

Dude, where's my password?

How passkeys might help to reduce dependency on passwords

At least one of you have a password which...

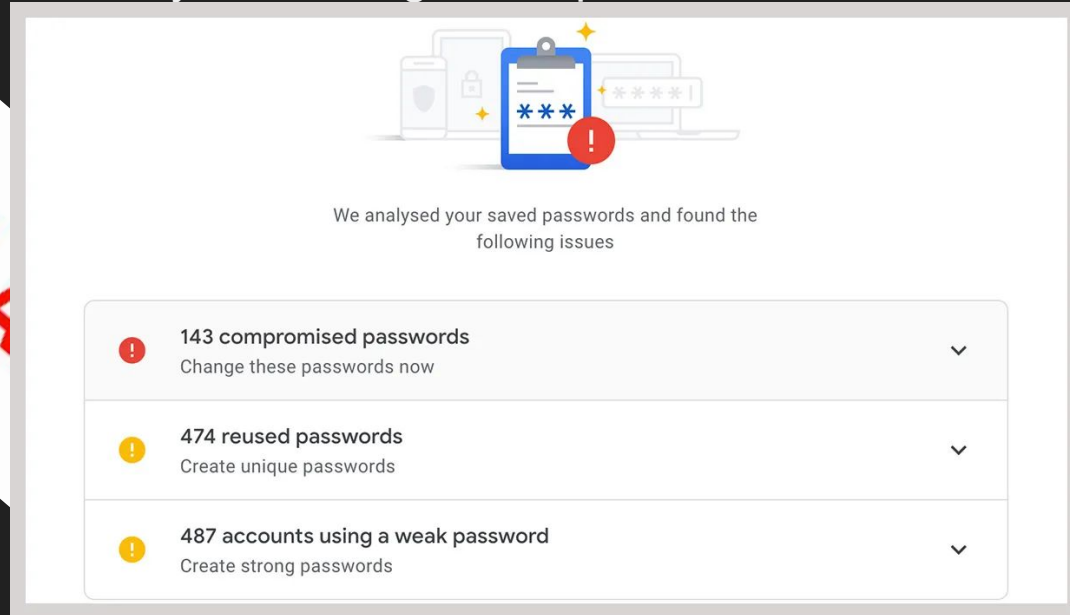
- Includes the ever-so-creative "1234" or "password" (Yeah, we're onto you!)
- Is basically a tribute to your pet (I hope "Pūkis" is doing well)
- Last changed when dinosaurs roamed the Earth
- Reused in at least 10 places
- Shorter than your morning attention span—yeah, that's under 12 characters!
- Shared with more people than your Netflix account

At least one of you have a password which...

- Includes the ever-so-creative "1234" or "password" (Yeah, we're onto you!)
- Is basically a tribute to your pet (I hope "Pūkis" is doing well)
- Last changed when dinosaurs roamed the Earth
- Reused in at least 10 places (including Netflix)
- Shorter than your morning attention span—yeah, that's under 12 characters!
- Shared with more people than your Netflix account

At least once...

- You clicked on a phishing link or a phishing training email from your company
- Website/Platform you're using had a password breach



But..but...2FA

Workarounds!



Multi Factor Authentication

- 2 Factors Facade - second layer on your weak password. Like putting a lock on a cardboard box and you can't find the key.

Great UX - said

- OTP - Email mag between apps to

lient to switch



Passkeys - Lord savior, Silver Bullet, Holy Grail of the auth

Drop-in password
replacement



Better UX



Improved
Security



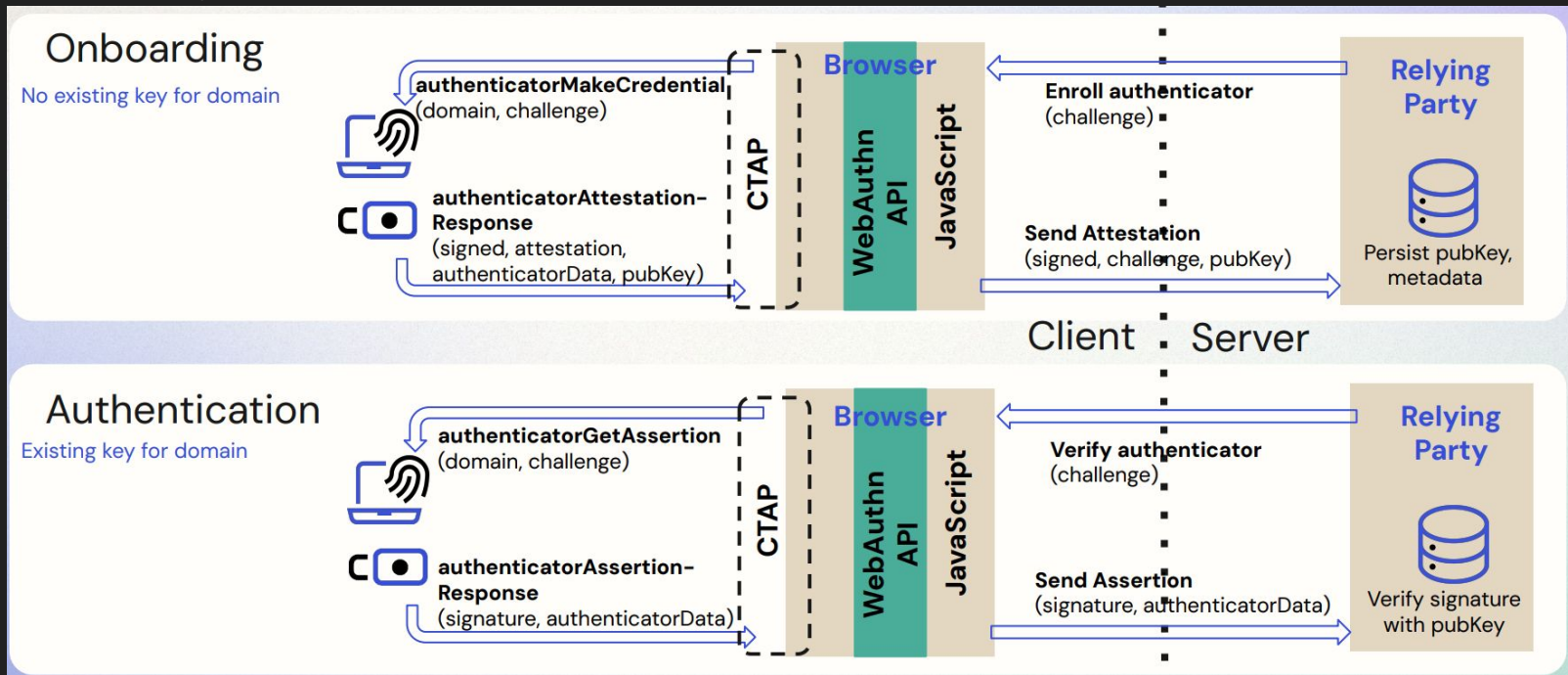
TLDR - an improved password manager

Demo O'clock

- Let's see how it might look in some real life examples
 - Registration
 - Login
 - Cross-device sign in

<https://webauthn.me/>

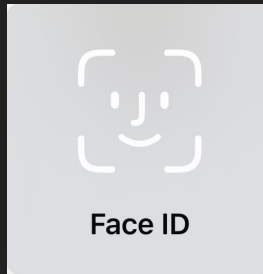
Passkeys Flows



Source: Auth0 - Ditch Passwords: Passkeys are the Future

So what is a passkey?

- Public Key Cryptography based FIDO credential
- Backed up and able to be replicated across devices
- Designed to be used in consumer space
- For non tech people - “Sign in with your face, your finger, or your PIN”



Breach protection

- Public-Private Key Infrastructure
 - Private key never leaves your infrastructure (device and/or password manager)
 - In case of breach, the best they can get is public key which is worthless on it's own - protection from credential stuffing
- Impractical to remotely compromise



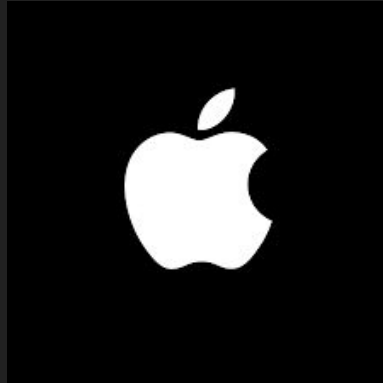
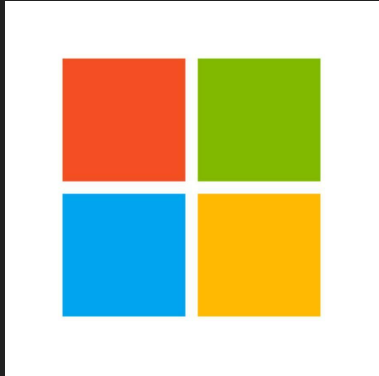
Phishing protection

- New private-public key pair for any combination of Relying party (Website) to username combination.
 - Because credentials are tied to domain name, they won't be useful anywhere else.
 - Private key is protected by OS/Platform - reduces the chance of human error



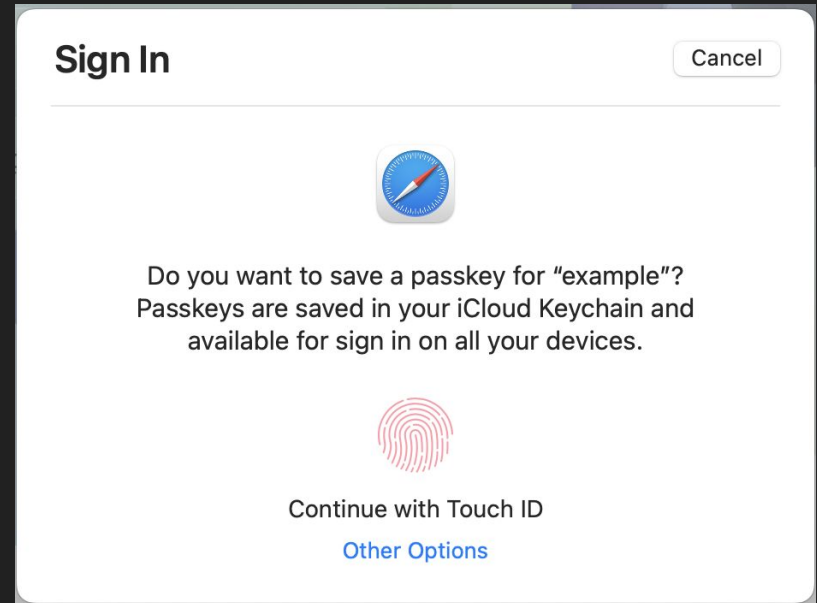
Users care most about UX

- Simplify authentication
 - Uses screen lock to create and use passkeys - users are used and sees this as a convenient and a fast way to authenticate
- Available out of the box on all major platforms



Cross-device, cross-platform

- For user convenience can be used across multiple devices as well as transferred across platforms.
- Easy to use on a new device due to seamless syncing






































Real life experience of using Webauthn (Passkeys)

Running webauthn in production since early 2022.

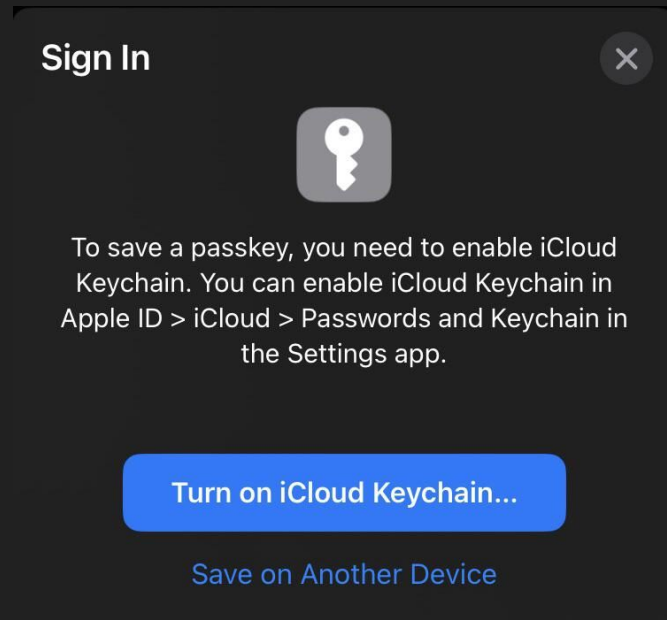
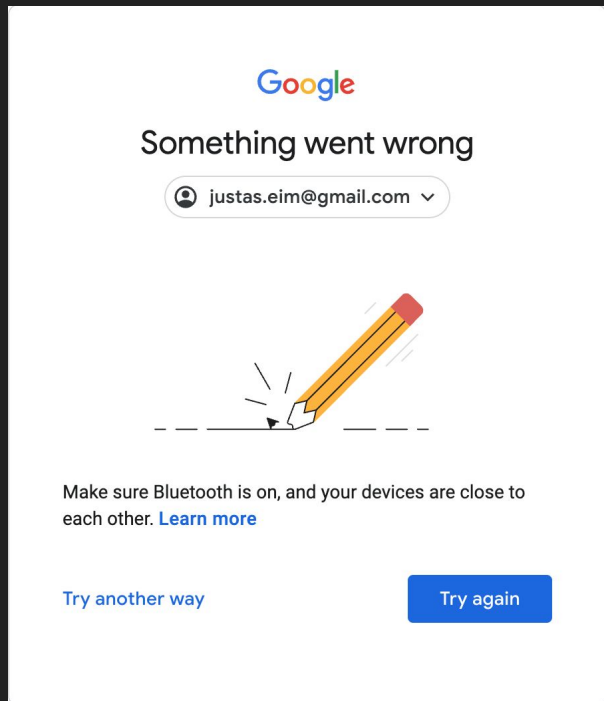
Device compatibility issues

Matrix

Capability	Android	Chrome OS	iOS/iPad OS	macOS	Ubuntu	Windows
Synced Passkeys	 v9+	 Planned ¹	 v16+	 v13+ ²	 Not Supported	 Planned ¹
Browser Autofill UI	 Chrome	 Planned	 Safari	 Safari	 Not Supported	 Chrome ³
	 Edge		Chrome Edge Firefox	 Edge		 Edge Firefox
	 Firefox			 Firefox		
Cross-Device Authentication Authenticator	 v9+	 Not Supported	 v16+	 Not Supported	 Not Supported	 Not Supported
Cross-Device Authentication Client	 Planned	 v108+	 v16+	 v13+	 Chrome Edge	 v23H2+
Third-Party Passkey Providers	 v14+	 Not Supported	 v17+	 v14+	 Not Supported	 Planned

Source: passkeys.dev/device-support

Tricky to debug



Additional security layer - additional complexity

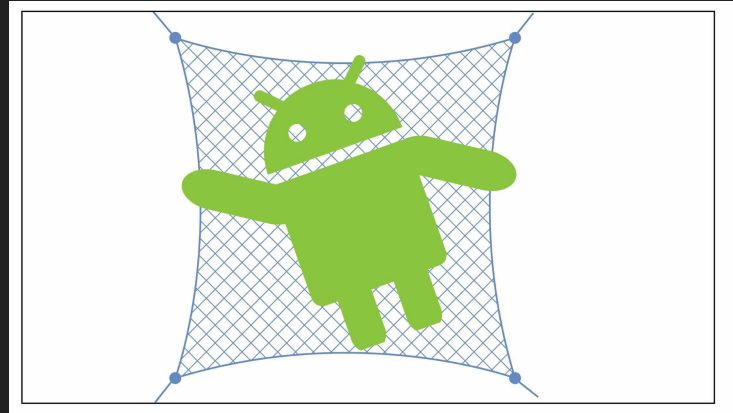
Attestation can be used to evaluate authenticator itself.

Example things to verify:

- Authenticator AAGUID (manufacturer GUID, so you can limit only to certified and known authenticators)
- Trust anchors to validate attestation certificate

Additional security layer - additional complexity v2

Additional security layers such as Android SafetyNet can be used to ensure device is not compromised during registration flow. Lead to intermittent failures of registration and subpar UX

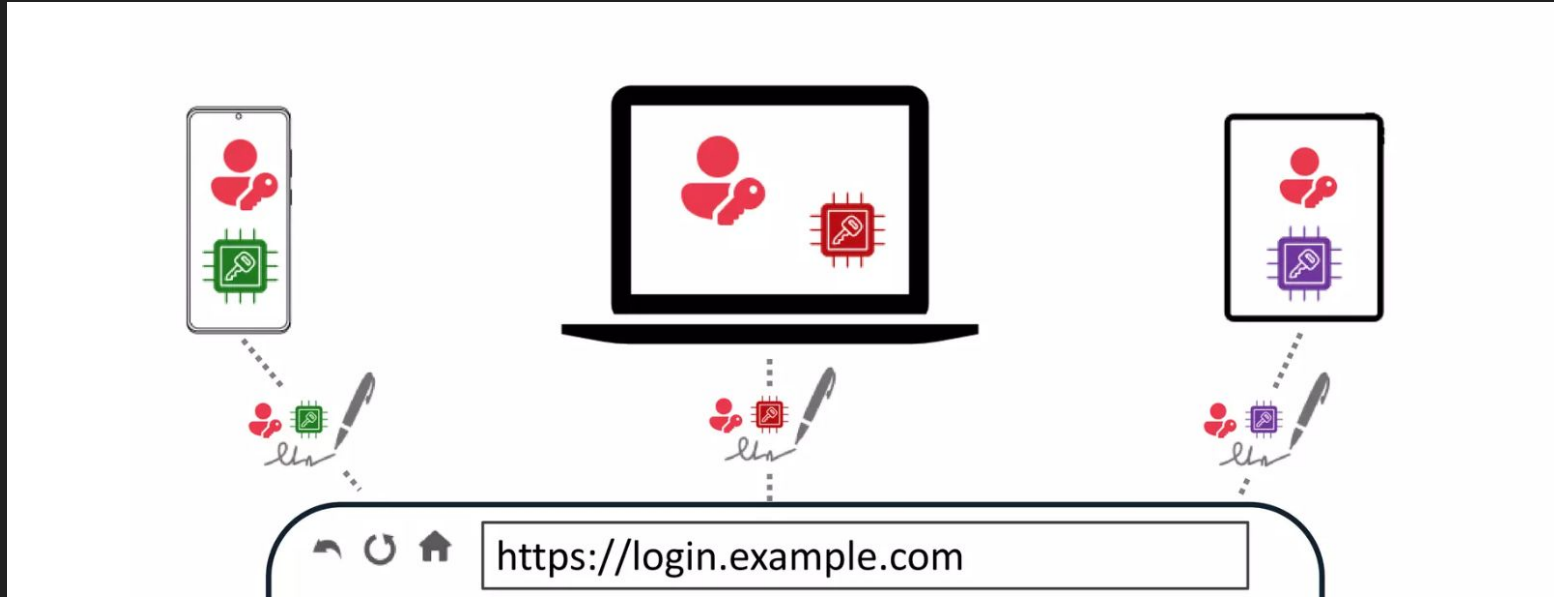


No more passwords

As of 2023 Autumn there's no longer a password option in Tide - it's only Passkeys in combination with Email Magic Links

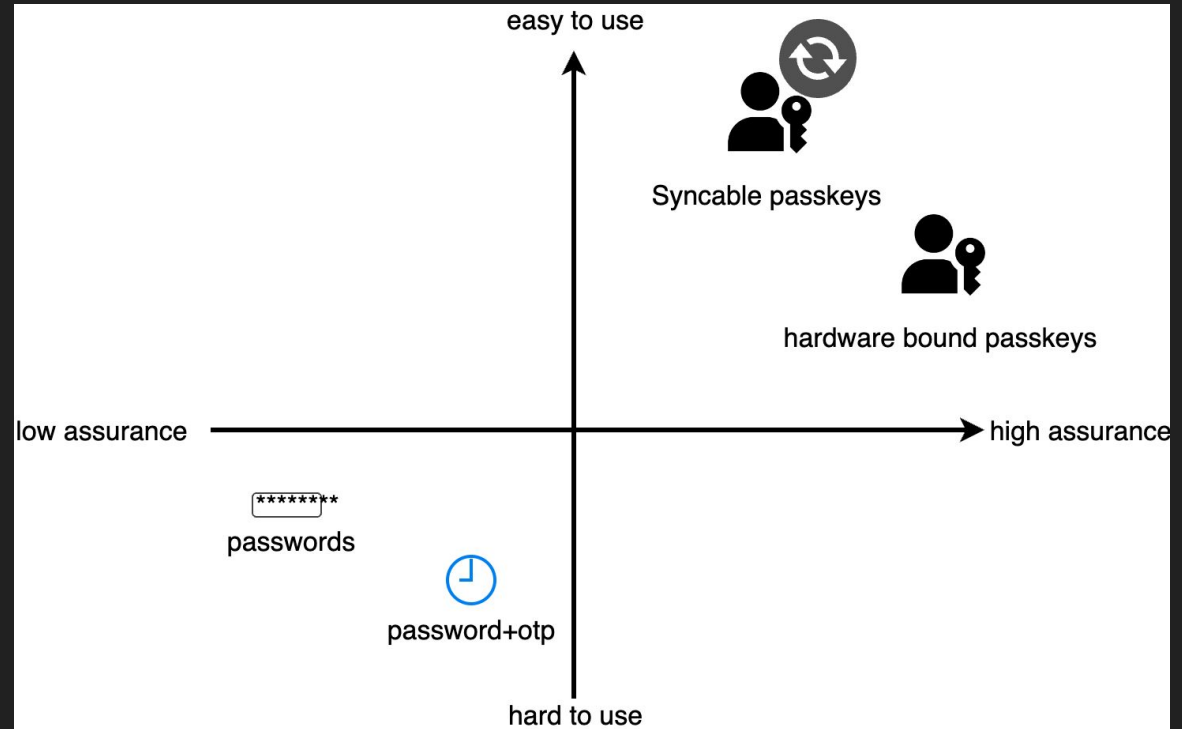


Device Public Key



Source: ibm-hey-fido-meet (RSA Conference 2022)

Security spectrum



Implementation

- DON'T TRY TO IMPLEMENT ON YOUR OWN. WHILE IT'S FUN AND THE SPEC IS QUITE GOOD YOU'LL MAKE MISTAKES - TRUST ME.
- Plays nicely with OAuth2
- A lot of libraries for WebAuthN on different server languages. As well as off-the-shelf solutions. Some Java libraries:
 - Spring Security
 - WebAuthN4j
 - Vertx
 - Yubico
- `navigator.credentials.[get/create]` in the browser

Wrapping up

- Password are bad
- Passkeys are better
- Phishing/Breach resistant
- Still a lot to improve to gain mass adoption, but on a right track

STAY SAFE!