

Passkeys

Passkeys are replacing passwords using advanced encryption and biometric data. These new technologies offer a user-friendly and secure method to access your online accounts. This article describes their operation, pros and cons as well as their impact on digital security.

User account encryption or securing has been developing from simple passwords via complex passwords right up to two-factor authentication, with a tendency of making the log-in process ever more complex and complicated for users for the sake of higher security. The latest passkey approach is meant to considerably simplify the log-in process and increase security further, too. Passkeys are considered an innovative solution which is both secure and user-friendly.

Some important points to remember:

- Using passkeys means you no longer have to remember or save passwords.
- Passkeys are [phishing \(https://www.ebas.ch/en/phishing/\)](https://www.ebas.ch/en/phishing/)-resistant since every passkey is firmly linked to a website or app cryptographically. No matter how sophisticated a phishing website is – it will never be able to capture the information required to log in.
- Passkeys are protected using a PIN or biometric data such as your fingerprint or facial recognition.
- It is mandatory to provide basic protection for your device using our [«5 steps for your digital security» \(https://www.ebas.ch/en/5-steps-for-your-digital-security/\)](https://www.ebas.ch/en/5-steps-for-your-digital-security/) to ensure all locally stored passkeys are secure.
- Data leaks suffered by online service providers involving login credentials doesn't affect passkey-secured access.

What are passkeys?

Passkeys are a method to log into your user accounts rendering passwords redundant. Instead of having to remember and enter a password, you can log in using a passkey.

A passkey is a digital key consisting of a public and a secret key. The secret key is stored on your device protected by a PIN or biometric data such as your fingerprint or facial recognition.

Passkeys are considered secure. They use strong encryption and biometric data which are difficult to fake. Even if your device is stolen, no-one can access your passkeys without your biometric data or PIN.

Passkeys are [phishing \(https://www.ebas.ch/en/phishing/\)](https://www.ebas.ch/en/phishing/)-resistant since every passkey is firmly linked to a website or app cryptographically. Your secret key also always remains on a local device such as a smartphone or USB stick, never leaving them.

In addition to the public key, you always need to provide authorisation via your local device to log in. This is also an advantage in case of any data leaks (an event where unauthorised parties obtain access to log-in data, for instance to a certain website). Even if third parties obtain your public key to access an account, they cannot access your user account without authorising this via the local device first.

The technology behind this has been developed by the FIDO Alliance, a non-commercial IT security organisation in-

involved in providing fast proof of identity for digital connections (**Fast IDentity Online**).

How does it work?

When you log in with a service provider offering passkey identification, this will communicate with your device. It will send a challenge to do so. You will then have to identify yourself using your PIN or your biometric data (face recognition or fingerprint). The device then returns a digital signature to the website to confirm that it is really you who wants to log in.

The operating principle of passkeys is relatively simple, even if there's advanced technology behind it. Here a simple sequence of how a passkey is created:

1. **Registration:** When you create an account on a website or app, a passkey consisting of a secret and a public key is generated on your device. This passkey is unique and linked to the website or app.
2. **Storage:** The passkey secret key is securely protected on your device or operating system using the same (biometric) authentication method used to unlock your device, e. g. facial recognition, fingerprint or PIN code. With macOS and iOS these are saved to the keychain; Windows uses Windows Hello and Android are employing Google Password Manager to save passkeys.
3. **Logging in:** When you want to log into this website or app next time, your device will use the secret key of your passkey saved locally. The website only has the public key of your passkey. You confirm your identity on the website using biometric data or your PIN, and you are all logged in.

Pros

- You no longer have to remember any complicated passwords and won't have to enter them when logging in either. Your biometric data or a PIN is all you need to log in.
- Logging in using a passkey is considerably easier and faster than entering a password or consulting a password manager.
- The secret key of your passkey is never transmitted to a website, which will prevent [phishing \(https://www.ebas.ch/en/phishing/\)](https://www.ebas.ch/en/phishing/) attacks.
- Since websites are only ever saving public and never private keys of your passkey, access is protected even if there are any service provider data leaks. The public key part of passkeys can be replaced with little effort.

Cons

- Due to the passkey being linked to your device, it cannot be easily shared. If any service is meant to be used by two different people, it can only be used by the one person having access to the device where the passkey is stored.
- Passkeys are stored on your device. Without this device, you cannot access your passkey and cannot therefore log into a website or app either.
- Passkeys are managed differently depending on your operating system; their easy use on several devices is only possible within the same operating system (e.g. Microsoft, Apple) or system family.
- There are only very limited options to use passkeys under the Linux operating system. You can however log-in using cross-system solutions, such as QR codes.

How are passkeys set up and used?

Windows

You can find instructions on how to create and use passkeys under Windows [here \(https://learn.microsoft.com/en-gb/windows/security/identity-protection/passkeys/?tabs=windows\)](https://learn.microsoft.com/en-gb/windows/security/identity-protection/passkeys/?tabs=windows).

macOS, iPhone/iPad

Apple synchronises passkeys using iCloud keychain on all devices of every user.

- [MacOS instructions \(https://support.apple.com/en-ca/guide/mac-help/mchl4af65d1a/mac\)](https://support.apple.com/en-ca/guide/mac-help/mchl4af65d1a/mac)
- [iPhone/iPad instructions \(https://support.apple.com/en-ca/guide/iphone/iphf538ea8d0/ios\)](https://support.apple.com/en-ca/guide/iphone/iphf538ea8d0/ios)

Android

To use passkeys under Google, your screen lock or potentially bluetooth needs to be activated.

You can find instructions on how to create and use passkeys with Google [here \(https://support.google.com/accounts/answer/13548313?sjid=10008299915686849826-EU&hl=en\)](https://support.google.com/accounts/answer/13548313?sjid=10008299915686849826-EU&hl=en).

Cross-system use

You can currently use QR codes or bluetooth to use passkeys across several different systems, where successful authentication is transmitted.

Certain password managers also support passkeys so that in principle, an exchange across several devices is possible. However there is one drawback remaining that providers manage passkeys using their own tools and want to save them in their own cloud.

Conclusion

Passkeys make logging into user accounts easier and safer. Since an increasing number of service providers are supporting passkeys, this could turn out to be the future of digital authentication. From a security point of view, passkeys have the edge in case of any data leaks and phishing. Still, attackers could increasingly feel tempted to attack user devices and cloud solutions to obtain secret keys. Such devices and cloud accounts must therefore be always well protected and remain updated to the latest security standards.

A “passkey” is a passwordless log-in method, consisting of a public and a private key, with the secret key always remaining on a local device such as a smartphone or USB stick, never leaving them. The device itself acts as a means of authentication. Contrary to passwords, passkeys are therefore device- and not person-specific.