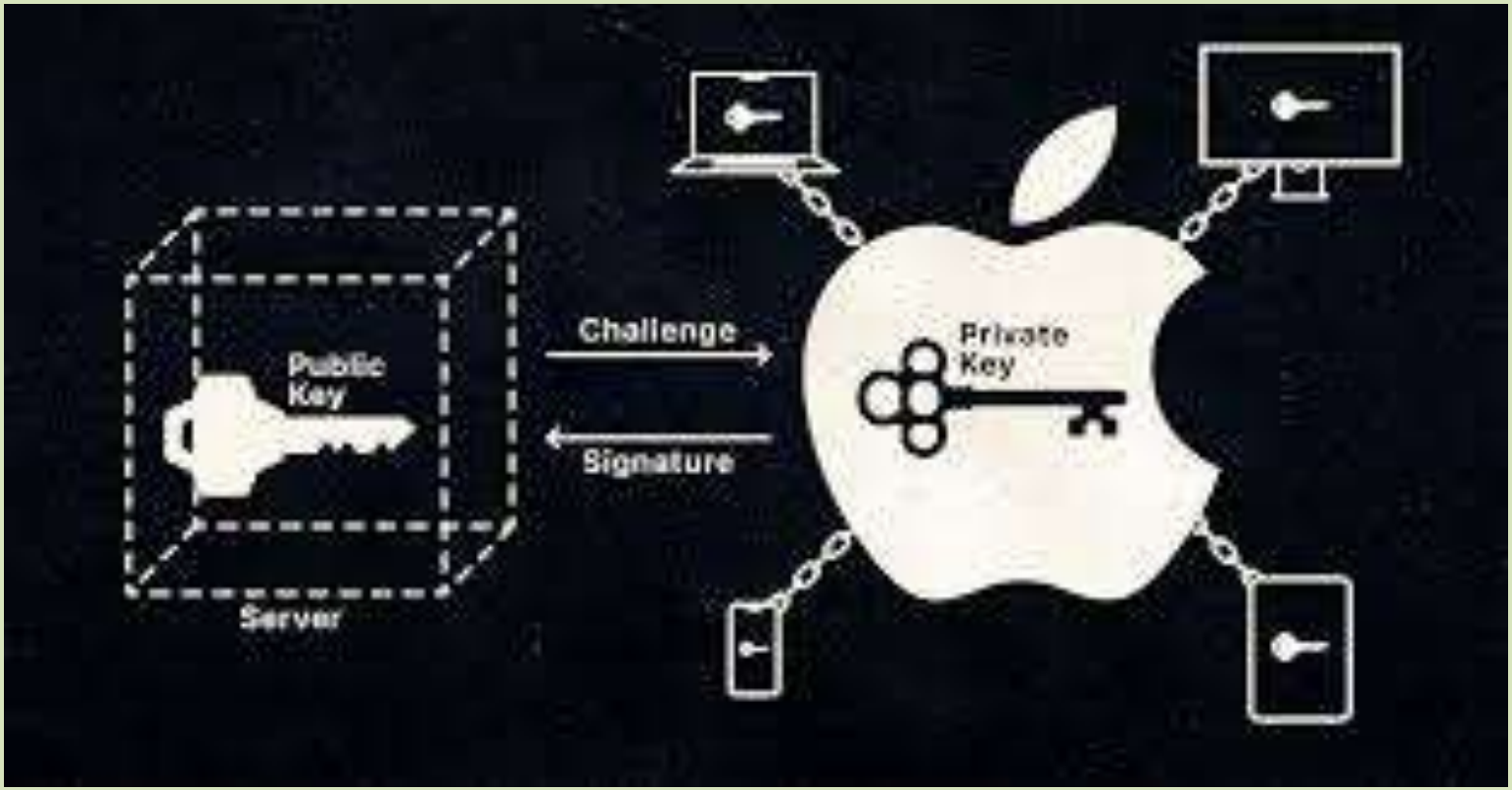
Using PassKeys



by Mike Quinn

August 8, 2024

How does it work?

- **During Registration (or when creating passkey)**
  - **“Authenticator” creates a private/public key pair**
  - **“Authenticator” stores the private key, remembering what it was used for**
  - **“Authenticator” gives the public key to the registrar**
- **Using a Passkey**
  - **App/website issues a challenge, encrypted with the public key (challenge = some random string)**
  - **“Authenticator” decrypts the challenge using the private key and responds.**
  - **If the response is the “challenge” string, the app/website knows it is you.**

Why are they good?

- **Don’t need to enter a password**
- **Use tried and true public key authentication**
  - **Encrypting something with private key can be decrypted with public key**
  - **Private key can be used to get the public key, but the reverse is not possible.**
- **You can share private keys between devices with an appropriate “authenticator” (of course, this is where you are vulnerable).**
- **Authenticators can be things like a browser, the Apple key chain, or password managers**

Why are passwords “bad”?

- **They’re sent to the other party, and the other party stores them. If the other party is breached, your passwords are compromised.**
  - **For Passkeys, the other party only stores a public key, which can only be used to verify the private key.**
- **Without a password manager, you have to remember them, write them down. Often people use the same password on multiple sites.**
- **You can be scammed into revealing your password. You can’t be scammed into revealing your private key.**

Things to be aware of

- **Best authenticators are ones that can run on all your devices (typically password managers), but the apple keychain can work if everything you use is Apple-based, or you install iCloud for windows, and add the iCloud browser extension.**
- **Your authenticator needs some other way to insure that you are you (fingerprint, face id, password, yubikey…)**
- **You can use your phone as a passkey for your laptop/desktop, which can be authenticated by your biometrics**
- **Things like Yubikeys can be used, but typically they have a limited number of passkeys they can be used for. Yubikeys are best used to log into your password manager (including iCloud) to provide good protection.**

Things to be aware of

- **I prefer using a separate password manager because if someone steals your phone and has your login code, they still need to log into the password manager in order to use your passkeys. If they were using the Apple keychain, they would automatically have access.**
- **You can also turn on 2FA for your icloud account to solve this issue.**
- **Sadly, some websites misunderstand passkeys, and use them for 2FA, which is not really what they're for (i.e. they make you log in with a password, then use your passkey, which is really dumb)**

One last thing

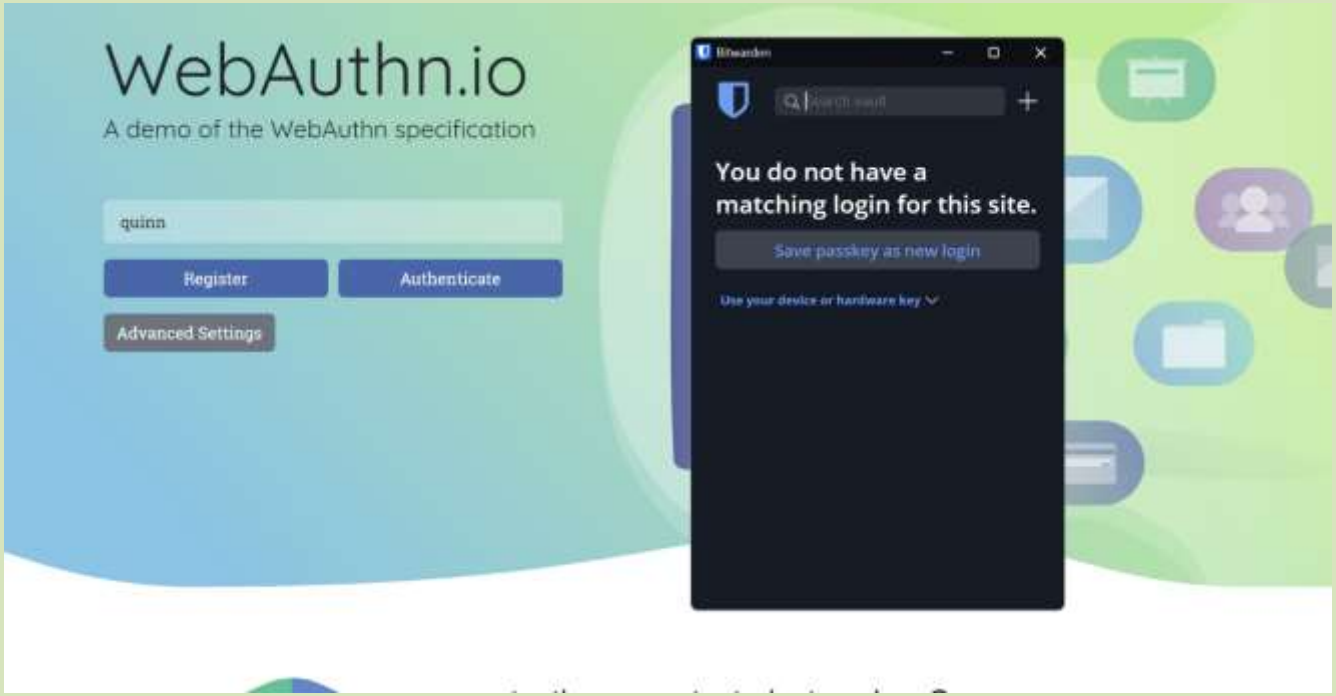
- **It's still early days for passkeys. Change over accounts to passkeys one at a time, and make sure you understand how it acts on all your devices before going on to another.**
- **Just for instance – it took me about ½ hour to get Amazon working kind of ok, and even then there are some rough edges on the support.**

Testing things out

- **Webauthn.io**
- **Passkeys.io**
- **https://demo.yubico.com/webauthn-technical/registration**

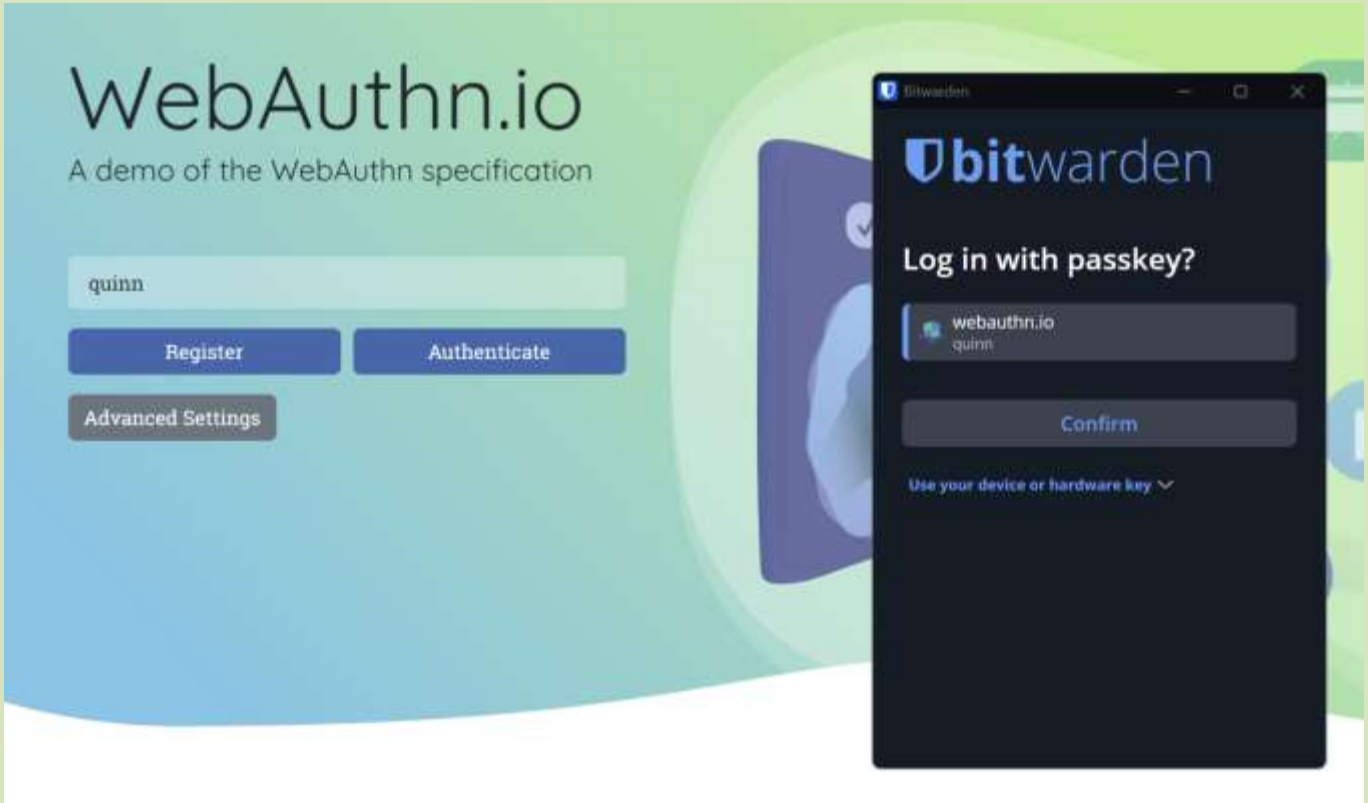
Testing things out - Registration

- **Webauthn.io**
  - **Click register – you're Authenticator will pop up to save your private key and create a public key**
  - **In this case, Bitwarden will ask about saving the passkey as a new login. Click that button and you're good to go.**



Testing things out - Authenticate

- **Webauthn.io**
  - **When you go to log in, the authenticator will pop up asking if you want to log in with the passkey.**
  - **On websites with multiple logins (google?), it will show the different user names, and you'll have to choose the right one.**

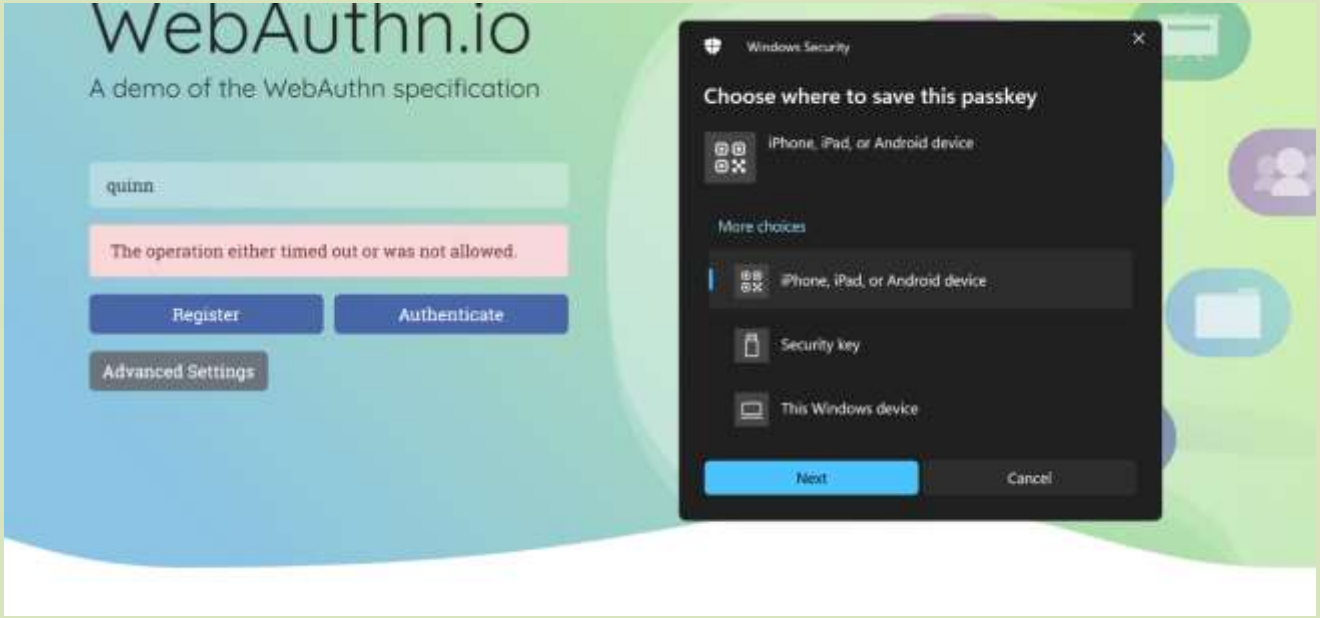


Testing things out – Alternate Registration

- **Webauthn.io**
  - **You can choose “Use your device or hardware key” to have more choices.**
  - **We’ll choose “Use another device” to choose our phone.**

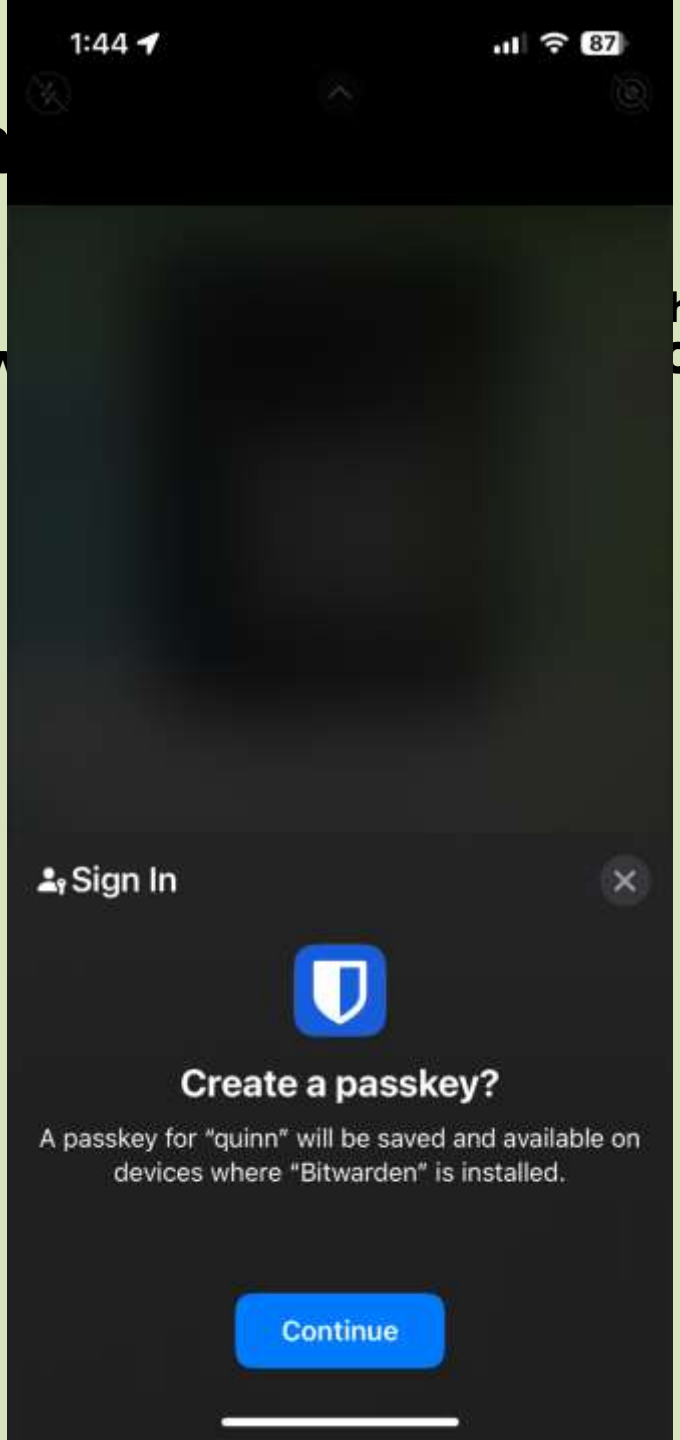
Testing things out – Register with phone

- **Webauthn.io**
  - **You can choose “Use your device or hardware key” to have more choices.**
  - **In this case, we’ll chose iPhone, iPad or Android Device.**



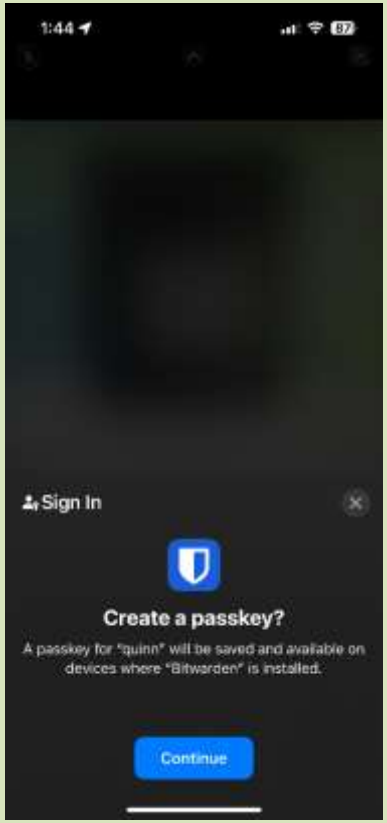
Testing thin with phone

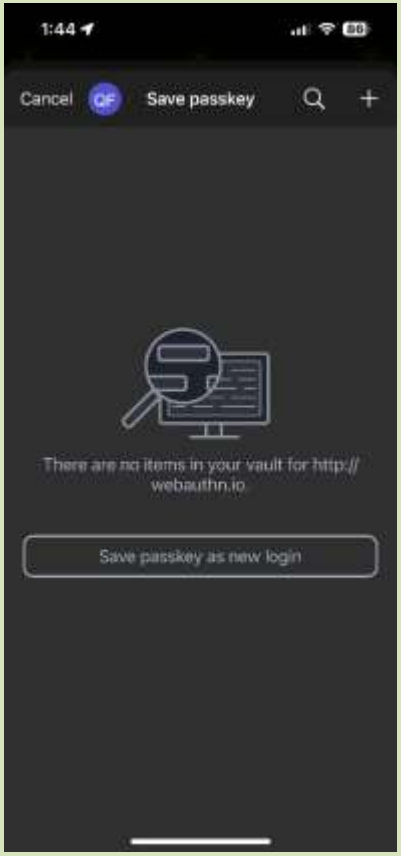
- **Webauthn.io**
  - **You'll get a hone/pad to scan it. It w Choose it to do so.**



Testing things out – Register with phone

- **Webauthn.io**
  - **Create the passkey. In this case, bitwarden is saving the passkey. If you don't have bitwarden, it will be the Apple keychain**





More Information

- https://www.youtube.com/watch?v=EA9mK3nJE1o (General Passkey Information)
- https://www.youtube.com/watch?v=o4asbRziCD0 (Bitwarden and Passkeys)
- https://www.youtube.com/watch?v=X6QecrNm9Wg (iCloud Passkeys with Windows)