Go Passwordless with Passkeys

A WebAuthn Developer Workshop

identiverse

#identiverse

Introductions

Nick Steele

Staff Product Manager

1Password

Matthew Miller

Engineering Tech Lead

Cisco

Shane Weeden

Senior Technical Staff Member

IBM

Megan Shamas

Senior Director of Marketing

FIDO Alliance

Today’s Agenda

- Why are we here?
- What is a passkey?
- Do you already have MFA? Here’s what do to
- Evolve into passwordless - demo time!
- Developer Gotchas & Myths
- Key Takeaways
- Q & A

Why are we here?


it's been 14 years...
imgflip.com

pass·key *noun*

Passkeys are a replacement for passwords that provide faster, easier, and more secure sign-ins to websites and apps across a user's devices.

https://fidoalliance.org/passkeys/

Embraced by platforms – and credential providers…

Google

Microsoft

1Password

DASHLANE

bitwarden

...and online services

DocuSign Google mercari HYATT

CVSHealth KAYAK docomo

PayPal SK telecom shopify YAHOO! JAPAN

What is a passkey?

pass·key *noun*

Passkeys are a replacement for passwords that provide faster, easier, and more secure sign-ins to websites and apps across a user's devices.

https://fidoalliance.org/passkeys/

Let’s unpack that marketing definition a bit…

A passkey:

- Is any discoverable FIDO credential
- Raises the bar for both security and UX
- Is most commonly synchronized across a user’s devices

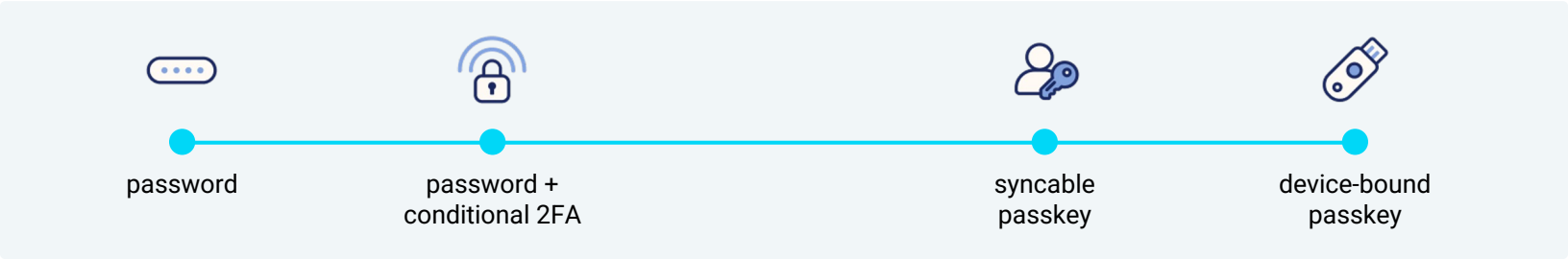
Synced Passkeys

A passkey that can be backed up and synchronized by the passkey provider across a user's devices.

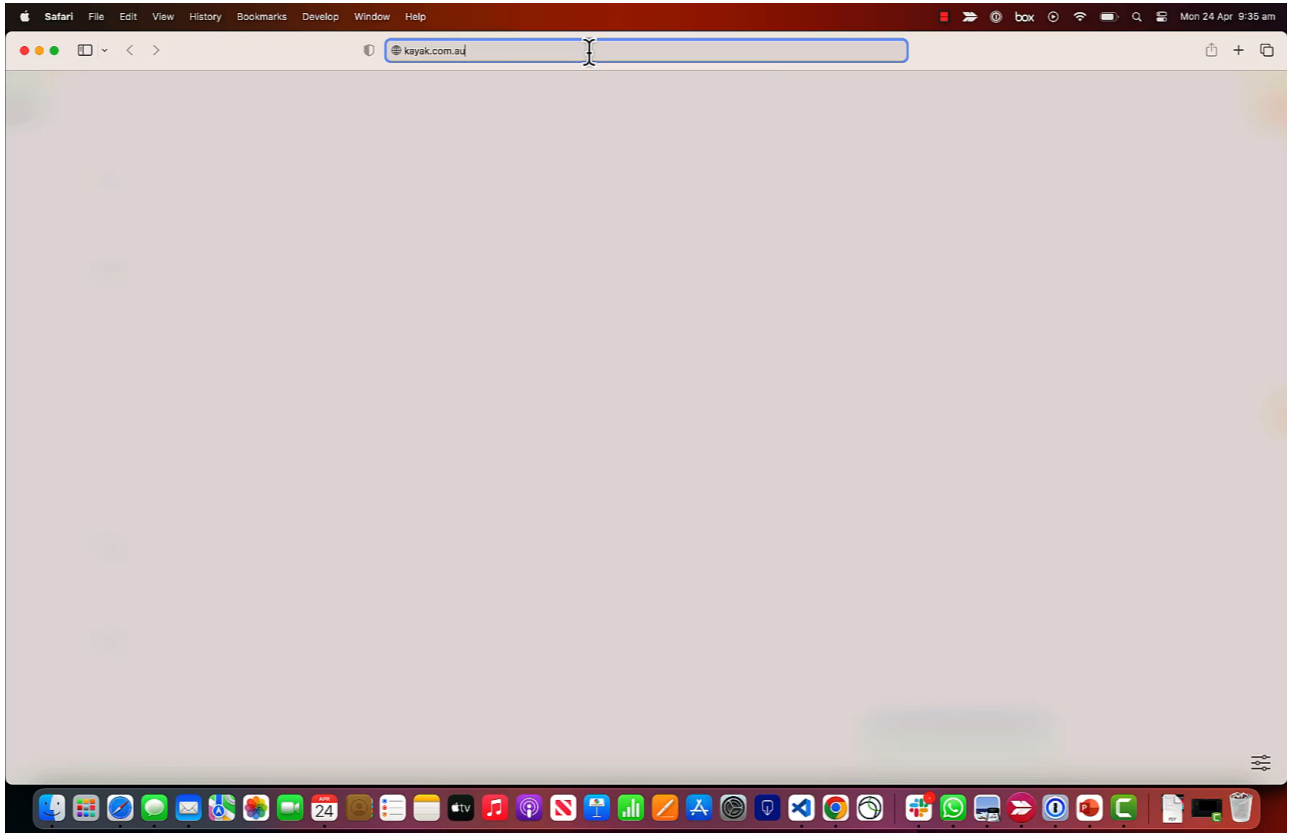
- A passkey provider might be a platform/OS vendor, or 3rd-party software such as a password manager.
- Facilitates new device bootstrapping and simplifies account recovery.
- Security of synced passkeys is the responsibility of the passkey provider.

But wait, don't I still need 2FA?

- 2FA was introduced to address the human-behavioural weaknesses associated with passwords leading to account takeover:
    - Simple, guessable or socially engineerable passwords
    - Password re-use
- FIDO credentials address these problems AND credential phishing



Let’s look at a passkey in action…



Are you...

...Already doing MFA?

- If you’re already using WebAuthn as a 2FA method, you’re all set to use passkeys!
- WebAuthn requests, without express disablement, can support passkey creation and login.
- This doesn't need to be an all or none scenario, in fact we recommend a rolling deployment.

...Not doing MFA at all?

If you don't, now is the time to cut over to passkeys:

- Offer more secure login covering 95%[1] of typical security requirements.
- Eliminate SMS expenses by removing SMS OTP entirely.
- Users are already comfortable with biometrics from using them with mobile apps.
- Users now bring their own hardware authenticators!

[1] https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/all-your-creds-are-belong-to-us/ba-p/855124

Evolve into passwordless…
and beyond!

Demo Time

Developer Gotchas & Myths

Developer Gotchas

- **Conditional UI fires a WebAuthn request on first load.**
  - Can make correlation of events difficult.
  - Conditional UI in general is still a work in progress.
- **Passkey Providers have to inject themselves into the DOM.**
  - Disabling JavaScript or extensions can cause some providers to be unable to operate.
- **There's limited ways to infer the type of passkey you'll receive before you receive it.**

Developer Myths

- **Passkeys are vendor-specific!** ❌
  - Vendors support passkeys, but don't own the standard.
  - Most users associate passkeys with Google, which can be good and bad.
- **Passkeys replace WebAuthn!** ❌
  - The WebAuthn standard covers the browser API that manages passkeys..
- **Passkeys are only for phones!** ❌
  - Passkeys can sync to devices of multiple form factors
  - They can also be device-bound
  - Imagine hybrid auth into an app on your TV…

Developer Myths, pt. 2

- **All passkeys are synced.** ❌
  - A hardware token can issue you a device-bound passkey.
- **I can't apply corporate policy with passkeys!** ❌
  - If you control the endpoint, you can control the passkey..
- **I can’t support passkeys without attestation!** ❌
  - Attestation can provide some assurances about authenticator identity, but the technology is more secure than typical password + 2FA techniques.
  - RP's in stricter regulatory environments can use existing out-of-band techniques for preventing passkey misuse.

So what’s next?

Key Takeaways

Passkeys are…

- Already being used at scale.
- Still phishing-resistant WebAuthn credentials.
    - Add features to reduce with account recovery the need for password resets.
- A superior alternative to MFA, and the means to move towards passwordless
- Easy to drop in and ready for browsers, especially if you're already using WebAuthn.

Resources

Learn more about adding passkeys to your site.

- For Developers:
  - https://passkeys.dev
  - https://webauthn.io
- For CXOs:
  - https://fidoalliance.org/passkeys/

Feel free to reach out to us!

Q & A

Thank you!