THE PASSKEY REALITY CHECK

Addressing 2025's Biggest Misconceptions

Tim Cappalli | Matthew Miller

Tim Cappalli

Sr. Architect, Identity Standards

Okta

https://timcappalli.me

Matthew Miller

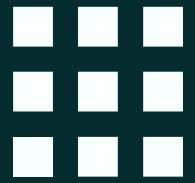
Principal Engineer

Cisco

https://millerti.me

The Passkey Ecosystem

Users



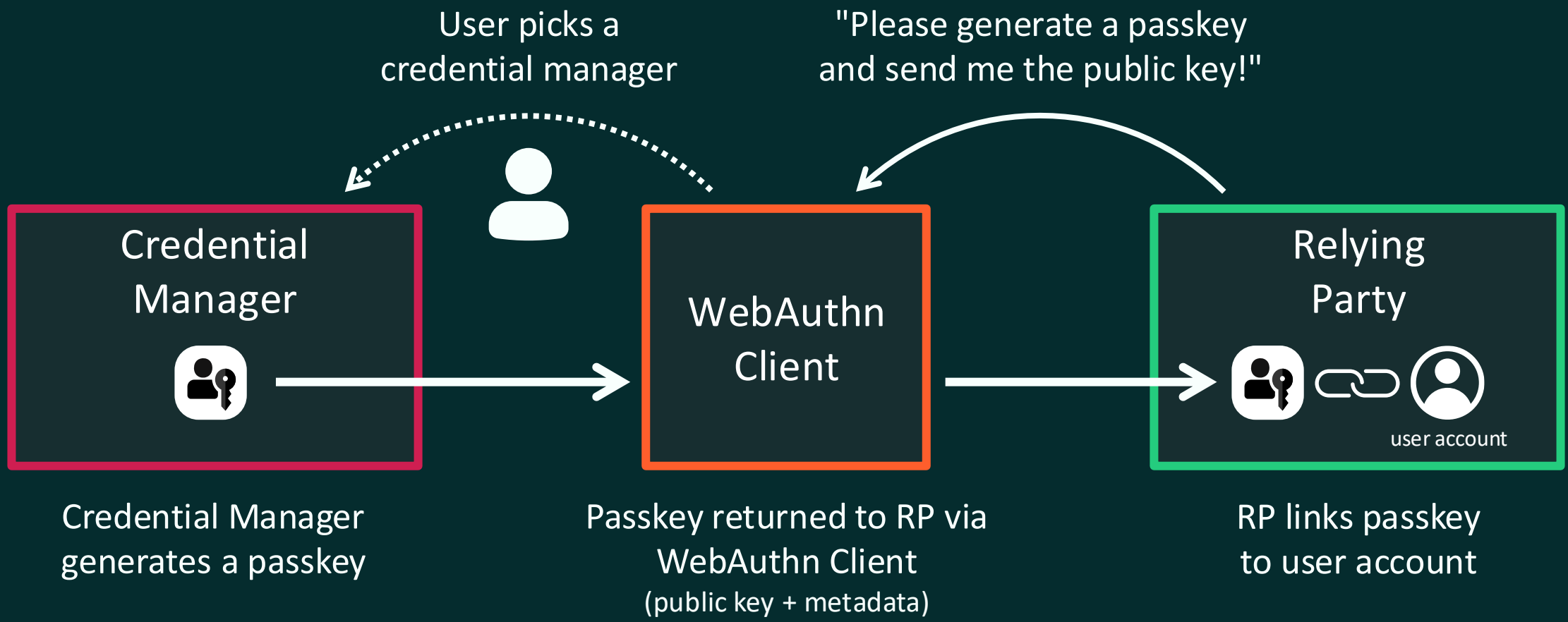
Browsers
& Apps

Devices
& OSes

Credential Managers
(Authenticators)

Relying
Parties

Bring Your Own Key



Misconceptions

Passkeys are a way for Big Tech to lock users into their ecosystem.

MISCONCEPTION

"Passkeys are a way for Big Tech to lock users into their ecosystem."

REALITY

The passkey ecosystem is open, and users can use whichever Credential Manager they wish!

Devices need to come with a Credential Manager out of the box.

My passkeys will get stuck on my iPhone if I switch to Pixel!

MISCONCEPTION

“My passkeys will get stuck on my iPhone if I switch to Pixel!”

REALITY

Credential Exchange allows a user to **securely** and **reliably** move passkeys (and other credentials) between Credential Managers.

Passkeys don’t protect against remote attacks.

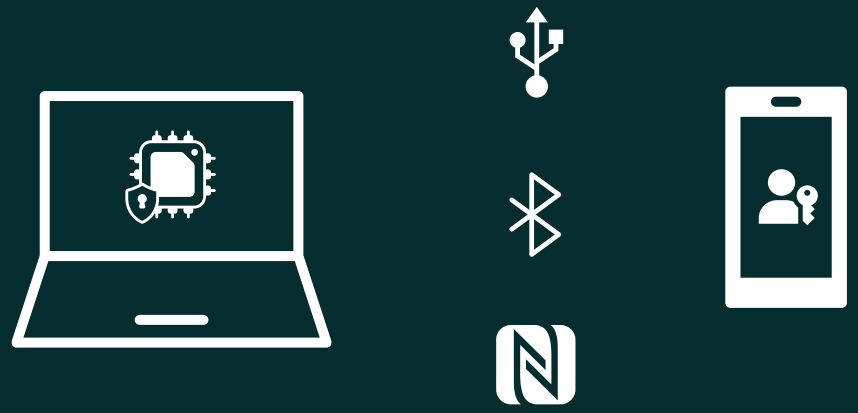
MISCONCEPTION

“Passkeys don’t protect against remote attacks.”

REALITY

FIDO2 mandates user control of the authentication device. Typically, this is the same as the access device.

FIDO ***Cross-Device Authentication*** allows a **nearby** device to be used for authentication but still enforces proximity.



The ‘QR code flow’ is phishable!

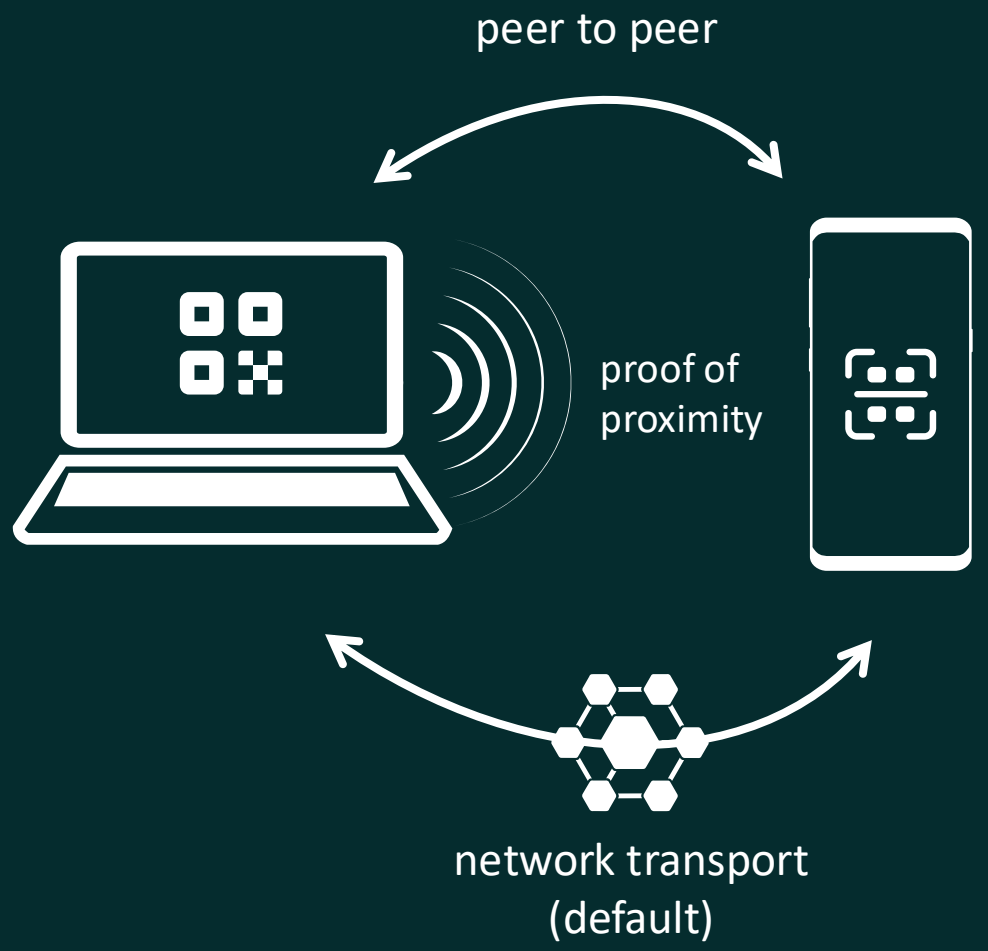
MISCONCEPTION

"The 'QR code flow' is phishable!"

REALITY

Cross-Device Authentication can use a QR code to bootstrap a secure connection between two devices.

Proof of proximity is required for the two devices to begin communicating either over the network or peer to peer.



Passkeys are not suitable for workforce use.

MISCONCEPTION

“Passkeys are not suitable for workforce use.”

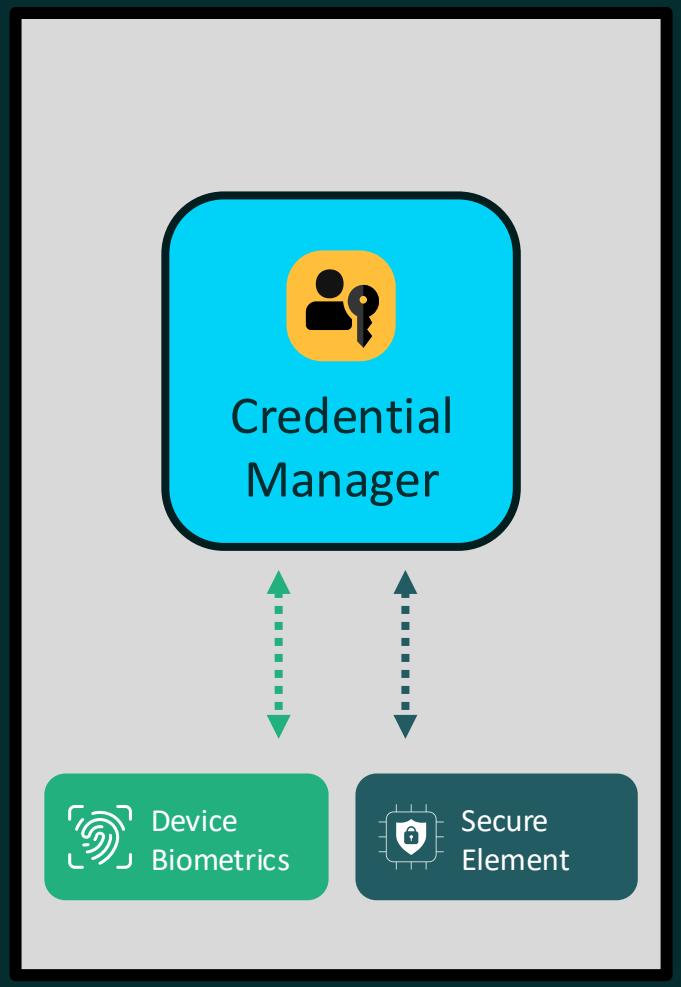
REALITY

There are more options there ever before for workforce usage!

Device-Bound Passkeys on Security Keys

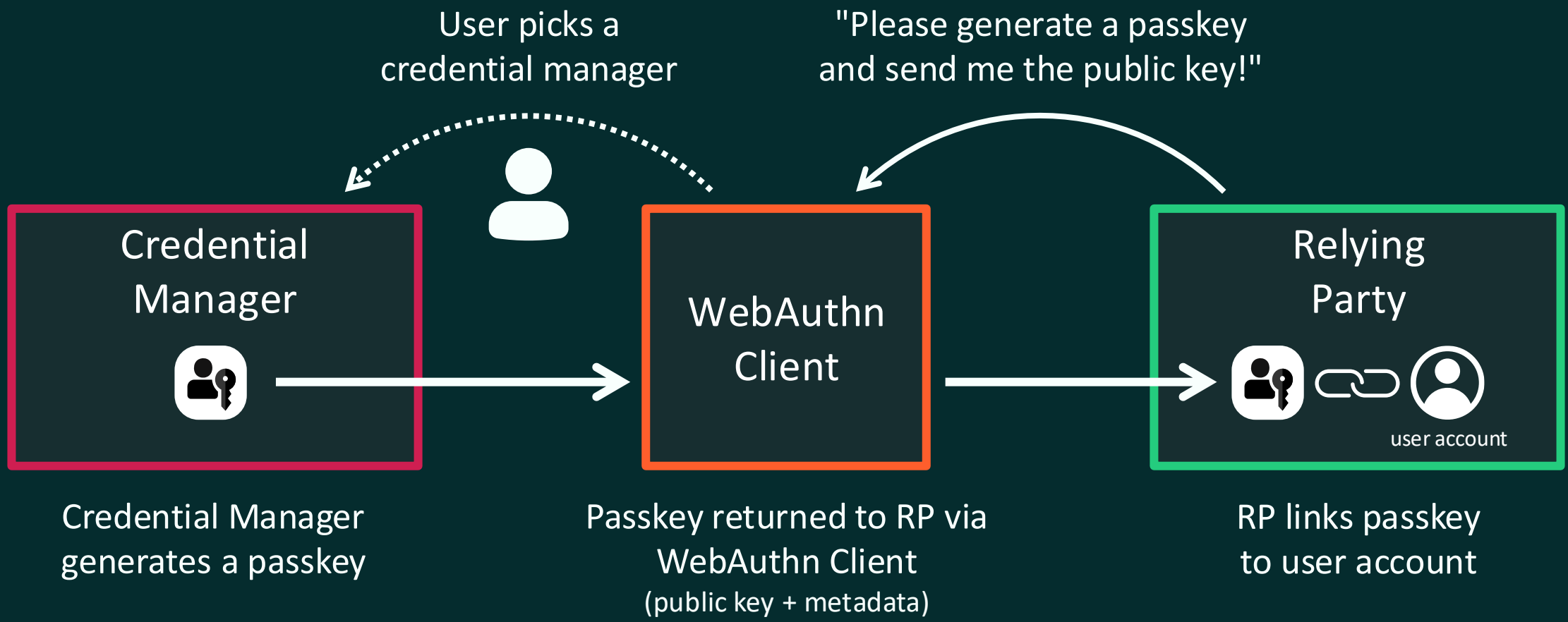
- Attested, device-bound passkeys
- Usable on multiple devices via USB and/or NFC
- Many form factors to choose from
- Great for both bootstrapping and day to day sign in
- “Gold standard”

Device-Bound Passkeys in Managed Credential Managers



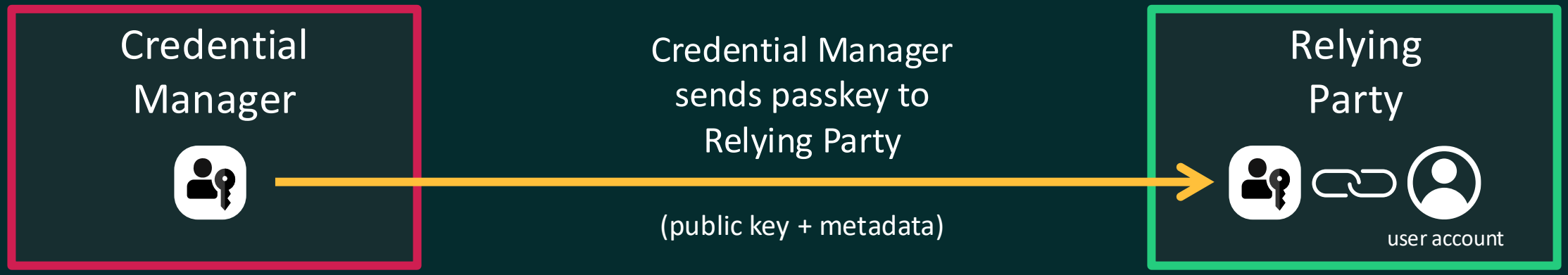
- Attested, device-bound passkeys
- Private key protected by the device's secure element
- User verification can leverage (or even require) device biometrics
- In-band (WebAuthn) or out-of-band enrollment (CM to RP)

Bring Your Own Key



Provide ~~Bring~~ Your ~~Own~~ Key

Credential Manager generates a passkey (user or admin initiated)



RP links passkey to user account

Synced Passkeys in Workforce

For users with access to only their own data

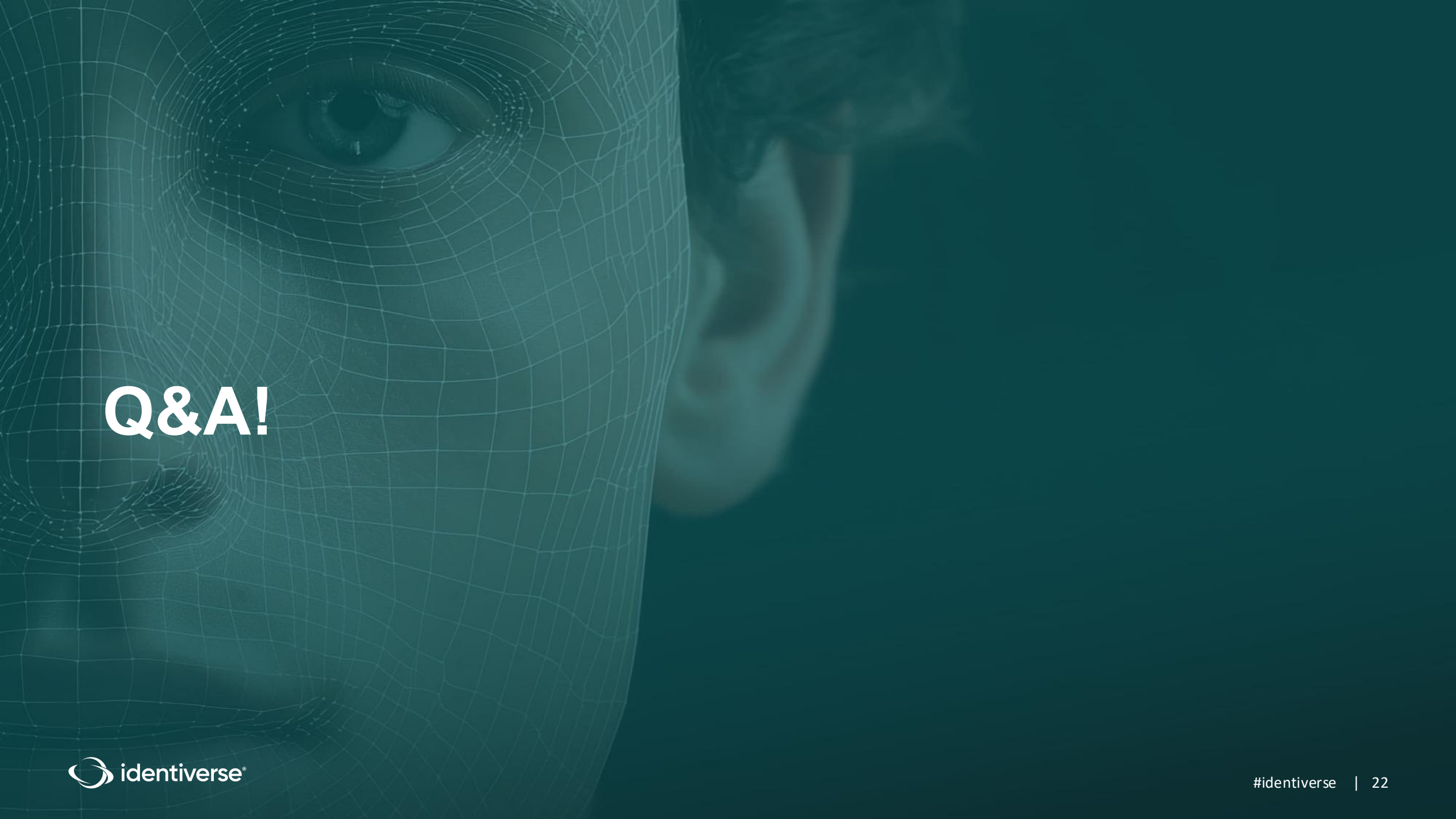
(*timecards, pay checks, class schedules*)

For all users in scenarios where passwords are still in use

(*s/password/passkey*)

For a recovery factor

(*synced passkey + additional factor*)


Q&A!

Thank You!