How passkeys work, their benefits and downsides

29 November 2023

Passkeys are a new way to log in without needing a username or password.

They sound almost too good to be true, right?

Big tech companies like Microsoft, Google, and Apple are part of the FIDO Alliance, who have worked together to develop passkeys.

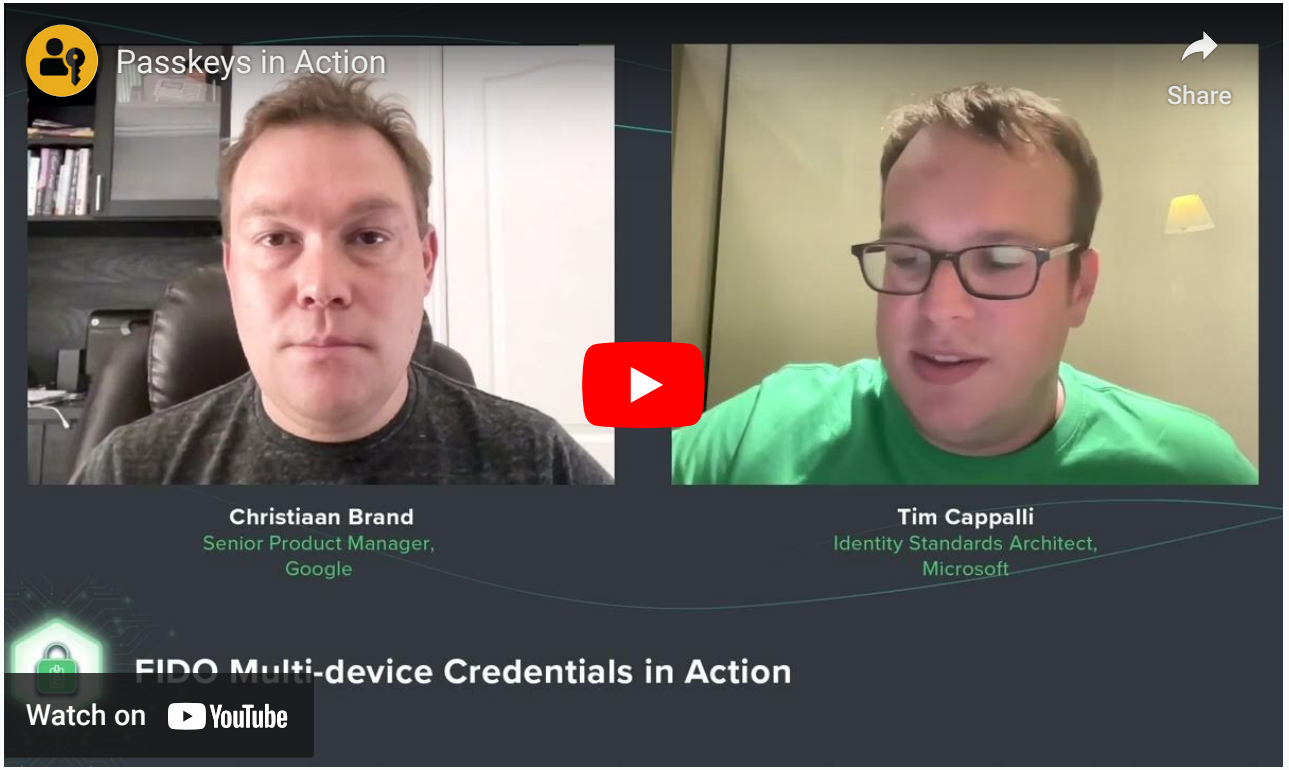
The FIDO Alliance aims to reduce our reliance on passwords and replace them with something:

- quicker
- more convenient
- more secure

How they work

With passkeys, you login to a website or app the same way you unlock your mobile, desktop or tablet, such as using a PIN, facial recognition, or fingerprint. They remove the need to create and remember a username or password.

The simplest way to understand passkeys is by watching this overview.



To use a passkey, the website or app must support this option, and currently most don't. You can check a list of sites that allow passkeys.

If a website supports passkeys, you'll likely have to create a password initially. At present, most sites are introducing passkeys as an additional way to sign in rather than completely replacing passwords.

Take GitHub as an example. You start by logging in with your username and password. Then go to 'Settings', find 'Password and authentication', and click on 'Add a passkey'. The site will see if your device supports passkeys.

Configure passwordless authentication

Add a passkey

Your device supports passkeys, a password replacement that validates your identity using touch, facial recognition, a device password, or a PIN.

Passkeys can be used for sign-in as a simple and secure alternative to your password and two-factor credentials.

Add passkey

Cancel

When you make a passkey, your device will ask you to prove it's you, just like when you unlock your phone or laptop – I use my fingerprint.

At this point passkeys work by automatically creating two types of keys, a public key and a private key.

The public key is shared and is used by websites or apps to verify your identity – in this example the public key is sent to GitHub.

The private key, which is used to authenticate your identity, is securely stored on your device and is never shared. This ensures that even if a service you use is compromised, your private key remains secure, significantly reducing the risk of unauthorised access.

Next time you log into GitHub, you can pick 'sign in with passkeys'. It'll ask for your passkey, and then you authenticate with your fingerprint, PIN, or face.

Sign in to GitHub

Username or email address

Password Forgot password?

Sign in

Or

Sign in with a passkey

Even though I normally use a password manager I've found the whole process of signing in a lot quicker using passkeys.

Passkey benefits

Phishing-resistant

Passkeys greatly reduce the risk of phishing attacks, where scammers trick individuals into revealing their passwords. With a passkey, you can only log in to the correct website or app. This security measure is a significant improvement over traditional passwords, as it eliminates the common human error of mistakenly entering credentials on a malicious website.

Inherently secure

Each passkey is unique and tough to crack, making them much more secure than traditional passwords. Often, passwords are weak and reused on different sites, leading to 'credential stuffing', where stolen passwords are tried on different websites to gain unauthorised access. Passkeys avoid this risk, keeping your accounts safer.

No shared secrets

Passkeys offer enhanced security because they don't depend on shared information vulnerable to interception. By using passkeys for website access,

you're protected against password breaches. Take the Yahoo incident, where 3 billion passwords were compromised. With passkeys, Yahoo would only possess your public key. Losing this doesn't compromise your account's safety, as the private key, crucial for access, is securely stored on your device, not with the service provider.

User-friendly

Passkeys streamline the account creation process, making it faster and more user-friendly. They eliminate the need for a password manager or the effort to create complex passwords that meet various criteria like length, uppercase and lowercase letters, and punctuation, which can be challenging for some users.

Built-in 2FA

Passkeys inherently function as two-factor authentication (2FA). When signing in with a passkey, it combines something you have (your device) with something you know or possess (such as a PIN, fingerprint, or facial recognition). This dual-layer approach enhances security beyond what traditional passwords offer.

Backed up within a ecosystem

If you use Apple's iCloud Keychain, Google, or Microsoft Windows Hello, your passkeys are automatically backed up within these ecosystems. This allows for

seamless use across different devices within the same ecosystem.

Passkey downsides

While passkeys offer many benefits, there are some downsides to consider.

Inequality

Passkeys are tied to individual devices, which poses a challenge for those without access to personal mobiles or laptops and who depend on shared computers, such as in libraries. This limitation makes passkeys inaccessible to them, leaving traditional passwords as their sole option. This shows a clear inequality in who can use passkey technology.

Compatibility issues

Many websites haven't adopted passkeys, meaning traditional passwords remain necessary. Additionally, passkey compatibility is limited to modern devices with the latest operating systems. This leaves users of older devices at a disadvantage, as their technology may never be updated to support passkeys.

Backup challenges

Switching between different ecosystems like from iPhone to Android with passkeys can be challenging due to compatibility issues. Each ecosystem, like Apple's iCloud Passkeys and Google's version for Android, uses distinct systems for storing and managing passkeys. These differences mean that there's no way to transfer passkeys directly from one to the other. This can make it difficult for users to move between ecosystems without having to reset or recreate their passkeys, adding a layer of inconvenience to the process.

Summary

Passkeys are a significant advancement in online security and user convenience. As someone who regularly uses a password manager, I understand the inconvenience of generating unique passwords for every site. The concept of logging into websites using your device's login method, like a PIN or a biometric feature such as a fingerprint, is amazingly simple.

However, the widespread adoption of passkeys encounters significant obstacles. A key challenge is the need for every website requiring a login to adopt this technology. Additionally, not everyone can benefit from passkeys, especially those who cannot afford modern devices.

Passwords are likely to stay around for a long time, perhaps never fully disappearing. But for those who can use passkeys, they offer a peek into a future with fewer passwords.

It’s a big step forward, even if it doesn’t entirely replace passwords.

Tags Security

About the author

Hi, I'm Peter Brumby, a Digital Product Manager. This is my blog on web development and technology. It's my brain dump and personal library, where I share and save useful info. Hope it helps you too.

Comment

Ethel says:
4 March, 2024 at 1:24 am

Hi Peter, we seniors need all the help we can get understanding and keeping

up with all this information. Thank you!

Reply

Leave a comment

Comment

Name

Email

Email not displayed

Post comment

More posts

Passkeys support by device, browser and password manager

3 December 2023

Is your website leaking personal data to Google?

24 September 2022

Categories

Accessibility | AI | Analytics | Co-op work blog | Copyrighting | Domains | Performance

Security | SEO | Testing | Tutorial | Work blog

Search