1Password

GUIDE

What are passkeys?

A beginner's guide to the passwordless login credential.

Table of contents

Introduction

What are passkeys?

We all use passwords to sign in to our devices and online accounts. They're an accepted part of our daily lives, and we all understand how they work. But that doesn't mean they're a perfect solution. Far from it.

If your organization doesn't use a password manager, it can be difficult for team members to create and remember hundreds of strong passwords. Many people forget their passwords on a routine basis and have to constantly reset them, wasting precious time at work. Others use the same password, or a few predictable passwords, which makes it easier for criminals to hijack their accounts and access confidential data.

82% **of breaches involve a human element, like a successful phishing attack or stolen credentials.**

- Verizon's 2022 Data Breach Investigations Report

Enter passkeys, a new kind of login credential that entirely replaces passwords.

Passkeys don't need to be written down or memorized. Instead, they're stored on the account owner's smartphone or other trusted devices, and protected by biometrics or a device PIN. Unlike passwords, there's no such thing as a "weak" passkey and they can't be reused, so each account gets the best protection possible.

Best of all, without physical access to your team members' devices (and a way to unlock them), no one can log in to their passkey-protected accounts.

In this guide, we'll break down how passkeys work, why they're more secure than passwords, and the reasons why every business should be excited to use them.

Ready to get started? Let's dive right in.

How passkeys work

Passkeys are more secure than passwords, easy to use, and supported by every major platform. To understand why, we have to unpack how they work.

Passkeys leverage an API called WebAuthn. Instead of a traditional password, WebAuthn uses public and private keys – otherwise known as public-key cryptography – to check that you are who you say you are.

It's these keys, and how they interact with each other, that make passkeys so secure.

What's an encryption key?

In cryptography, a key is a tool that can turn readable data into something indecipherable. It’s not, as it may sound, a plot device in Indiana Jones. Instead, an encryption key – or cryptographic key – is usually a string of numbers and letters. It’s processed through an encryption algorithm to convert unencrypted data (plaintext) into seemingly random jargon (ciphertext).

Do you ever chat with your friends on a secure messaging app? Maybe you’ve seen a lock icon in your browser or address bar while shopping online? Then you’ve used encryption keys before. Apps will usually generate and call upon these keys automatically, so you never have to remember or type them in.

How does public-key cryptography work?

First, you need to understand that public and private keys are mathematically linked to one another. You can think of them like interlocking puzzle pieces. They're designed to go together, and you need both to authenticate and prove that you are who you say you are.

As the name implies, the public key can be shared publicly. That means the website or app you want to sign in to can see and store your public key.

The private key, meanwhile, is kept secret and safe on your device. Unlike a traditional password, it's never shared with the website or app you want to sign in to, or stored on its servers.

When you want to sign in with a passkey, the website or app needs to check that you possess the correct private key. But how is this possible if your private key never leaves your device and is never shared with the website or app?

We'll tackle that question next.

What happens when you create an account with a passkey

Now that we've covered the fundamentals of public-key cryptography, let's break down how passkeys work in practice.

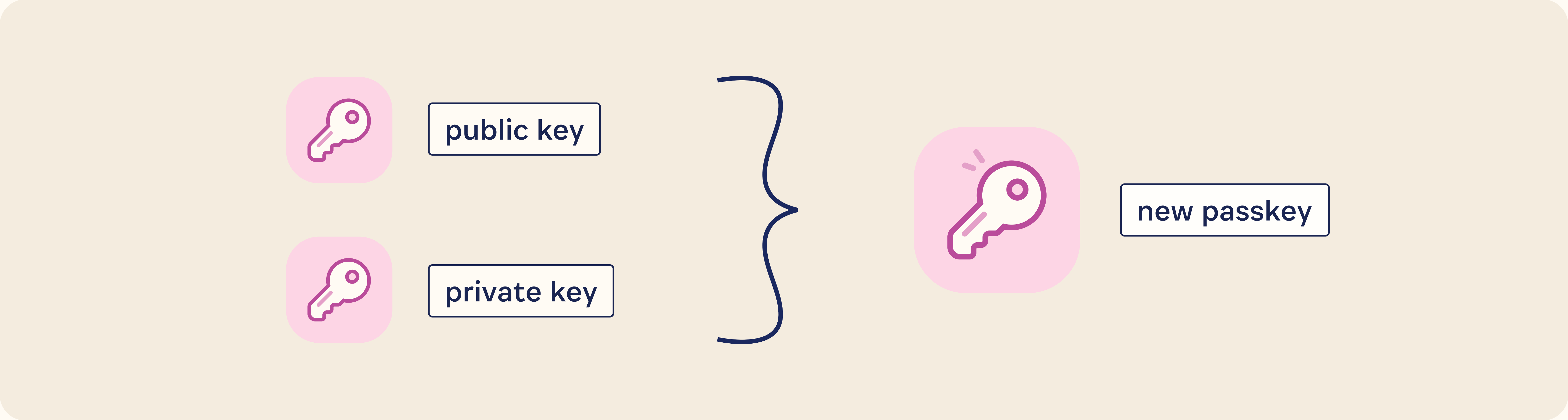
Imagine you visit a website that supports passkeys.

You can check **passkeys.directory** to find websites, apps, and other services that support passkeys!

First, you create an account and choose the option to secure it with a passkey, rather than a traditional password.

Behind the scenes, the website's server will share some information about the website. You'll then be prompted to confirm the hardware that your private key will be stored on. (This is known as an "authenticator".) The device could be your phone, tablet, PC, or even a **hardware security key**, like the ones created by **Yubico**.

A new passkey – which includes your public and private key pair – will then be generated for that specific website. This process happens locally, on your device. The public key will be sent to the website's server for storage, while the private key is stored on your authenticator.



This process happens behind the scenes, and near instantaneously. From your perspective, you simply choose your authenticator and then see the confirmation that your account has been created.

Unlike a password, there's nothing that you manually have to create or memorize. You simply choose the passkey option, pick an authenticator, and relax.

What happens when you sign in to an account with a passkey

Signing in with a passkey couldn't be simpler.

The next time you visit the website, you won't have to enter a traditional password. Instead, you'll be asked to authenticate using biometrics. That could be Face ID, Touch ID, Windows Hello, or a similar solution. If you don't have access to biometrics – let's say the webcam on your laptop is broken – the system will request the pincode or password that you normally use to unlock your device.

Once you've authenticated, that's it! The website or app will grant access to your account.

You might be asking: Why am I asked to authenticate when I sign in with a passkey?

Behind the scenes, the website creates a technical “challenge” when you ask to sign in. You can think of this "challenge" like a special one-time puzzle.

Your authenticator needs to "sign" the challenge using your securely-stored private key. But before that happens, the system has to check that you – and not a hacker who's somehow stolen your laptop – are the person requesting access to your private key.

Once you've successfully authenticated, your device “signs” the challenge using your private key. The completed “signature” is then sent to the website. Finally, the website uses its copy of your public key to verify the signature’s authenticity.

Why passkeys are more secure than passwords

Passkeys are more secure than passwords because they utilize a true secret, rather than a shared secret.

As we've already established, behind every passkey is a private key that never leaves your device. It’s a true secret that isn't shared with the app or website.

The best an attacker can hope to find on a website's server is your public key. This can’t be used to sign in to your account, and can’t be reverse-engineered to reveal your private key.

That means you don’t have to worry about how the website is storing your credentials, because the public key on its own can’t be used to gain access to your account.

By comparison, a traditional password is a shared secret. That means the secret required to sign in – for example your password – is stored (or memorized) by you and the app or website.

~80%

of basic web application breaches can be attributed to stolen credentials.

Verizon’s 2022 Data Breach Investigations Report

Your passwords might be disguised onscreen as a series of asterisks or bullets, but you always have to type or autofill them in plain text.

When you create an online account, the website uses an algorithm – complex, predetermined math – to encrypt, or scramble, that text. The result, which is called a hash, is then saved by the website or app.

When you sign in, the website performs the same math on the password you enter or fill. If the hash matches what was stored when you signed up, you’re in.

Hashing is a great way to protect passwords and other sensitive information. But the process does have some weaknesses. If an attacker breaches a website's server and finds a database of encrypted passwords, they might be able to crack them using a dictionary attack, look-up rainbow tables, and other techniques.

The bottom line? Passkeys are more secure than traditional passwords because you hold onto the private key and never have to entrust a website or app with it.

5 reasons why your business should be excited about passkeys

Passkeys provide a strong defense to safeguard your employee and customer data. Here are just a few reasons why your organization should adopt them at the earliest opportunity:

1. Fewer password resets

The average person spends more than 10 hours each year resetting passwords. Passkeys solve this problem because they don't require team members to memorize or type out anything. When they want to sign in to an account, they simply authenticate when prompted.

The result? Fewer colleagues getting locked out of their work-related accounts. And, by extension, your IT team has to spend less time assisting co-workers with password resets and account recovery.

2. A more productive workforce

Fewer password resets mean your team can spend more time on growing your business. And who doesn't love a more productive workforce?

Passkeys are also incredibly quick to use. You simply authenticate with biometrics or your device pincode, and you're in. If you don't use a password manager, that's considerably faster than endlessly typing out passwords and two-factor authentication (2FA) codes.

3. No more worrying about weak passwords

Remembering strong passwords is difficult if you don't have a password manager like 1Password. That's why so many people choose weak and predictable ones like "password123". These passwords pose a security risk because while they might be easy to memorize, they're also simple for attackers to crack or guess.

Passkeys, meanwhile, are always strong. That means better workplace security and more peace of mind.

4. A defense against social engineering

Reread the latest news reports and you'll notice that most data breaches can be traced back to a single cause: social engineering. Hackers are using phishing, SIM swapping, and other techniques to trick someone into sharing sensitive data, or doing something that helps them gain access to confidential information.

Passkeys, meanwhile, are resistant to phishing. Your private key never leaves your devices, which means – unlike a password – you can't be tricked into sharing it or typing it into a fake but authentic-looking website.

5. Better protection against breaches

Every time you create an online account, you're trusting that the company behind the website or app will look after your password. If they don't encrypt it properly and their servers are breached, there's a chance that your account password will be exposed.

If you use 1Password, Watchtower will tell you when any of your saved credentials have been affected by a known data breach. That way, you can quickly change them before attackers have a chance to exploit them.

Passkeys are different because your private key is never stored on the website or app's server. If an attacker breaches the server, they won't find everything they need to sign in to your account.

1Password and passkeys

Here at 1Password, we're all in on passkeys.

That's why we joined the FIDO Alliance, which includes other passkey supporters like Apple, Google, and Microsoft. Together, we have an opportunity to build safe, simple, and fast login solutions for everyone.

We're already working to integrate passkeys into our password manager, so you can continue to manage and protect everything that's important in your digital life.

That includes:

CREATE, **SAVE**, and **AUTOFILL** passkeys with 1Password **(coming soon)**

Use 1Password

in the browser to secure your online accounts with strong, unique passkeys.

Store and manage passkeys

alongside your traditional login credentials.

View, edit, tag, and share

passkeys from the 1Password apps.

UNLOCK 1Password with a passkey **(coming soon)**

Create a 1Password account

without a password or a Secret Key.

Accelerate onboarding

for team members.

Sign in on new,

trusted devices with ease.

Use built-in biometric authenticators

everywhere you use 1Password.