TV, and web browsers on other platforms.

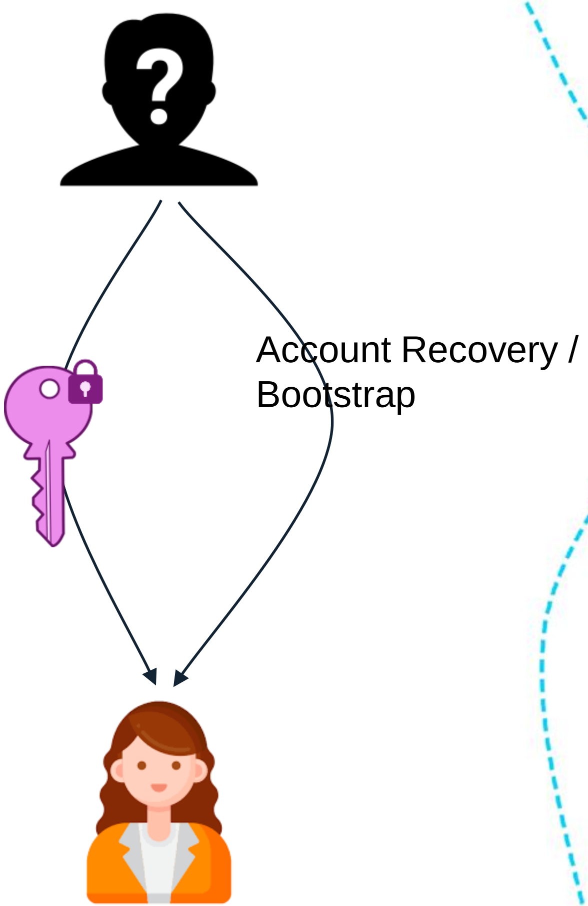
Passkeys keep your accounts more secure than passwords do. They use powerful cryptography, which makes every passkey strong. Unlike passwords, malicious websites cannot trick you into giving away your passkeys.

You sign in to apps and websites with passkeys differently than you do with passwords. When prompted to sign in with a passkey, you use Face ID, Touch ID, or your device passcode. Your biometric information and device passcode are never sent to the service you're signing in to.

Build a backup plan

- Add a Bootstrap/Account Recovery option in case users cannot login

- You are as strong as your weakest link



Summary

- Passkey transition will take many years
- Platform capabilities are complex and nuanced
- Understand constraints, and build a great user experience around it