Passkeys explained: How to embrace a passwordless future today

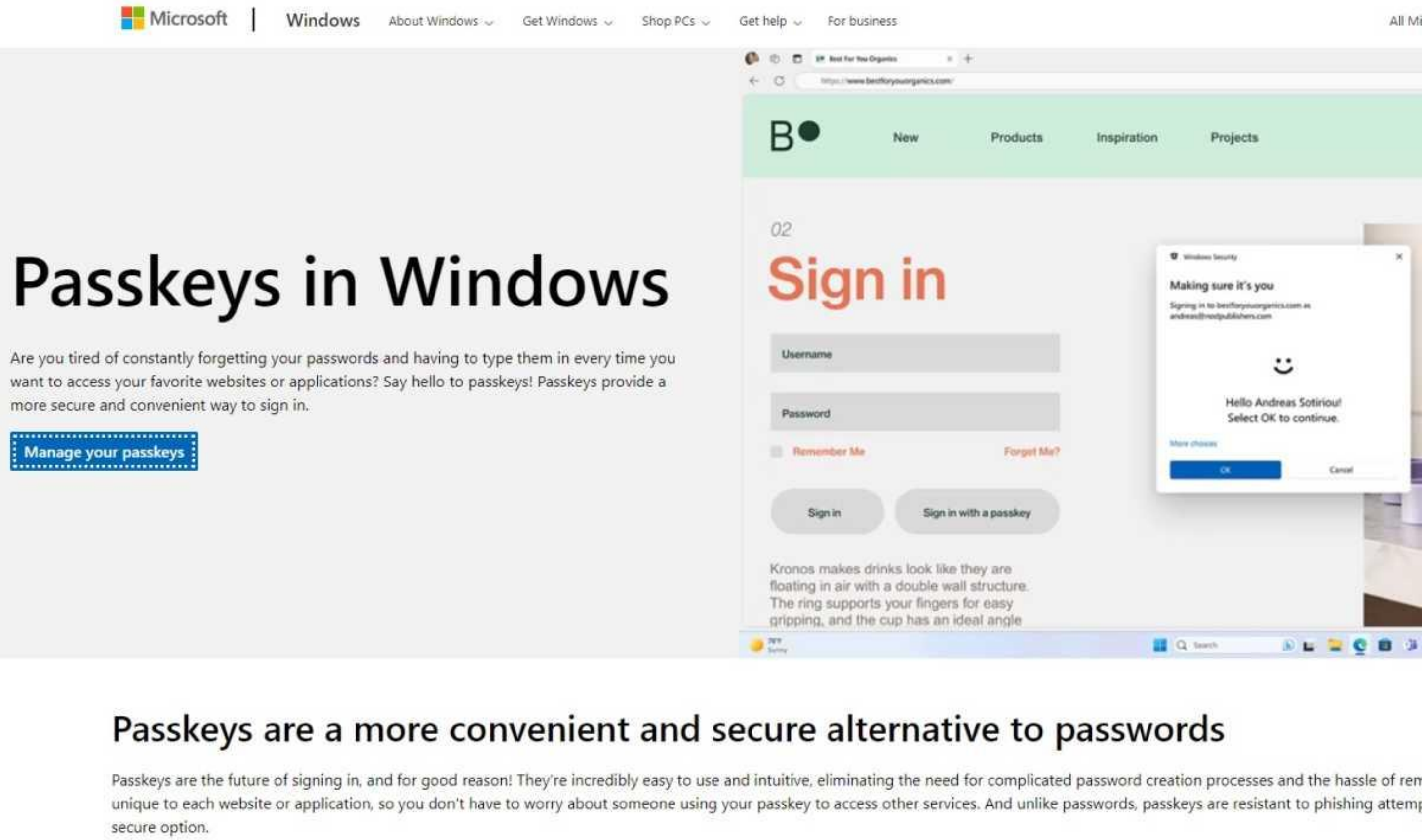
By Peter Stelzel-Morawietz, pcworld.com, MAY 6, 2024

Passkeys are increasingly replacing traditional passwords. This makes logging on to the internet much more convenient and secure. You can create your first passkey in just one minute.

“Logging in without any passwords, how’s that supposed to work?” you may be asking yourself. After all, user names and passwords are so much a part of everyday life that it’s hard to imagine whether it might not work without them.

Yes, you can log in without a password, and it’s even more convenient, faster, and more secure than before. This time it’s not just an advertising promise, a fundamental change is actually underway.

Because the status quo is downright sobering: Billions of personal accounts have been hacked worldwide. In Germany, almost one in three people have had their online accounts spied on, according to a representative survey commissioned by the consumer advice center.



Passkeys in Windows

Are you tired of constantly forgetting your passwords and having to type them in every time you want to access your favorite websites or applications? Say hello to passkeys! Passkeys provide a more secure and convenient way to sign in.

Manage your passkeys

Making sure it's you

Signing in to bestforyouorganics.com as andreas@reedpublishers.com

Hello Andreas Sotiriou! Select OK to continue.

Kronos makes drinks look like they are floating in air with a double wall structure. The ring supports your fingers for easy gripping, and the cup has an ideal angle

Passkeys are a more convenient and secure alternative to passwords

Passkeys are the future of signing in, and for good reason! They're incredibly easy to use and intuitive, eliminating the need for complicated password creation processes and the hassle of ren unique to each website or application, so you don't have to worry about someone using your passkey to access other services. And unlike passwords, passkeys are resistant to phishing attem secure option.

Microsoft not only advises using passkeys to increase security and convenience when logging in, but also offers the option of not using passwords at all.
Foundry

There are many reasons for this, some of which are due to the carelessness of some users. After all, not everyone wants to assign a unique and secure password to all of their 100 or so accounts — despite all the well-intentioned advice. The consequences are well known.

However, the situation is not as hopeless as it seemed for a long time. You can log in to more and more internet services, from Amazon to Whatsapp, using the new “passkeys.” Not only are they easier and more convenient to manage, they are also much more secure.

You no longer have to remember anything, so you can’t forget anything, and you don’t even need new equipment. You can get started straight away with your PC or smartphone.

PC and smartphone are all you need to log in securely

We focus on the practical use of passkeys and only explain the technology behind them to the extent that it helps you understand them and have the necessary trust. Passkeys are a further development of the established Fido 2 security standard with asymmetric encryption.

When you set up a passkey to log in to an online service, your PC or mobile phone generates a key pair. The public key is sent to the website and stored there, the private key is secret and remains in the crypto chip of your device — i.e. in the Trusted Platform Module (TPM) on a computer.

If you use a smartphone, the private key is also securely synchronized in the cloud of the operating system, i.e. Apple or Google. This is one of several advantages of the smartphone, which we will come back to in a moment.

Once a passkey has been set up, the next time you visit the website (or app), you simply tell it that you want to log in. The online service then sends your device a so-called challenge: a task that can only be solved with the help of your private key stored in your device and which you authorize using your fingerprint, face scan, or PIN.

Only the digitally signed solution to the challenge is sent back, not the private key itself.

As this process also takes the original domain into account, it provides reliable protection against phishing. Even if a website is a deceptively genuine imitation, the passkey refuses the log-in.

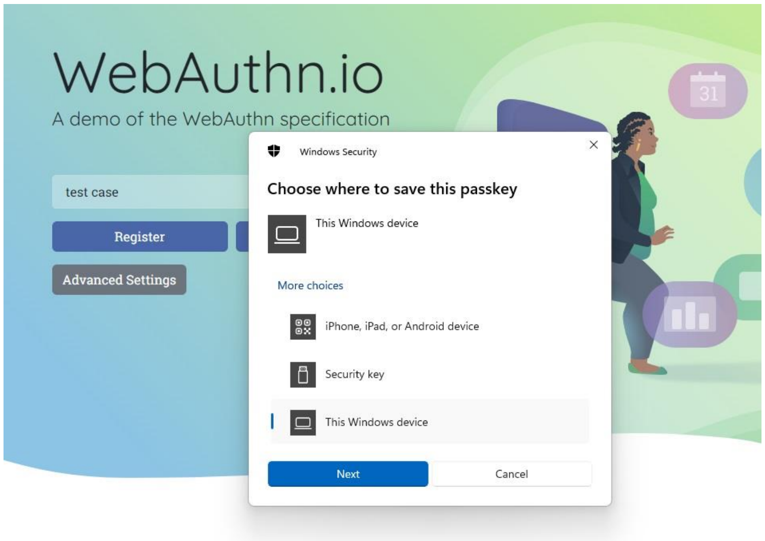
Services with passkey support

There is no official directory of all providers with passwordless login. Lists are provided by Passkeys.io, Passkeys Directory, and Keeper, among others. New providers with Passkey support may not be included at first. Important services are listed below.

- 1Password
- Adobe
- Amazon
- Apple
- Bitwarden (passwords)
- Dashlane (passwords)
- Ebay
- GitHub (Software)
- Google
- Kayak (Travelling)
- Keepass XC (passwords)
- Keeper (Passwords)
- Linkedin
- Microsoft
- Mozilla (Firefox)
- Nintendo
- Nvidia

- PayPal
- Shopify (E-Commerce)
- Sony Playstation
- Synology
- Tiktok
- Uber (e.g. taxi)
- Whatsapp
- X (Twitter)
- Yahoo
- Zoho (e.g. Office)

Here we go: Try out Passkeys



WebAuthn.io

A demo of the WebAuthn specification

test case

Windows Security

Choose where to save this passkey

This Windows device

More choices

iPhone, iPad, or Android device

Security key

This Windows device

A Hello-enabled camera or a fingerprint sensor on the laptop or PC make logging in via Passkeys particularly convenient.
Foundry

If you only want to use Passkeys on your PC at home, you can store your private keys exclusively on your computer. The requirements are straightforward, a compatible browser such as Chrome, Edge, or, more recently, Firefox (from version 122) is all you need.

First create a login PIN for Windows Hello in the Windows settings under *Accounts* > *Login options*. This is hardware-bound, so unlike a password, it’s only valid for this one computer. If available, you can also set up fingerprint or face recognition for greater convenience.

For our passkey-in-a-minute promise, open the test page https://webauthn.io in your browser. In the “example_ username” field, enter a name of your choice, click on “Register,” and authenticate yourself via Windows Hello in the next step.

You may need to confirm the “This device” option, followed by the messages “Master key saved” and “Success! Now try to authenticate …” — all in less than 60 seconds.

Please take this request literally and log in without a password using the passkey you have just created. To do this, click on the “Authenticate” button and authenticate yourself again: “You’re logged in”!

As your Webauthn test account is automatically deleted after one day, you do not need to do anything else.

Log in to your PC with a smartphone

Smartphones are more practical than PCs for passwordless logins for several reasons:

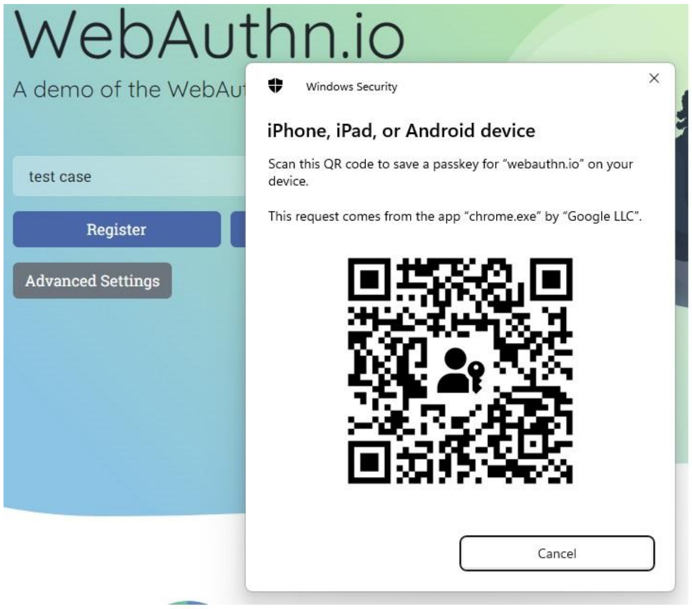
- Firstly, it stores the passkeys in the mobile operating system’s password manager just as securely
- Secondly, as we will show in a moment, it also enables the new login procedure on the PC
- Thirdly, you almost always have it with you
- Fourthly, the Android (from version 9) and iOS (from version 16) operating systems synchronize the passkeys automatically and in encrypted form in the cloud

If the mobile device breaks or is lost, you have a backup right away. Synchronization is not yet available for Windows. You can read more about the backup strategy for passkeys in the box at the bottom of this page.

This is how it works: To create a passkey via your smartphone, open the test page https://webauthn.io on your PC again, assign a user name, click on “Register” and then on the option “iPhone, iPad or Android device.”

Confirm with “Next” and hold the phone camera on the QR code shown on the PC monitor. Now confirm the passkey option shown on the smartphone and follow the next steps.

Android and iOS differ only slightly here. Depending on the device configuration, you may still need to enter the unlock PIN before authenticating with a fingerprint or face scan. You already know the rest.



iPhone, iPad, or Android device

Scan this QR code to save a passkey for “webauthn.io” on your device.

This request comes from the app “chrome.exe” by “Google LLC”.

Aim your phone’s camera at the QR code to complete the registration process for your phone.
Foundry

Logging in is even quicker and more convenient if you allow this step to be skipped on your smartphone after the QR scan. In the future, all you need to do to log in on the PC is select the linked mobile device and authorize the login using a finger or face scan. Authentication takes place via Bluetooth (from version 5.0). If your computer fails to fulfil this requirement, a USB Bluetooth dongle for around $10 will help.

You can log in to the actual online accounts later in the same way using a passkey. The challenge request runs in the background, the solution is sent back digitally signed in a matter of seconds — and you are securely logged in.

Logging in without a password in practice

You now know how passkeys work. To familiarize yourself with the concept, we recommend only switching one or two accounts to begin with. The box above lists important providers that support the method.

Most of these services currently still allow the parallel use of passkey and password. This makes logging in convenient for you, but insecure passwords still pose a risk.

Microsoft at least offers the option of removing the password completely in the personal settings under *Security > Advanced security options > Passwordless account*. With NAS manufacturer Synology, you even have to choose between a password and a passkey.

To create a passkey, first log in to the service of your choice in the PC browser. The setup option can usually be found in the account configuration under “Security.” The next steps differ from provider to provider, both in terms of the terminology and the setup itself. In some cases, you may also encounter unexpected things such as additional apps and other hurdles.

For example, the Google passkey was initially linked to Windows Hello and thus to the PC during testing. Only afterwards was it possible to create another passkey on a “different device” via the passkey management — i.e. on the smartphone as desired.

Microsoft, on the other hand, first requires its own Authenticator app on the smartphone, only then can you switch to the operating system’s password manager. These examples show how important it is to familiarize yourself with passkeys. However, if you know that it works, you can get there by trying it out or using a Google search.

Tip: Passkeys are also suitable for particularly security-relevant applications, such as payments, which should be protected by a second factor. You can quickly authorize, say, Paypal transactions with your fingerprint without having to enter a short code or do anything else first.

Conclusion

Cloud synchronization of passkeys offers the advantage over conventional hardware-based Fido 2 authentication in that you don’t have to set up passwordless login for every device.

At the same time, management with the smartphone ensures a backup of all private keys and thus the possibility of restoring them if the hardware breaks down or is lost. If you only use the passkeys on your computer at home, you can in principle also save them on your PC.

However, please do not forget to create a restore option just in case (see box below). The passkeys can be managed on the Windows PC in the Settings app under *Accounts > Passkeys*, or on the smartphone in the password managers from Apple or Google also under “Settings.”

Protection from being locked out

A Fido 2 stick like this is one of several backup options for passkeys. However, the most convenient option is synchronization with the smartphone in the cloud.
Yubico

If you forget a conventional online password, you can simply create a new one using the option of the same name: so convenient, but also so insecure. But what happens if the hardware with the stored private keys is defective or lost? Because only you have these keys — which is the central component of this security concept.

So take precautions to avoid locking yourself out. If you follow our advice and use your smartphone to store your passkeys instead of your PC, there is hardly any danger. This is because Apple and Google automatically synchronize the passkeys in encrypted form in the cloud. If your mobile phone is lost or defective, you can then quickly restore the keys on a replacement device.

Things are more difficult on a Windows PC: Although Microsoft also wants to implement synchronization, it has so far only been implemented in Insider pre-release versions of the operating system.

A Fido 2 stick with a crypto chip, which is available from around $30, is also suitable as a backup. However, you must also save your passkeys on the stick beforehand (!) using the “Security key” option.

Many online services also offer additional options for two-factor authentication and recovery. Please remember to set these up beforehand.

This article was translated from German to English and originally appeared on pcwelt.de.

This article originally appeared on our sister publication PC-WELT and was translated and localized from German.