authenticate 2023

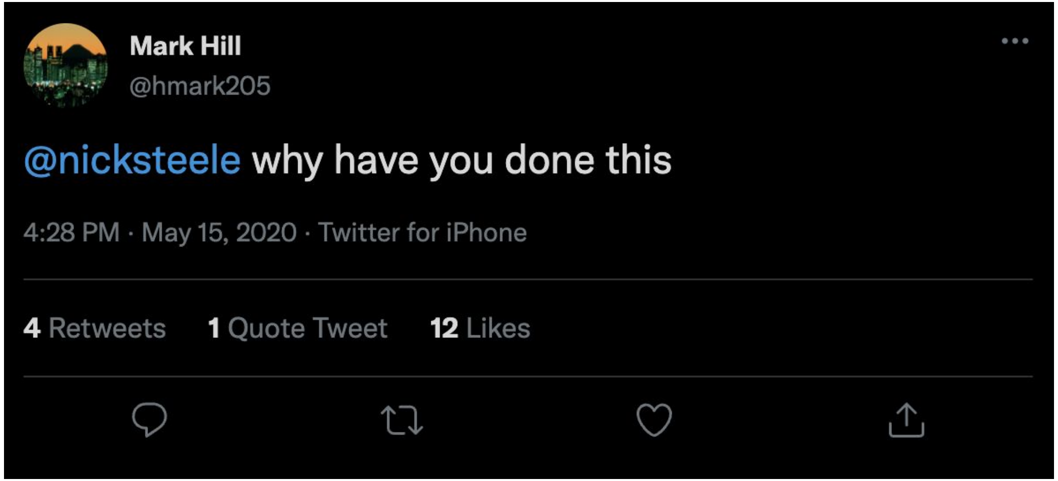
THE FIDO CONFERENCE

Demystifying WebAuthn and Passkeys

Nick Steele
Product Manager
1Password

Matthew Miller
Tech Lead
Duo Security @ Cisco

Why are we here?



Mark Hill
@hmark205

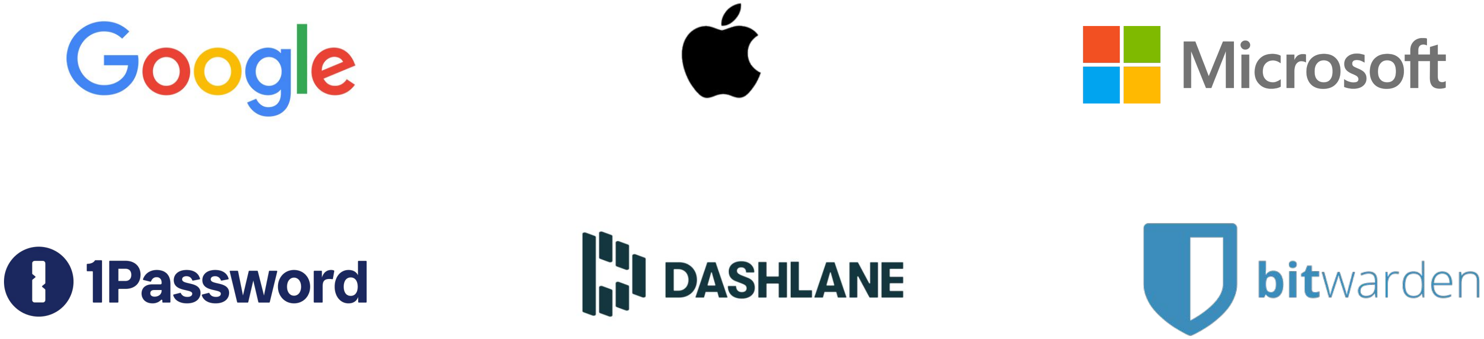
@nicksteele why have you done this

4:28 PM · May 15, 2020 · Twitter for iPhone

4 Retweets **1** Quote Tweet **12** Likes

Where are we at?

Embraced by platforms and credential providers...



…and online services

DocuSign

Google

mercari

HYATT®

CVS Health®

KAYAK

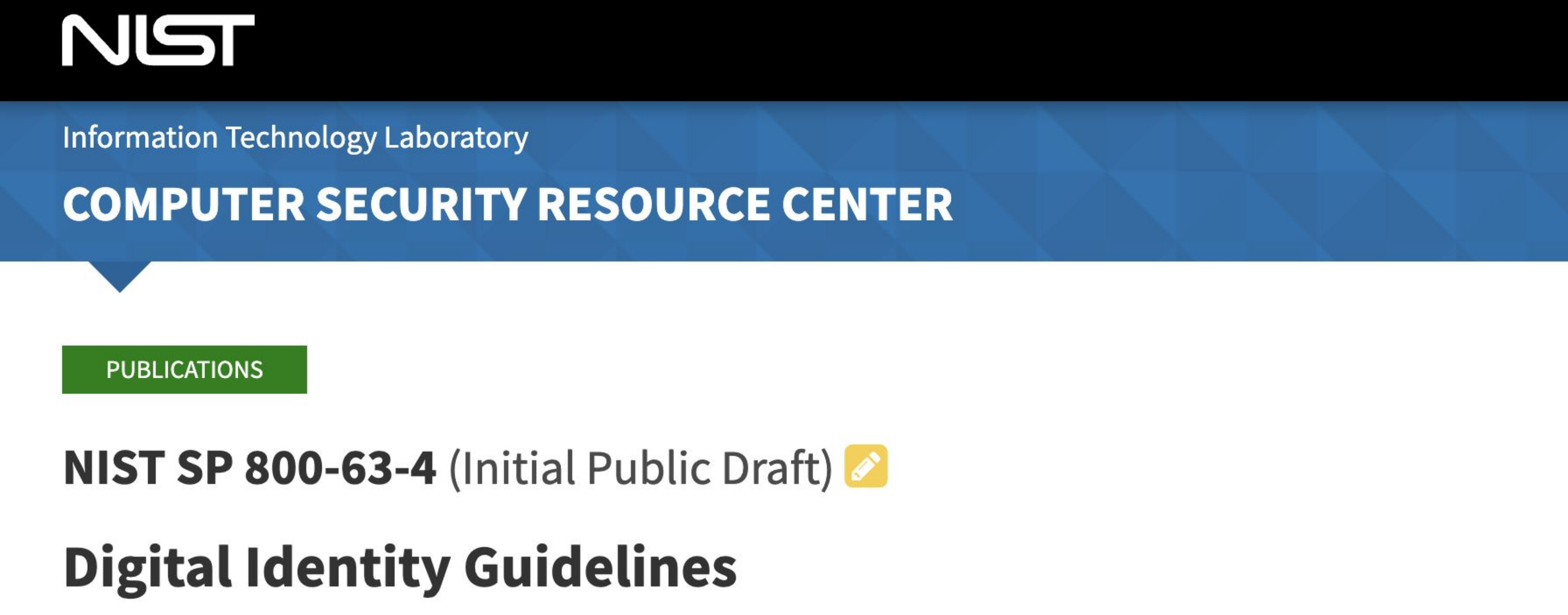
NTT docomo

PayPal

SK telecom

shopify

YAHOO! JAPAN



NIST

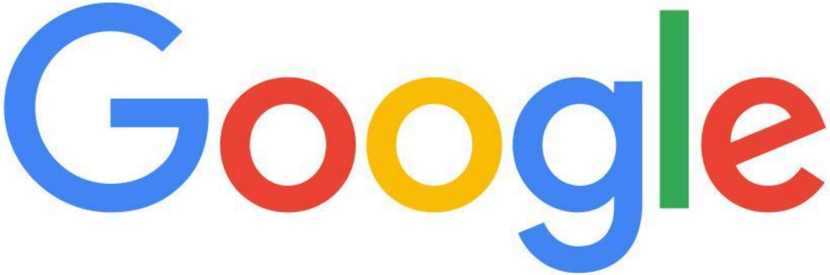
Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

NIST SP 800-63-4 (Initial Public Draft)

Digital Identity Guidelines


Google

1Password

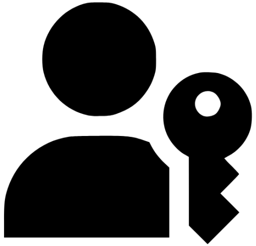
Since September 15th...

Over 150,000 passkeys

This is how we’re doing it.

Let’s talk about passkeys

- The term **passkey** is the most important term to understand outside of FIDO2 and WebAuthn, especially for consumers and executive leadership.

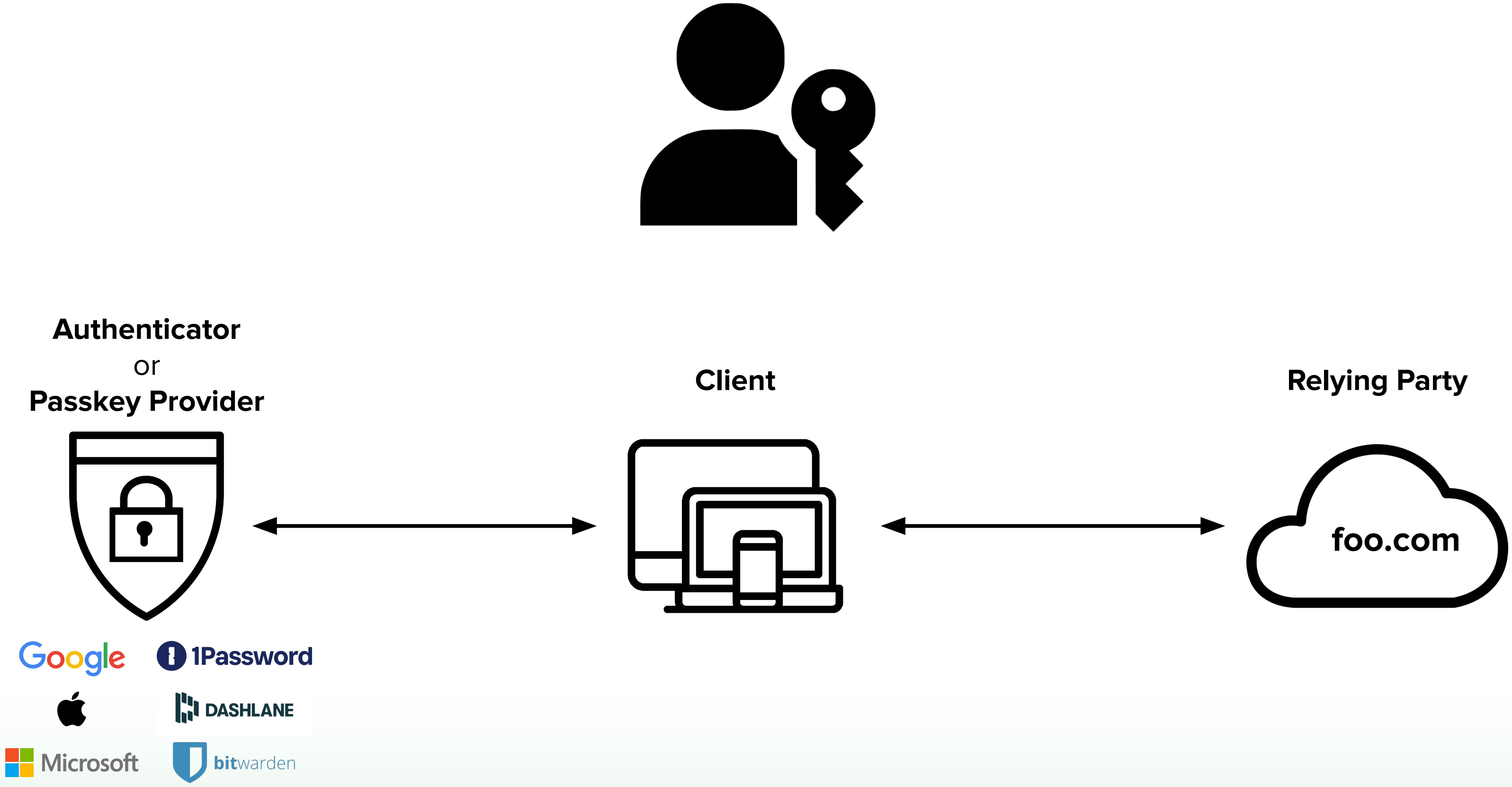


Let’s talk about passkeys

- Passkeys are probably the most accessible and common means by which people will be introduced to passwordless authentication for the web.

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

- They’re mostly a marketing term. Describing it in technical terms is possible, but quickly introduce complexity!



Authenticator
or
Passkey Provider

Client

Relying Party

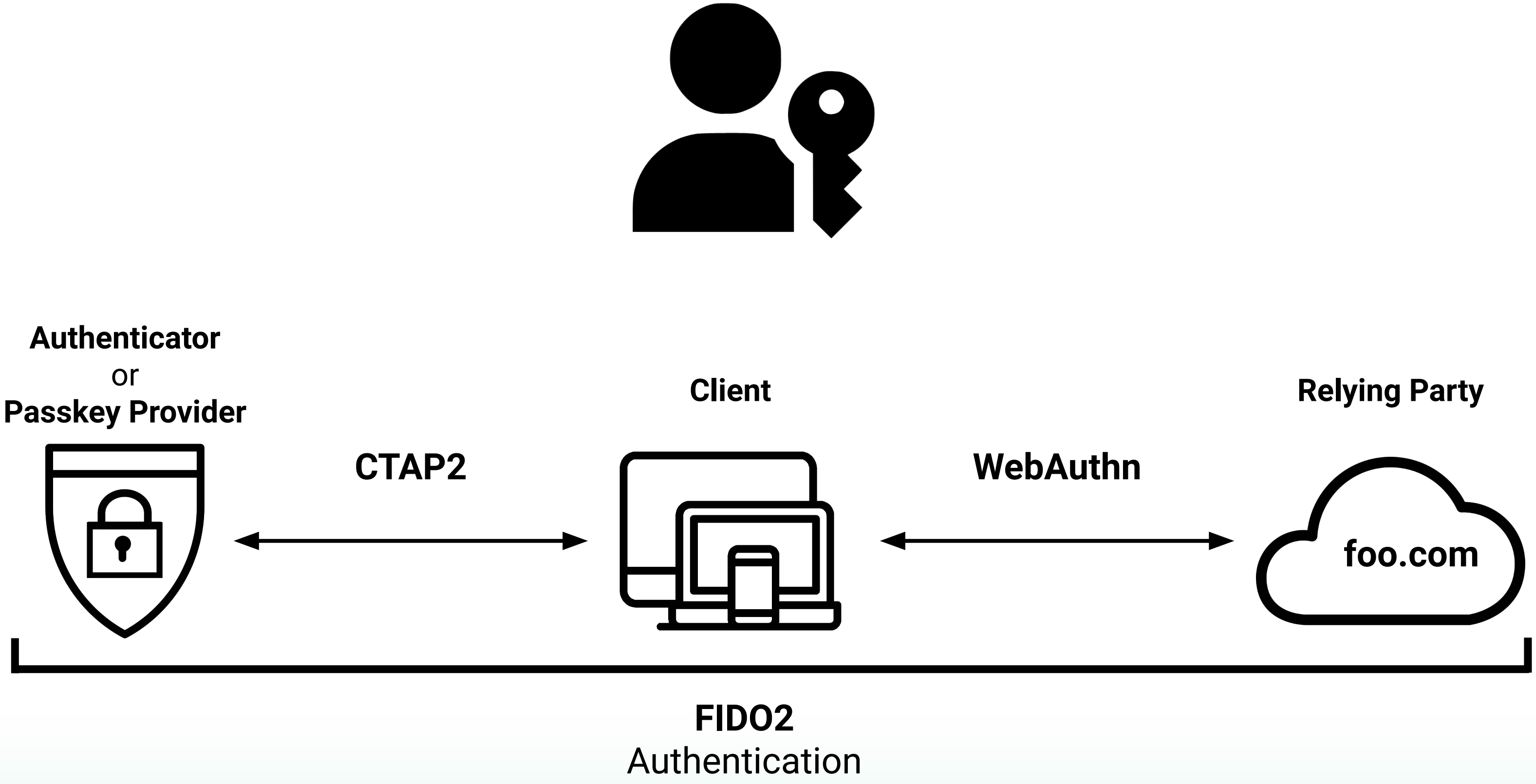
foo.com

How about WebAuthn?

- WebAuthn makes passkeys possible.
  - WebAuthn is the **browser API** that facilitates the creation and use of WebAuthn/FIDO credentials.

- One half of the **FIDO2** Framework.
  - **WebAuthn** and **CTAP2** work together to also allow **cross-platform authenticators** to communicate with a relying party.

- **CTAP2** is mainly used with hardware tokens, and is not a requirement for responding to a WebAuthn request.



Authenticator
or
Passkey Provider

Client

Relying Party

CTAP2

WebAuthn

FIDO2
Authentication

So what’s the technical side of passkeys?

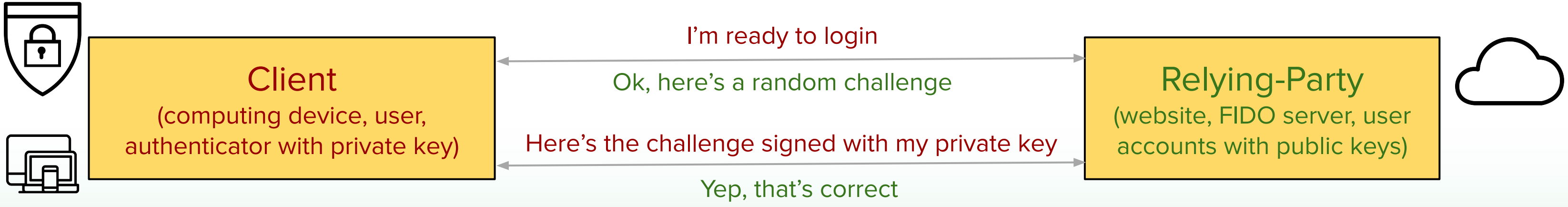
- Passkeys are **discoverable FIDO2 credentials**. Depending on their **backup-eligibility** and **backup-status** they can be "synced" or "device-bound." Synced passkeys are typically synced between devices by a **passkey provider**'s sync fabric.

- Passkeys, as with **all WebAuthn credentials**, still **require user proximity**.

- **Synced** passkeys and **device-bound** passkeys hold different and nuanced security properties.

Recap of FIDO2 authentication....

Passwords	FIDO
Human generated symmetric secret	Machine generated private/public keypair
Often re-used across websites	Bound to a single RP (relying party)
Easily phished	Phishing-resistant
Subject to credential stuffing, social engineering and server leakage	Impractical to remotely attack



Client (computing device, user, authenticator with private key)

I'm ready to login

Ok, here's a random challenge

Here's the challenge signed with my private key

Yep, that's correct

Relying-Party (website, FIDO server, user accounts with public keys)

User Presence

- User presence is important for achieving **phishing resistance** during the WebAuthn ceremony.
  - Requiring that a user performs a physical action (**biometric** scan, **PIN entry**, device interaction) gives RP's assurance that the user is near the authenticator and it is not being initiated remotely.
    - Provides **something you have.**

PIN Support and Biometrics

- During registration and authentication, passwordless RP's also look for **user verification.**
  - **User verification** assures that the human initiating the request is the true owner of the authenticator.
  - Provides **something you know** or **something you are.**

- Generally, devices that support biometrics can fall back to PIN. There is **no guarantee of biometric-only use** of WebAuthn.

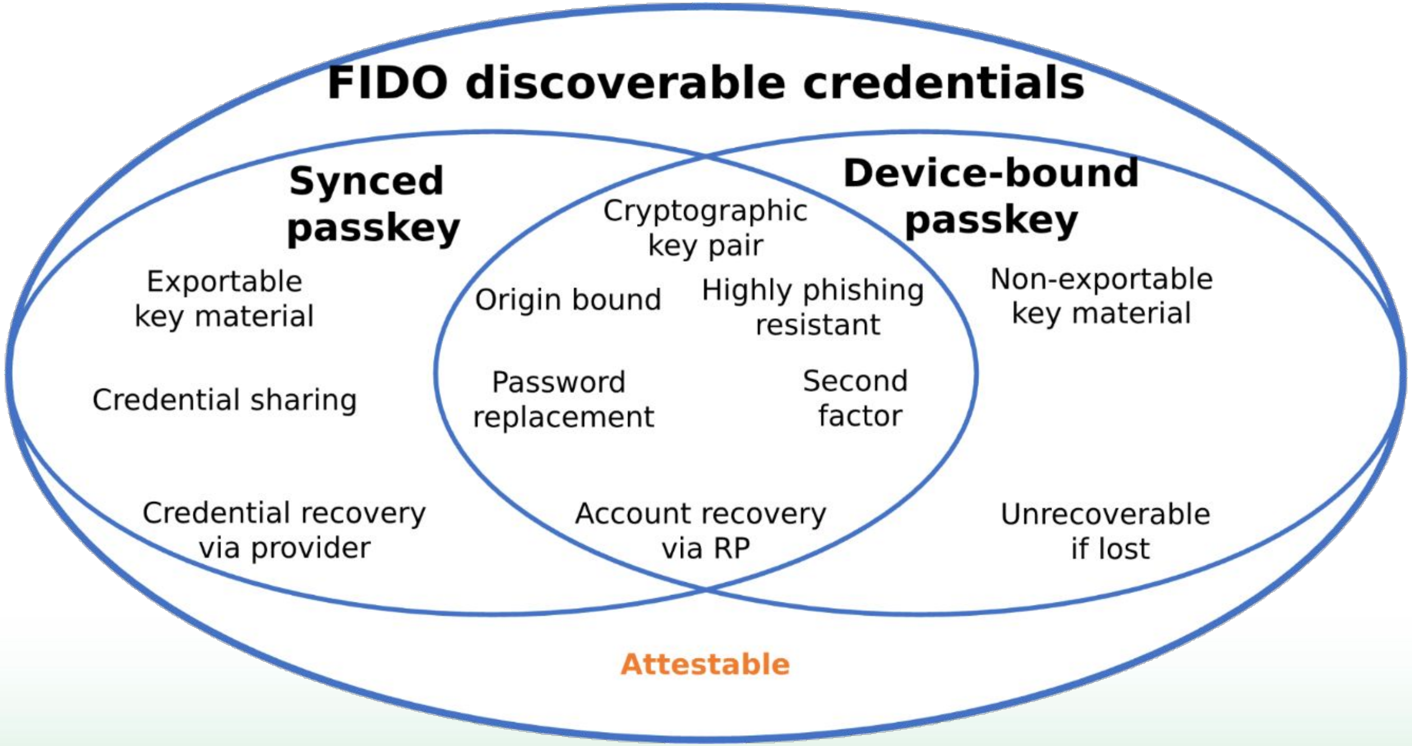
Synced vs Device-Bound

- A **passkey** is a **discoverable credential**.

- When a passkey can be used from **multiple devices**, it is a **synced passkey**.

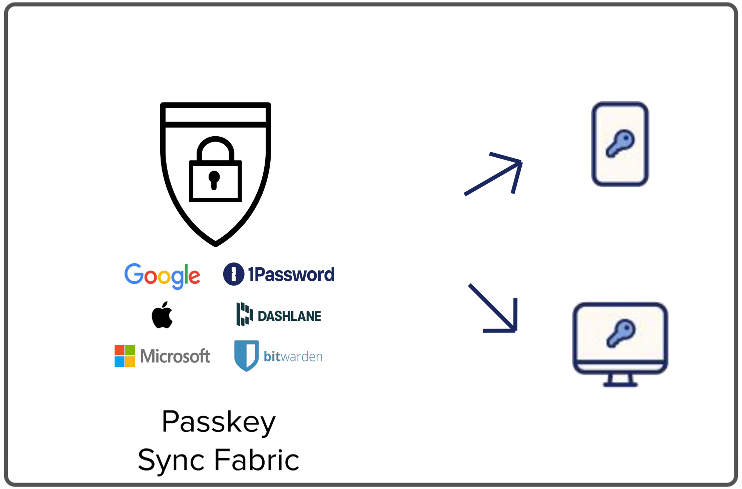
- When a passkey can only be used from a **single device**, it is a **device-bound passkey.**

Many overlapping circles...



Synced Passkeys

A passkey that can be backed up and synchronized by a 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.

How can you tell what you got?

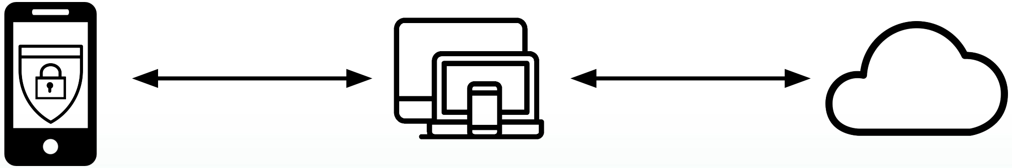
- Many passkey providers return a unique but **unattested AAGUID**…
    - Good for UX hints, but you can't trust it without attestation.

- **Direct attestation** can still be requested, but it is often returned exclusively by security keys.

- Additional signals like browser **user agent**, **transports**, and **attachment** can be used to infer provider identity as a fallback.

Hybrid Authentication

- Hybrid authentication allows for passkeys, **bound to one device**, to be used to authenticate into a **separate device**.
- The device with the passkey generates a WebAuthn request and hands it back to the requesting client.



The Good.

- Passkeys can be used to define most types of FIDO credentials.
- More passkey providers are becoming available!
- Some passkeys can be synced across devices! Great for availability and recovery!

The Bad.

- Passkeys can be used to define most types of FIDO credentials.
- Many providers have to intercept WebAuthn API calls in the browser.
- This is a potential showstopper for regulated and high assurance companies.

The Ugly.

- Differences in keys can cause confusion.
- There isn't an easy solution for this problem!
- Solving this is an ongoing discussion.

This is where we’re headed.

Streamlining Passkey Enrollment

- There is work currently being done in the **FIDO Alliance** and the **W3C** to provide RPs, clients, and passkey providers with a way to **register a passkey after a user authenticates** with existing login credentials.

- This aims to reduce user frictions when **migrating users from traditional username + password + 2FA** auth to passkeys.

Better Credential Metadata Management

- Passkey providers store **metadata** with passkeys, including the **user name** that gets shown to users during authentication.

- It's a tricky problem. **W3C** is working on how best to enable RP's to inform providers of metadata changes in response to real life: legal name changes, email address updates, etc…

Where is this work taking place?

- Discussions about passkeys, providers, and authenticators happen right here in **The FIDO Alliance:**
  - **Technical Working Group** (TWG)
  - **Credential Provider SIG**
  - **Consumer/Enterprise Deployment Working Groups**

- Discussions about WebAuthn, browser extensions, and browser features take place in the **World Wide Web Consortium** (W3C):
  - **Web Authentication Working Group** (WAWG)
  - **WebAuthn Adoption Community Group** (WACG)

Resources

Learn more about adding passkeys to your site:

- For **Developers**:
  - https://passkeys.dev
  - https://webauthn.io
  - https://www.w3.org/groups/cg/webauthn-adoption
- For **C-levels:**
  - https://fidoalliance.org/passkeys/

Feel free to
reach out to us!

Q & A

authenticate 2023
THE FIDO CONFERENCE

Thank you.

Signature Sponsors:

1Password | Microsoft | yubico | Google

authenticatecon.com