authenticate 2024
THE FIDO CONFERENCE

Peeling back the passkeys onion

Tim Cappalli

Signature Sponsors:
cisco | Microsoft | yubico | Google

authenticatecon.com

About Me

socials: **timcappalli.me** 👀

live in **Boston** and work on **identity standards** relating to **digital credentials** at **Okta**

maintain
passkeys.dev and **digitalcredentials.dev**

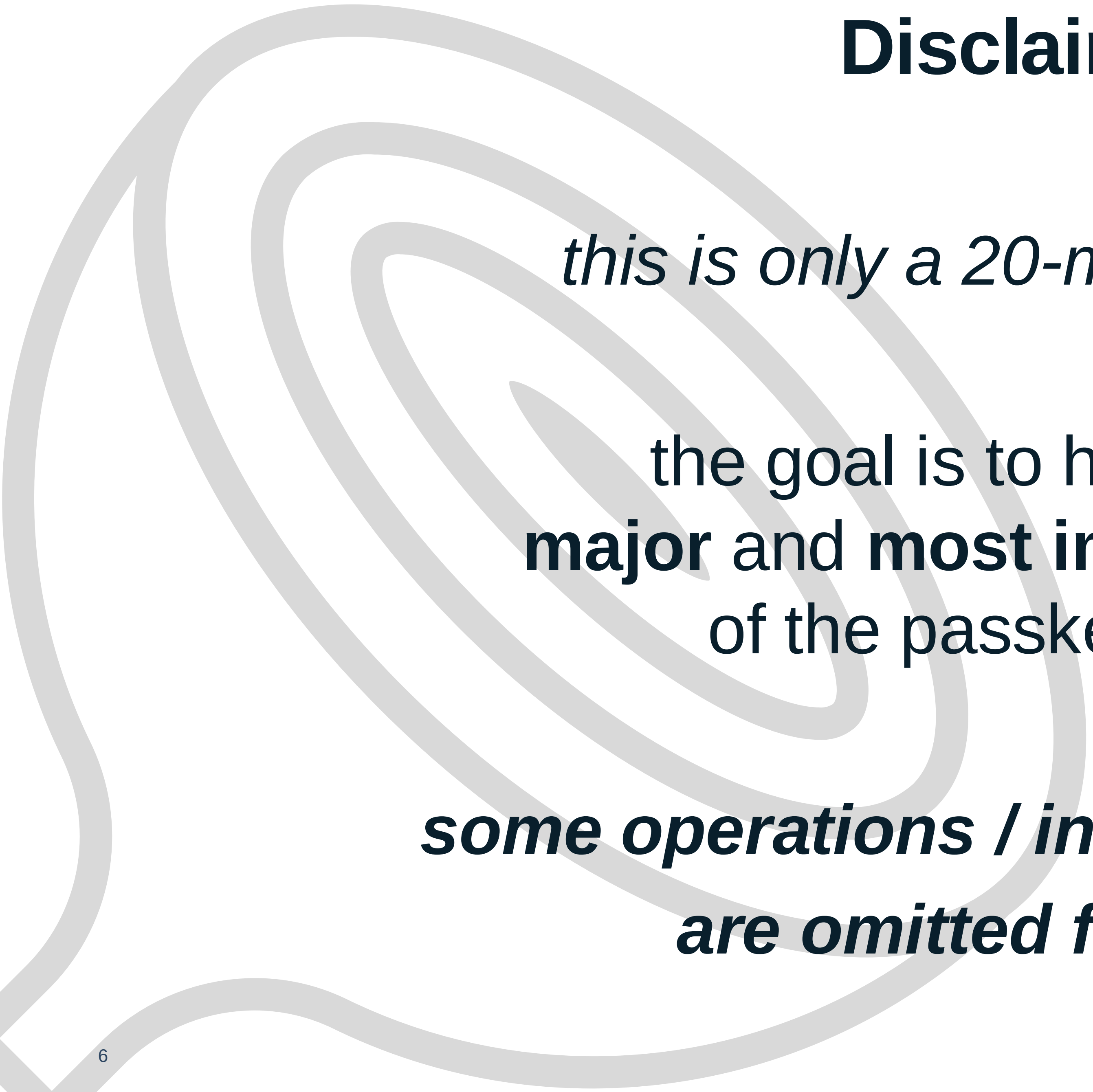
love to take photos
(shameless plug: ***photos.timcappalli.me***)

Shrek is a trademark of Dreamworks Animation LLC. This image is the property of its respective owner. It is used here without permission for educational purposes only. No copyright infringement is intended, and no ownership is claimed. Thank you AI overlords for assuring me this statement is OK..

Agenda

- The **Terminology**
- The **Flows**
- The **Players**
- The **Layers**
- Q&A

Disclaimer!



this is only a 20-minute session

the goal is to highlight the
major and **most impactful** layers
of the passkeys onion

***some operations / interactions / steps
are omitted for brevity***

The **Terminology**

Web Platform

a collection of standardized technologies like HTML, CSS, and JavaScript that enable the creation and interaction of web content across different devices and browsers

(ex: browsers, WebViews, PWAs)

App Platform

the operating system platform and its native APIs

(Android, iOS, macOS, Ubuntu, Windows, etc)

WebAuthn Client

the entity implementing the WebAuthn API

dispatches requests to authenticators and returns response to callers (RPs)

(typically web browsers or app platform native APIs)

Credential Provider

aka

Passkey Provider

aka

Authenticator

Credential Provider

aka

Passkey Provider

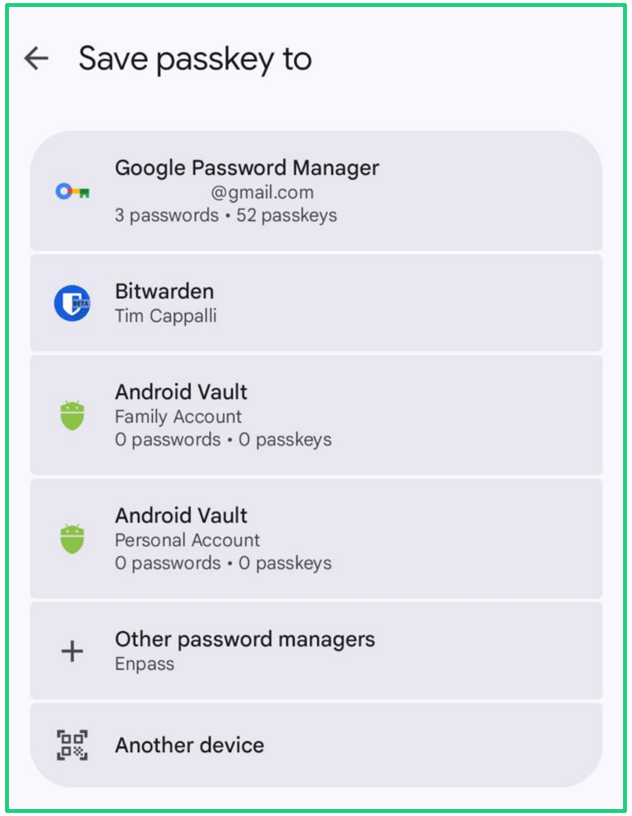
aka

Authenticator

aka

the thing that holds your credentials

Authenticator Selection



Save passkey to

Google Password Manager
@gmail.com
3 passwords • 52 passkeys

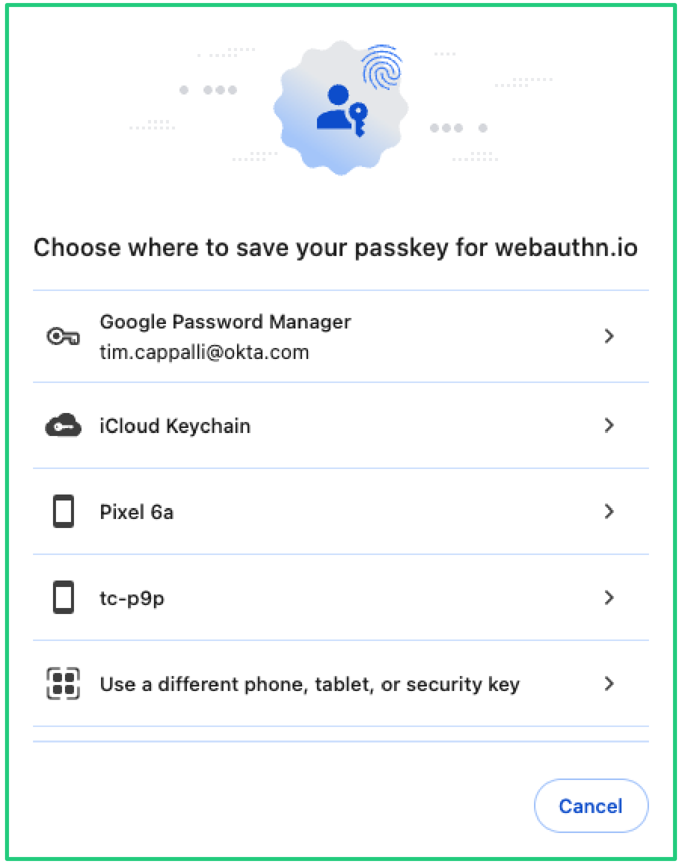
Bitwarden
Tim Cappalli

Android Vault
Family Account
0 passwords • 0 passkeys

Android Vault
Personal Account
0 passwords • 0 passkeys

Other password managers
Enpass

Another device



Choose where to save your passkey for webauthn.io

Google Password Manager
tim.cappalli@okta.com

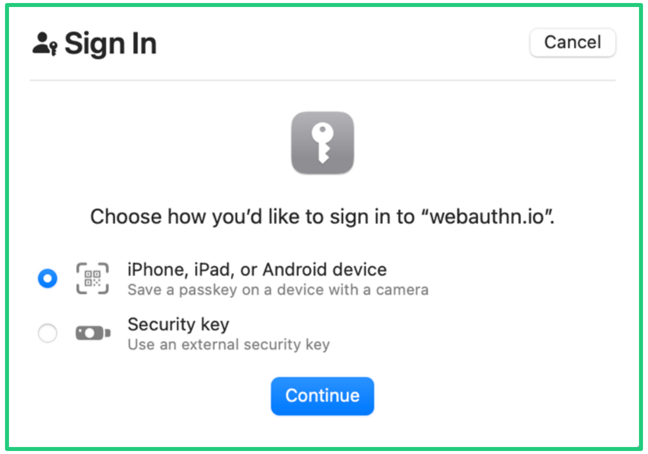
iCloud Keychain

Pixel 6a

tc-p9p

Use a different phone, tablet, or security key

Cancel



Sign In

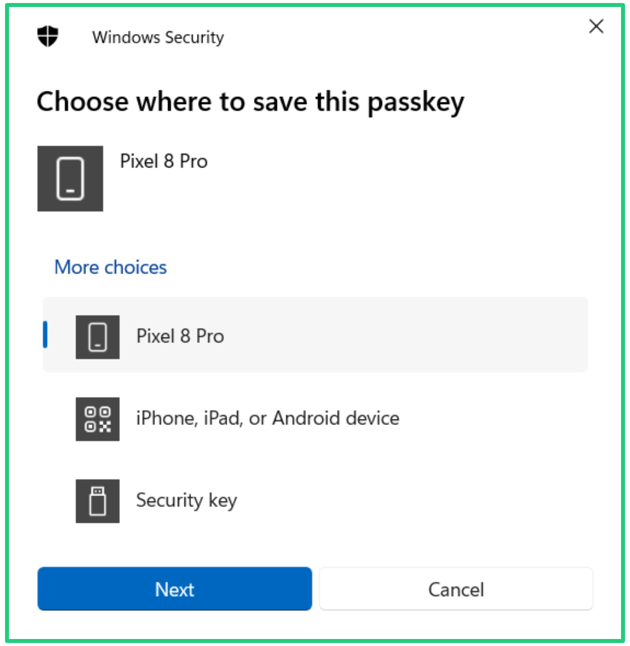
Cancel

Choose how you'd like to sign in to "webauthn.io".

● iPhone, iPad, or Android device
Save a passkey on a device with a camera

○ Security key
Use an external security key

Continue



Windows Security

Choose where to save this passkey

Pixel 8 Pro

More choices

Pixel 8 Pro

iPhone, iPad, or Android device

Security key

Next

Cancel

The **Flows**

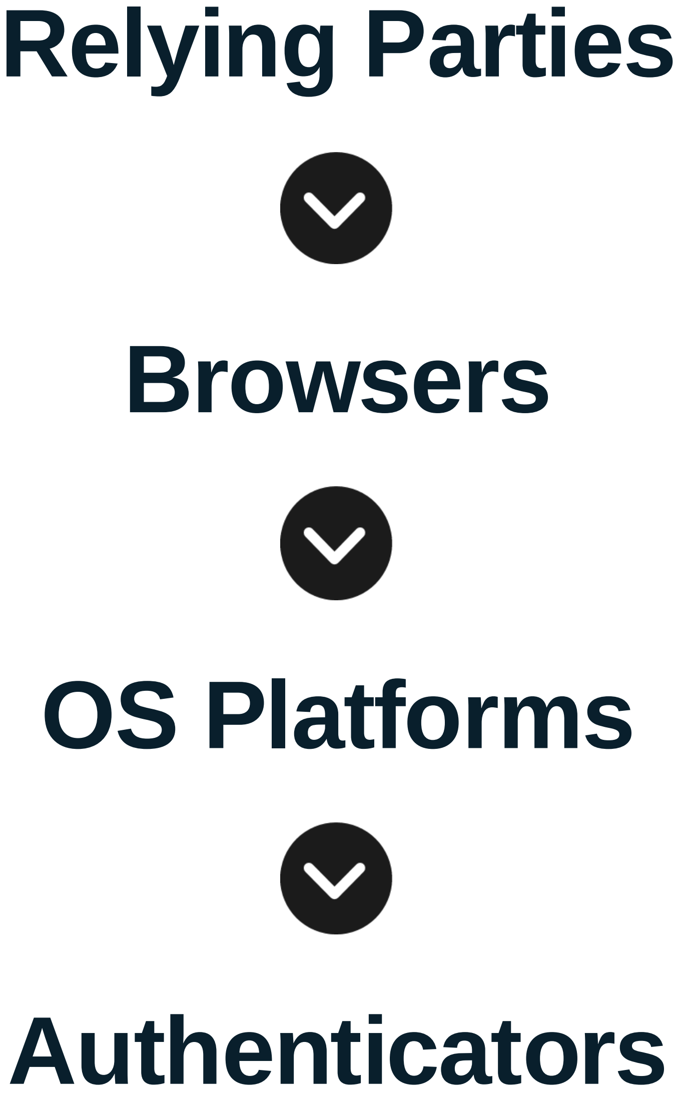
Registration / Creation

higher
cognitive load

Authentication

lower
cognitive load

The **Players**



Relying Parties

↓

Browsers

↓

OS Platforms

↓

Authenticators

Relying Parties

⌄

Browsers

⌄

OS Platforms

⌄

Authenticators

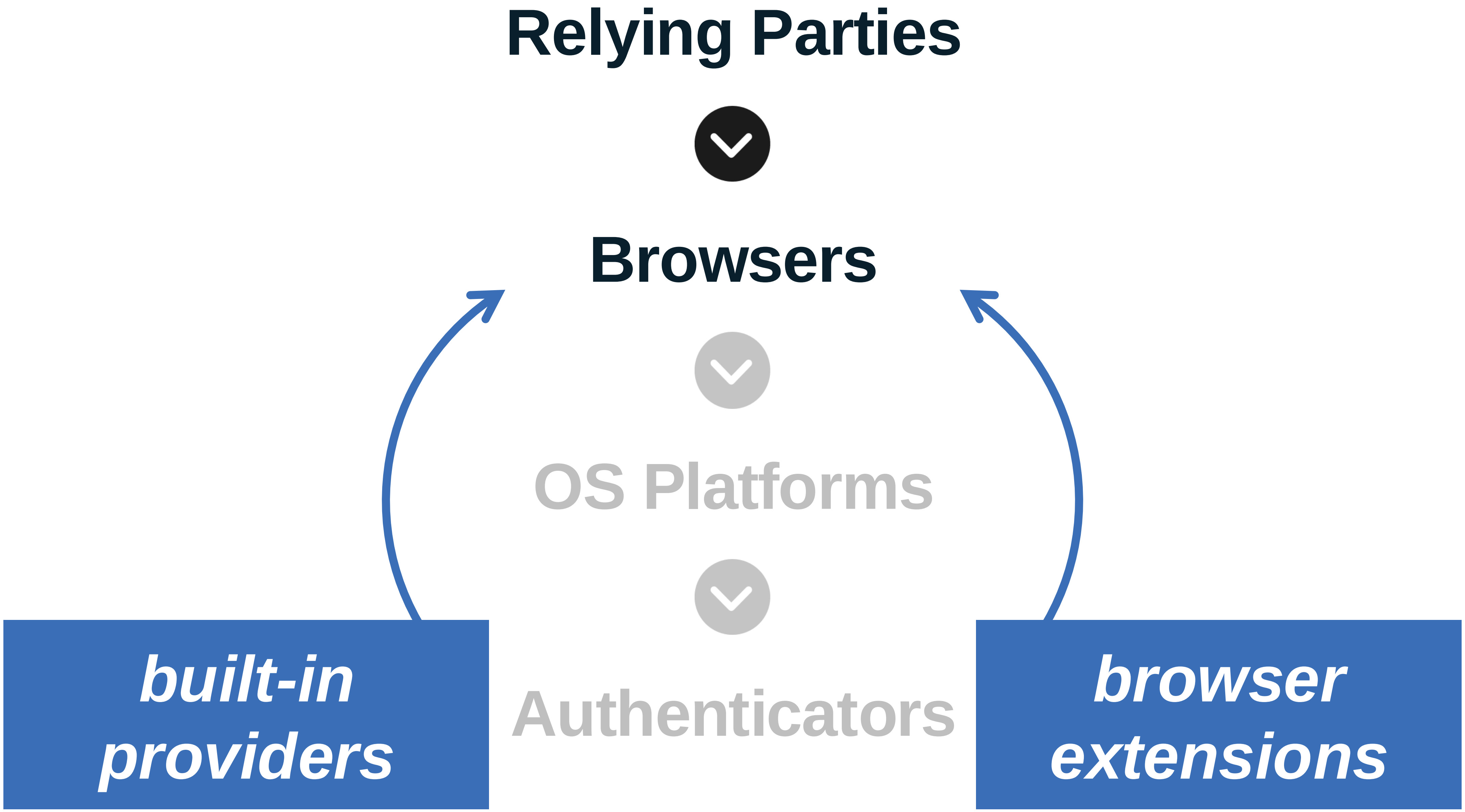
Relying Parties

Browsers

OS Platforms

Authenticators

this is it, right?



Relying Parties

Browsers

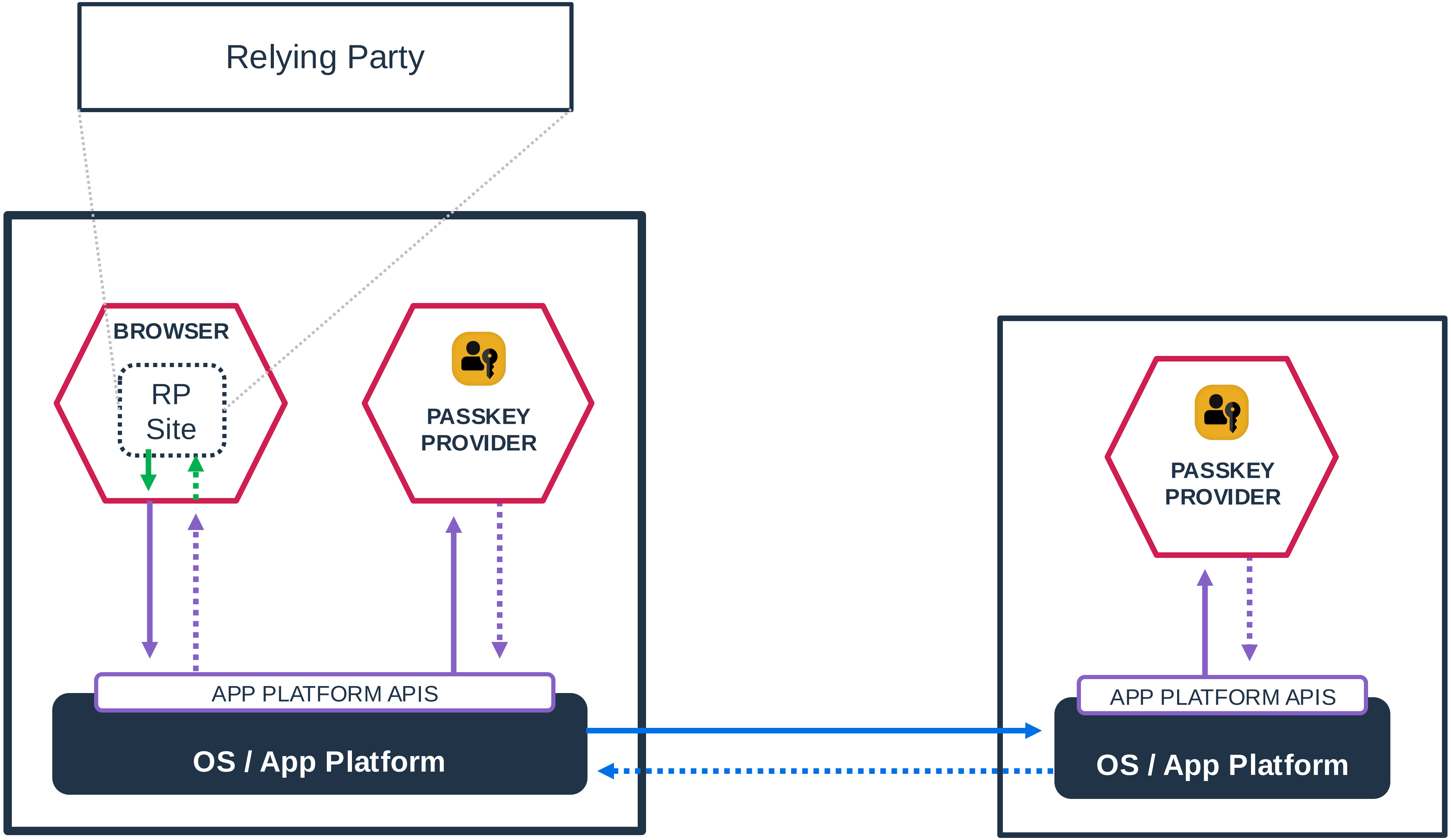
OS Platforms

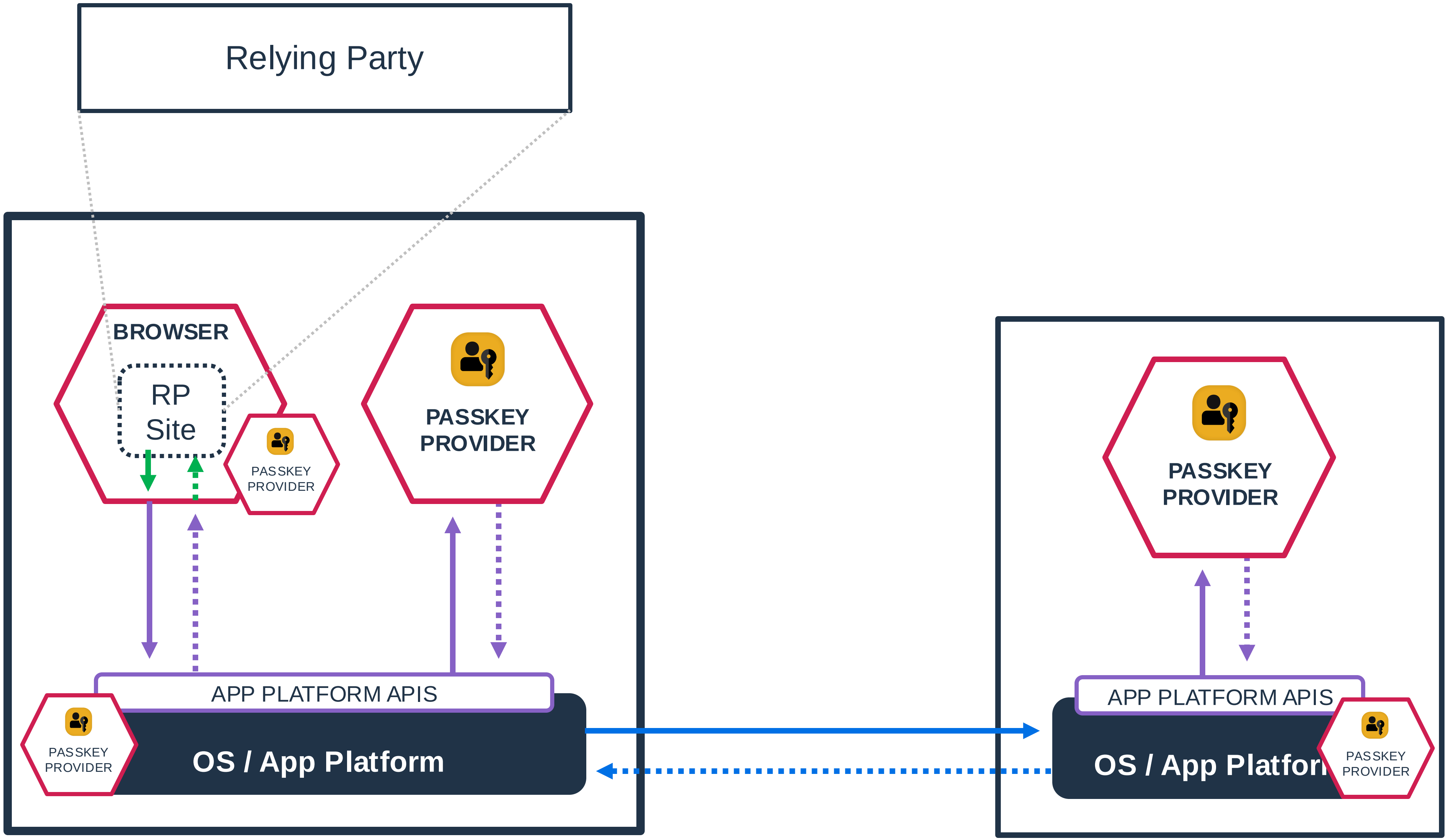
Authenticators

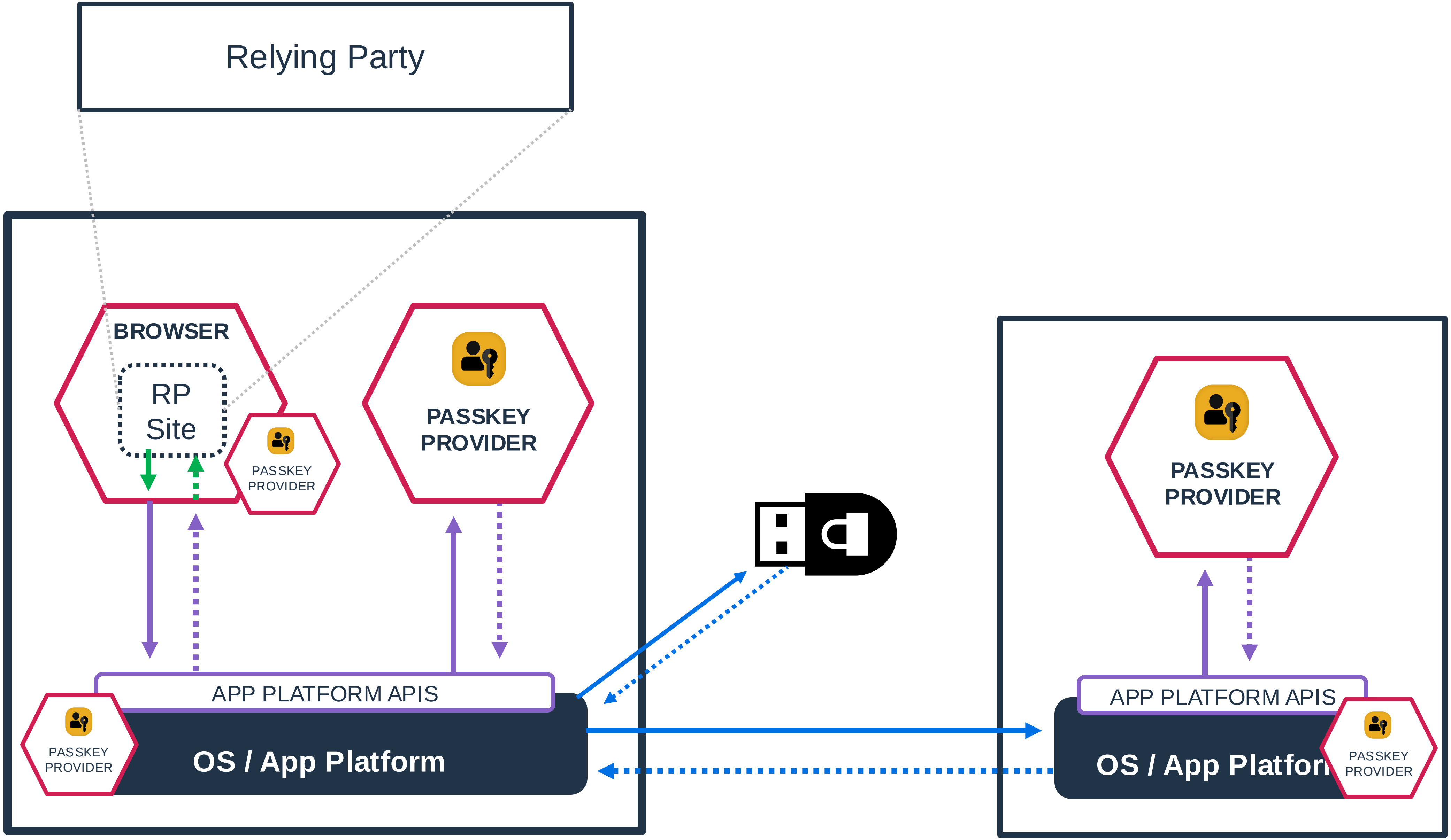
built-in providers

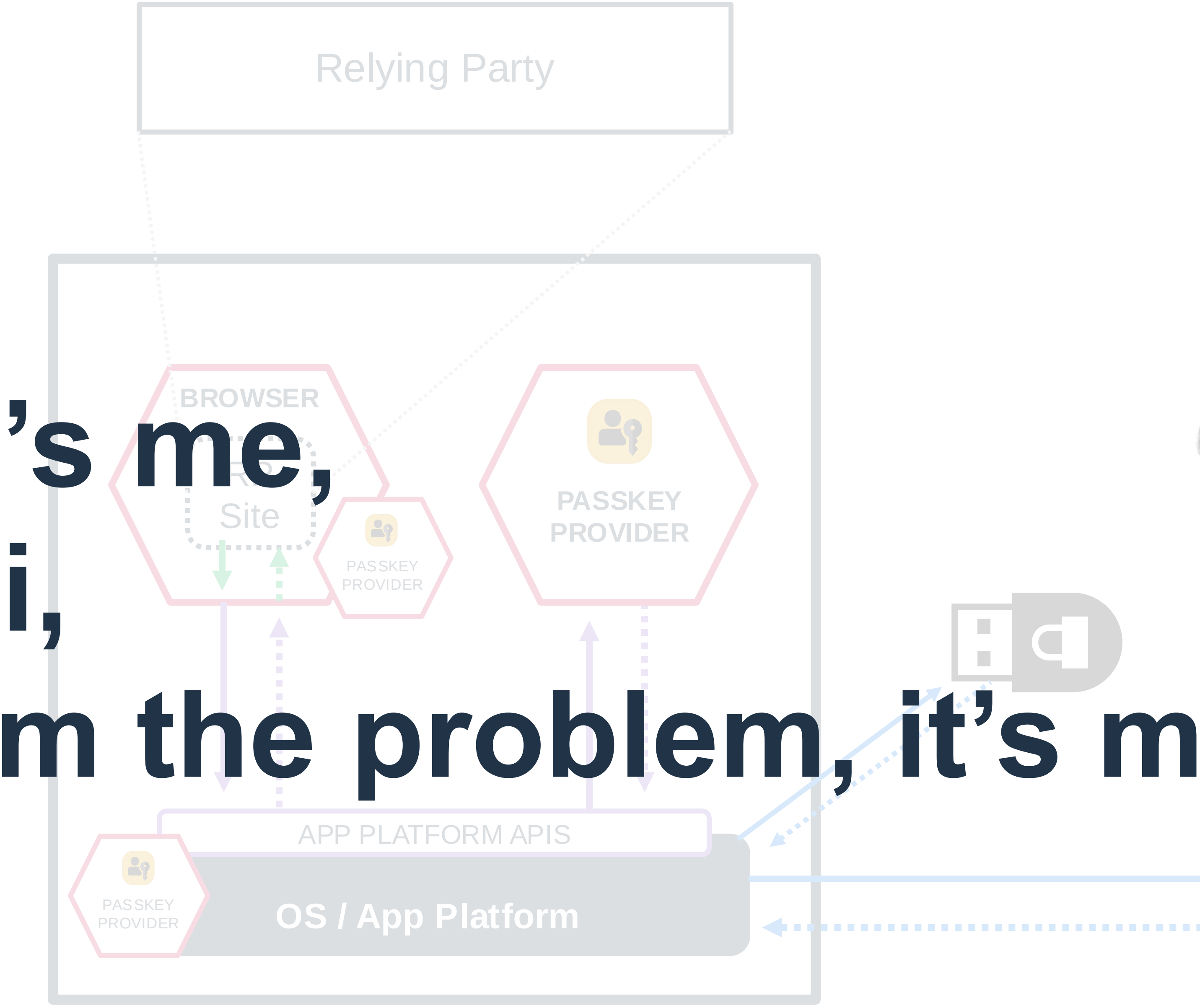
browser extensions

The **Layers**


Relying Party
BROWSER
RP
Site
PASSKEY
PROVIDER
APP PLATFORM APIS
OS / App Platform
PASSKEY
PROVIDER
APP PLATFORM APIS
OS / App Platform

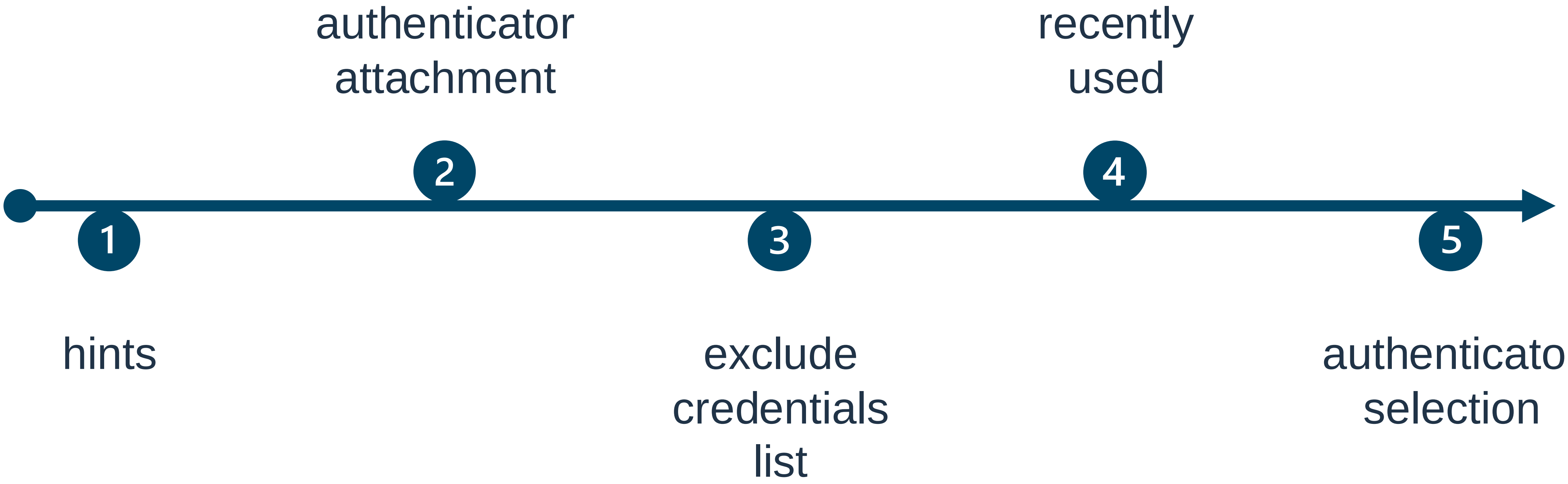

Relying Party
BROWSER
RP Site
PASSKEY PROVIDER
PASSKEY PROVIDER
APP PLATFORM APIS
PASSKEY PROVIDER
OS / App Platform
PASSKEY PROVIDER
APP PLATFORM APIS
OS / App Platform
PASSKEY PROVIDER


Relying Party
BROWSER
RP
Site
PASSKEY
PROVIDER
PASSKEY
PROVIDER
APP PLATFORM APIS
PASSKEY
PROVIDER
OS / App Platform
PASSKEY
PROVIDER
APP PLATFORM APIS
OS / App Platform
PASSKEY
PROVIDER



It’s me,
hi,
I’m the problem, it’s me

Registration / Creation



1 hints

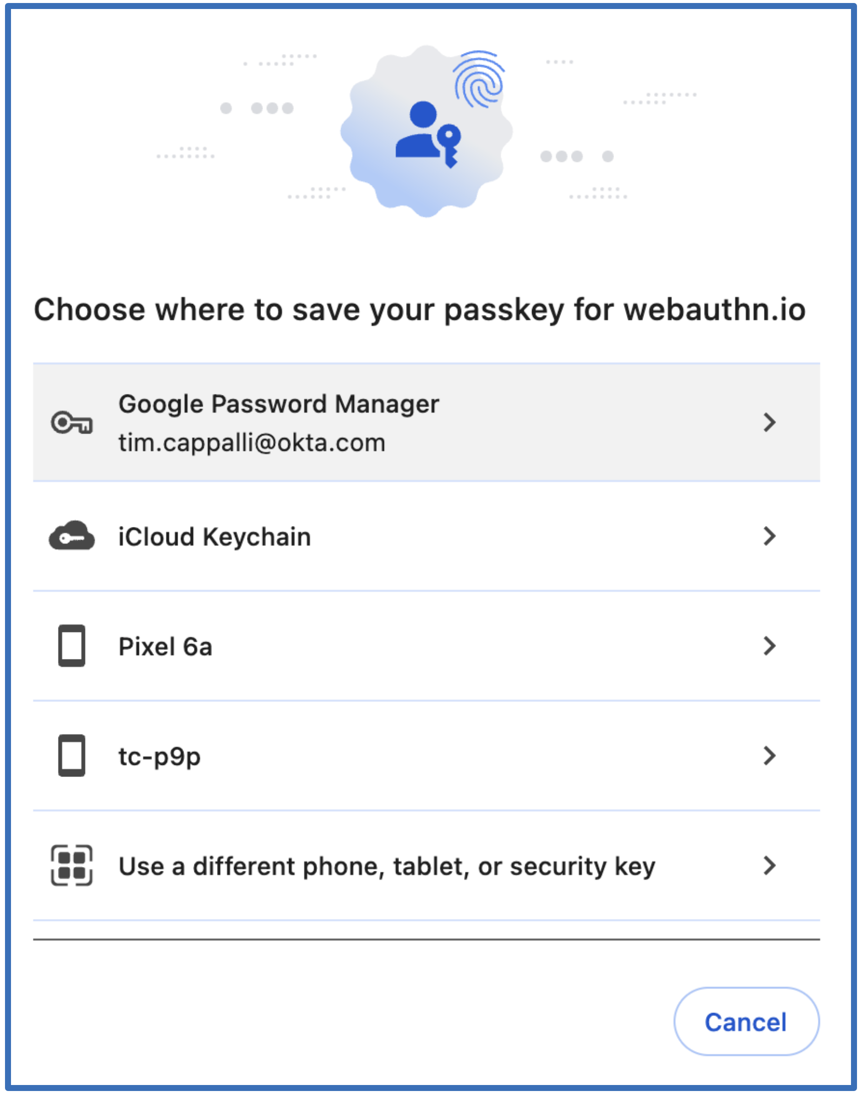
2 authenticator attachment

3 exclude credentials list

4 recently used

5 authenticator selection

Registration / Creation



Choose where to save your passkey for webauthn.io

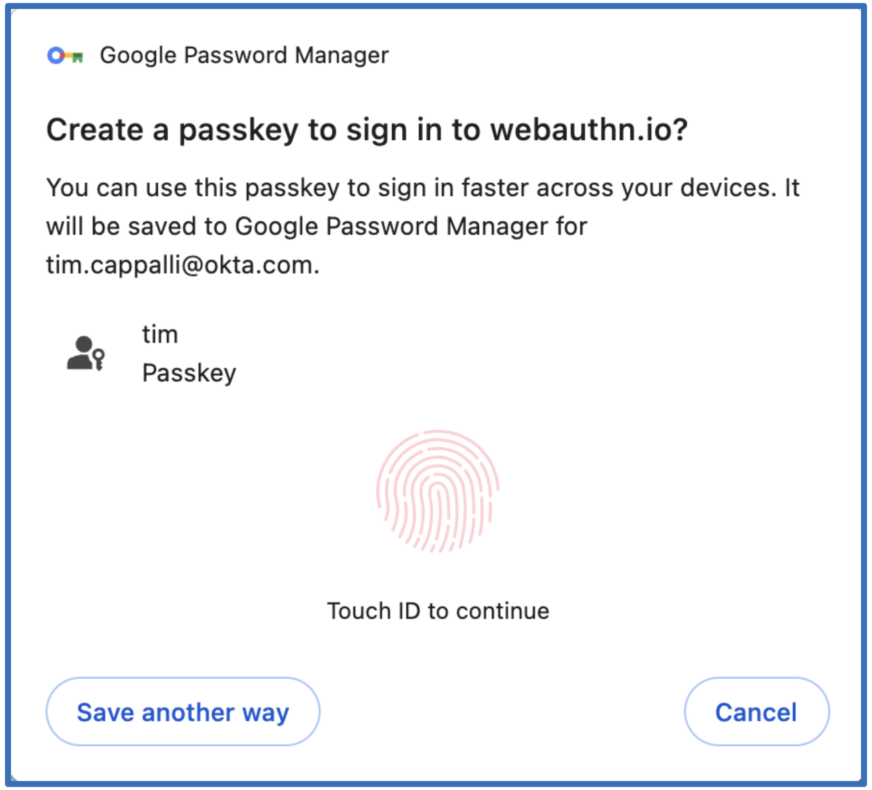
Google Password Manager
tim.cappalli@okta.com

iCloud Keychain

Pixel 6a

tc-p9p

Use a different phone, tablet, or security key



Google Password Manager

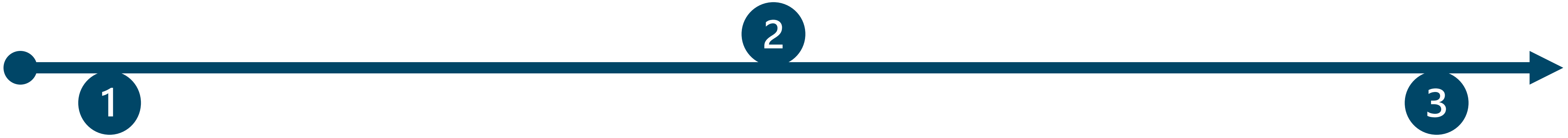
Create a passkey to sign in to webauthn.io?

You can use this passkey to sign in faster across your devices. It will be saved to Google Password Manager for tim.cappalli@okta.com.

tim
Passkey

Touch ID to continue

Authentication



1 allow credentials list

2 local passkeys

3 external authenticators

❶ *allowCredentials* list?

list of credential identifiers which are valid for the ceremony

optionally includes transports

(typically used with reauthentication scenarios)

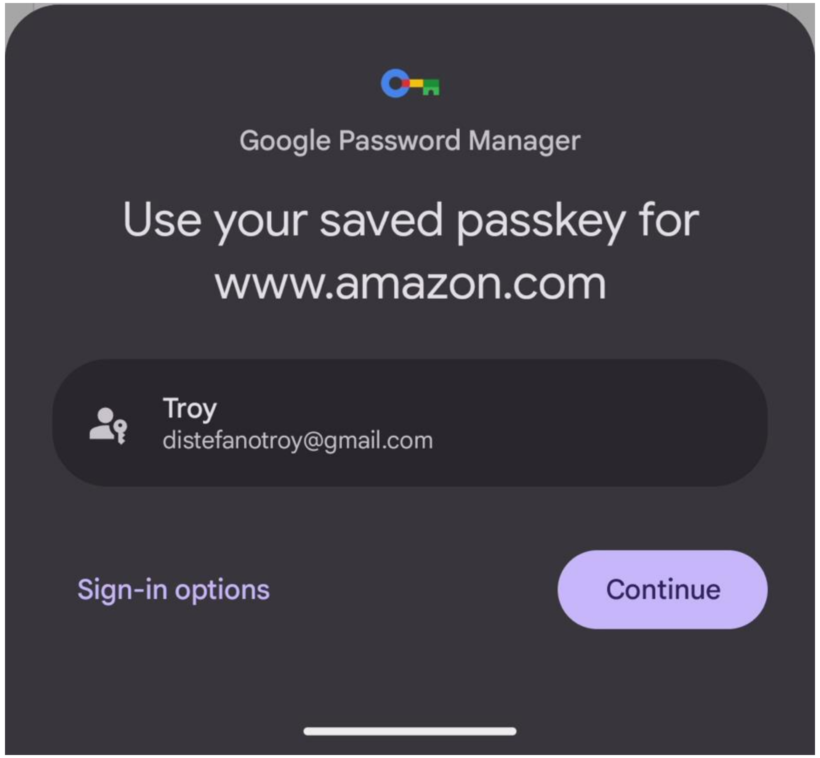
synced passkey provider

security key

device-bound passkey provider

```
{
  "allowCredentials": [
    {
      "id": "qEKGOxAiUAyUZ337M5y9Lg",
      "type": "public-key",
      "transports": [
        "hybrid",
        "internal"
      ]
    },
    {
      "id": "P4XIrL3ELl6I0dc3Oih3cCdya",
      "type": "public-key",
      "transports": [
        "usb"
      ]
    },
    {
      "id": "NsrebzBwd8JNVD2S23JwCa",
      "type": "public-key",
      "transports": [
        "internal"
      ]
    }
  ]
}
```

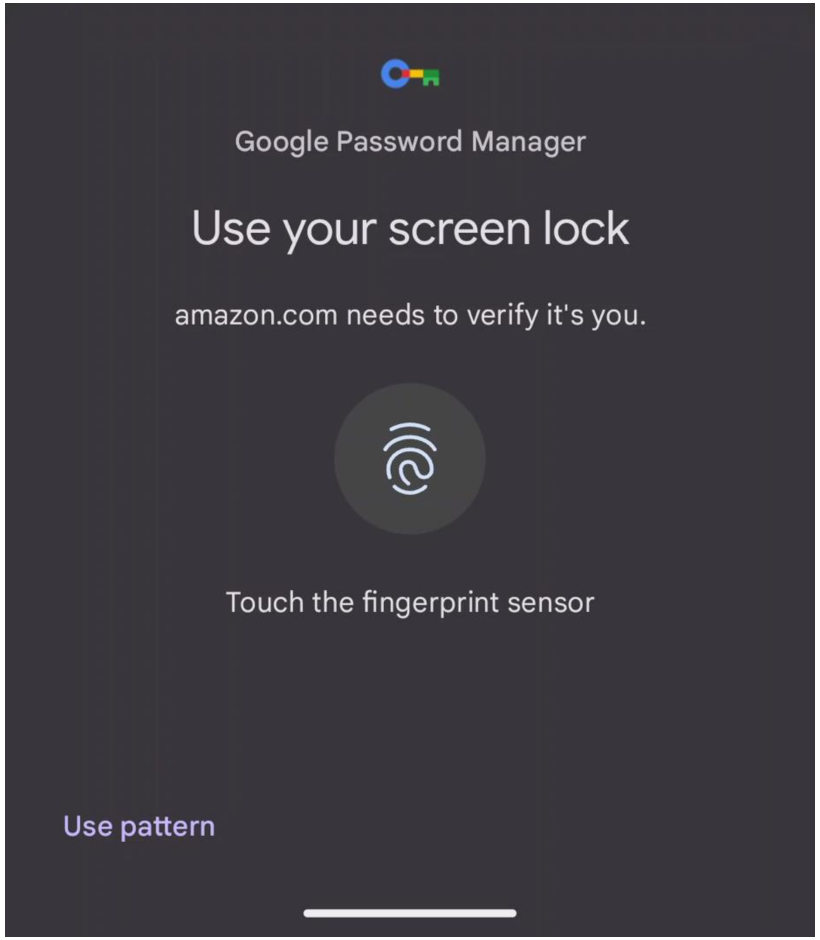
❶ *allowCredentials* list?



Google Password Manager

Use your saved passkey for www.amazon.com

Troy
distefanotroy@gmail.com



Google Password Manager

Use your screen lock

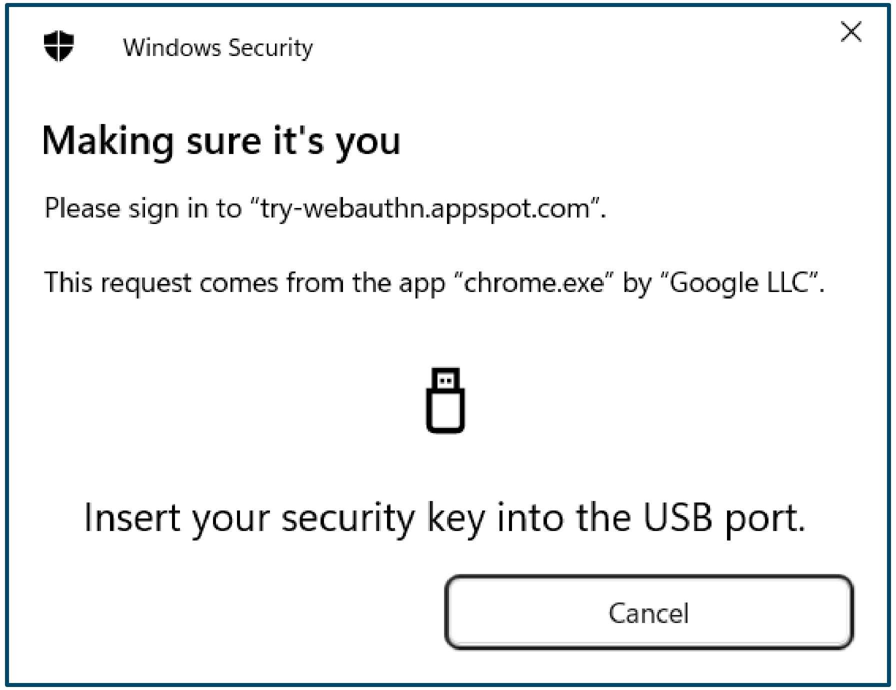
amazon.com needs to verify it's you.

Touch the fingerprint sensor

sign in with a passkey

re-auth with allowCredentials

❶ *allowCredentials* list?



Windows Security

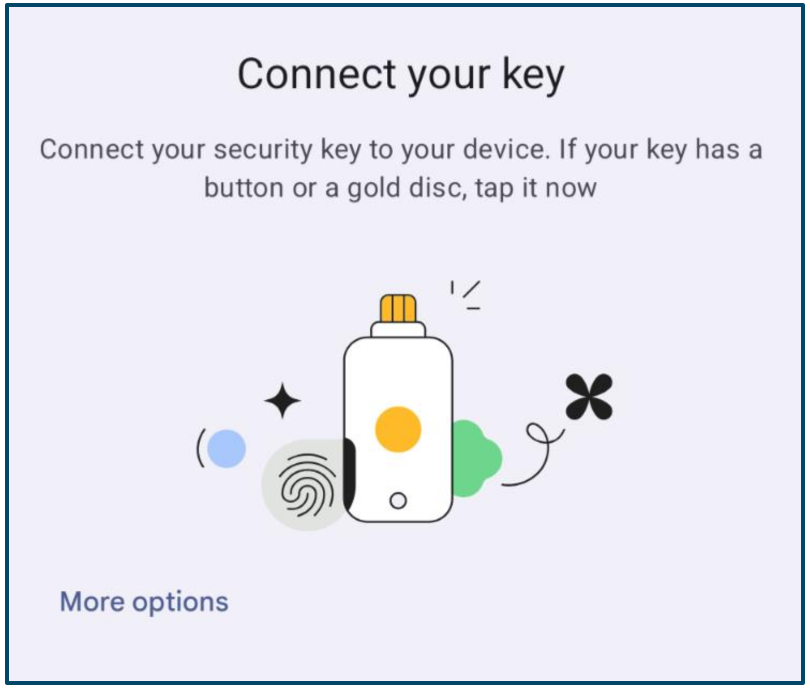
Making sure it's you

Please sign in to "try-webauthn.appspot.com".

This request comes from the app "chrome.exe" by "Google LLC".

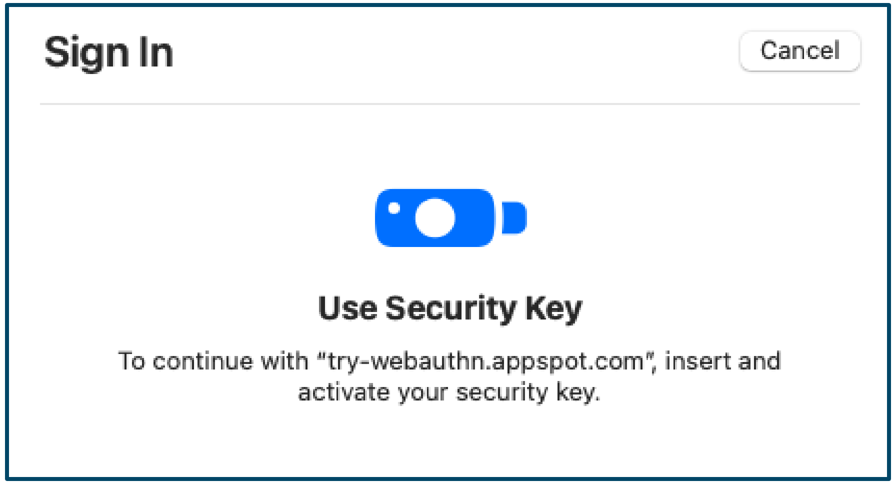
Insert your security key into the USB port.

passkey on a security key



Connect your key

Connect your security key to your device. If your key has a button or a gold disc, tap it now



Sign In

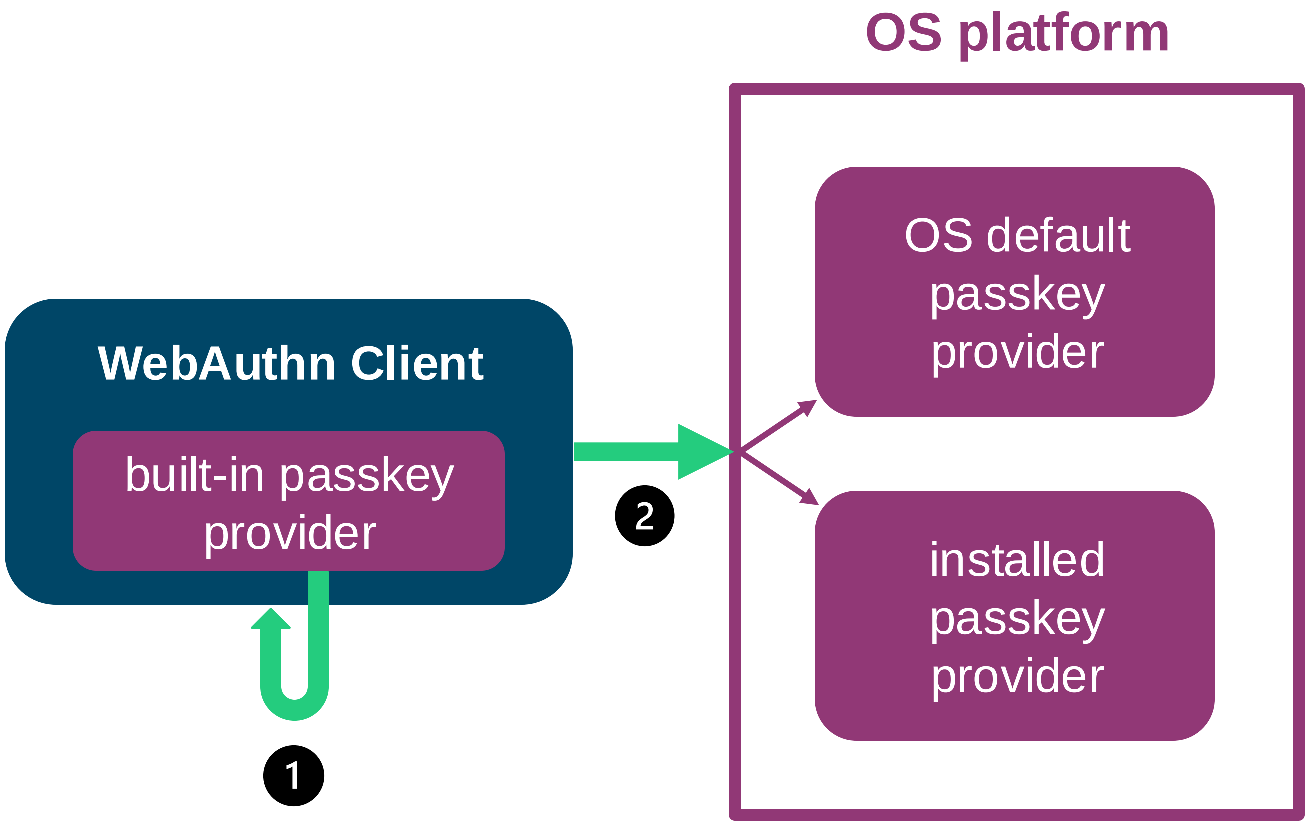
Use Security Key

To continue with "try-webauthn.appspot.com", insert and activate your security key.

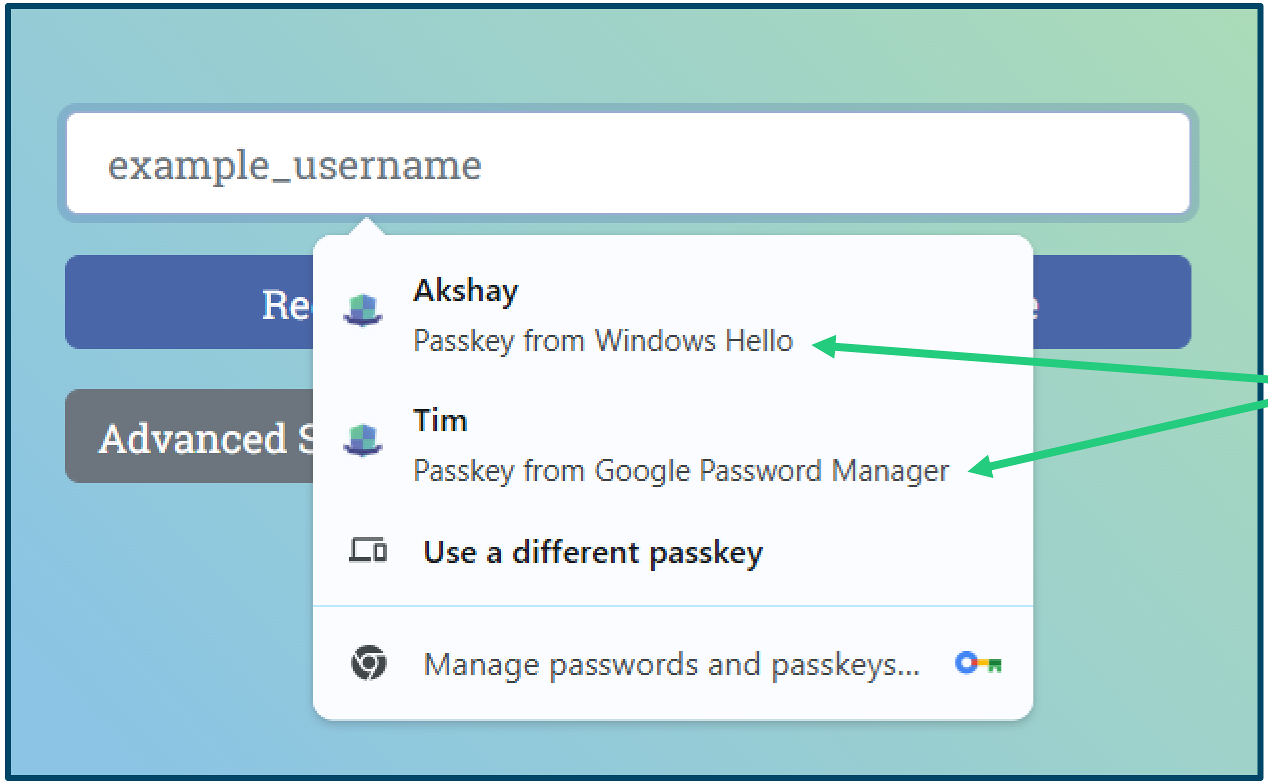
❷ local passkeys?

1. Query built-in provider

2. Query the platform


OS platform
WebAuthn Client
built-in passkey provider
OS default passkey provider
installed passkey provider
1
2

❷ local passkeys?



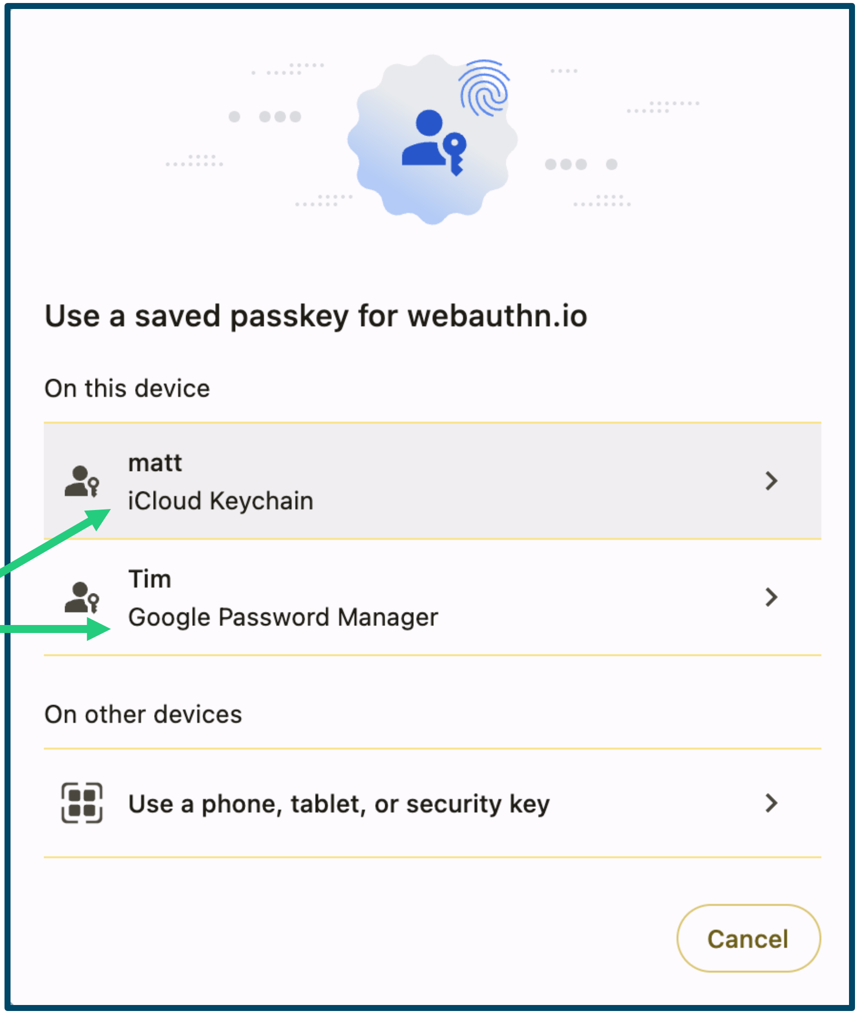
Akshay
Passkey from Windows Hello

Tim
Passkey from Google Password Manager

Use a different passkey

Manage passwords and passkeys...

Autofill UI Example



Use a saved passkey for webauthn.io

On this device

matt
iCloud Keychain

Tim
Google Password Manager

On other devices

Use a phone, tablet, or security key

Cancel

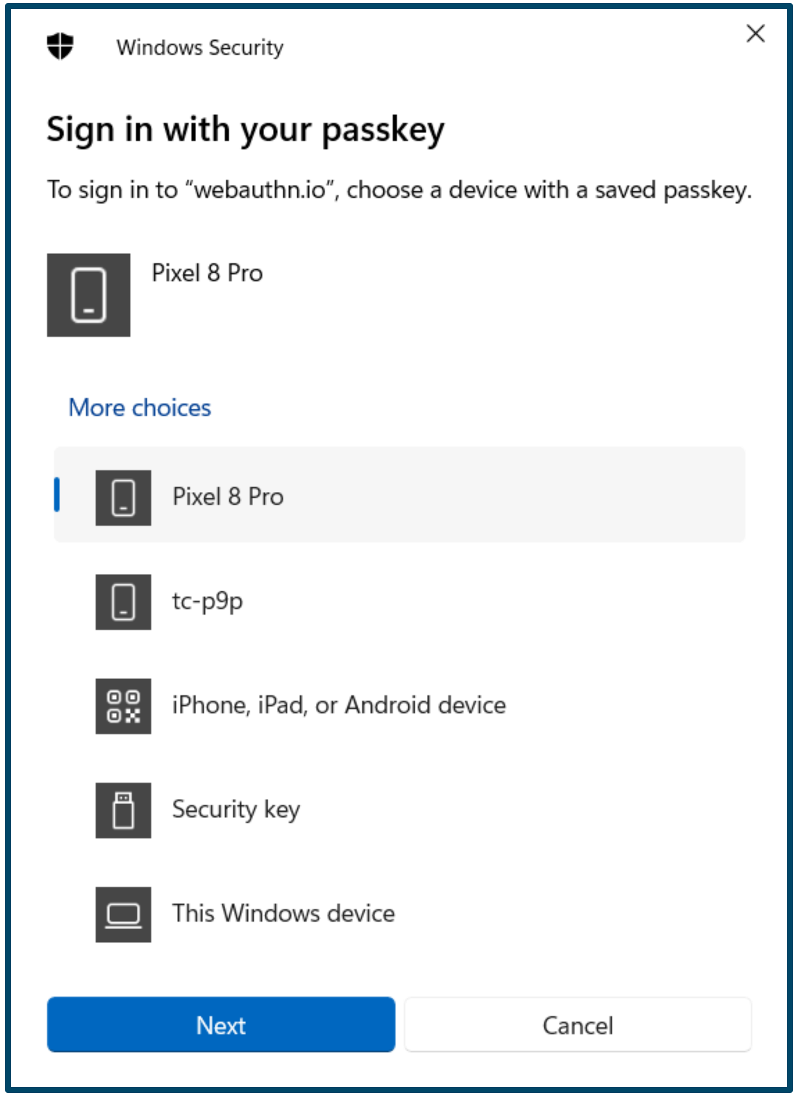
Button UI Example

❸ external authenticators

if no local passkeys are found, the external **authenticator selection** list is displayed

an existing **linked** phone/tablet, a **new** phone/tablet,
or a **security key** can be selected

❸ external authenticators



Windows Security

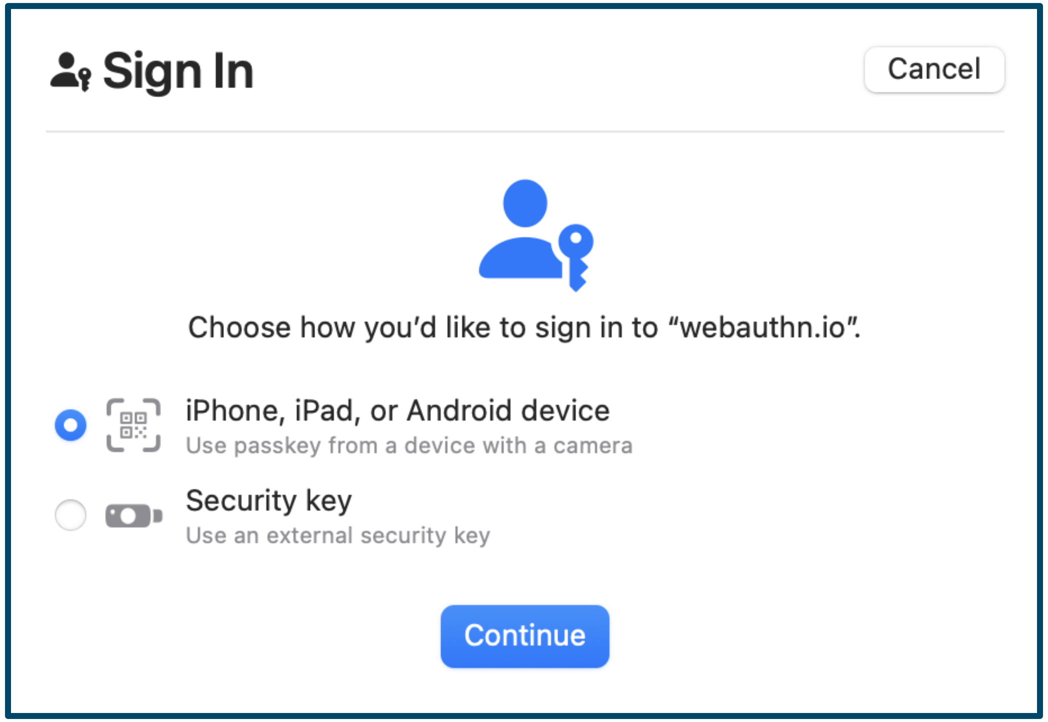
Sign in with your passkey

To sign in to “webauthn.io”, choose a device with a saved passkey.

Pixel 8 Pro

More choices

- Pixel 8 Pro
- tc-p9p
- iPhone, iPad, or Android device
- Security key
- This Windows device



Sign In

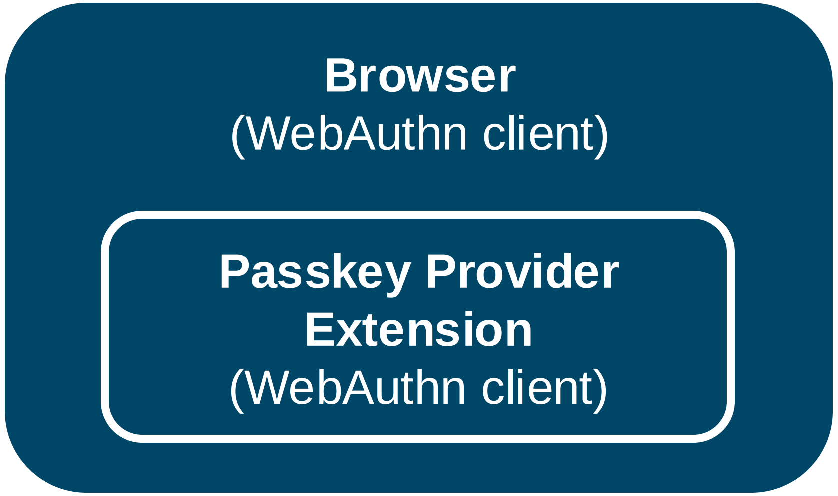
Choose how you’d like to sign in to “webauthn.io”.

● iPhone, iPad, or Android device
Use passkey from a device with a camera

○ Security key
Use an external security key

What about browser extensions?

What about browser extensions?



passkey providers running as browser extensions are a WebAuthn client running inside another WebAuthn client

What about browser extensions?

passkey providers ru wser extensions are a WebAuthn client running inside another WebAuthn client

Takeaways

Takeaways

open ecosystems are complex, with many components

Takeaways

WebAuthn clients are smart and use all available context to guide the user through the best experience, while abstracting away complexity from RPs

Takeaways

WebAuthn clients are adapting to provide better experiences based on user and RP feedback

What We Didn’t Talk About

The App Platform

(aka native apps and native APIs)

next year, same time, same place?

Q&A

authenticate 2024

THE FIDO CONFERENCE

Thank you

Signature Sponsors:

cisco | Microsoft | yubico | Google

authenticatecon.com