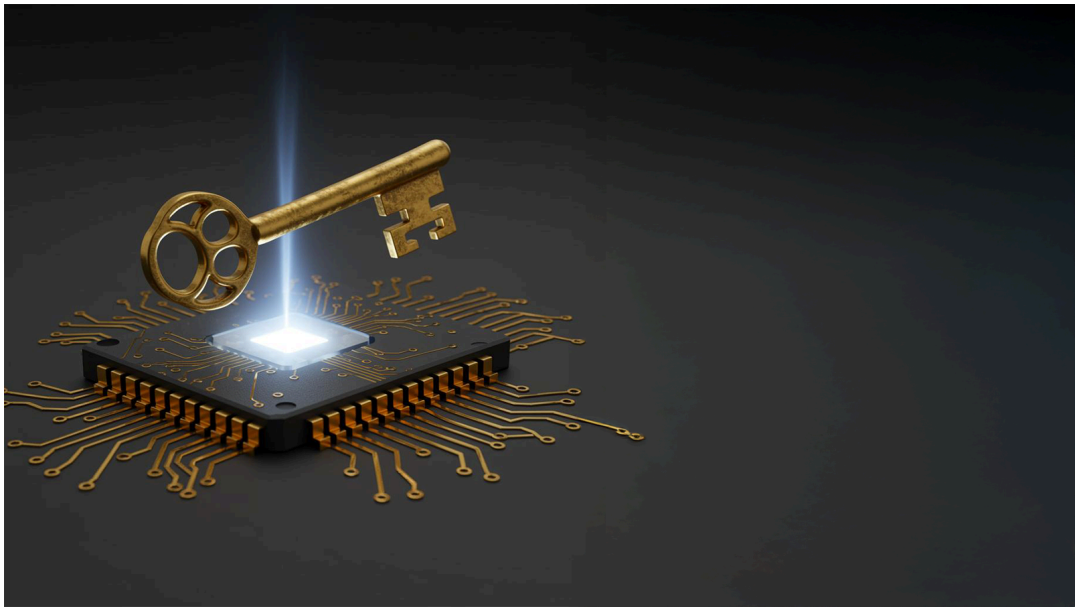
Passkeys:
Die moderne Alternative zu Passwörtern



Passkeys sind ein digitaler Schlüssel für Ihre Online-Konten - und bieten gegenüber Passwörtern viele Vorteile

Vorwort

Passwörter, lange Zeit das Standardmittel zur Absicherung unserer Online-Konten, erweisen sich zunehmend als problematisch: Sie sind schwer zu merken, leicht zu knacken und werden oft mehrfach verwendet.

Mit Passkeys haben wir als Anwender nun eine benutzerfreundliche und gleichzeitig sicherere Alternative. Diese digitalen Schlüssel versprechen nicht nur mehr Sicherheit, sondern auch eine deutlich vereinfachte Handhabung – ideal für alle, die sich nicht mit komplexen Passwörtern herumschlagen möchten. Wie Passkeys funktionieren, zeige ich Ihnen auf den nächsten Seiten.

Ihr Kaner Etem

Was sind Passkeys?

Das Prinzip ist einfach: Jeder Passkey besteht aus zwei Teilen – einem privaten Schlüssel, der sicher auf Ihrem Gerät verbleibt, und einem öffentlichen Schlüssel, der auf dem Server des jeweiligen Dienstes gespeichert wird.

Bei der Anmeldung läuft folgendes ab: Der Dienst, bei dem Sie sich anmelden möchten, sendet eine einzigartige Anfrage an Ihr Gerät. Ihr Gerät verwendet dann Ihren privaten Schlüssel, um diese Anfrage zu "unterschreiben" - aber erst, nachdem Sie bestätigt haben, dass Sie es wirklich sind. Diese Bestätigung erfolgt ganz einfach über Methoden, die Sie bereits kennen und nutzen - wie Ihr Fingerabdruck, die Gesichtserkennung oder Ihre persönliche PIN.

Nachdem Sie sich identifiziert haben, erstellt Ihr Gerät automatisch eine digitale Signatur und sendet diese zurück an den Server. Der Server überprüft mit dem zuvor gespeicherten öffentlichen Schlüssel, ob die Signatur tatsächlich von Ihrem privaten Schlüssel stammt. Das Besondere: Selbst wenn jemand diese Signatur abfangen würde, könnte er sie nicht wiederverwenden, da für jede Anmeldung eine neue, einzigartige Signatur erstellt wird.

Der große Vorteil: Ihr privater Schlüssel verlässt niemals Ihr Gerät. Anders als Passwörter, die auf Servern gespeichert werden müssen (wenn auch verschlüsselt), bleibt Ihr geheimer Schlüssel immer sicher in der geschützten Umgebung Ihres Smartphones oder Computers. Dadurch sind Passkeys deutlich sicherer gegen Hacker-Angriffe - denn was nicht übertragen wird, kann auch nicht gestohlen werden.

Die wesentlichen Vorteile von Passkeys sind:

- **Erhöhte Sicherheit**: Der private Schlüssel verlässt niemals Ihr Gerät
- **Benutzerfreundlichkeit**: Sie müssen sich keine komplexen Passwörter mehr merken
- **Phishing-Schutz**: Passkeys sind an spezifische Websites gebunden und können nicht für gefälschte Seiten verwendet werden
- **Datenschutz**: Selbst bei Datenlecks bleiben Ihre Anmeldedaten sicher

Achtung: Passkeys sind eine Ergänzung zu Ihren bestehenden Zugangsdaten wie Benutzername und Passwort. Mit Passkeys können Sie sich bei Ihren Online-Konten anmelden, ohne jedes Mal das Passwort eintippen zu müssen. Ihre normalen Passwörter sollten dennoch sicher bleiben und mindestens 12 Zeichen, Groß- und Kleinbuchstaben sowie Sonderzeichen enthalten. Denken Sie an Passkeys wie einen digitalen Schlüssel, der die lästige Passworteingabe überflüssig macht, während Ihre bisherigen Passwörter als Sicherheitsreserve bestehen bleiben.

Praktische Anwendung im Alltag

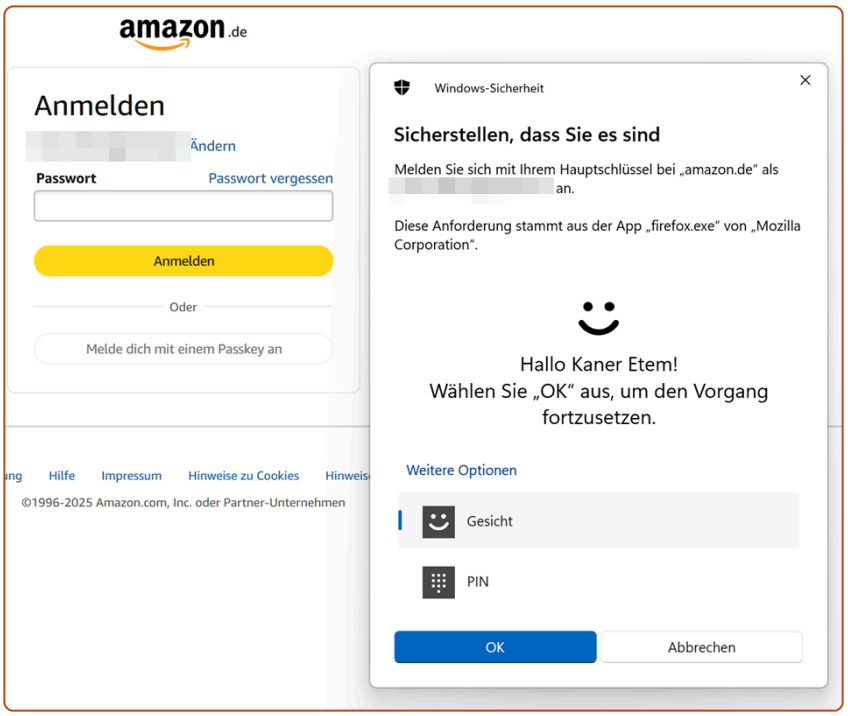
Die Nutzung von Passkeys gestaltet sich im Alltag bemerkenswert einfach. Nach der einmaligen Einrichtung erfolgt die Anmeldung bei unterstützten Diensten mit wenigen Klicks oder Taps, gefolgt von einer biometrischen Bestätigung oder PIN-Eingabe.

Immer mehr namhafte Unternehmen und Dienste unterstützen Passkeys, darunter:

- Amazon, Apple, Google und Microsoft
- PayPal, eBay und LinkedIn
- Zahlreiche soziale Netzwerke und E-Mail-Anbieter
- Die vollständige Liste können auf dieser Webseite einsehen: passkeys.directory

Der Anmeldeprozess läuft mit Passkeys typischerweise so ab:

1. Sie besuchen die Website oder öffnen die App
2. Sie geben Ihren Benutzernamen ein oder wählen Ihr Konto aus
3. Statt ein Passwort einzugeben, bestätigen Sie die Anmeldung mit Ihrem Fingerabdruck, Gesichtserkennung oder PIN
4. Die Anmeldung erfolgt sofort und sicher



Besonders praktisch: Auch auf fremden Geräten können Sie sich mit einem Passkey anmelden. Wenn Sie sich auf einem neuen Gerät anmelden möchten, scannen Sie einfach einen angezeigten QR-Code mit Ihrem Smartphone und bestätigen die Anmeldung per Fingerabdruck oder Gesichtserkennung.

Einrichtung von Passkeys

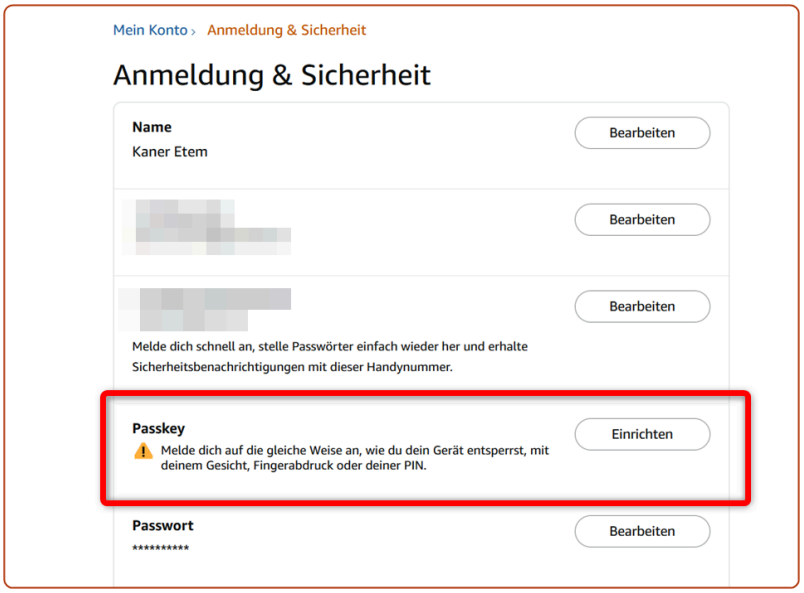
Die Einrichtung von Passkeys erfolgt in wenigen Schritten und ist bewusst benutzerfreundlich gestaltet. Zunächst melden Sie sich bei dem gewünschten Dienst mit Ihrem bestehenden Passwort an. Anschließend navigieren Sie zu den Sicherheitseinstellungen oder Ihrem Profil, wo Sie die Option zur Einrichtung eines Passkeys finden sollten.

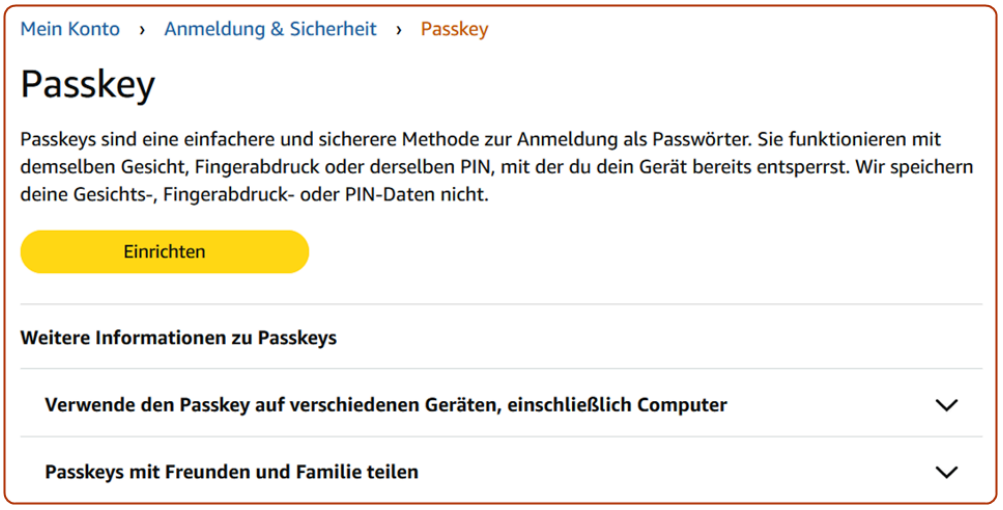
Der Einrichtungsprozess variiert leicht je nach Plattform und Gerät, folgt aber einem ähnlichen Muster:

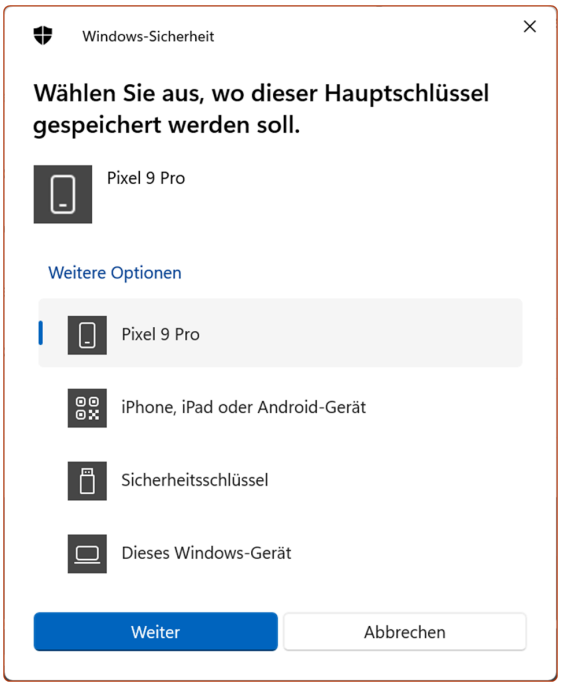
Auf dem PC / Laptop:

1. Navigieren Sie zur Webseite
2. Melden Sie sich mit Benutzername und Passwort an
3. Oftmals bekommen Sie hier schon ein Angebot, einen Passkey zu erstellen, oder:
4. Sie navigieren zu Ihren Kontoeinstellungen. Häufig befindet sich die Passkey-Erstellung unter dem Punkt “Sicherheit” oder “Kontosicherheit”
5. Wählen Sie aus, mit welcher Methode Sie Ihr Passkey verifizieren möchten
    a. per Fingerabdruck (sofern der Laptop diese Funktion anbietet)
    b. per Gesichtserkennung (sofern der Laptop diese Funktion anbietet)
    c. per Smartphone
6. Bestätigen Sie die ausgewählte Methode
7. Der Passkey ist fertig erstellt → Sie können sich nun zukünftig bequem per Passkey anmelden.

Beispiel für Amazon:

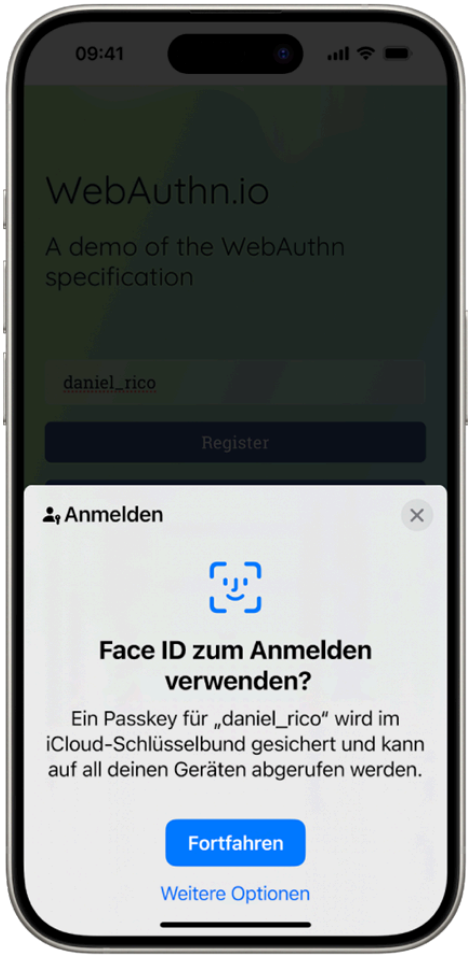






Für Smartphones:

1. Auf iPhone- und Android-Geräten wird auf kompatiblen Webseiten die Erstellung von Passkeys automatisch angeboten
2. Sie müssen die Erstellung eines Passkeys nur noch per Fingerabdruck oder Gesichtserkennung (je nach Smartphone-Modell) auswählen
3. Ab sofort können Sie Passkeys zur Anmeldung nutzen



Besonders praktisch: Sowohl Apple- als auch Android-Smartphones synchronisieren Ihre Passkeys sicher zwischen Ihren Geräten. Die Synchronisierung erfolgt mit Ende-zu-Ende-Verschlüsselung. Das heißt: Selbst Apple und Google können Ihre Passkeys nicht im Klartext lesen.

So können Sie Ihre Passkeys bei Verwendung eines iPhones auch auf Ihren anderen Apple-Geräten nutzen und bei Android-Smartphones können Sie Passkeys nahtlos auf dem Chrome-Browser weiter nutzen.

Häufig gestellte Fragen

“Was passiert, wenn ich mein Smartphone verliere, worauf die Passkeys gespeichert sind?”

Bei Verlust Ihres Geräts bleiben Ihre Passkeys in der Regel über Cloud-Dienste gesichert:

- **Apple-Nutzer:** iCloud Schlüsselbund
- **Android-Nutzer:** Google Passwort Manager

Wenn Sie ein neues Gerät kaufen und mit Ihrer Apple-ID bzw. Ihrem Google-Konto wiederherstellen, sind auch die Passkeys wieder einsatzbereit.

Auch brauchen Sie sich keine Sorgen bei einem Diebstahl zu machen: Ohne biometrische Entsperrung per Fingerabdruck oder Gesichtserkennung ist ein Zugriff auf die gespeicherten Passkeys nicht möglich. Dennoch ist Vorsicht die Mutter der Porzellankiste: Entfernen Sie aus den Online-Konten die Passkey-Anmeldemöglichkeit für das gestohlene Gerät in den jeweiligen Passkey-Einstellungen. Das geht in der Regel über jeden beliebigen Browser.

Zusätzlich empfehle ich

- Richten Sie mehrere Passkeys für wichtige Dienste ein – Sie sind nicht auf ein Passkey pro Online-Konto beschränkt, sondern können auch mehrere Methoden für die Passkey-Verifizierung nutzen

- Behalten Sie alternative Anmeldemethoden (E-Mail-Wiederherstellung, Sicherheitsfragen) bei

“Kann ich Passkeys auf mehreren Geräten nutzen?”

Ja, Passkeys sind für die geräteübergreifende Nutzung konzipiert. Die Synchronisation erfolgt über:

- Cloud-Dienste der jeweiligen Plattform (Apple, Google, Microsoft)

- Manuelle Übertragung per QR-Code

“Wie sind Passkeys in der Apple und Google Cloud abgesichert?”

Apple iCloud Keychain:

- Ende-zu-Ende-Verschlüsselung, wobei Apple keinen Zugriff auf die Entschlüsselungsschlüssel hat
- Zwei-Faktor-Authentifizierung für zusätzlichen Schutz
- Sichere Speicherung in der Secure Enclave des Apple-Geräts
- Wiederherstellungsmechanismen mit mehrschichtiger Authentifizierung

Google Password Manager:

- Ende-zu-Ende-Verschlüsselung der synchronisierten Daten
- Unterstützung für Zwei-Faktor-Authentifizierung, einschließlich physischer Sicherheitsschlüssel
- Geräteübergreifende Synchronisation mit Ihrem Google-Konto
- Biometrische Authentifizierung für den Zugriff

Zusammenfassung

Passkeys stellen einen bedeutenden Fortschritt in der Online-Sicherheit dar und bieten besonders für weniger technikaffine Nutzer erhebliche Vorteile:

- **Einfachere Handhabung**: Keine komplexen Passwörter mehr zum Merken oder Eingeben
- **Höhere Sicherheit**: Schutz vor Phishing und Datenlecks
- **Benutzerfreundlichkeit**: Schnelle Anmeldung mit Fingerabdruck oder Gesichtserkennung
- **Zukunftssicherheit**: Wachsende Unterstützung durch immer mehr Dienste und Plattformen

Die Umstellung auf Passkeys mag zunächst eine kleine Hürde darstellen, doch die Vorteile überwiegen bei weitem. Mit der schrittweisen Einführung bei Ihren wichtigsten Online-Diensten können Sie die Sicherheit Ihrer digitalen Identität deutlich verbessern und gleichzeitig den Anmeldevorgang vereinfachen.

Impressum: Computerwissen, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2-4, 53177 Bonn, Vorstand: Richard Rentrop, Bonn, Redaktionell Verantwortlicher: Sven Udert, VNR Verlag für die Deutsche Wirtschaft AG, Redaktion, Satz & Layout: Kaner Etem, München