INTERNET2 | TECHex24 BOSTON DEC 9-13

THE END OF PASSWORDS IS FINALLY IN SIGHT

The past, present, and future of **passkeys**

Tim Cappalli | December 2024

About Me

socials: **timcappalli.me** 👀

live here in **Boston** and work on **identity standards** for **digital credentials** at **Okta**

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

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

for the hockey fans

INTERNET2

TECH ex 24
BOSTON DEC 9-13

The past, present, and future of **passkeys**

THE PAST

- A brief history of FIDO2/WebAuthn

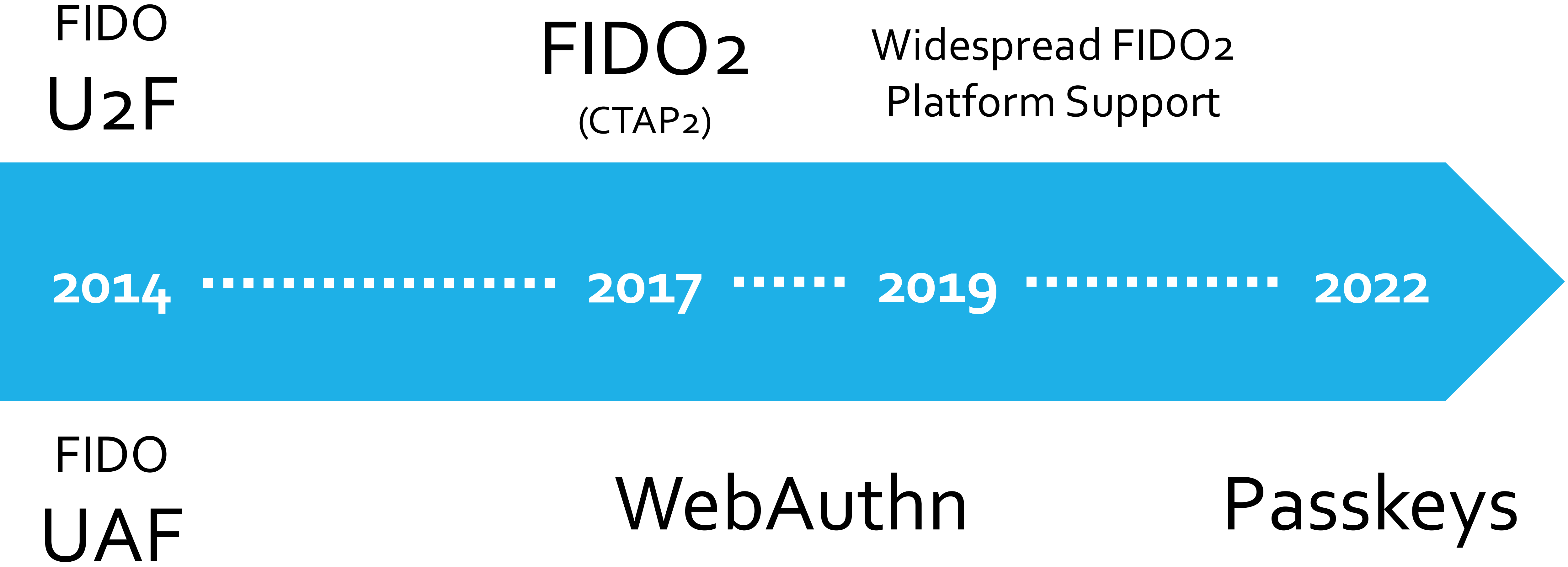
THE PRESENT

- What is a passkey?
- Benefits for research & education
- Adoption & challenges

THE FUTURE

- New capabilities & improvements
- Federation + digital credentials + passkeys

A brief history of FIDO2/WebAuthn



FIDO U2F

FIDO2 (CTAP2)

Widespread FIDO2 Platform Support

2014 2017 2019 2022

FIDO UAF

WebAuthn

Passkeys

FIDO
U2F

FIDO2
(CTAP2)

Widespread FIDO2
Platform Support

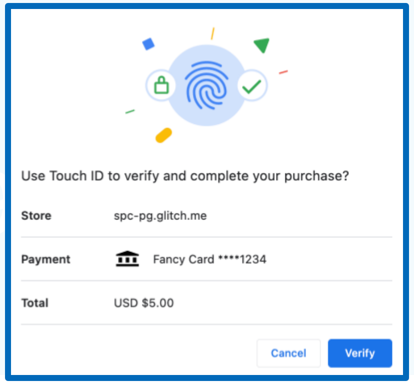
20 2017 2019 2

"FIDO
tokens"

FIDO
UAF

"Built-in"
authenticators

WebAuthn


Use Touch ID to verify and complete your purchase?

Store	spc-pg.glitch.me
Payment	Fancy Card ****1234
Total	USD $5.00

Purpose-built
use cases

Passkeys

Passkeys

Why FIDO2 WebAuthn?

1:1

Unique Credential
Per Service

Standards-based

Phishing
Resistant

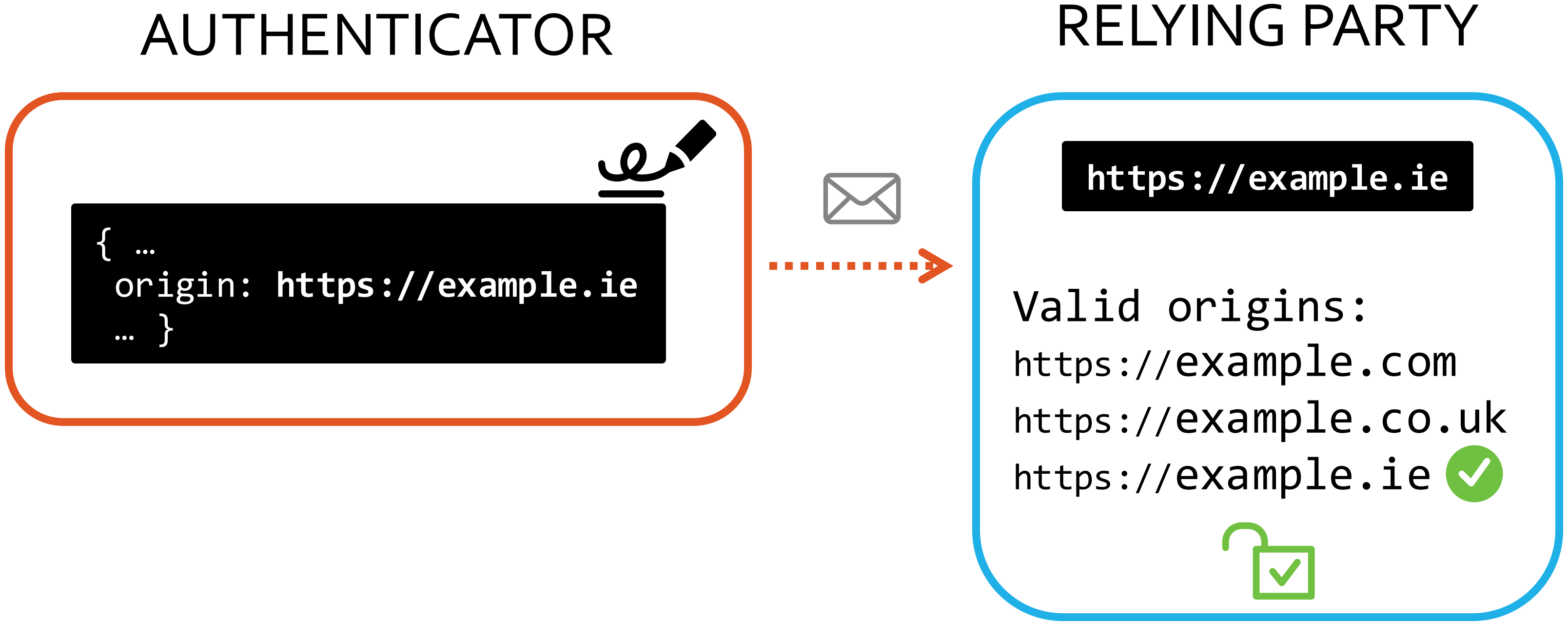
Asymmetric Cryptography
without a PKI

Native
Support

Phishing Resistance

Primary Protection

Signature Over Origin



AUTHENTICATOR

```
{ …
 origin: https://example.ie
 … }
```

RELYING PARTY

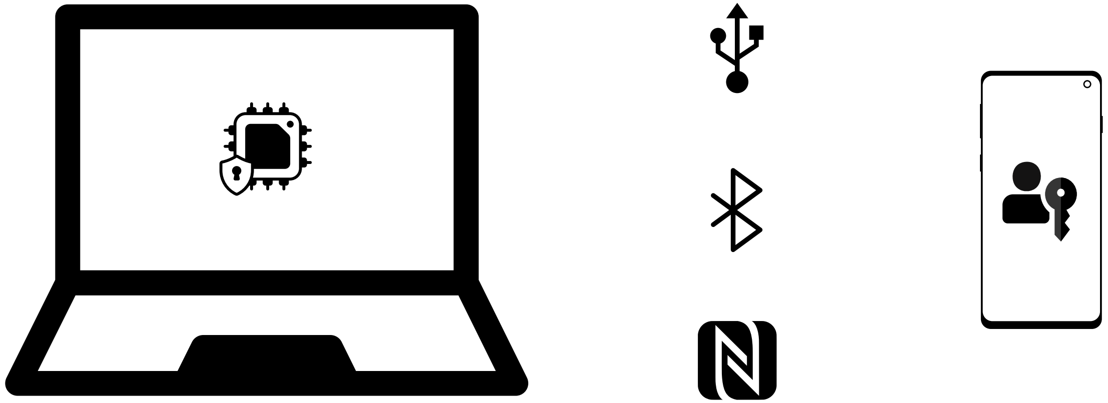
```
https://example.ie
```

```
Valid origins:
https://example.com
https://example.co.uk
https://example.ie ✓
```

Phishing Resistance

Additional Protections

Proximity



Phishing Resistance

Additional Protections

Relying Party Binding

tim@mymail.com
`login.capptoso.com`

- ✓ login.capptoso.com
- ✗ login.capptoso.com.site.xyz
- ✗ myaccount.com
- ✗ Iogin.capptoso.com `login.capptoso.com`

What is a passkey?

passkeys

are replacements for

passwords

(and all the baggage that comes with them)

Four Big Things

a new name

a new icon

a new flavor

new features

A New Credential Name

discoverable credentials

FIDO credentials

WebAuthn discoverable credentials

FIDO2 credentials

passkeys

a password

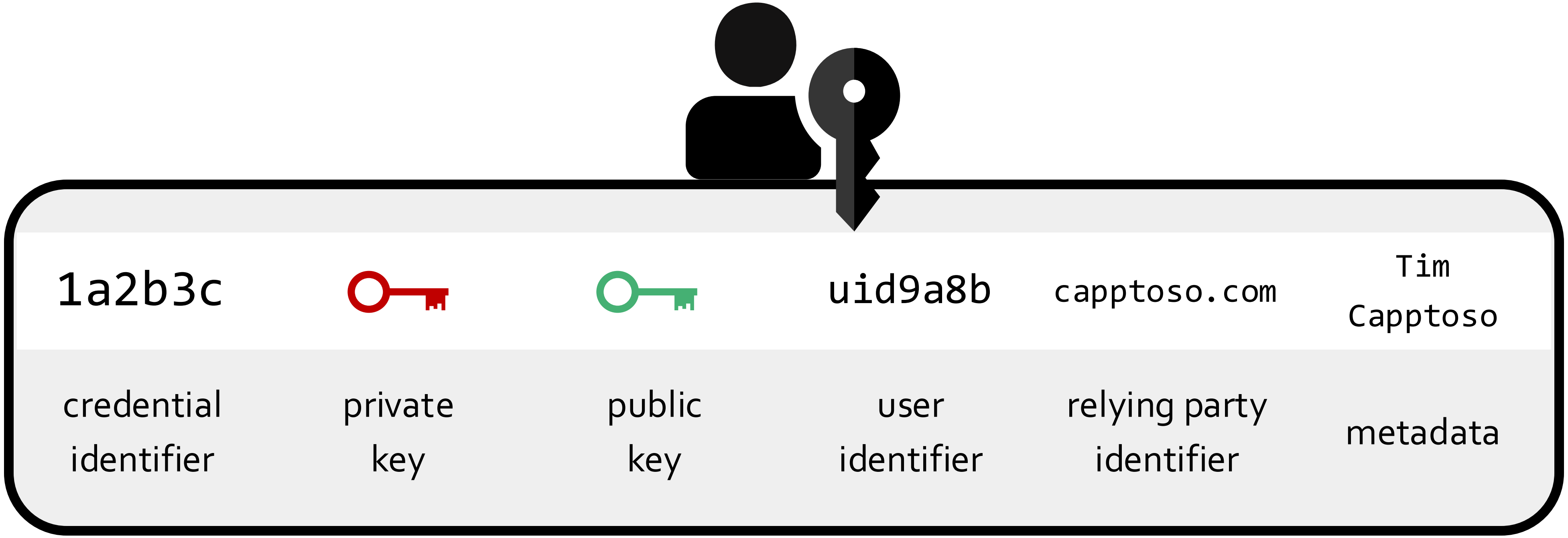
a passkey

common noun

passwords

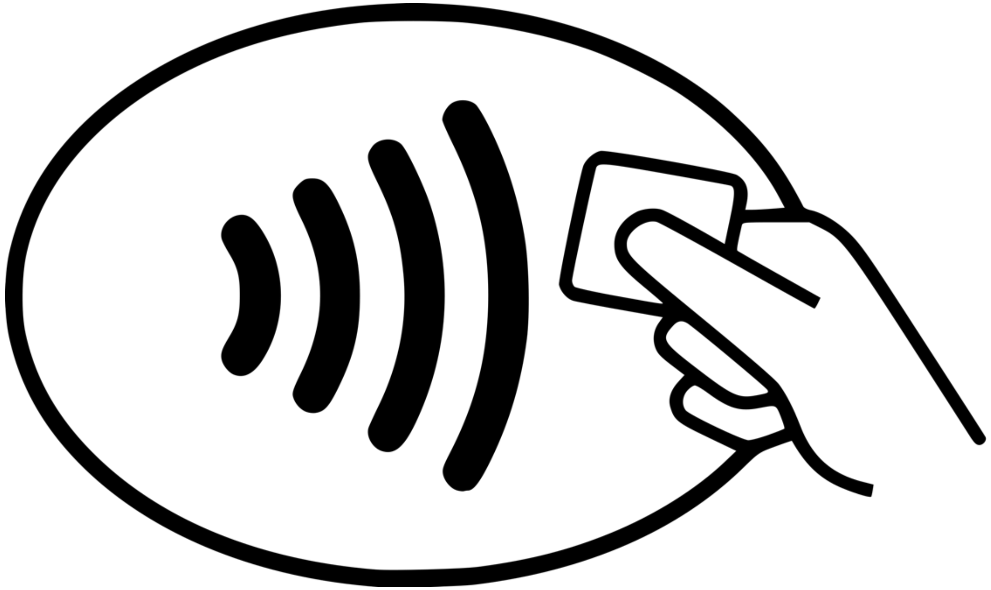
passkeys

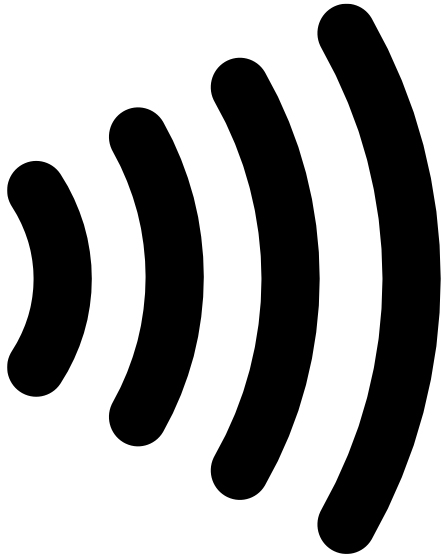
…but what actually is it?



1a2b3c	🔑	🔑	uid9a8b	capptoso.com	Tim Capptoso
credential identifier	private key	public key	user identifier	relying party identifier	metadata

Hands up if you know what these mean!

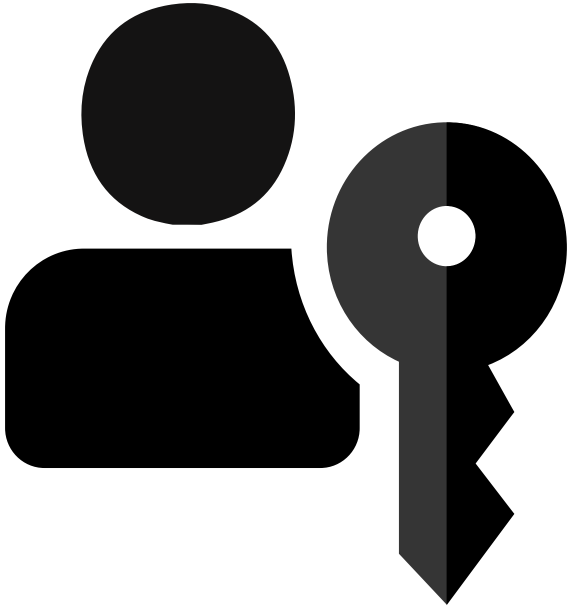




An Icon

???

»



New Flavors

synced
passkeys

What About Security Keys?

synced passkeys

device-bound passkeys

New Features

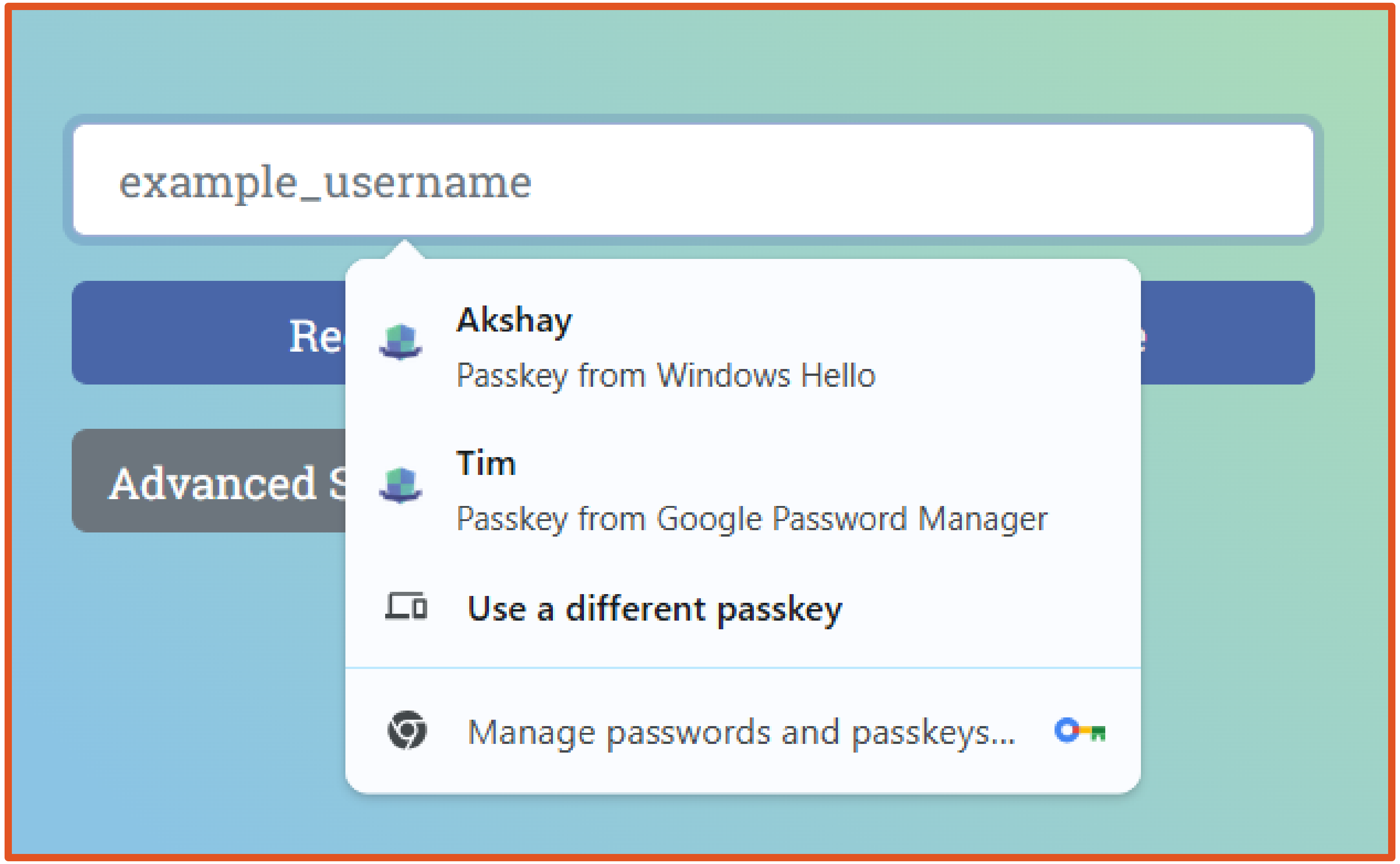
Autofill UI

Cross-Device Authentication

Automatic Upgrades

New Features

Autofill UI



example_username

Re

Advanced S

Akshay
Passkey from Windows Hello

Tim
Passkey from Google Password Manager

Use a different passkey

Manage passwords and passkeys...

tcslides.link/passkeysonion

New Features

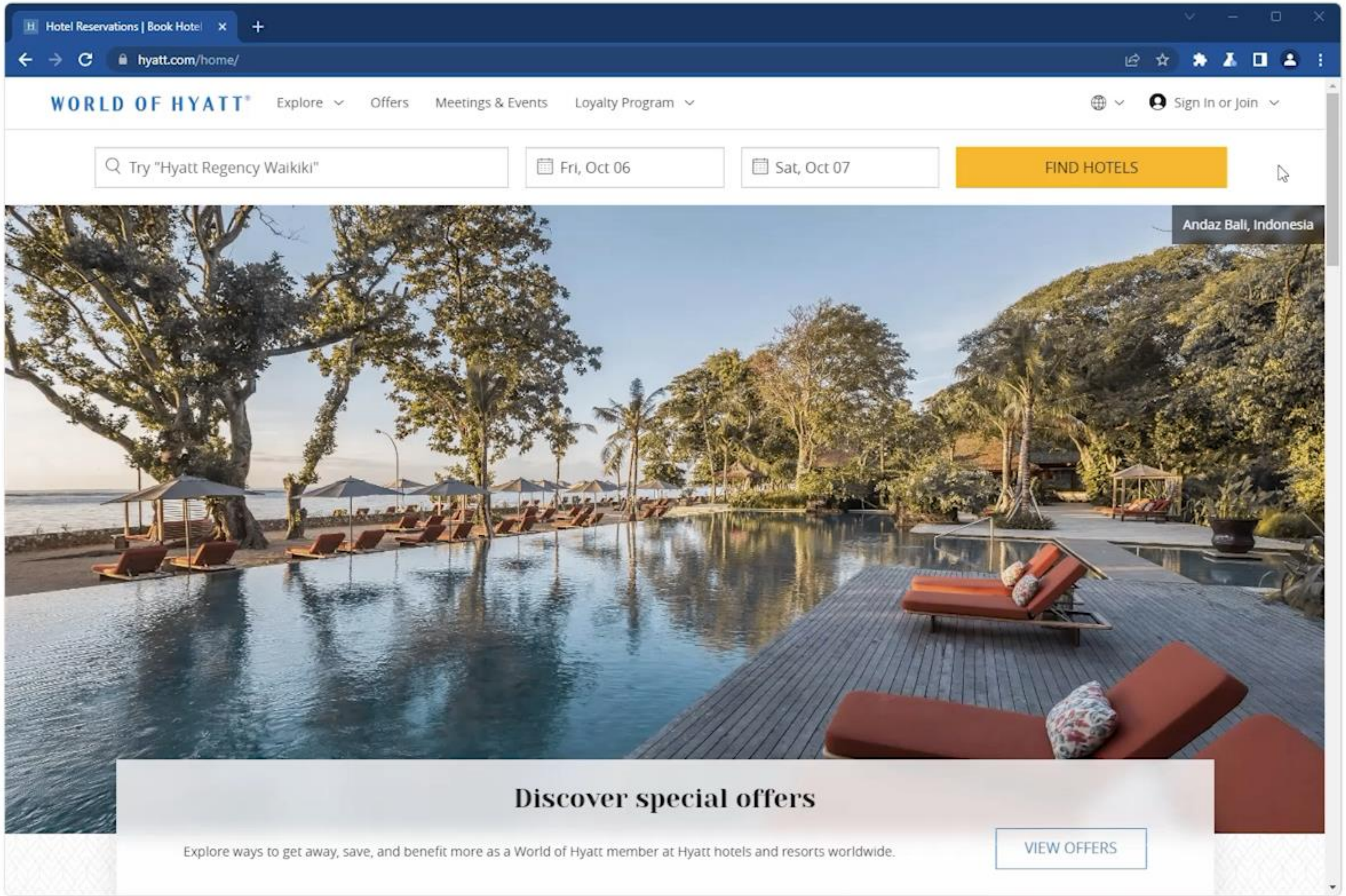
Cross Device Authentication

Shared devices & kiosks

Visitors

Temporary access

Bootstrapping



Discover special offers

Explore ways to get away, save, and benefit more as a World of Hyatt member at Hyatt hotels and resorts worldwide.

New Features

Automatic Upgrades

A relying party can ask the client to **automatically create a passkey** after a successful sign in using other methods!

Benefits for research & education

Students

Phishing-resistant authenticator built-in to all their devices!

- No subscription or purchase required
- No app required
- No additional configuration required

Faculty & Staff

- Traditional app-based MFA solutions can evolve to support passkeys
- Passkey provider app itself can be managed, without managing the device!
- Security keys remain a strong solution

Researchers

- Mix and match depending on security requirements!

What about *eduroam*?

- No direct impact

- Passkeys can be used to sign in to the provisioning service used to configure eduroam

Adoption
& challenges

Passkey Providers

BUILT-IN PROVIDERS

- Apple Passwords
  (iOS/iPadOS/macOS)
- Google Password Manager
  (Android, **Chrome**)
- Samsung Pass
  (Android on Galaxy)
- Windows Hello

EXTERNAL PROVIDERS

- 1Password
- Bitwarden
- Dashlane
- Enpass

…and many more!

Chrome on Windows

Chrome on Android

Apps on iOS

Chrome on Mac

Edge on Ubuntu

Edge on iOS

Apps on Android

Safari on Mac

Apps on Windows

Edge on Android

Safari on iOS

Edge on Mac

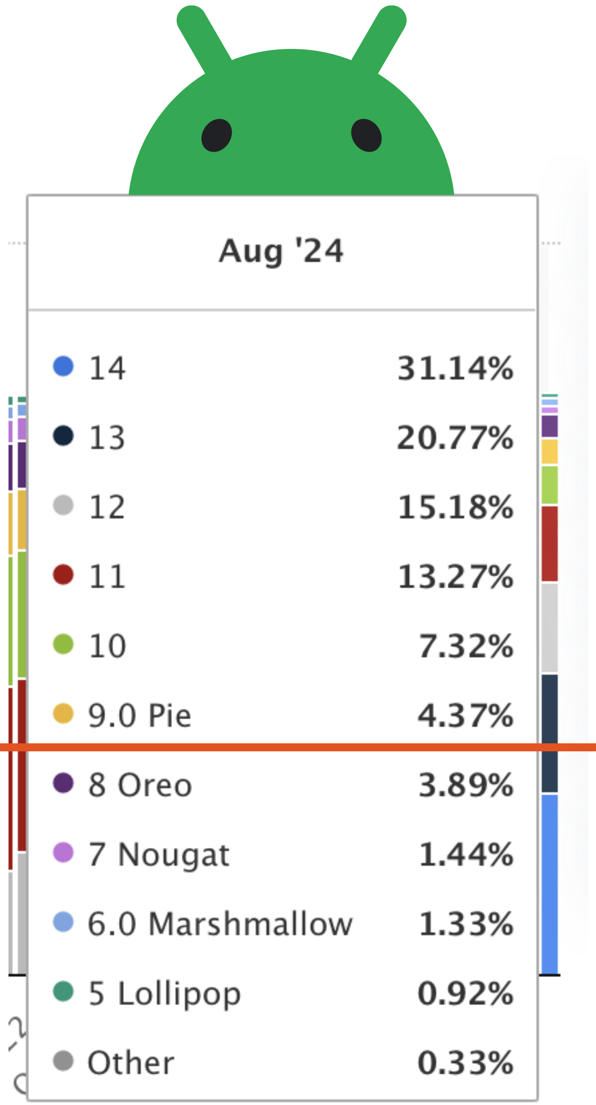
Chrome on iOS

Apps on Mac

Chrome on Ubuntu

Edge on Windows

Device Support



Aug '24

● 14	31.14%
● 13	20.77%
● 12	15.18%
● 11	13.27%
● 10	7.32%
● 9.0 Pie	4.37%
● 8 Oreo	3.89%
● 7 Nougat	1.44%
● 6.0 Marshmallow	1.33%
● 5 Lollipop	0.92%
● Other	0.33%

~92%

Source: Statistica

15 billion

accounts can now leverage passkeys for sign in

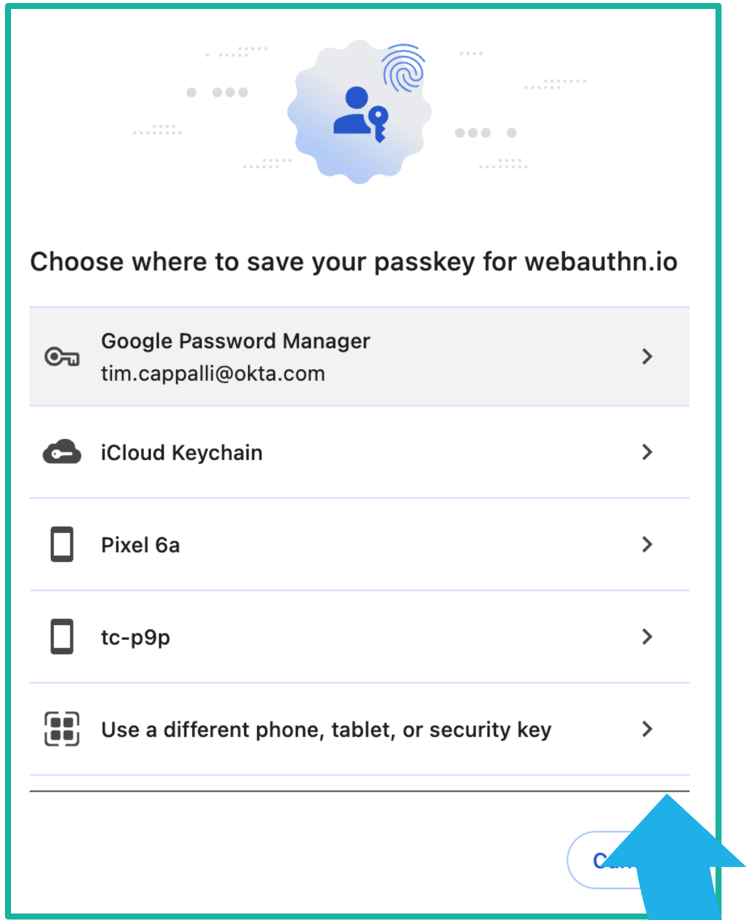
fido™
ALLIANCE

Some Growing Pains

- UI optimizations
- “Orphaned passkeys”
- Complex deployments with many domains
- Concerns about “vendor lock-in”

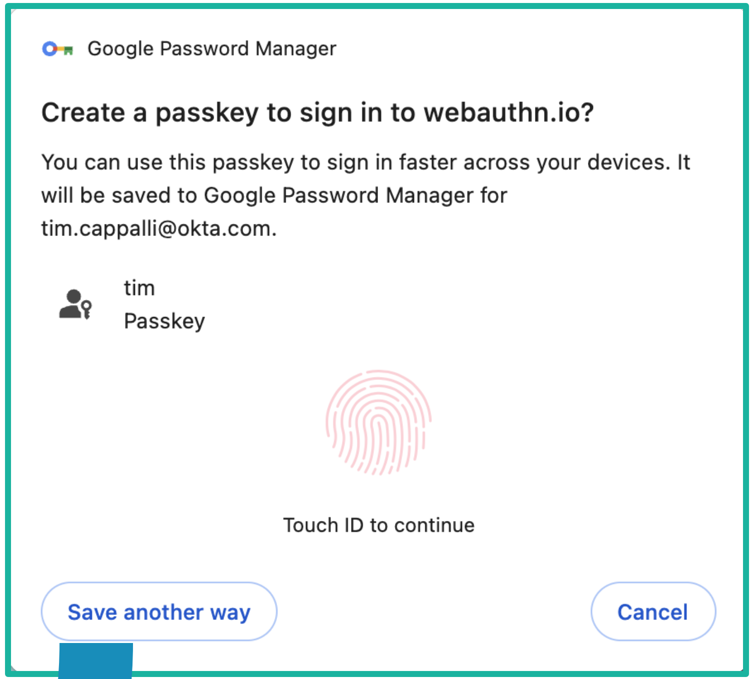
New Capabilities & Improvements

UI/UX Optimizations



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

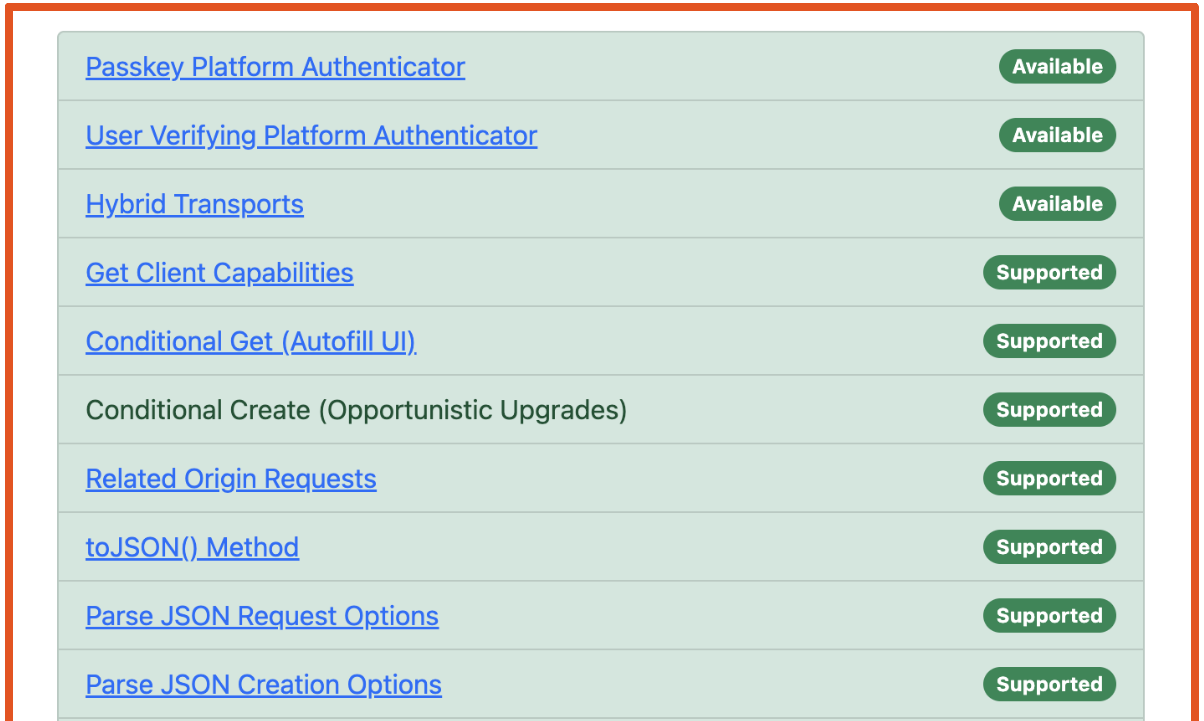
Touch ID to continue

tcslides.link/passkeysonion

Feature Detection

Developers can now detect support for passkeys features prior to offering an experience

featuredetect.passkeys.dev uses this new feature detection capability (example)



Passkey Platform Authenticator	Available
User Verifying Platform Authenticator	Available
Hybrid Transports	Available
Get Client Capabilities	Supported
Conditional Get (Autofill UI)	Supported
Conditional Create (Opportunistic Upgrades)	Supported
Related Origin Requests	Supported
toJSON() Method	Supported
Parse JSON Request Options	Supported
Parse JSON Creation Options	Supported

Related Origins

Create and use passkeys across a limited set of related origins

Designed for situations where federation is not possible

EXAMPLES

Country-code TLDs (ccTLDs)

Branded domains

RP Signals

Allows the RP to tell the client/authenticator which passkeys are still valid and/or update metadata

USE CASES

User deletes a passkey from their account, but not from their provider

User changes their name, and their account identifier changes

Passkey Migration

Work is wrapping up on a family of specifications to enable secure migration of credentials, including passkeys, between credential providers

CREDENTIAL EXCHANGE SPECIFICATIONS

Credential Exchange Protocol (CXP)

Credential Exchange Format (CXF)

Federation
+ digital credentials
+ passkeys

FRIENDS OR COMPETITORS?

passkeys

federation

digital credentials

Verifiable Digital Credentials (VDCs)

Verifiable

The ability to cryptographically verify the authenticity and integrity of the credential and information it contains.

Digital

Stored in a digital format... designed to supplement the physical credentials you already use.

Credential

Statements about an individual, their identity, their status and/or privileges. These can be government credentials, education credentials, or proof of certain personal attributes.

https://www.nist.gov/blogs/cybersecurity-insights/digital-identities-getting-know-verifiable-digital-credential-ecosystem

RESEARCH & EDUCATION

digital credentials

bootstrap

passkeys

sign in

(home IdP)

federation -or-
digital credentials

sign in

(SPs)

digital
credentials

recovery

CONSUMER SCENARIOS

federation -or- digital credentials

sign up

passkeys

sign in

digital credentials

proof up

digital credentials

recovery

Q&A

CONTACT INFO

timcappalli.me