

What are Passkeys and why is it the future of online security?

 By [Lindsey Schutters](#)

11 Oct 2023

In the 10 years since the Fast Identity Online (FIDO) Alliance was formed its newest technology, Passkeys, may finally end our reliance on remembering complex passwords forever. This is such a big deal in digital privacy that [Google is making it the default sign-in method](#) for its nearly two billion users.



What is Passkeys? Picture your online account as a house. Traditionally, you'd use a password, or a key, to enter. But what if someone else gets your key? They can enter your house too. Passkeys is like a unique device that unlocks your door and can't be duplicated.

But isn't that how passwords work? No. Passkeys are stored securely on your device, not on some server; this means they're safe even if a company's data is breached.



City Press denies 'brown envelope' allegations

Karabo Ledwaba 11 Oct 2023



Although passkeys are a form of passwordless authentication, the tech cannot be termed *trustless* because the crypto and blockchain community has reserved that term for systems where trust is distributed and doesn't rely on a central authority. The central authority in this case is the systems and protocols of the service you're using, but passkeys can be called trustless in the interpretation where it means not storing your password with a third party.

So how does it sign me in? When you log into an account that uses a passkey, the account server sends a request to the authenticator device that consists of a string of data. Only a device with the private key can resolve the request and sends a response back - this is called *signing* the data - that verifies the user's identity.

What's the catch? If someone steals your authenticator device (with the passkey stored on it) and can sign in using your biometrics or password, they can gain access to your account. But just like with Google Wallet or ApplePay, you aren't vulnerable to outside data breaches.

What if I already use a password manager? Great. All the major password manager services like 1Password and LastPass have announced that they will support passkeys in the near future. [Apple has baked support into iCloud](#), so your other Apple devices signed into your AppleID will have access to passkeys through Keychain. The Google Chrome browser and Microsoft's Edge browser also offer multidevice support.

In the future all major services will replace password-only logins with passkeys and the world will be better for it.

ABOUT LINDSEY SCHUTTERS

Lindsey is the editor for ICT, Construction&Engineering and Energy&Mining at Bizcommunity

- DCDT overhauls radio frequency spectrum policy - 31 May 2024
- Vodacom goes to war against spectrum pooling - 30 May 2024
- Icasas extends deadline for digital migration regulations review - 27 May 2024
- HPE takes aim at Cisco, emphasises partner ecosystem and AI focus - 24 May 2024
- OpenAI inks News Corp deal, Google threatens to cut news funding - 23 May 2024

[View my profile and articles...](#)

For more, visit: <https://www.bizcommunity.com>