Everything You Never Knew You Wanted to Know About Passkeys

Modern, Low Friction Authentication

yubico

Disclaimer

The views and opinions expressed in this presentation are those of the speakers and do not necessarily reflect the views or positions of any entities they represent. This presentation is provided “as is” without any express or implied warranty. This presentation is for educational and informational purposes only and does not constitute legal advice.

whoami

- Solutions Architect, Yubico
  - Standards & Regulations
  - Office of the CTO
  - More white papers by the day!
- Contributor
  - EDWG - FIDO Alliance (https://fidoalliance.org/)
  - Cyber Resilience SIG, ISSA (https://www.issa.org/)
  - IDPro, BoK Editor (recovering) (https://idpro.org/)
- General Nerd
  - Board Games! (Ask me about Big Stompy Robots)
  - Bow-tie enthusiast
  - ‘Lowbrow’ beer snob
  - Is there such a thing as too many Lego??

IGA Evangelist

What are passkeys?

/ˈpasˌkēs/
noun
Based on FIDO standards, passkeys are a replacement for passwords that provide faster, easier, and more secure sign-ins to websites and apps across a user's devices. Unlike passwords, passkeys are always strong and phishing-resistant.

Passkeys simplify account registration for apps and websites, are easy to use, work across most of a user's devices, and even work on other devices within physical proximity.

Kindly taken from - https://fidoalliance.org/passkeys/

tldr;

Passkeys (passkeys) are FIDO2 credentials designed to replace passwords!

FIDO Authentication

Passwords	FIDO
Human generated symmetric secret	Machine generated Public/Private keypair
Often reused across tools	Bound to single RP (relying party)
Easily phished	Phishing resistant
Subject to credential stuffing, social engineering and data leakage	Impractical to remotely compromise

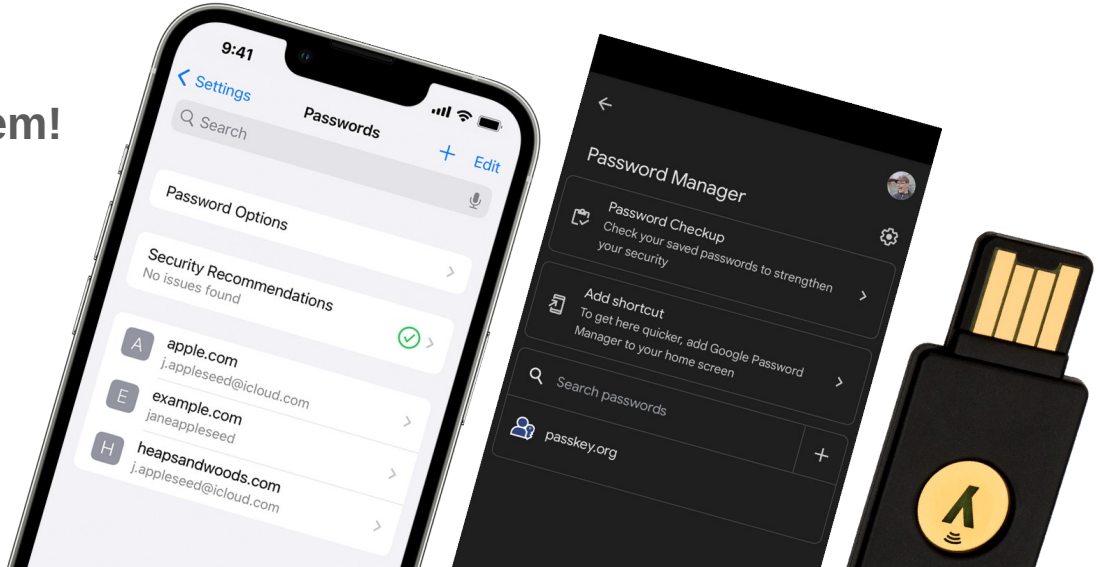
Who has a passkey already?

Raise your hand if you have a(n)

- Apple Device?
- Android device?
- FIDO2 Authenticator?

Congrats!

You've already got 'em!



Big ‘P’ or little ‘p’?

Names are confusing!

Vendor specific branding normally includes “Passkey”

- Apple Passkey
- Google Passkey
- 1Password Passkey

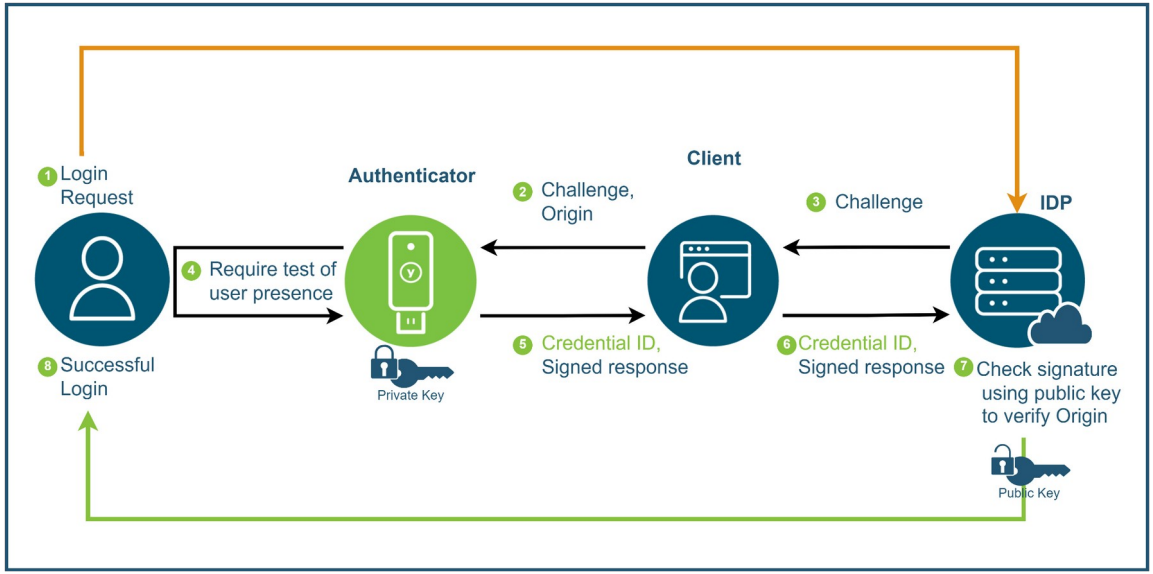
How do they compare?

- Same standard
- Same technology
- Just branding

How do passkeys work?

Private/Public key cryptography

- Private keys are held by the user.
- Public keys are shared during a registration process.
- On future authentication challenges users prove possession of private key.
- Bob’s your uncle!



How are passkeys easy?

Sharing & Synching

- Some passkeys can be shared across ecosystems.
- Some providers allow for synchronization across devices.

Authenticators Leverage inbuilt platform tool for checks

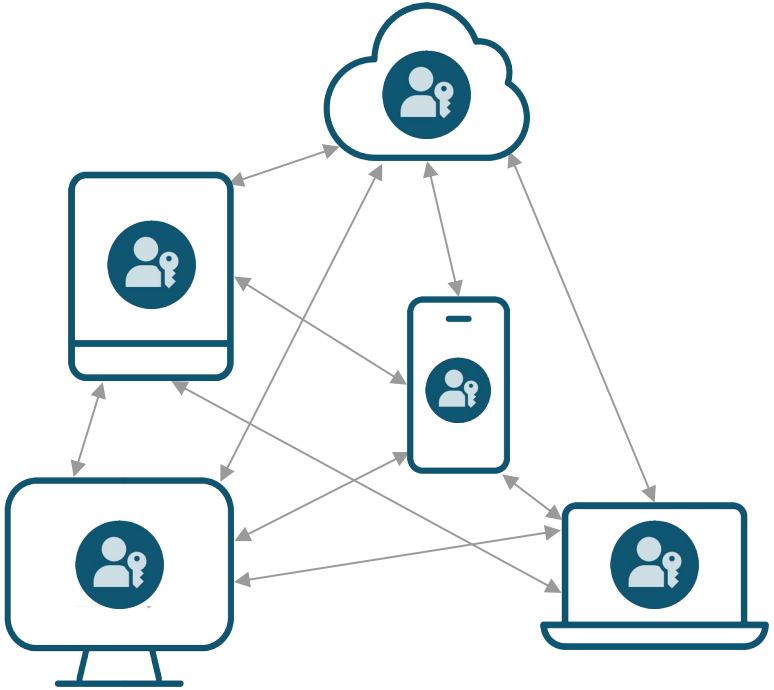
- Touch/FaceID/Pin to unlock passkey for use.

UX can ‘Hide’ complexity

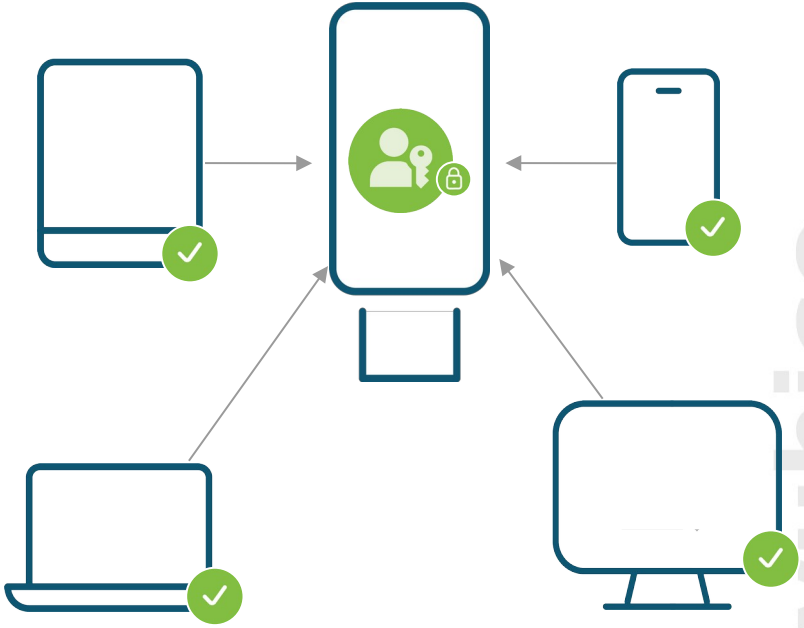
- Leverages common ceremonies to secure accounts
- UX can allows for ‘Passwordless’ flows.

Synced vs device bound passkeys

Synced & Copyable



device bound

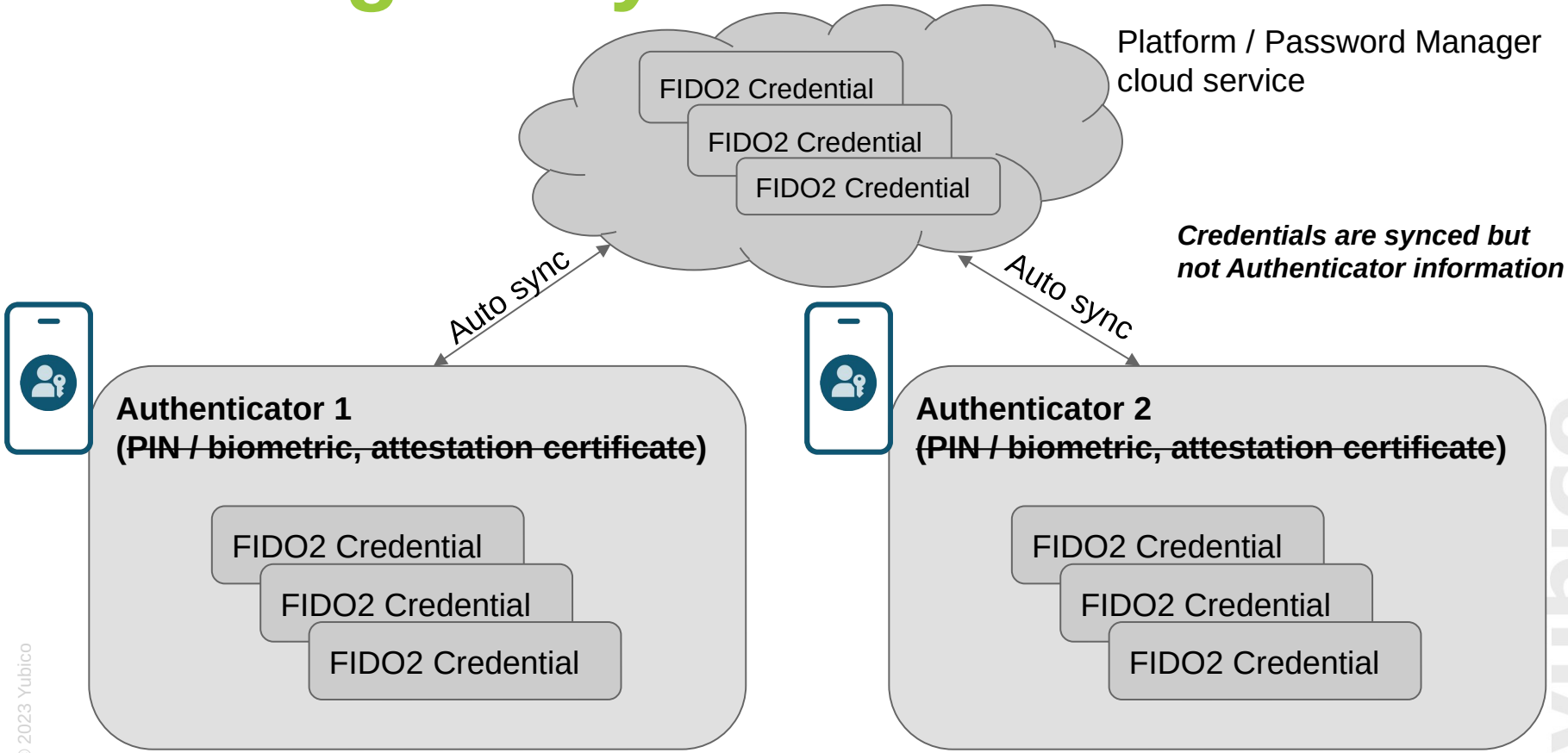


What’s a sync fabric?

- Sum total of all places an individual passkey private key resides.
- Encompass cross device and cross platform models
- Describes how synched credentials move from one authenticator to another
- Different nodes need not be aware of each other!!

★ Google’s proposed terminology - may not be accepted in official final standard.

What gets synced?



Credentials are synced but not Authenticator information

How (else) do passkeys work?

WebAuthn

- Established authentication standard codified by W3C.
- Public key is associated with a user on the RP.
- Supported by most major browsers.
- Interacts with CTAP to talk to the authenticator device.

CTAP2 Protocol

- Facilitates interactions at OS level.
- Extensible to include/return attestation & origin data.
- Most of the time you wont need to touch it!

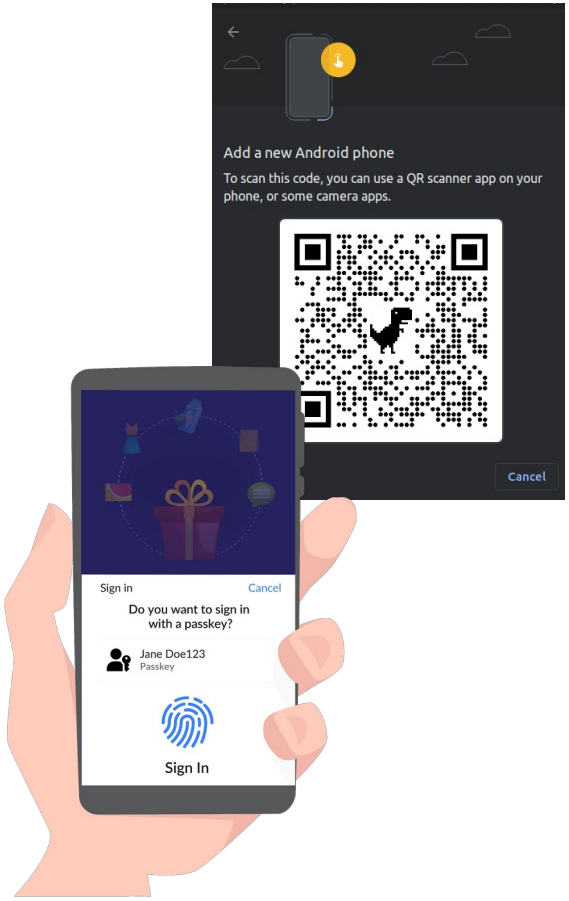
Putting it Together

Phishing resistance

- Legacy MFA is unidirectional.
  - No validity check of target.
- Phishing toolkits make overcoming legacy MFA trivial.
  - AitM - Replay/Relay
  - Pushbombing
- WebAuthn uses origin bound checks to confirm credentials are used in the correct place.
  - URI checking
  - Imposter & proxied sites wind up forming different signatures, assuming they can trick the CTAP protocol to even sign a response.

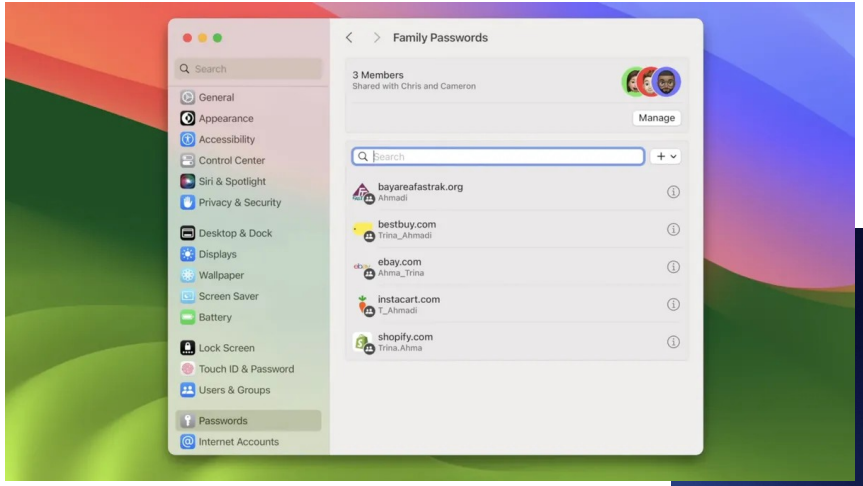
Hybrid Transport

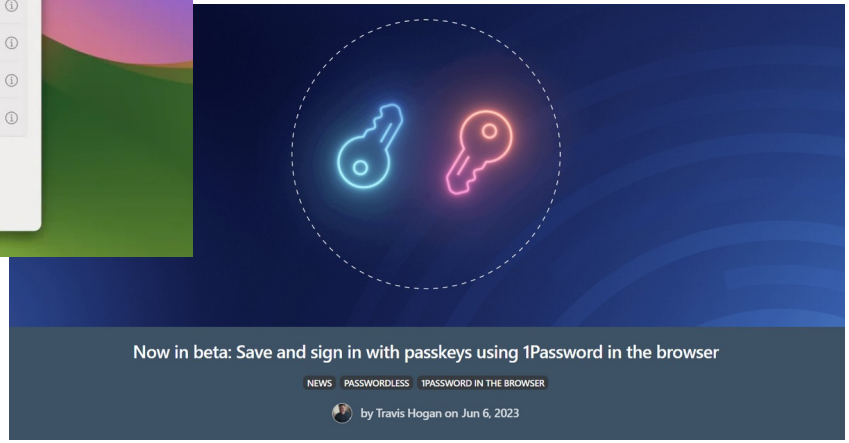
- Facilitates registration of new keys or cross device authentication.
- Leverages QR codes and Bluetooth capability to securely facilitate transmission.
- Devices must be within BLE range



Announcements are dropping..

Watch this space!





Where can you use passkeys

	iOS16+	macOS13+	Android	Windows	Linux*
Passkeys Multi-device fido credentials	✓ Safari ✓ Native Apps	✓ Safari ✗ Chrome*	✓ Chrome ✓ Edge ✓ Native Apps	✓ Chrome ✓ Edge	✓ Chrome ✗ Firefox*
Single device credentials			✓ Chrome ✓ Native apps	✓ Chrome ✓ Edge	✓ Chrome* ✗ Firefox*
Security keys	✓	✓	✗	✓	✓
Passwordless Discoverable credentials	✓ Safari	✓ Chrome ✓ Native Apps	✗ Chrome* ✗ Native Apps*	✓ Chrome ✓ Edge	
Passkey autofill Conditional UI	✓ Safari	✓ Safari ✗ Chrome*	✗ Chrome*	✗ Chrome* ✗ Edge*	

Benefits for your org/platform

- **Passwords are Bad, m’kay**
  - Created for accounting, not security.
  - Shared secrets, RP dependant on storing secrets material.
- **Passkeys allow for passwordless workflows**
  - 50% - 80% of all cyber incidents are caused by compromised credentials
  - Less passwords, less risk (all around!)
- **Backup and recovery**
  - Sync allows for easy recovery.
- **Easy to use**
  - OS & browser adoption and integration allows for great user experience.

Challenges & Pitfalls

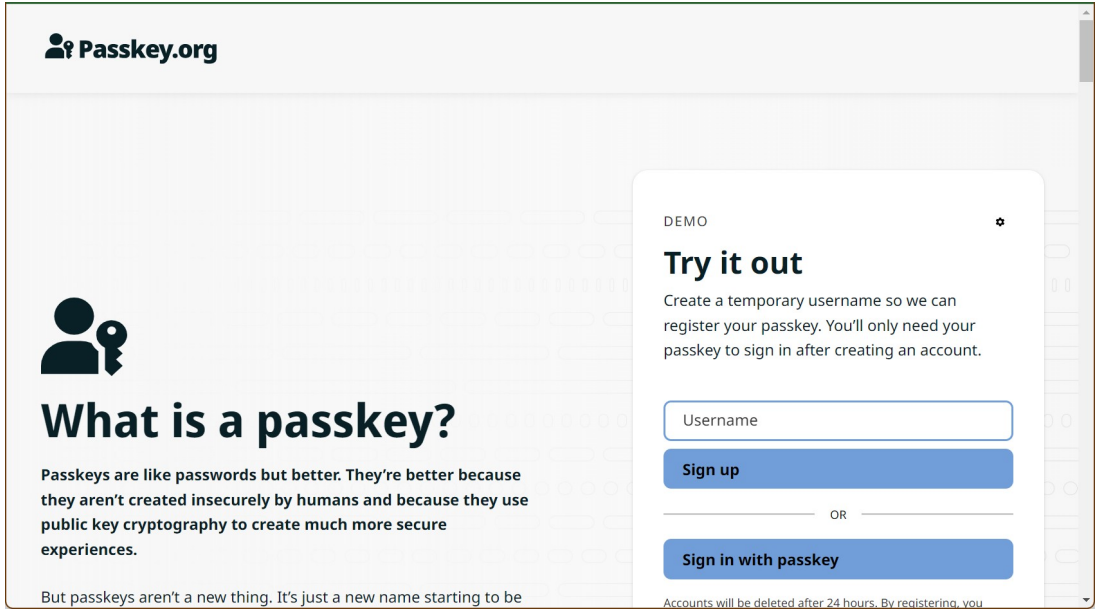
- **Synced keys have no visibility to each other**
  - Once a key is shared it is impossible to recall it.
- **FIDO Adoption**
  - Many RPs support FIDO, but mileage may still vary based on platform.
- **Plan for re-enrolment**
  - While synchable credentials are good for recovery, you still need a strong re-enrollment process.
- **Know your customer**
  - What is the risk level of your customer/company?

Passkeys and security keys

- Passkeys are FIDO2 credentials. They reside in security keys already!
- More passkey adoption means more security key adoption and more flexibility for systems that already support FIDO2.
- Synchable passkeys are great for consumer and low assurance use cases.
- Hardware bound (roaming) passkeys are great for enterprises, mobile free environments and high assurance use cases.
    - Achieves AAL3

A wild demo appears!!??

Your mileage (bandwidth) may vary..



Vocabulary lesson

Passkey - A FIDO2 Credential

Single device passkey - A credential that is bound to a single authenticator, like a security key.

Multi device passkey- A credential that can be synced to more than one device. iCloud or 1Password are example transport mechanisms.

Hybrid Mode - The capability of leveraging passkeys from one platform on another. (Apple to Google for example)

Authenticator - A device that holds credentials and facilitates authentication.

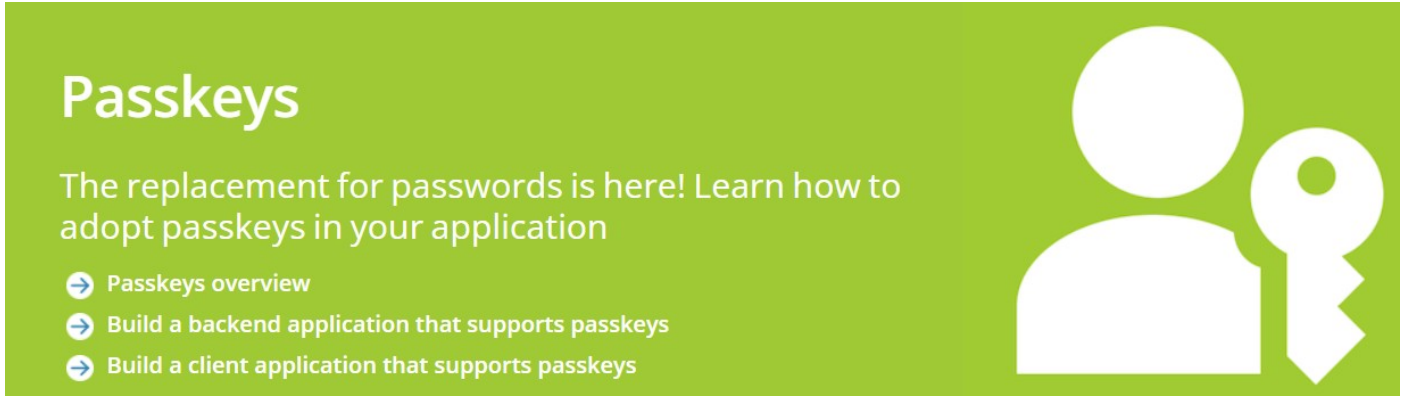
- Roaming - stores single device passkeys.
- Platform - stores multi device passkeys. Interacts with sync fabric.

Device Public Keys (DPKs) - A proposed extension to the WebAuthn specification to provide information of the device that is storing the synced passkey

- DPKs don’t control the syncing process but provide signals about the device holding the synced passkeys

How do you use passkeys?

- **Check with your RP (IDP/SSO!)**
  - Many already support FIDO2 Authentication
- **Build your own**
  - Visit https://developers.yubico.com/



How can I dive deeper?

‘Official’ Links -

https://passkeys.dev/

https://passkey.org

https://fidoalliance.org/passkeys/

https://developer.apple.com/passkeys/

https://developers.google.com/identity/passkeys

Community Links -

https://github.com/herrjemand/awesome-webauthn

Thanks!

Questions? Reach out!!

Josh.Cigna@Yubico.com

@sporksan@infosec.exchange

linkedin.com/in/joshcigna