What are Passkeys, and how do they work?

Posted on March 22nd, 2023 - Intego - by Kirk McElhearn

When Apple released iOS 16 and macOS Ventura in late 2022, they introduced support for passkeys. **Passkeys** are an authentication technology designed to replace passwords. There are many advantages to using passkeys instead of passwords.

In this article, I will explain what passkeys are, how they work, and why they may be the future of secure authentication on websites and in apps.

A brief history of passwords

Passwords have been used for thousands of years as a means of authenticating people. They have been used in military contexts to separate friends from foes. Simple spoken passwords were

also used to gain entry to speakeasies in the United States during prohibition; this clip from the Marx Brothers' film Horse Feathers shows some lax security in that context.

With computers, passwords became the only way to identify who should have access to various computer systems. The combination of a username and password is supposed to ensure that someone logging into a computer, website, or service is uniquely identified, authorized, and has access only to their own data.

The importance of password security

Before the Internet, password security was somewhat less important, because anyone wanting to access a computer generally needed physical access. While you needed passwords to identify yourself on computers at universities and in some businesses, individual users rarely used them.

On the Mac in particular, basic functionality for creating separate local user accounts was added in 1999, to Mac OS 9. However, it wasn't until the release of Mac OS X in 2001 that separate user accounts became more mainstream.

With the advent of the Internet, authentication to online services via a username and password became essential, because of the need to log into computers remotely. Passwords were, in some cases, encrypted to ensure that nobody other than the intended user could access them—though that wasn't universally true in some early systems.

Over time, the need for more secure passwords has become essential. Not only because passwords protect sensitive data, such as military secrets and bank accounts, but because there

are more threats to computer security as hackers attempt to get access to accounts.

For many years, it was normal for people to use the same combination of username and password on multiple websites and services, but continuous data breaches of major companies had led to leaks of these username/password pairs, allowing hackers to try to use them on different services, in a technique called credential stuffing.

It's important to create unique, strong passwords to prevent hackers from accessing accounts, either via credential stuffing, or via brute force or dictionary attacks—automated methods to try millions of words, common passwords, and likely variations.

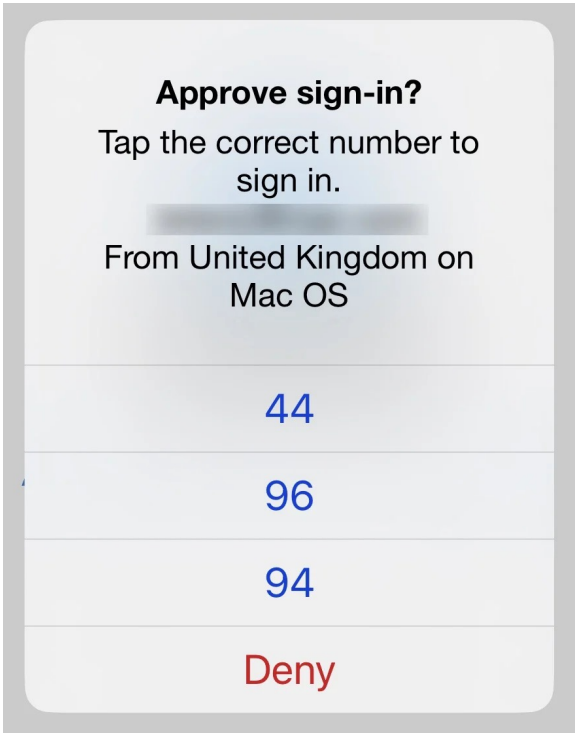
As the stakes have risen, and as hackers have developed more techniques for breaching accounts, the need has come for more secure authentication methods. While many people use password managers that generate long pseudorandom passwords—which is often the best option available, along with multifactor authentication—this can still be an onerous process. The majority of computer users today still create passwords that are insecure and reuse them across multiple sites, and rarely use multifactor authentication.

Over time, multifactor authentication or MFA — more commonly known as two-factor authentication or 2FA — was developed to thwart hackers. This involves entering something you know (your user name and password) along with something you have (a code received by SMS or generated by an app) and/or something you are (biometrics, like Face ID or Touch ID). Even some forms of 2FA are imperfect at protecting accounts, especially in scenarios where a phishing site acts as a man-in-the-middle relay between the victim and the real site (as discussed on episode 283 of the Intego Mac Podcast). Nevertheless, even imperfect 2FA is better than not using 2FA at all.

An improved form of two-factor authentication is the use of a physical security key; you can even use a security key to protect your iCloud account.

Passwordless logins

Some websites and services allow you to log in without a password, but this still requires a username/password pair, and leverages an additional device to log in. For example, Microsoft's passwordless authentication works via the company's Authenticator app on a smartphone. After you've set up the process, using your username and password, you can log into any Microsoft site or service by answering a challenge. The website displays a two-digit number, and instructs you to choose that number in the app. A dialog in the Microsoft Authenticator app gives you three options; tap the correct one, and the app communicates with the site or service to confirm your identity.



This form of authentication is only passwordless at the moment you log into a site or service. It depends on an existing username

and password, which you have confirmed in the app, and biometric identification, via Face ID or Touch ID, on your iPhone. You still need a password, but the fact that you don't need to type it each time you log in means that it is easy to use a long, secure password. And you can still use the username and password combination to log into these sites and services.

Passkeys: a step beyond passwordless

Passkeys take this one step further. As Google says, "A passkey is a digital credential, tied to a user account and a website or application." Passkeys contain all the information needed to identify users: their account name and the key that authenticates them.

As Apple points out, "Passkeys are built on the WebAuthentication – or WebAuthn standard – and use public-key cryptography. Rather than having a typable word or string, unique cryptographic key pairs are generated for every account." These cryptographic keys are very long strings of characters, and you never need to know what they are.

The authentication occurs via your smartphone, on which you have identified yourself, and each time you log into a site or service with a passkey, your phone's biometric authentication proves that you are you, and sends the passkey to the site or service. **One way to think of passkeys is that they make your smartphone act as a physical security key.**

Passkeys can be backed up, synced, and transferred to new devices, and they are end-to-end encrypted. When you save a passkey for a site or service, you can use it on other devices that share your passwords. With Apple devices, passkeys sync using iCloud Keychain, and you can access them on every Apple device you own that is signed into your iCloud account.

You can also bootstrap passkeys, using one device to log into another. Since Apple, Google, and Microsoft are all members of the FIDO Alliance, there is true cross-platform compatibility for passkeys. You can use your iPhone to log into a site or service on a Windows computer, or an Android phone to log in on your Mac. This uses CTAP2, the Client to Authenticator Protocol 2, which is a way that devices can communicate with other devices, to transfer the authentication from your smartphone to the device on which you're logging in.

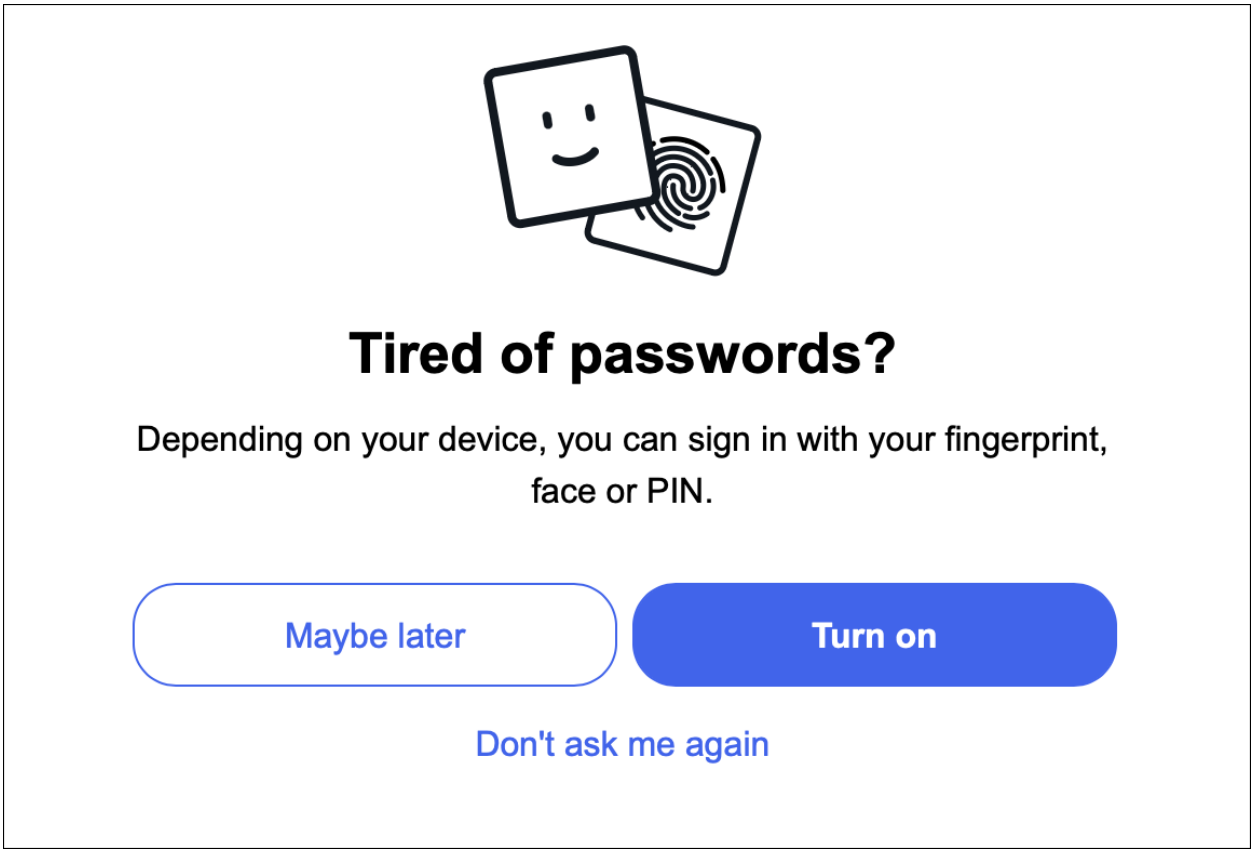
This video from the FIDO Alliance, the group behind new passkey standards, shows how passkeys work in practice.

How passkeys work on Macs, iPhones, and iPads

Although it's great that Apple's operating systems support passkeys, unfortunately there aren't very many sites or services that support them yet. A password manager company, 1Password, maintains a site called Passkeys.directory that has a list of some sites that currently support passkeys as a sign-in and/or multifactor authentication method.

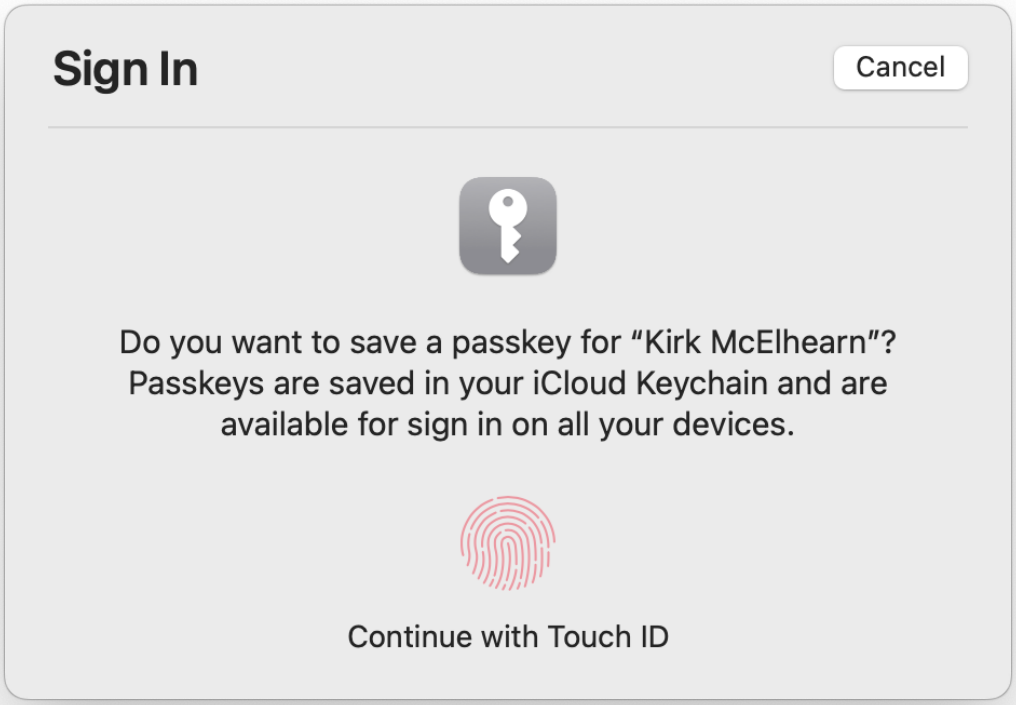
Some notable sites that support passkeys as of early 2023 include Best Buy, Cloudflare, eBay, Kayak, and PayPal (in the U.S.). And Google added passkeys to their accounts in early May 2023.

Let's take a look at how to set up passkeys with one of those sites supports passkeys already: eBay. If you go to your eBay account settings, then Sign-in and security, then Password, you'll see an option to set up a passkey, though they don't use that term.

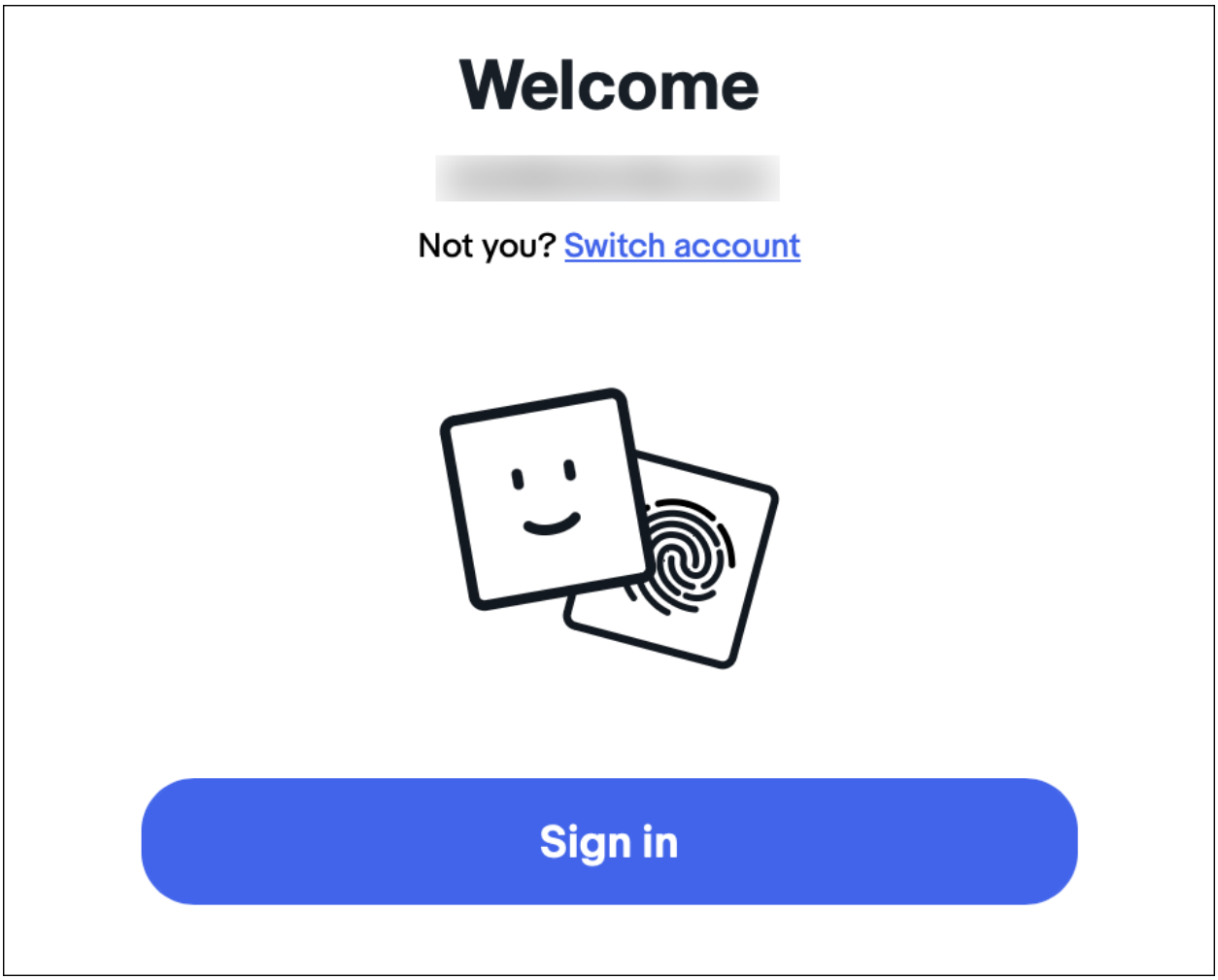


eBay's passkey-enabling setting doesn't mention passkeys.

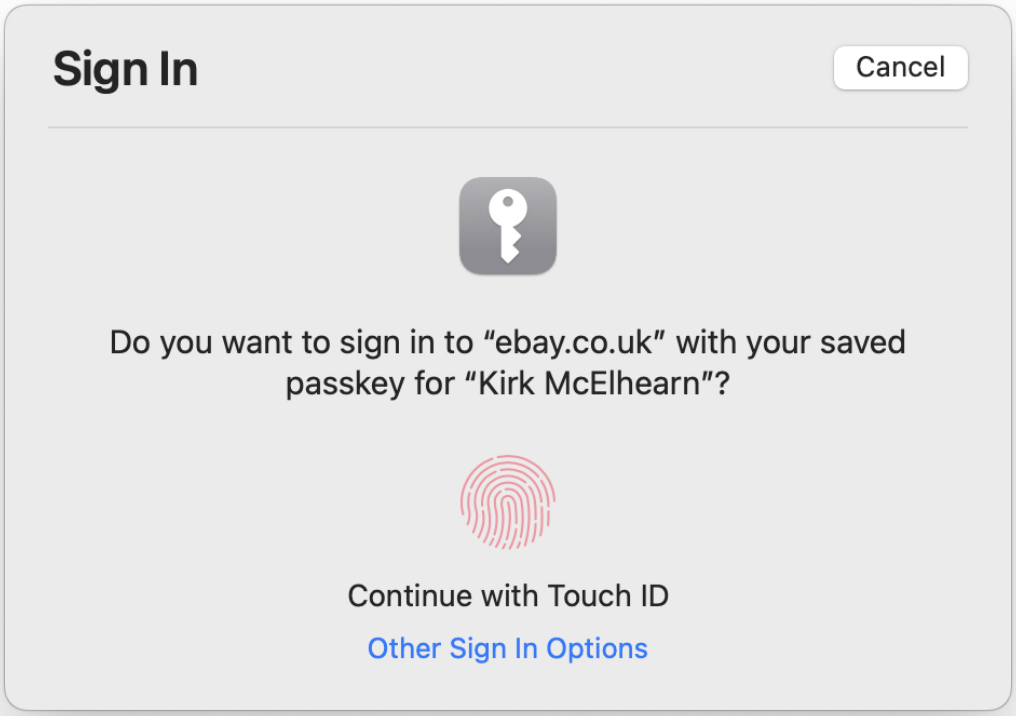
Click Turn On, and Safari displays a dialog like this:



After you’ve completed this process, you’ll see this the next time you go to sign in on eBay:

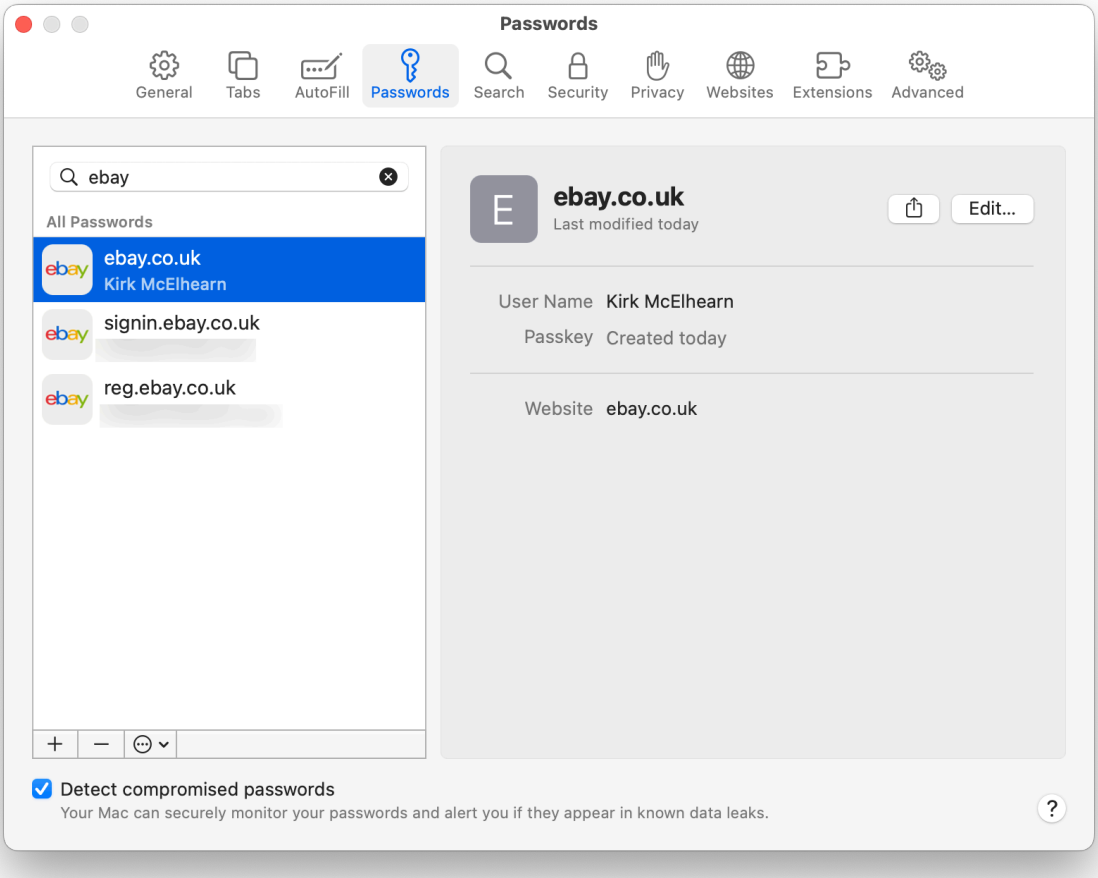


Click Sign In, and Safari displays this:



Authenticate on your device — in this case, I was using a Mac with Touch ID — and you log in immediately.

In the Password tab of Safari’s Settings, you can see that a passkey has been saved for eBay. But you cannot view the contents of the passkey.



This passkey syncs across devices, so you can use it on any device signed into your iCloud account.

Advantages and disadvantages of passkeys

There are many advantages to passkeys. In use, they are not very different from using a strong password and a password manager, and confirming your identity via biometrics. So users will not find the process complex or complicated, and are likely to easily adopt this technology, once they understand the value.

Passkeys free up the need for password requirements (a certain number of characters, capital letters, and special characters), and

ensure that users don't have to remember passwords. However, you will still need to know some passwords: the one for your Apple, Google, or Microsoft accounts; the one you use to log into your computer; and the passcode for your smartphone.

The fact that passkeys are syncable, and their ability to be backed up, exported, and imported, means that they are not limited to being used on one device. And the cross-platform nature of the FIDO standard, combined with the support from all major operating system makers, guarantees that there will not be a VHS vs. Betamax war going forward. It's in everyone's interest to have a common standard.

As for security, phishing should theoretically be impossible with passkeys. Websites identify themselves via a certificate, and fake websites, which may look legitimate, cannot accept a passkey and pass it on to the real site.

However, there are some disadvantages. For now, websites and services will allow you to log in using either a passkey or a username/password combination, so that latter is still susceptible to hacking and phishing.

If you get locked out of your iCloud account (or similar accounts on Android or Windows), then you may no longer have access to your passkeys. Several password managers, such as 1Password and Dashlane, have announced support for passkeys; it seems essential that passkeys are not limited in access to only operating system providers, and should be fully portable.

Finally, passkeys are personal, and this poses problems for businesses who need to manage access to sites and services for employees. Since corporate IT people can't get access to a user's passkeys, and can't control their use, additional technology may be needed before some businesses will adopt this form of credential management.

Passkeys are an excellent improvement on existing authentication methods, and at least in the future could free users from having to create and remember passwords. There are some limitations, and passkeys are only in their infancy, but over time, there's a good chance that they may come to replace passwords.

original article:

https://www.intego.com/mac-security-blog/what-are-passkeys-and-how-do-they-work/