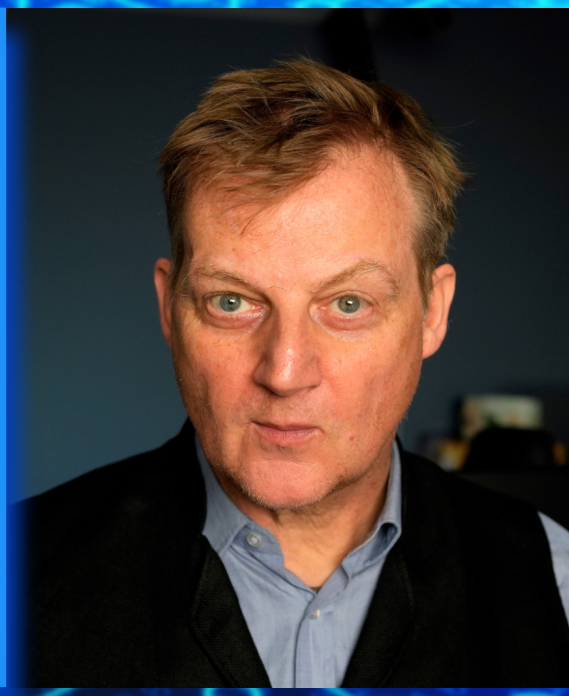
So geht's leichter...



Ciao Passwörter
Hallo Passkeys

- **Einfach. Sicher. Jetzt.**
- **Nie mehr Passwörter vergessen**
- **Auf allen Geräten sicher einrichten**
- **Passwortklau adé**
- **Einfacher als gedacht**

Jörg Schieb

Autoren:
Jörg Schieb
Andreas Erle

Impressum:
Redaktion schieb.de
Humboldtstr. 10
40667 Meerbusch
Kontakt: fragen@schieb.de
www.schieb.de

So geht's leichter | Passkeys: Online-Konten sichern

schieb.de

Inhalt

So geht’s leichter | Passkeys: Online-Konten sichern

Passkey

Stell dir vor, du könntest dich in der digitalen Welt genauso einfach und sicher bewegen wie in deinem Zuhause. Kein Grübeln mehr über komplizierte Passwörter, keine Angst vor Datendiebstahl. Willkommen in der Ära der **Passkeys** – der Revolution, die deine Online-Sicherheit grundlegend verändern wird.

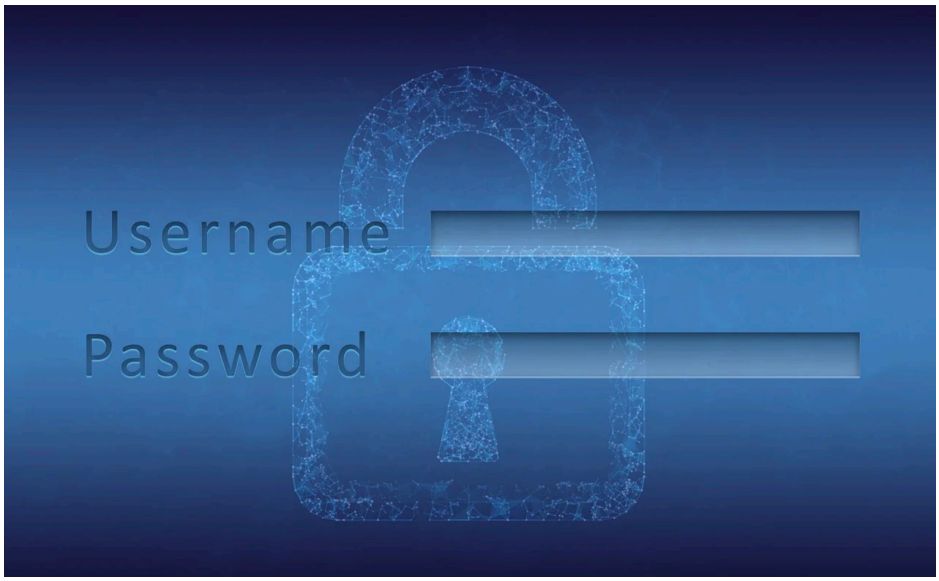
Seit den 1960er Jahren, als Passwörter erstmals in Computersystemen eingeführt wurden, haben sie unsere digitale Identität geschützt.

Doch mit der zunehmenden Vernetzung unseres Lebens zeigen sich ihre Schwächen: Sie sind oft zu einfach zu erraten, werden wiederverwendet oder fallen Phishing-Attacken zum Opfer. Die ständige Mahnung, komplexere Passwörter zu verwenden, hat uns in einen Teufelskreis aus Unsicherheit und Unbequemlichkeit getrieben.

So geht’s leichter | Passkeys: Online-Konten sichern

Passkeys versprechen, diesen Kreislauf zu durchbrechen. Sie kombinieren modernste Kryptographie mit der Einfachheit, die du von deinem Smartphone kennst.

Aber wie funktionieren sie genau? Welche Vorteile bieten sie im Vergleich zu herkömmlichen Methoden? Und was bedeutet ihre Einführung für deine tägliche Online-Routine? In diesem eBook tauchen wir ein in die Welt der Passkeys und zeigen dir, wie du schon heute von dieser bahnbrechenden Technologie profitieren kannst.



Passkeys sind also eine interessante Alternative, die deutlich mehr Sicherheit verspricht. Passkeys werden von immer mehr Diensten und Webseiten unterstützt.

Eine sehr umfangreiche Liste der Dienste findet ihr hier: Diese Dienste unterstützen bereich die Anmeldung per Passkey.

So geht’s leichter | Passkeys: Online-Konten sichern

Was sind Passkeys und warum sind sie hilfreich?

Passkeys bieten dir eine einfachere und sicherere Alternative zu Passwörtern, die deine Online-Konten besser schützt und dir den Alltag erleichtert. Es lohnt sich wirklich, sich auf diese Technologie einzulassen. Sie bringt nur Vorteile.

Der Begriff Passkey setzt sich zusammen auf dem „Pass“ von Passwort und „Key“, dem englischen Wort für Schlüssel zusammen.

Einfach gesprochen sind Passkeys der Schlüssel zum passwortlosen Anmelden. Die Unterschiede zwischen Passkeys und Passwörtern findet ihr im nächsten Abschnitt.

Das Grundprinzip ist recht simpel: Wenn ihr Passkeys nutzt, dann gibt es keine Information mehr, die Euch Angreifer stehlen könntet, die ihr verlieren könntet oder die erraten werden können.

Der Abgleich findet zwischen dem Gerät statt, mit dem ihr euch anmeldet und dem Dienst, an dem ihr euch anmeldet. Ihr selbst seht

den Passkey nicht mal und kommt auch nicht an eine lesbare Version davon heran.

Die Idee dahinter: Sicherheit anwendbar zu machen.

Ihr erinnert euch an die diversen Artikel zu den Themen Passwortsicherheit, Datenlecks und Phishing erinnert. Die Anforderungen an die sichere Verwendung von Passwörtern sind sehr hoch und damit der Komfort für den Anwender eher gering.

Passkeys schaffen deutlich mehr Komfort: Ihr müsst euch keine Zahlen und Ziffern merken, nicht darauf achten, für jede Webseite ein eigenes Passwort zu verwenden und viele Vereinfachungen mehr:

Vorteile zu herkömmlichen Passwörtern

Passwörter sind nicht per se schlecht oder unsicher, sie benötigen nur eine Menge an Aufwand und Aufmerksamkeit von Euch. Darin unterscheiden sich Passkeys von Passwörtern:

- Passkeys müssen nicht lang und komplex sein, Passwörter in gewissem Maße schon.
- Passkeys sind in den Geräten gespeichert und nicht in eurem Kopf, sie können nicht vergessen werden.
- Passkeys unterscheiden sich automatisch von Konto zu Konto. Das Risiko des „ein Passwort für alle" besteht damit nicht.
- Passkeys sind unempfindlich gehen Phishing-Angriffe und Datendiebstahl, weil sie nicht ausgelesen oder abgegriffen werden können (mehr dazu im folgenden Abschnitt).

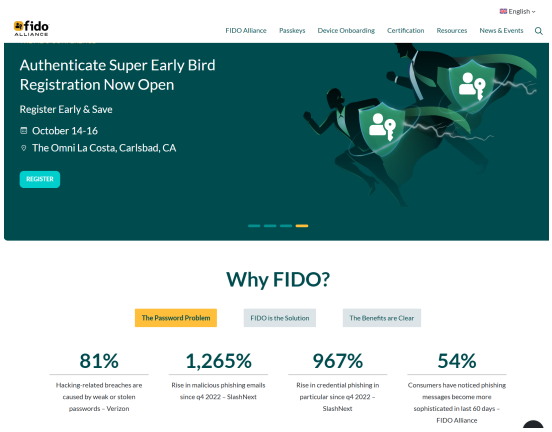
So geht’s leichter | Passkeys: Online-Konten sichern

Grundlagen der Passkey-Technologie

Was in der Einleitung so einfach klingt, hat natürlich einen technischen Hintergrund, der für die Sicherheit des Verfahrens sorgt. Ohne zu tief in die Details einzusteigen hier ein kurzer Überblick:

Die Rolle von FIDO2 und WebAuthN

Ein Verfahren wie Passkeys kann nur funktionieren, wenn die Partner, die es betreiben, vertrauenswürdig sind.



Hinter den Passkeys steht die FIDO Alliance (Fast Identity Online). Diese Allianz, ein Zusammenschluss von über 250 Unternehmen, darunter eben auch Apple, Google, Microsoft, Amazon und viele andere, entwickelt Standards für die Industrie, die die lizenzfrei eingesetzt werden können.

Viele große Unternehmen und Netzwerke sind Mitglieder. Das sorgt dafür, dass neue Sicherheitsmechanismen schnell und übergreifend eingeführt werden.

Technisch basieren Passkeys auf dem offenen FIDO2-Standard. Die Grundlage dafür ist das Web-Authentication Protocol (WebAuthN) und nutzt asymmetrische Kryptografie in Verbindung mit einem Challenge Response-Verfahren. Soweit der Technikteil, aber was bedeutet das?

So geht's leichter | Passkeys: Online-Konten sichern

Wie Passkeys funktionieren

Im Kern handelt es sich bei Passkeys um digitale Schlüssel, die das herkömmliche Passwort ersetzen sollen. Statt sich einen kryptischen Mix aus Buchstaben, Zahlen und Sonderzeichen merken zu müssen, übernimmt das Smartphone oder der Computer die sichere Anmeldung.

Das Prinzip: Für jede Website, bei der man sich registriert, wird ein eigenes Schlüsselpaar erzeugt. Der öffentliche Schlüssel liegt auf den Servern des Anbieters, während der private Schlüssel das Gerät nicht verlässt.

Beim Login gleichen sich die beiden Hälften ab und gewähren nur bei Übereinstimmung den Zugang zum Konto – einfach per Fingerabdruck, Gesichtsscan oder PIN-Eingabe.

Ein wichtiger Aspekt bei der Funktionsweise von Passkeys ist die Ende-zu-Ende-Verschlüsselung. Die privaten Schlüssel verlassen nie das eigene Gerät und werden auch nicht an die Server des Anbieters übertragen. Selbst wenn diese gehackt werden, sind die Anmeldedaten nicht kompromittiert:

- Wenn ihr euch auf einer Webseite per Passkey anmeldet, dann müsst ihr euch mit dem Gerät erst einmal für die Nutzung des Passkeys registrieren.
- Die Webseite erzeugt ein neues Schlüsselpaar, das aus einem öffentlichen und einem privaten, geheimen Schlüssel besteht. Das Verfahren kennt ihr vielleicht aus der Verschlüsselung bzw. Signierung von E-Mails.
- Der private Schlüssel bleibt sicher bei euch, der öffentliche Schlüssel wird auf der Webseite hinterlegt.

So geht’s leichter | Passkeys: Online-Konten sichern

- Für jede Webseite wird für jeden Benutzer ein eigenes Schlüsselpaar erzeigt, jeder Passkey ist also einzigartig und damit kaum zu fälschen.

Wenn ihr euch nach der initialen Anmeldung an der Webseite mit eurem Passkey anmeldet, dann funktioniert es wie bei einem Ratespiel:

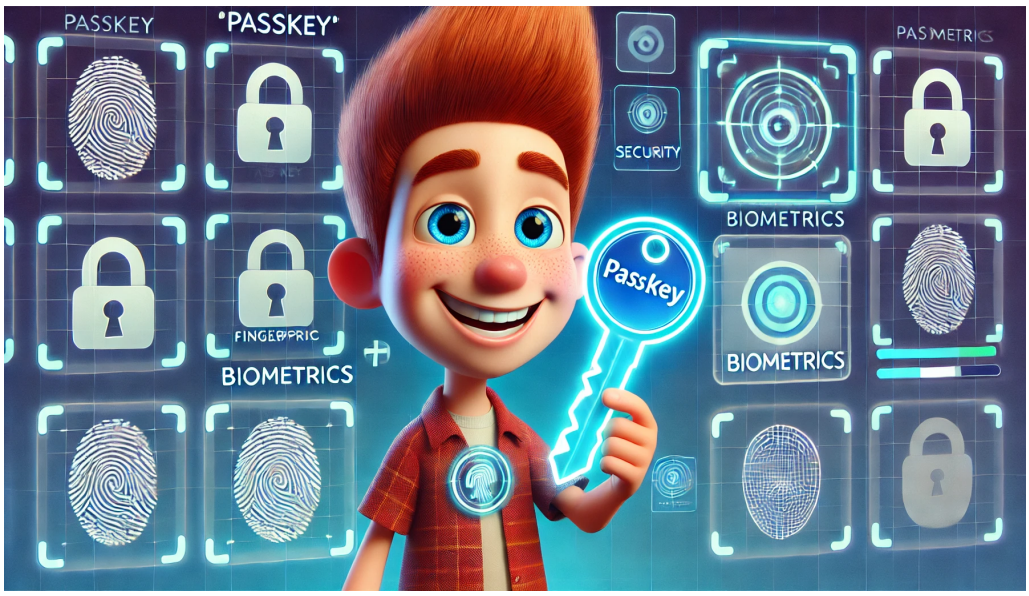
- Die Webseite schickt eine zu lösende Aufgabe an das Gerät, das sich anmelden soll.
- Das Gerät löst diese Aufgabe und nutzt dafür den geheimen Schlüssel, der ja auf ihm selbst gespeichert ist. Die so erzeugte Antwort schickt es wieder zurück.
- Die Webseite wiederum kann über den bei ihr vorliegenden öffentlichen Schlüssel diese Antwort entschlüsseln und überprüfen, ohne den privaten Schlüssel zu kennen.

So geht's leichter | Passkeys: Online-Konten sichern

- Ist die Antwort korrekt, dann hat sich euer Gerät erfolgreich „ausgewiesen" und die Webseite gewährt ihm (und damit euch) Zugriff.

Zwei-Faktor-Authentifizierung: Trotzdem!

Was auf den ersten Blick wie eine runde Lösung klingt, die alle anderen Sicherungsmechanismen überflüssig macht, hat natürlich auch einen kleinen Haken, der sich aber über bekannte Maßnahmen beseitigen lässt:



Schon bei den Passwörtern war das Prinzip von Wissen und Besitz ein zusätzlicher Sicherheitsfaktor:

- Das Passwort müsst ihr kennen, um es eingeben zu können („Wissen"). Das können aber natürlich auch Unbefugte erfahren, dies es dann auch wissen.
- Um das zu umgehen, wird als zweiter Faktor oft das Smartphone verwendet, dem zusätzlich nach Eingabe des Passworts eine SMS

mit einem zufälligen Zahlencode geschickt wird. Euer Smartphone hat ein Angreifer natürlich nicht („Besitz").

Passkeys konzentrieren sich vor allem auf den Besitz, denn der private Schlüssel ist ja auch eurem Gerät gespeichert. Kommt das abhanden, dann könnte sich der neue Besitzer damit an den per Passkey gesicherte Webseiten anmelden.

Aus diesem Grund verlangt die Anmeldung per Passkey ebenfalls einen zweiten Faktor und nutzt dabei die Mechanismen, die auf dem Smartphone ohnehin genutzt werden: Die PIN oder Biometrie wie Gesichtserkennung oder der Fingerabdruck. Ihr müsst eine dieser Sicherheitsmethoden aktiviert haben und nutzen, wenn ihr euch per Passkey anmeldet.

Passkeys bei Google-Konten

Google bietet eine Vielzahl von Diensten, Apps und Geräten an, die sich tief in euer tägliches Leben integrieren und eine große Menge sensibler und vertraulicher Daten enthalten. Wenig verwunderlich, dass Passkeys hier schon seit einiger Zeit verfügbar sind:

So geht’s leichter | Passkeys: Online-Konten sichern

Passkeys im Google-Konto aktivieren

Schon 2023 hat sich Google entschieden, für alle seine Dienste und alle Google-Konten weltweit die Verwendung von Passkeys zu aktivieren. Ein „Kann“, kein „Muß“, denn wenn ihr lieber weiterhin mit Passwort und zweitem Faktor arbeiten wollt, ist das weiterhin möglich.

Google geht hier noch ein wenig weiter: Neben der Anmeldung erlaubt die Verwendung von Google Passkeys auch den Nachweis der Identität bei Diensten, die das unterstützen.

Voraussetzungen

Wenn ihr entweder euer Konto sowieso schon für die Zwei-Faktor-Authentifizierung eingerichtet habt oder am erweiterten Sicherheitsprogramm von Google teilnehmt, dann könnt ihr auf diesen zweiten Bestätigungsschritt verzichten.

So geht’s leichter | Passkeys: Online-Konten sichern

Wenn ihr einen Passkey bei Google erstellen wollt, dann müsst Ihr einige Voraussetzungen erfüllen:

- Bei jedem Gerät müssen die Displaysperre (die ja nicht nur das Smartphone, sondern auch der Desktop-PC/Tablet verwenden) aktiviert sein.
- Bei einem Smartphone, das zur Anmeldung mit einem darauf gespeicherten Passkey am PC genutzt werden soll, muss Bluetooth aktiviert sein, auf dem stationären Gerät auch.
- Alternativ könnt ihr auch einen Hardware-Sicherheitsschlüssel verwenden, der das FIDO2-Protokoll unterstützt (mehr dazu später).
- Bei iOS und macOS muss der iCloud-Schlüsselbund verwendet werden, weil dieser zur Speicherung des privaten Schlüssels verwendet wird.

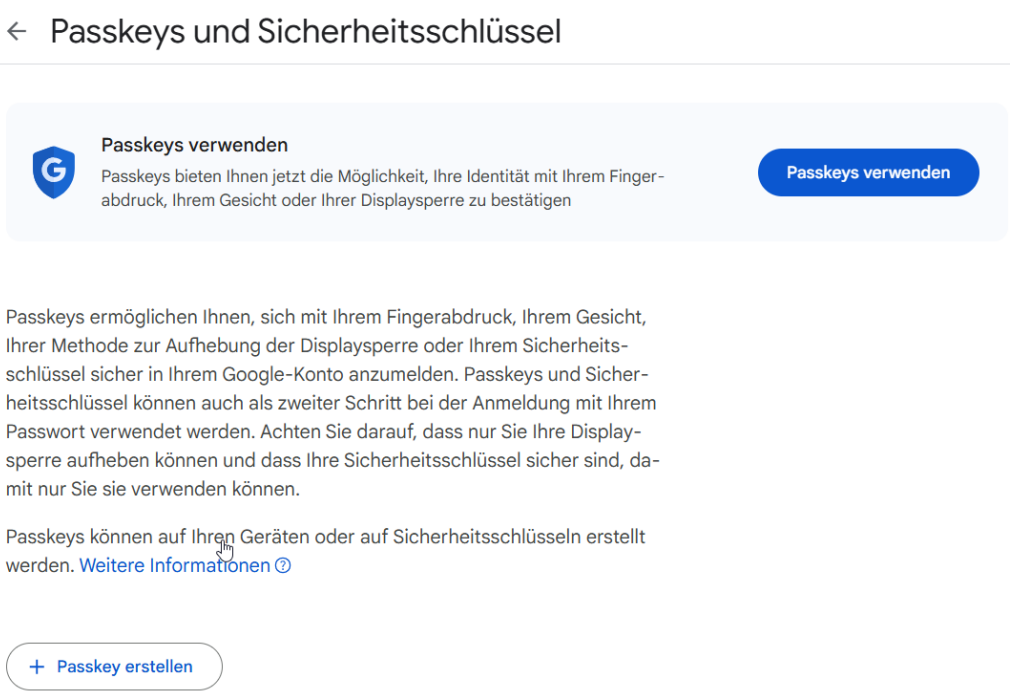
Auch an den Browser bestehen einige Anforderungen, ihr benötigt einen der folgenden Browser ab der angegebenen Version:

- Chrome 109 oder höher
- Safari 16 oder höher
- Edge 109 oder höher
- Firefox 122 oder höher

Allgemein gilt: Bevor ihr Passkeys anlegt, aktualisiert alle Geräte und Apps auf die jeweils aktuelle Version!

So geht's leichter | Passkeys: Online-Konten sichern

WICHTIG: Passkeys solltet ihr nur auf „privaten" Geräten anlegen. Das können durchaus auch beruflich genutzte Geräte sein, wichtig ist nur, dass ihr alleine den Zugang dazu habt. Wenn ihr das Gerät mit anderen Anwendern teilt, dann haben die ja Zugriff auf das Gerät und auf die PIN/das Passwort und können damit ungehindert eure Passkeys nutzen!



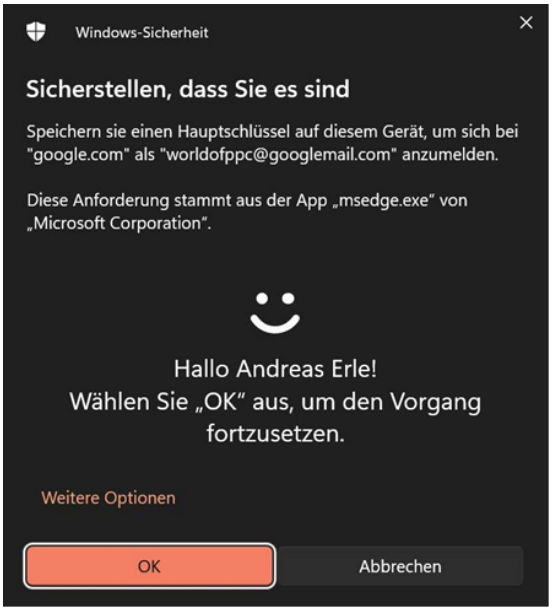
Anlegen eines Passkeys

Zum Anlegen eines Passkeys benötigt ihr nur die Zugangsdaten zu eurem Google-Account und ein Gerät, das die oben beschriebenen Anforderungen für Passkeys erfüllt.

- ☐ Öffnet die Passkey-Webseite von Google.

So geht's leichter | Passkeys: Online-Konten sichern

- Solltet ihr bisher nicht mit eurem Google-Konto angemeldet sein, dann holt das auf Aufforderung nach.
- Um einen neuen Passkey anzulegen, klickt auf der Seite unter dem Text auf **+ Passkey erstellen**.
- Ihr könnt jetzt entscheiden, ob ihr den Passkey auf dem aktuellen Gerät erstellen wollt. In dem, Fall klickt auf **Passkey erstellen**.



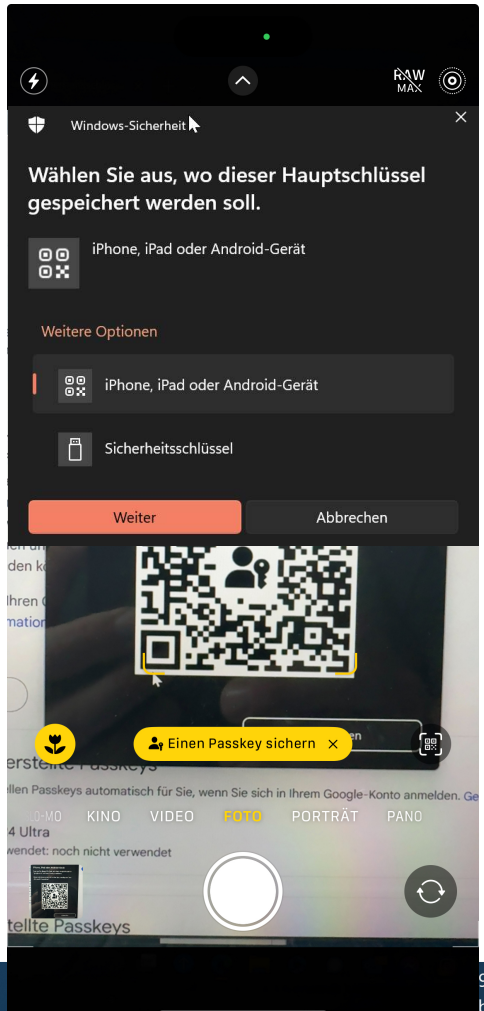
- Bestätigt, dass ihr einen Passkey erstellen wollt.
- Google nutzt nun die Sicherheitsmechanismen des Geräts, auf dem ihr euch anmeldet: Bei Windows Hello (mit Gesichtserkennung, PIN, Fingerabdruck), bei macOS den Schlüsselbund etc.
- Wenn ihr eine Fehlermeldung bekommt, dass auf dem entsprechenden Gerät kein Passkey erstellt werden kann, dann liegt das meist daran, dass dieses gerade nicht auf die biometrischen Sensoren zugreifen kann. Ein beliebter Fehler: Ihr habt euer Notebook mit Windows Hello-Gesichtserkennung zugeklappt und an einen Monitor angeschlossen. In dem Fall kann die Gesichtserkennung nicht gestartet werden, die ist aber für die Erzeugung des Passkeys nötig!

So geht’s leichter | Passkeys: Online-Konten sichern

- Die Lösung: Klappt das Notebook auf und startet den Prozess neu!

Wenn ihr möchtet, dass der Passkey/Hauptschlüssel nicht auf dem Desktop gespeichert wird, sondern auf einem anderen Gerät, dann müsst ihr etwas anders vorgehen:

- Klickt im ersten Menü auf **Anderes Gerät verwenden**.
- Ihr könnt nun auswählen, ob ihr ein Android-, ein iOS-Gerät oder einen Hardware-Sicherheitsschlüssel verwenden wollt. Im Normalfall werdet ihr euer Handy verwenden.
- Klickt auf **Weiter**.
- Google zeigt euch nun einen QR-Code an. Öffnet die Kamera-App auf dem Handy und richtet die Kamera auf den QR-Code.
- Dieser wird von allen gängigen mobilen



So geht's leichter | Passkeys: Online-Konten sichern

Betriebssystemen erkannt und gelb eingerahmt. Darunter seht ihr einen gelben Text „Einen Passkey sichern". Tippt darauf.

- Je nach der Konfiguration eures Smartphones fragt Google euch jetzt, wo ihr den Schlüssel speichern wollt. Normalerweise ist das der Standard-Passwortspeicher des Geräts, bei iOS also der Schlüsselbund. Wenn ihr aber den Microsoft Authenticator installiert habt, dann könnt ihr auch festlegen, dass dieser stattdessen verwendet wird.
- Ihr müsst euch dann am Gerät einmal authentifizieren (indem ihr den Fingerabdruck auflegt oder das Gesicht scannen lasst), dann wird der Passkey im Google-Konto gespeichert.

Tritt dabei ein Fehler auf, dass der Schlüssel nicht gespeichert werden kann, dann liegt das meist daran, dass ihr nicht mehrere Schlüssel für ein Gerät anlegen könnt:

- Wenn ihr erst den Passkey direkt auf dem PC anlegt, dann wird dieser dort gespeichert.
- Wenn ihr dann auf demselben PC einen Passkey anlegt und dafür das iPhone nutzt, dann ist das ja immer noch dasselbe Konto und dasselbe Gerät, das ihr mit einem Passkey schützt.
- In einem solchen Fall löscht den Passkey, den ihr auf dem PC angelegt habt und erstellt ihn dann neu auf dem Smartphone, wie oben beschrieben.

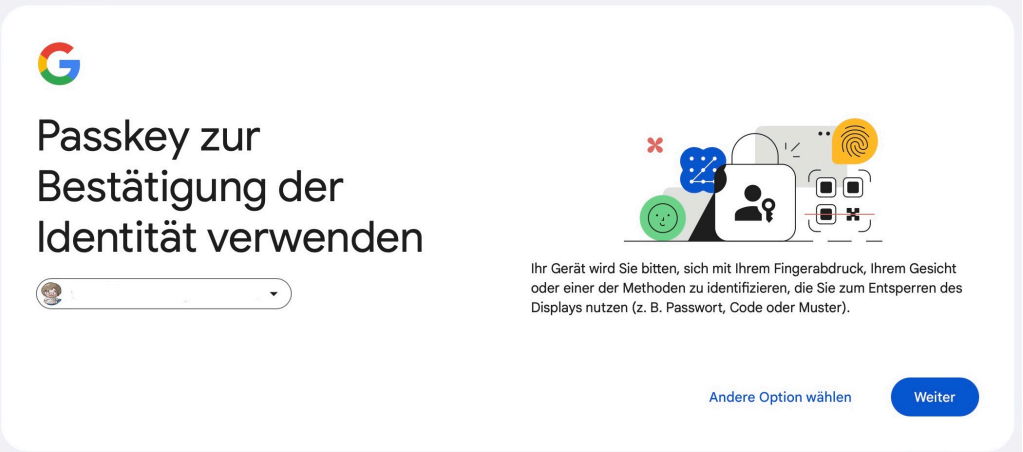
Anmeldung mit Passkeys bei Google-Diensten

Die Google-Dienste haben einen großen Vorteil: Sie nutzen alle dieselben Mechanismen. Ob ihr euch im Internet an eurem Google-Konto anmeldet, Google Drive als Cloud-Speicher nutzt oder mit

So geht’s leichter | Passkeys: Online-Konten sichern

Google Docs ein Dokument erstellt: Google erkennt, dass ihr für das Konto auf dem Gerät einen Passkey vergeben habt und nutzt diesen – es sei denn, ihr bestimmt aktiv etwas anderes:

- Geht auf die Webseite des Google-Dienstes, an dem ihr euch anmelden wollt.
- Klickt auf **Login** und gebt dann Eure Google E-Mail-Adresse ein.
- Der Dienst schaut nun in euren Kontoeinstellungen nach, ob ihr bereits einen Passkey vergeben habt. Ist das der Fall, dann wird dieser als Standard-Anmeldemethode angeboten:



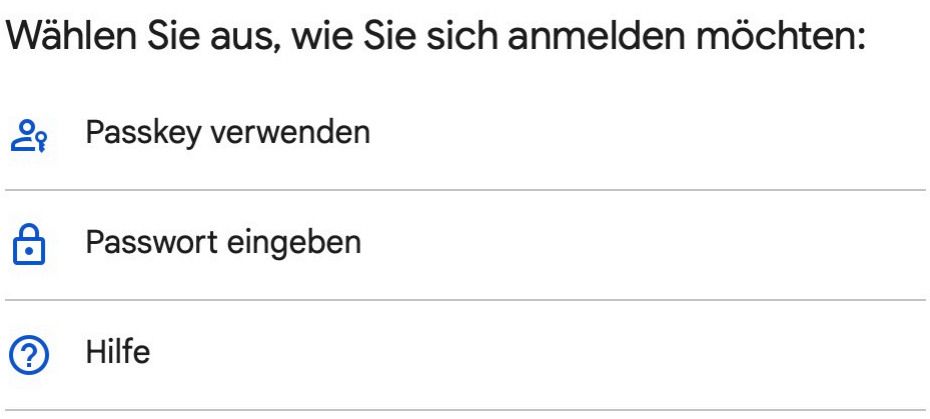
- Klickt dann auf **Weiter**.
- Jetzt kommt es darauf an, welche Art von Gerät ihr verwendet: Bei einem Mac reicht es, dass der Passkey im Schlüsselbund gespeichert ist, die Anmeldung erfolgt ohne weitere Abfrage.
- Wenn ihr den Passkey auf dem Smartphone gespeichert habt, muss dieses mit Bluetooth mit dem PC Verbindung aufnehmen können und kann dann die Freigabe erteilen.

So geht’s leichter | Passkeys: Online-Konten sichern

- Auf einem Windows-PC wird automatisch Windows Hello gestartet und ihr müsst euch mit Fingerabdruck oder Gesichtserkennung authentifizieren.
- Egal, um welches Gerät es sich handelt: Ihr müsst keine Informationen über die Tastatur eingeben, die Anmeldung funktioniert rein über die Verwendung des gespeicherten Passkeys und Biometrie!

Nun mag es Gelegenheiten heben, bei denen ihr den Passkey nicht nutzen könnt oder wollt. Beispielsweise, weil ihr ihn auf dem Smartphone gespeichert habt, das aber liegt zu Hause. In diesem Fall wäre guter Rat teuer, wenn ihr nicht alternative Anmeldemethoden anwählen könntet.

- Geht auf die Webseite des Google-Dienstes, an den ihr euch anmelden wollt.
- Klickt auf **Login** und gebt dann Eure Google E-Mail-Adresse ein.
- Wenn Google euch den Passkey anbietet, dann klickt auf **Andere Option wählen**.



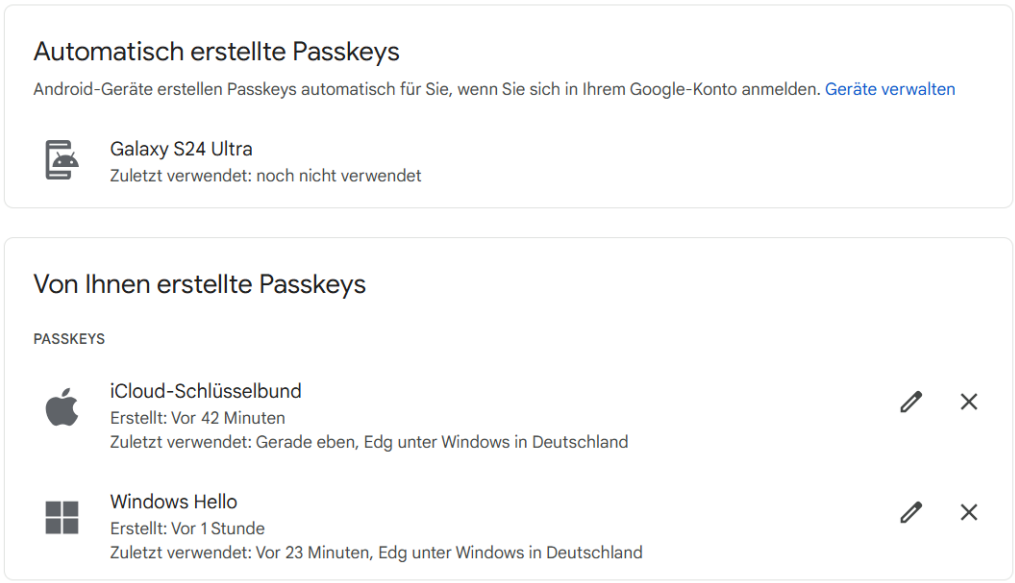
So geht’s leichter | Passkeys: Online-Konten sichern

- Klickt auf Passwort eingeben, um euch ganz normal mit dem Passwort anzumelden. Wichtig: Wenn ihr das noch nicht gemacht habt, dann aktiviert auf jeden Fall die Zwei-Faktor-Authentifizierung, um zumindest einen gewissen zusätzlichen Schutz zum Passwort zu haben.

Verwaltung von mit Passkeys im Google-Konto

Auch Passkeys haben eine gewisse Halbwertszeit. Wenn diese abgelaufen ist und etwa ein Gerät nicht mehr existiert oder ihr den Überblick verliert, dann könnt ihr die Passkeys eures Google-Kontos bearbeiten:

- Öffnet die Passkey-Webseite von Google.
- Solltet ihr bislang nicht mit eurem Google-Konto angemeldet sein, dann holt das auf Aufforderung nach.
- Google zeigt euch jetzt all eure Passkeys in einer Übersicht an:



So geht's leichter | Passkeys: Online-Konten sichern

- Im oberen Teil der Übersicht seht ihr alle Android-Geräte in eurem Google-Konto. Diese haben die Besonderheit, dass sie automatisch einen Passkey erzeugen. Diese könnt ihr durch einen Klick auf **Geräte verwalten** in der Übersicht der Geräte löschen.
- Unter von Ihnen erstellte Passkeys seht ihr alle Passkeys, die ihr auf Geräten für euer Google-Konto angelegt habt.
- Wenn ihr viele Geräte verwendet, dann macht es Sinn, den einzelnen Passkeys einen Namen zu geben. Dazu klickt auf den **Stift** neben dem entsprechenden Passkey und gebt einen sprechenden Namen ein, sinnvollerweise den Gerätenamen.
- Wenn ihr einen Passkey deaktivieren wollt, dann klickt stattdessen auf das X neben dem Passkey. Dieser wird dann aus eurem Google-Konto gelöscht und das zugehörige Gerät kann sich nicht mehr an eurem Google-Konto anmelden.
- Um für das Gerät wieder eine Anmeldung per Passkey zu erlauben, müsst ihr dann einfach nur einen neuen Passkey anlegen. Reaktivieren lässt sich der gelöschte nicht mehr.

Passkeys auf Geräten und Plattformen

Passkeys haben den Vorteil, dass sie aufgrund der dahinterliegenden Technologie nicht audf ein spezielles Gerät beschränkt sind. Da die meisten Hersteller der FIDO-Alliance angeschlossen sind, unterstützen die allermeisten Betriebssysteme, Apps und Dienste die Anmeldung darüber. Unterschiede gibt es aber natürlich in der Konfiguration und Anwendung:

So geht's leichter | Passkeys: Online-Konten sichern

Verwendung von Passkeys auf dem Smartphone

Immer mehr Internetverkehr wandert von PC auf das Smartphone. Klar, schließlich habt ihr das immer dabei und werdet immer mobiler. Android und iOS unterstützen beide die native Verwendung von Passkeys.

Android

Passkeys auf Android passen sich nahtlos in die ohnehin schon vorhandene Integration aller Google-Dienste ein. Um einen neuen Passkey anzulegen, ruft einfach die Webseite des Dienstes auf und meldet euch an.

Um Passkeys nutzen zu können, müsst ihr den Google-Passwortmanager aktivieren:

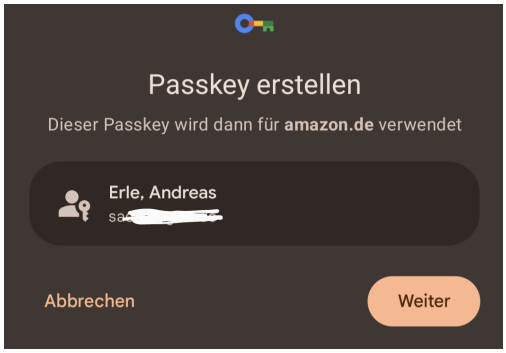
- Streicht von oben nach unten über den Bildschirm und tippt dann auf das Zahnrad. Alternativ öffnet sie Einstellungen über die App-Übersicht.
- Der Weg zu den Passworteinstellungen unterscheidet sich zwischen den einzelnen Android-Versionen. Bei Android 14 tippt auf **Passwörter und Konten**.

- Aktiviert dann den Schalter neben **Google**.

Das Anlegen eines neuen Passkeys funktioniert wieder über die Webseite des Anbieters oder Dienstes:

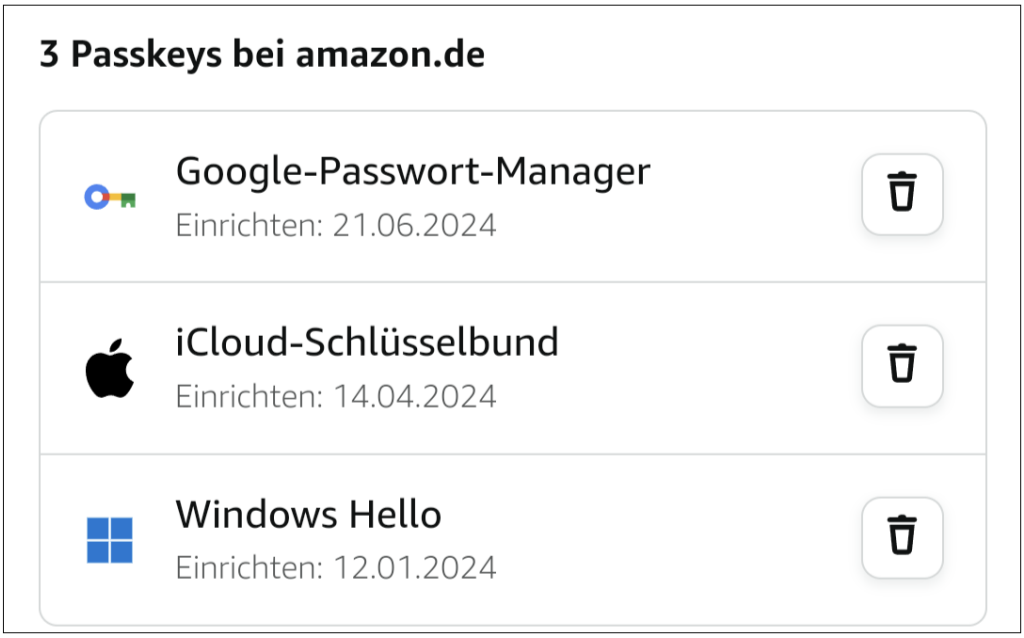
So geht’s leichter | Passkeys: Online-Konten sichern

- Entweder findet ihr schon direkt auf dem Anmeldebildschirm die Option, einen Passkey anzulegen, oder sie wird euch nach der Anmeldung angeboten.
- Ist das nicht der Fall, dann sucht sie in eurem Konto unter **Passwörter und Sicherheit**.
- Tippt auf **Weiter**, um den Passkey anzulegen.
- Meldet euch per Fingerabdruck oder Gesichtsscan (je nach Gerät) an eurem Smartphone an.



- Der Passkey wird automatisch gespeichert. Da Google automatisch die Synchronisation mit den Passwörtern im Google-Account aktiviert, findet ihr den neuen Passkey dann unter „Google Passwort Manager“.

So geht's leichter | Passkeys: Online-Konten sichern



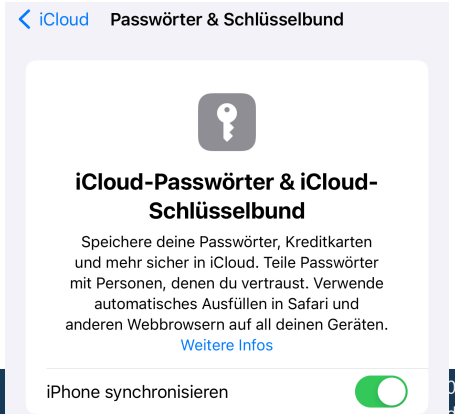
Passkeys unter iOS

Die Voraussetzung für die Nutzung von Passkeys auf einem iPhone oder iPad sind gering. Ihr benötigt:

- Mindestens iOS/iPadOS 16
- Der iCloud-Schlüsselbund muss aktiviert sein.
- Die Zwei-Faktor-Authentifizierung muss ebenfalls aktiviert sein.

Der iCloud-Schlüsselbund aktiviert ihr so:

- Öffnet die Einstellungen des iPhones.
- Tippt auf euer Kontobild ganz oben, um die iCloud-Einstellungen zu öffnen.

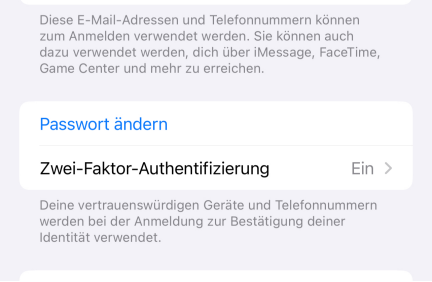


So geht’s leichter | Passkeys: Online-Konten sichern

- Tippt auf **iCloud** > **Passwörter & Schlüsselbund**.
- Tippt auf den Schalter neben **iPhone synchronisieren**, wenn dieser nicht bereits aktiviert ist. Der iCloud Schlüsselbund wird aktiviert.

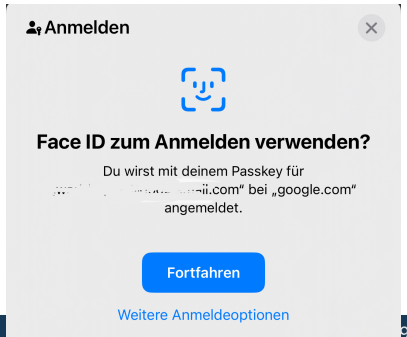
Die Zwei-Faktor-Authentifizierung (bei der ihr bei der Anmeldung mit der Apple ID ein anderes Apple-Gerät oder ein Telefon zum Empfang eines Codes als zweiten Faktor benötigt, aktiviert ihr so:

- Tippt in den iCloud-Einstellungen auf **Anmeldung und Sicherheit**.
- Dann könnt ihr – so das nötig ist – noch die vertrauenswürdigen Nummern bearbeiten.



Das Erzeugen eines Passkeys für eine Webseite oder Dienst wird meist automatisch angestoßen, wenn Passkeys unterstützt werden:

- Meldet euch bei dem Dienst an.
- Dieser fragt euch nach erfolgreicher Anmeldung, ob ihr einen Passkey erzeugen wollt, wenn das bis jetzt nicht geschehen ist, bestätigt das.
- Das iPhone fordert euch nun auf, euch mit Gesichtserkennung, Fingerabdruck oder PIN anzumelden, um eure Identität zu bestätigen.
- Habt ihr das erfolgreich gemacht, dann wird der Passkey auf dem iPhone gespeichert und lässt sich



So geht's leichter | Passkeys: Online-Konten sichern

bei den folgenden Anmeldungen direkt nutzen.

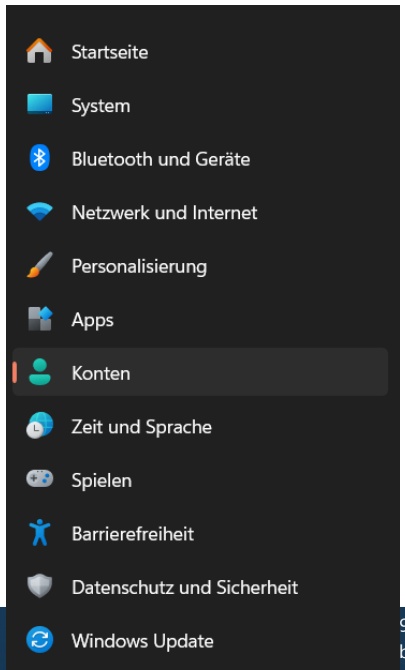
- Bietet die Seite das Anlegen eines Passkeys nicht direkt an, dann hilft es oft, in den Kontoeinstellungen nachzusehen und dann – wie oben am Beispiel Google beschrieben – die Erstellung des Passkeys manuell zu starten.
- Die Passkeys findet ihr wie die Passwörter unter **Einstellungen** > **Passwörter** unter der jeweiligen Webseite. Dort könnt ihr sie auch entfernen, wenn sie nicht mehr benötigt werden.

Passkeys auf dem Desktop-Computer

Wenn ihr einen Desktop-Computer wie einen Windows-PC oder Mac nutzt, dann gibt es zwei unterschiedliche Arten, wie Passkeys abgelegt werden. Den einen Teil findet ihr im Browser beziehungsweise auf der Webseite des Anbieters. Die Desktops speichern aber natürlich den privaten Teil des Passkeys lokal auf dem Rechner, und dort könnt ihr ihn verwalten.

Passkeys unter Windows

Im Gegensatz zum Smartphone habt ihr unter Windows keine Möglichkeit, die Passkeys zu erzeugen (das macht ihr im Browser des Geräts, wenn ihr auf die Seite zugreift. Natürlich könnt ihr sie aber ansehen und auch löschen:



So geht's leichter | Passkeys: Online-Konten sichern

- Wechselt in die **Einstellungen** von Windows, dann klickt auf der linken Seite auf **Konten**.
- Es wäre schön, wenn sich alle Anbieter auf eine Begrifflichkeit einigen könnten, das ist bei Passkeys leider nicht der Fall: Einige – und dazu auch Microsoft – haben den Begriff eingedeutscht. Klickt hier also auf **Hauptschlüsseleinstellungen**.
- Windows zeigt euch nun eine Übersicht der auf dem Gerät gespeicherten Passkeys/ Hauptschlüssel an. Über die Zeit wird deren Zahl stark zunehmen. Um einen bestimmten zu finden, gebt dessen Namen unter **Gespeicherte Hauptschlüssel** in das Suchfeld ein.
- Wenn ihr den Passkey löschen wollt, dann klickt auf die drei Punkte und dann auf **Hauptschlüssel löschen**.
- Um für das Gerät wieder eine Anmeldung per Passkey zu erlauben, müsst ihr dann einfach nur einen neuen Passkey anlegen. Reaktivieren lässt sich der gelöschte nicht mehr.

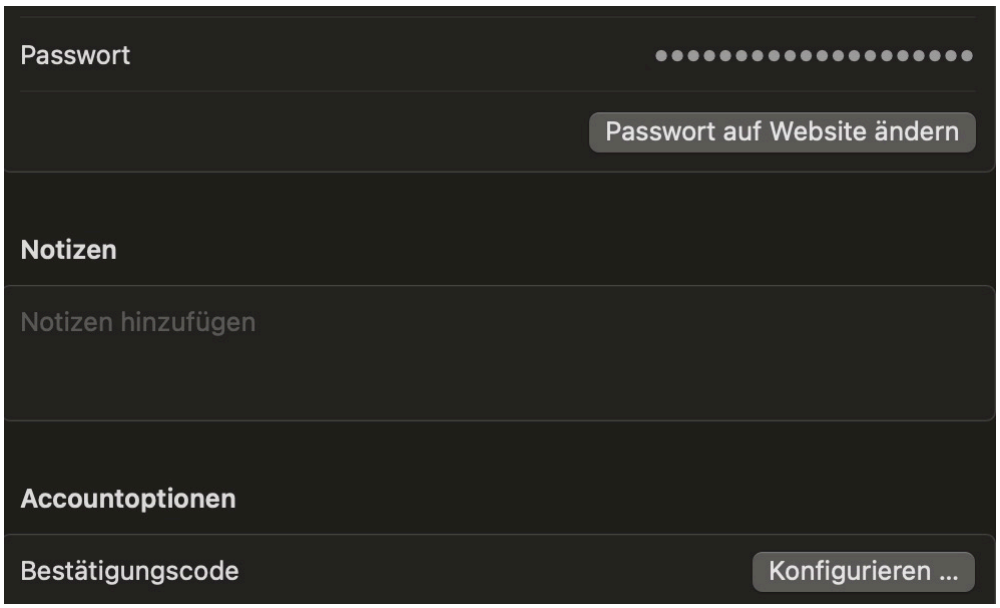
Passkeys unter macOS

Auch macOS auf MacBooks, Mac Minis und iMacs unterstützt Passkeys. Voraussetzung ist, dass die Geräte den Schlüsselbund aktiviert haben und einen zweiten Faktor verwenden können.

Bei Tastaturen mit Touch ID geht das direkt, alternativ könnt ihr euer iPhone nutzen. Das gilt am Ende nur für die initiale Erzeugung des Passkeys, danach reicht es aus, dass dieser im Schlüsselbund gespeichert ist.

So geht’s leichter | Passkeys: Online-Konten sichern

Im Gegensatz zum Smartphone habt ihr unter macOS keine Möglichkeit, die Passkeys zu erzeugen (das macht ihr im Browser des Geräts, wenn ihr auf die Seite zugreift und authentifiziert euch dann einmal).



Eine interessante Besonderheit von macOS ist der Wechsel von Passwort zu einem Passkey direkt aus den gespeicherten Passwörtern:

- Meldet euch am Mac an. Ruft dann im Browser eurer Wahl die Webseite an, auf der ihr das Passwort durch einen Passkey ersetzen wollt, und meldet euch dort an eurem Konto an.
- Klickt dann auf den **Apfel** oben links in der Titelleiste, dann auf **Systemeinstellungen**.
- Klickt unter dem ausgegrauten Bereich auf **Passwort auf Webseite ändern**.
- macOS führt euch direkt zur Passwortänderung. Hier könnt ihr dann stattdessen das Anlegen eines Passkeys auswählen.

So geht's leichter | Passkeys: Online-Konten sichern

Das Anmelden mit einem Passkey an einer Webseite oder bei einem Dienst ist bei macOS nichts anderes als würdet ihr ein Passwort verwenden:

- Ruft die Webseite auf, dann klickt auf den Link zur Anmeldung mit eurem Konto.
- Klickt in das Eingabefeld für den Benutzernamen, dann wählt den Account aus.
- Ist die Anmeldemethode für das Konto ein Passkey, dann verwendet macOS ihn automatisch.

Wollt ihr einen Passkey löschen? Dann wechselt wieder wie oben beschrieben in die Liste der Passwörter und klickt unten links auf **Passwort löschen**. Damit werden alle Zugangsdaten für den Account und die Seite gelöscht!

Passkeys im Web-Browser

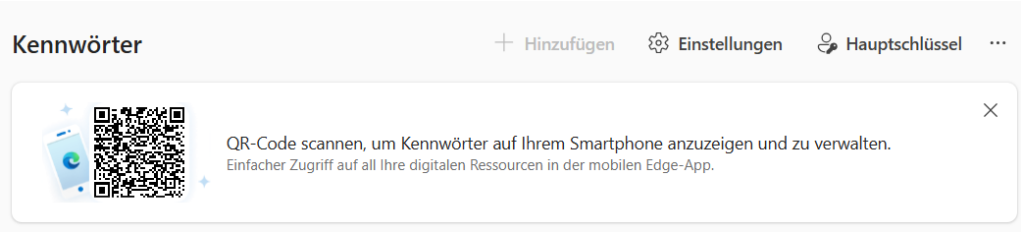
In den allermeisten Fällen werdet ihr mit einem Webbrowser auf die Seite zugreifen, für die ihr einen Passkey anlegt und über den ihr euch dann anmelden wollt. Die einzelnen Browser behandeln Passkeys unterschiedlich, wir haben euch für die vier Standard-Browser aufgelistet, wie ihr Passkeys verwenden könnt.

Microsoft Edge

Microsoft Edge ist der Standard-Browser von Windows und aus dem Grund damit tief verzahnt. Unter Windows erlaubt er direkt die Verwaltung der Passkeys:

So geht’s leichter | Passkeys: Online-Konten sichern

- Klickt auf die drei Punkte in Edge, dann auf **Einstellungen** > **Profile** > **Kennwörter**.
- Klickt dann oben rechts auf **Hauptschlüssel**.



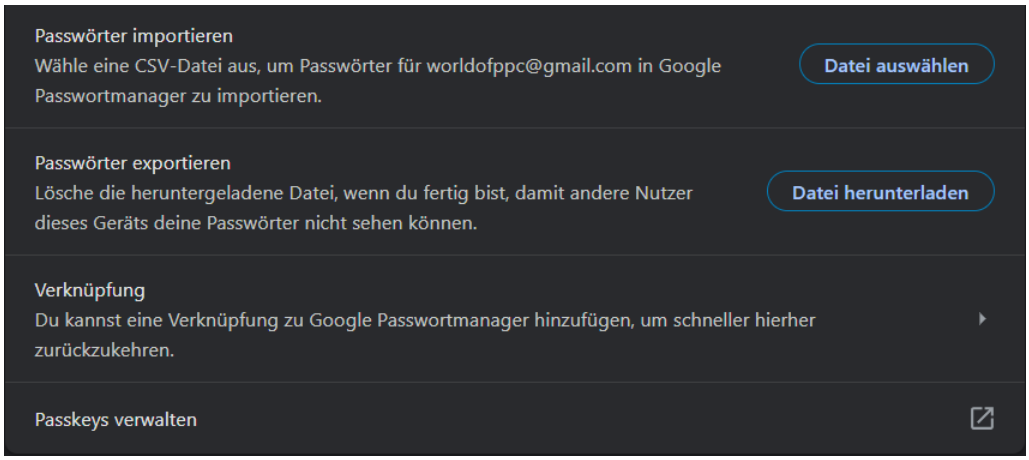
- Edge wechselt in die Windows-Einstellungen. Windows zeigt euch nun eine Übersicht der auf dem Gerät gespeicherten Passkeys/ Hauptschlüssel an. Über die Zeit wird deren Zahl stark zunehmen. Um einen bestimmten zu finden, gebt dessen Namen unter **Gespeicherte Hauptschlüssel** in das Suchfeld ein.
- Wenn ihr den Passkey löschen wollt, dann klickt auf die drei Punkte und dann auf **Hauptschlüssel löschen**.
- Um für das Gerät wieder eine Anmeldung per Passkey zu erlauben, müsst ihr dann einfach nur einen neuen Passkey anlegen. Reaktivieren lässt sich der gelöschte Passkey nicht mehr.
- Bei Edge auf anderen Plattformen müsst ihr die Verwaltung der Passkeys manuell über die Funktionen des Betriebssystems durchführen. Die haben wir euch oben ja schon beschrieben.

Google Chrome

Bei Google Chrome e ist der Weg zur Verwaltung von Passkeys ein wenig anders, auch wenn der Browser wie Microsoft Edge die Chromium-Engine nutzt:

So geht's leichter | Passkeys: Online-Konten sichern

- Klickt auf die drei Punkte in Chrome, dann auf **Einstellungen** > **Autofill und Passwörter** > **Google Passwortmanager**.
- Klickt dann oben links auf **Einstellungen**.
- Im sich öffnenden Menü klickt dann auf **Passkeys** verwalten.
- Chrome öffnet die eurem Betriebssystem entsprechende Seite der Passkeyverwaltung.



- Ihr seht nun eine Übersicht der auf dem Gerät gespeicherten Passkeys/ Hauptschlüssel an.
- Wenn ihr den Passkey löschen wollt, dann klickt auf die drei Punkte und dann auf **Hauptschlüssel löschen**.

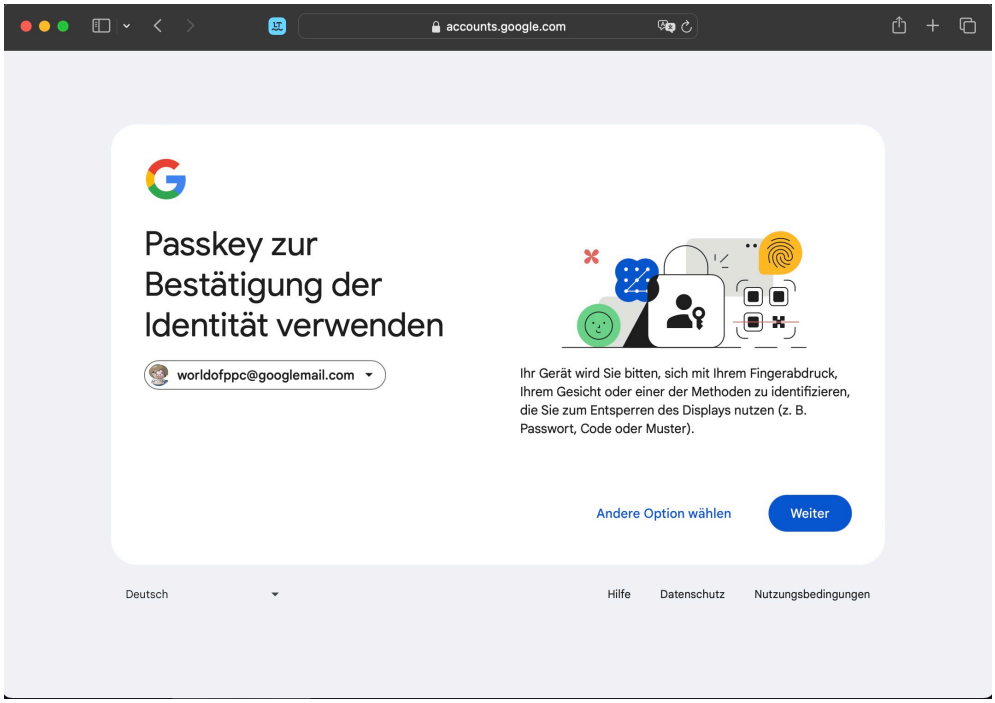
Mozilla Firefox und Safari

Firefox ist immer noch weitverbreitet, hat aber erst mit der Version 122 die Unterstützung von Passkeys bekommen. Solltet ihr Firefox schon ein wenig länger nutzen, dann führt auf jeden Fall ein Update aus!

Firefox hat allerdings keine separate Verwaltungsoberfläche für Passkeys. Hier bleibt euch nichts anderes übrig, als diese wie oben

So geht’s leichter | Passkeys: Online-Konten sichern

beschrieben über die internen Funktionen des Betriebssystems eurer Geräts zu verwalten.



Safari hat diese Möglichkeit schon ein wenig länger, verlässt sich aber wie Firefox ganz auf die Funktionen des Betriebssystems. Beide Browser funktionieren also alleine als Zugangsmedium zu den Webseiten und Diensten und reichen die Passkeys ans Betriebssystem weiter.

Passkeys sicher speichern und verwalten

Auch wenn Passkeys einen deutlich höheren Sicherheitsstandard bieten als Passwörter, unangreifbar sind sie natürlich nicht. Ihr solltet also auf die ein oder andere Vorgabe achten, damit diese auch sicher gespeichert sind und nicht von jemandem genutzt werden können, der auf euren Rechner zugreifen kann.

So geht's leichter | Passkeys: Online-Konten sichern

Speicherung von Passkeys im Gerät

‚Der Standardfall wird das Speichern der Passkeys im Gerät sein. Wobei diese Formulierung trügerisch ist: Am Ende speichert ihr ja „nur" den privaten Teil des Schlüssels auf dem Gerät, der dann mit dem auf der Webseite des Anbieters/Kontos gespeicherten öffentlichen Teil des Schlüssels zusammengebracht wird. Gerade der aber ist ja der kritischere der beiden Schlüsselteile.

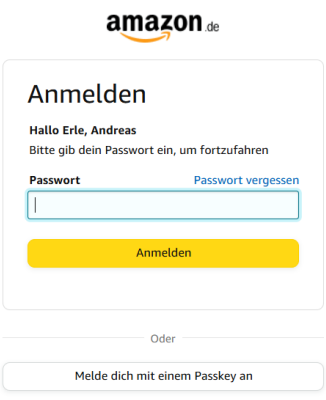
Im Gegensatz zu einem – nicht gespeicherten – Passwort verbleibt dieser aber auf jeden Fall auf dem Gerät. Stellt also sicher, dass euer Gerät mindestens mit einer PIN, idealerweise mit Biometrie geschützt ist. Das stellt sicher, dass ihr nur alleine darauf zugreifen könnt.

Wenn ihr das nicht sicherstellen könnt, weil der Rechner mit anderen Anwendern geteilt werden muss (und diese dann logischerweise die Zugangsdaten kennen), dann nutzt für die Speicherung des Passkeys stattdessen euer Smartphone:

Speichern eines Passkeys auf dem Smartphone

Wenn ihr einen PC mit anderen Anwendern teilen müsst, dann kann es eine Alternative sein, ein anderes Gerät, etwa euer persönliches Smartphone zu verwenden. Das zeigen wir euch am Beispiel von Amazon, das funktioniert aber mit allen anderen Webseiten genauso:

- Öffnet in eurem Browser die Webseite des Anbieters, hier Amazon.
- Klickt auf den Link zu eurem Kundenkonto. Bevor ihr das Passwort



So geht's leichter | Passkeys: Online-Konten sichern

eingebt, klickt darunter auf **Melde Dich mit einem Passkey an**.

- In der nun folgenden Eingabeaufforderung klickt unten auf **Verwenden eines anderen Geräts**.
- Beim ersten Mal müsst ihr den Passkey im Smartphone anlegen. Dazu klickt auf **iPhone, iPad oder Android-Gerät**.
- Die Webseite zeigt euch einen QR-Code an. Startet die Kamera-App des Smartphones und erfasst den QR-Code. Wenn darunter kein Text erscheint, dann tippt den QR-Code einmal an und tippt dann auf den Text im gelben Fenster **Mit einem Passkey…**.

- Euer Smartphone fordert euch jetzt einmal auf, euch zu authentifizieren und nutzt dazu Fingerabdruck, Gesicht oder PIN, so, wie es auf eurem Gerät konfiguriert ist.

Wenn ihr euch dann bei der Webseite das nächste Mal anmeldet, funktioniert die Anmeldung ganz ähnlich:

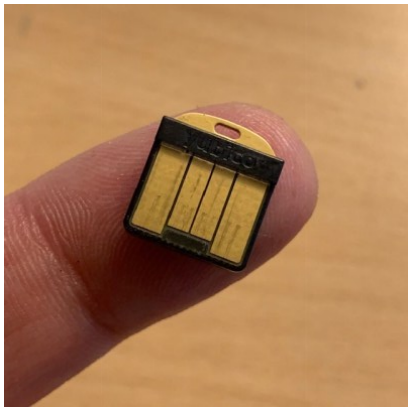
- In der Eingabeaufforderung klickt unten auf **Verwenden eines anderen Geräts**, dann auf **iPhone, iPad oder Android-Gerät**.
- Ihr bekommt wieder einen QR-Code angezeigt, öffnet den wie oben beschrieben in der Kamera-App des Smartphones und tippt auf den Link zur Anmeldung.
- Nach der Authentifizierung mit Fingerabdruck, Gesicht oder PIN am Smartphone führt die Webseite die Anmeldung automatisch

So geht's leichter | Passkeys: Online-Konten sichern

durch. Der Passkey ist aber nicht auf dem PC, sondern auf dem Smartphone gespeichert!

Verwendung von FIDO-Keys

Wo früher noch eine Smartcard oder ein großer USB-Stick nötig waren, hat die Miniaturisierung ebenfalls Einzug gehalten: Security Keys haben heute oft nur die Größe eines Fingernagels und können an einem normalen USB- oder sogar USB-C-Anschluss verwendet werden.

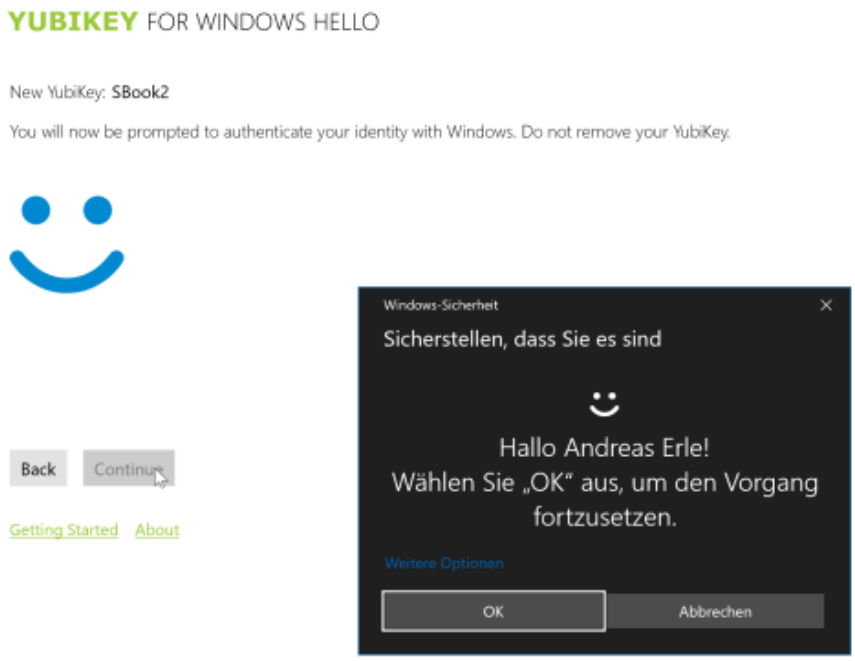


Wichtig dabei: Windows 11 beziehungsweise das verwendete Betriebssystem muss diese auch unterstützen! Für Android- und iOS-Geräte der neueren Generationen lassen sich diese auch per USB-C anschließen

Nicht viele Sicherheit-Tokens unterstützen auch die Anmeldung bei Windows 10/11 direkt. Yubicos Yubikeys erreichen dies durch eine separate Windows Store-App, die dem Anmeldebildschirm von

So geht's leichter | Passkeys: Online-Konten sichern

Windows 11 eine weitere Authentifizierungsmethode hinzufügt.



Einmal konfiguriert wird der Anmeldebildschirm automatisch geschlossen, wenn das Token bei der Anmeldung eingelegt ist. Keine Passworteingabe mehr, denn die Berechtigung für die Anmeldung an Ihren PC ist mit der initialen Einrichtung auf dem Token abgelegt worden.

Noch interessanter ist die Nutzung mit Diensten, die FIDO unterstützen. Bei der Registrierung der FIDO-Unterstützung bei einem Dienst wird auf dem Rechner des Benutzers ein Schlüsselpaar generiert. Der öffentliche Schlüssel geht an den Dienst, der private bleibt alleine auf dem Token. Das Token wiederum wird dann noch einmal geschützt, beispielsweise durch einen Fingerabdruck.

Bei der Anmeldung wird dann die Anfrage zur Anmeldung vom Server auf dem PC des Benutzers verschlüsselt und an den Dienst gesendet. Der Dienst kann diese mit dem öffentlichen Schlüssel entschlüsseln und

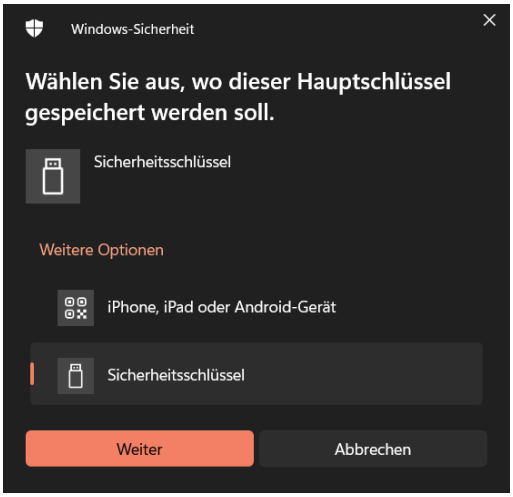
So geht's leichter | Passkeys: Online-Konten sichern

damit die Identität des Anmeldenden bestätigen. Der private Schlüssel bleibt immer beim Benutzer. Auch diese Anmeldeart wird von Windows 11 direkt unterstützt.

Kommt euch bekannt vor? Genau, das ist das Prinzip der Passkeys. Und folgerichtig könnt Ihr FIDO-Keys auch als externen, sicheren Speicher für Passkeys nutzen:

Zum Anlegen eines Passkeys auf einem externen Sicherheitsschlüssel benötigt ihr nur die Zugangsdaten zu eurem Google-Account und eben den FIDO-Key. Am Beispiel von Google:

- Öffnet die Passkey-Webseite von Google.
- Solltet ihr bislang nicht mit eurem Google-Konto angemeldet sein, dann holt das auf Aufforderung nach.
- Um einen neuen Passkey anzulegen, klickt auf der Seite unter dem Text auf **+ Passkey erstellen**.



- Um den Passkey nicht lokal, sondern auf dem FIDO-Key zu erstellen, klickt auf **Anderes Gerät verwenden** und dann auf **Sicherheitsschlüssel**.
- Bestätigt, dass ihr einen Sicherheitsschlüssel konfigurieren wollt und dann auf **OK**.
- Ihr müsst nun den Sicherheitsschlüssel in einen USB-Port einlegen und erkennen lassen. Google greift darauf zu und prüft, ob dieser geeignet ist. Klickt dazu auf **OK**.

So geht's leichter | Passkeys: Online-Konten sichern

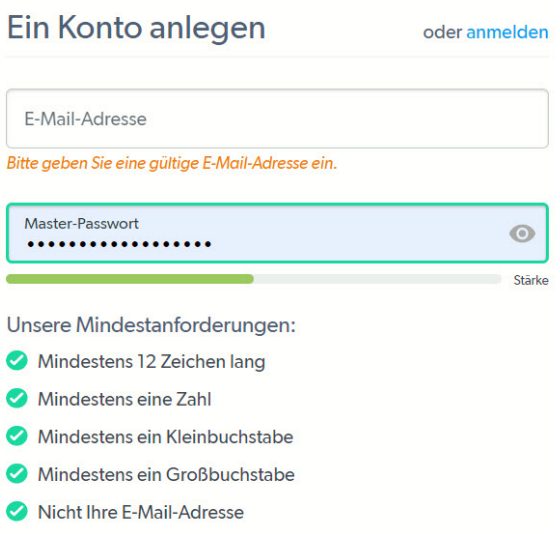
- Ist der Sicherheitsschlüssel geeignet, dann schreibt Google die Anmeldeinformationen in den Passkey auf den Sicherheitsschlüssel.
- Der Vorteil: Der Sicherheitsschlüssel ist ja nichts anderes als ein technisch sehr ausgeklügelter USB-Stick. Den könnt ihr entnehmen und damit vom Gerät trennen. Wenn ein gemeinsam genutzter PC die Möglichkeit und Rechte bietet, einen Sicherheitsschlüssel zu nutzen, dann ist das die optimale Lösung zur Nutzung von Passkeys!

Integration von Passkeys in Passwort-Manager

Passkeys? Passwort-Manager? Was ist da der Zusammenhang? Tatsächlich rühmen sich immer mehr Passwort-Manager wie beispielsweise 1Password und LastPass, dass sie mittlerweile auch Passkeys unterstützen.

Erste Schritte mit einem Password-Manager

Die meisten der Passwort-Manager bieten ein eigenes Konto an, dass dann alle Plattformen (Web, Desktop/Tablet/Notebook, Smartphone) zusammenführt.



- Legt dieses auf der Webseite des Herstellers an. Einmalig vergebt dann ein Masterpasswort. Das ist das einzige Passwort, das ihr

So geht's leichter | Passkeys: Online-Konten sichern

sich nachher noch merken müsst. Alle anderen landen dann in dem über dieses Masterpasswort verschlüsselten Passwort-Safe.

- Wichtig ist hier, dass ihr euch dieses Masterpasswort sicher und nachhaltig merkt. Ohne dieses kommt ihr an kein einziges der Passwörter mehr heran.
- Eine Möglichkeit kann hier sein, es in einen verschlossenen Briefumschlag in einem physischen Safe, wie die meisten Haushalte ihn mittlerweile haben, abzulegen.
- Als Nächstes installiert ihr die Passwort-App und/oder die Browsererweiterungen auf jedem der Geräte, auf denen ihr Passwörter verwenden müsst. Viele der Passwortmanager bieten auch Smartphones-Apps an. Damit habt ihr eine gewisse Unabhängigkeit von einer lokalen Installation. Das Smartphone habt ihr schließlich immer dabei!

Im nächsten Schritt geht es an die Nutzung des neuen Passwort-Managers. Gebt Passwörter, die ihr bisher irgendwo anders abgelegt habt, ein. Importiert sie aus einem anderen Programm, idealerweise sogar dem Browser.

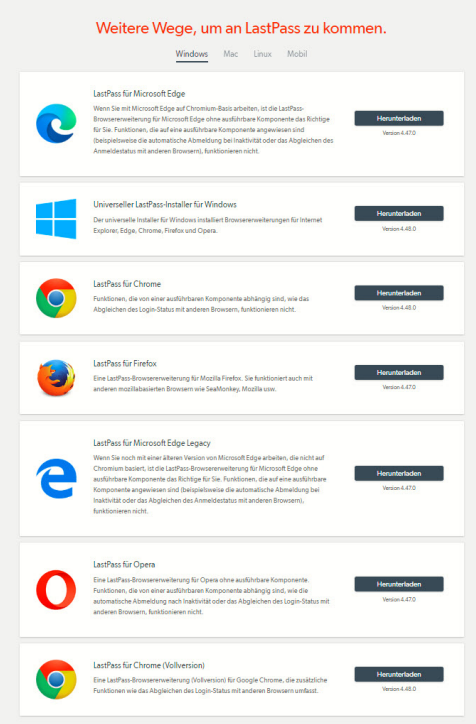
LastPass

LastPass ist mit einer der beliebtesten Passwort-Manager. Unter anderem deshalb, weil er in der kostenlosen Variante schon eine Menge Funktionen mitbringt.

Die kostenpflichtige Version bietet dann für ab USD 3,- im Monat das Teilen von Passwörtern mit anderen Benutzern an, einen 1GB großen, verschlüsselten Seitenspeicher und die Möglichkeit, ein Hardwaretoken als Schutz des Passwort-Tresors zu verwenden.

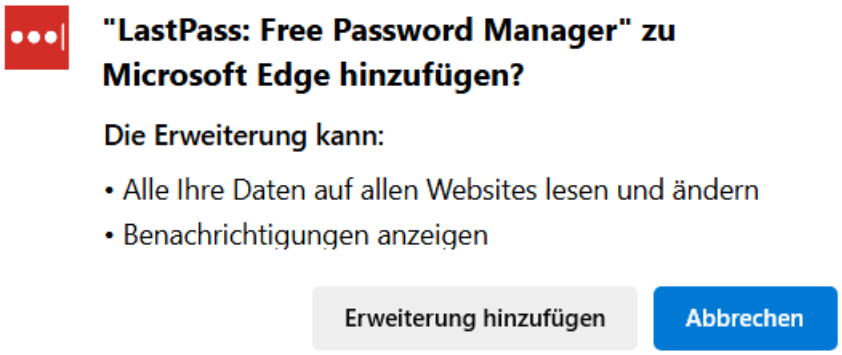
So geht's leichter | Passkeys: Online-Konten sichern

- Unter https://lastpass.com/download findet ihr die verschiedenen Versionen für alle Desktop-Betriebssysteme und die Plug-ins für die gängigen Webbrowser.



- Ganz rechts in der Menüleiste über den Links könnt ihr auf **mobil** klicken und von dort aus direkt in den App Store des Smartphones gelangen.

- Beim ersten Start der LastPass Desktop-App zeigt Ihnen diese alle unsicher gespeicherten Passwörter an, die auf Ihrem Rechner gefunden wurden und bietet deren Import in LastPass an. Das sind meist Passwörter aus dem alten Internet Explorer und WLAN-Zugänge.



- Für die Nutzung der Passkeys ist die Installation im Browser verpflichtend. Im Gegensatz zu Passwörter werden die Passkeys ja automatisch auf einer Webseite erzeugt und sind nicht

eintippbar. Diese Installation könnt ihr direkt nach Anlegen eures Benutzerkontos auf der Lastpass-Webseite vornehmen oder durch manuelle Installation aus dem Store eures jeweiligen Browsers.

- Bei der Anmeldung mit aktivierter Browsererweiterung werden die Passkeys der besuchten Seiten in dem gesicherten Speicher des Passwort-Managers abgelegt.
- Ihr habt damit zum einen eine zusätzliche Verschlüsselungsstufe, zum anderen werden die Passkeys im Konto des Passwortmanagers gesichert, und werden über Geräte hinweg synchronisiert.
- Die Unterstützung von Passkeys in Passwortmanagern ist noch in den Kinderschuhen, viele Anbieter beginnen erst jetzt mit der Integration. Die dürfte aber schnell gehen!

Häufig gestellte Fragen (FAQ)

Ihr seht: Passkey bringt eine Menge Vorteile und sind auch einfach in der Handhabung. Für den Fall, dass noch Fragen offen sind: Hier ein FAQ zu Passkeys.

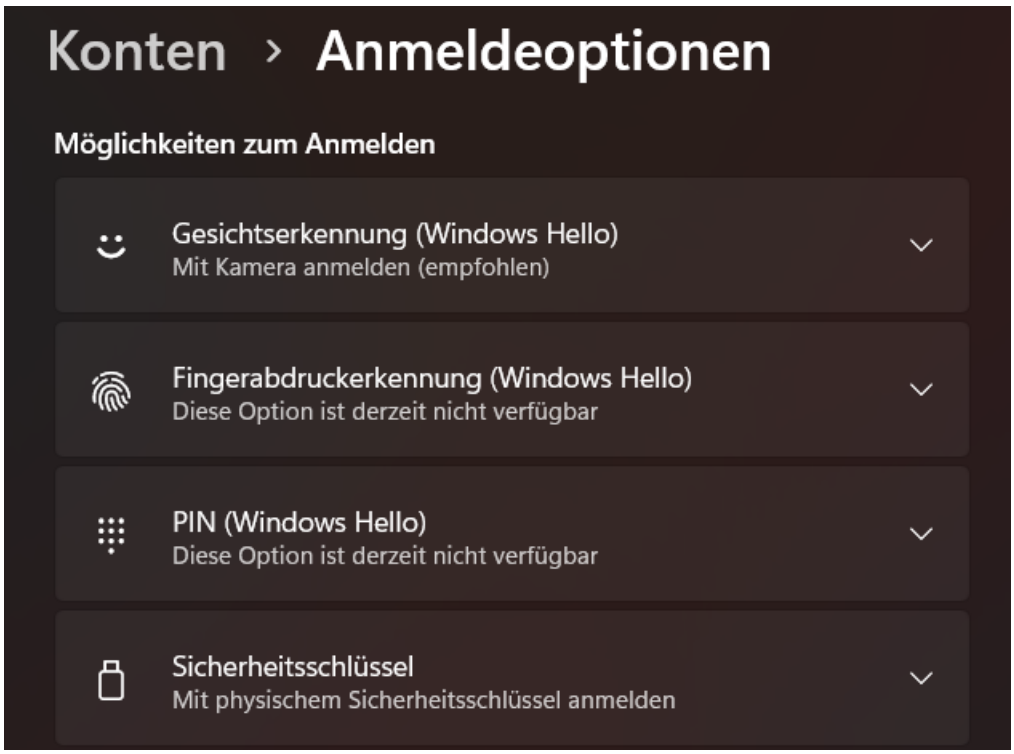
Was tun, wenn ich mein Gerät verliere oder es gestohlen wird?

Ein Passkey ist immer eine Kombination von zwei Schlüsselteilen. Wenn euch ein Gerät mit einem Passkey darauf verloren geht, dann ist „nur" der eine in den Händen der Diebe oder Finder. Allerdings: Es handelt sich dann um den privaten Teil des Schlüssels, der deutlich kritischer ist

So geht’s leichter | Passkeys: Online-Konten sichern

als der öffentliche Teil, den die Webseite zur Anmeldung verwendet. Trotzdem: Ein Geräteverlust ist nie angenehm:

- Stellt im Vorfeld sicher, dass die Methode, mit der ihr euch am Gerät anmelden müsst, so sicher wie möglich ist. Eine PIN ist ein gewisser Schutz, aber schnell zu erraten

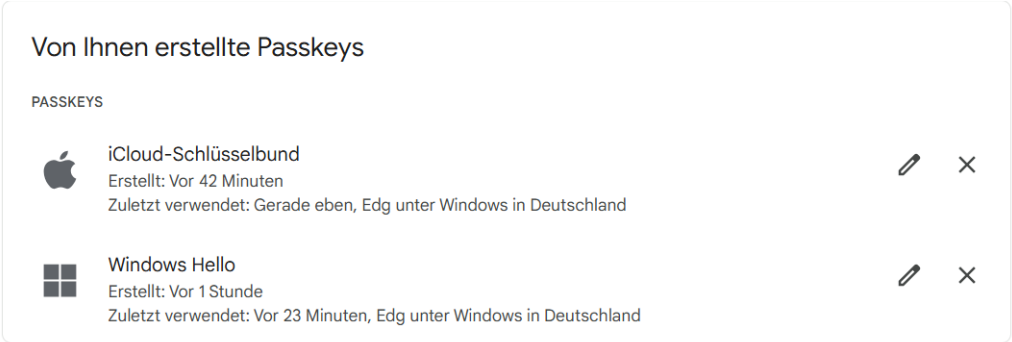


- Besser sind hier Die Gesichts- oder Fingerabdruckerkennung, denn ohne euer Auge oder Finger funktionieren die nicht. Die hat ein Finder oder Dieb eher nicht zur Verfügung.

Wenn das Gerät dann abhanden kommt, dann solltet ihr schnell alle Passkeys löschen. Das gestaltet sich im gestohlenen Gerät schwierig, das macht aber nicht. Es reicht schon, wenn ihr den öffentlichen Teil des Passkeys löscht:

So geht's leichter | Passkeys: Online-Konten sichern

- Meldet euch an der Webseite an und navigiert zu den Passworteinstellungen (dort finden sich auch die Passkeys). Die Seite zeigt euch jetzt all eure Passkeys in einer Übersicht an:



- Wenn ihr einen Passkey deaktivieren wollt, dann klickt auf das X neben dem Passkey. Dieser wird dann aus eurem Konto gelöscht und das zugehörige Gerät kann sich nicht mehr an eurem Google-Konto anmelden.
- Ansonsten gilt: Wenn das Gerät eine Fernlöschung unterstützt, dann nutzt diese. Denn nicht nur eure Passkeys, sondern auch alle anderen Daten sind potenziell in Gefahr!

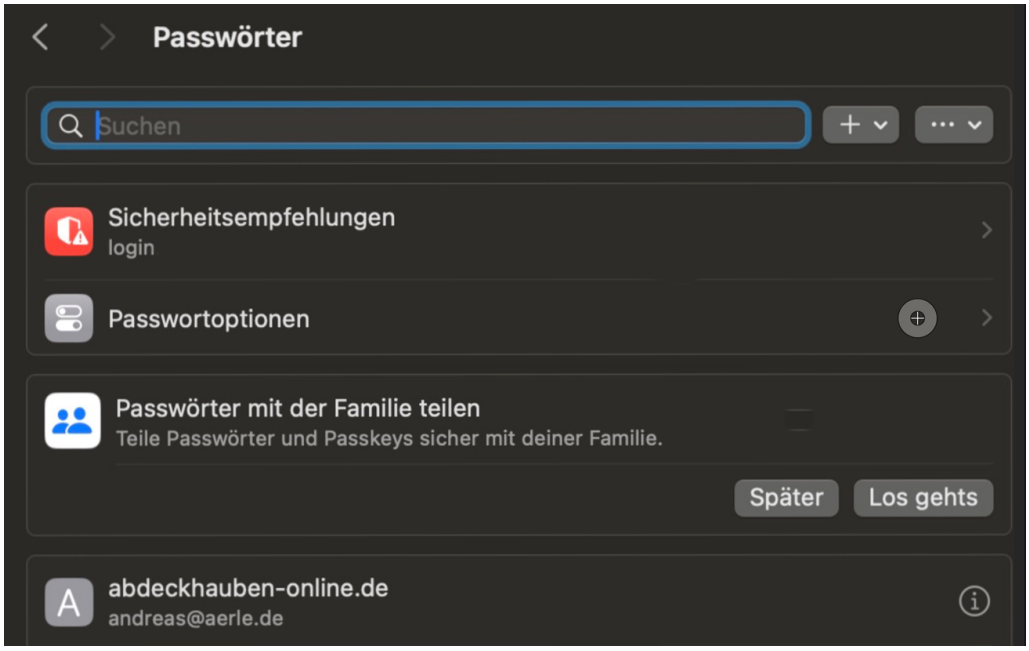
Kann ich Passkeys auf mehreren Geräten verwenden?

Das kommt immer darauf an, welchen Dienst und welches Betriebssystem ihr nutzt. Ernst einmal sind Passkeys ein Schlüssel zwischen einem Dienst und einem Gerät und sollen damit sicherstellen, dass das Gerät beim Benutzer sein muss, um die Anmeldung durchzuführen. Allerdings gibt es immer mehr Ausnahmen – der Bequemlichkeit wegen.

So geht’s leichter | Passkeys: Online-Konten sichern

- Wenn ihr den Passkey nicht auf dem zugreifenden Gerät anlegt, sondern mit einem weiteren Gerät, beispielsweise einem FIDO2-Sicherheitsschlüssel oder einem Smartphone ablegt, dann dient dieses Gerät ja als Authentifizierung für alle Geräte, mit denen ihr auf den Dienst zugreift.

  Einfacher formuliert: Ob ihr am PC, am Mac, einem Tablet oder dem Terminal in einem Internetcafé zugreifen wollt, es ist immer euer Smartphone, das den Zugriff freischaltet. Damit funktioniert ein solcher Passkey auf mehreren Geräten.



- Bei den großen Anbietern wie Google, Microsoft und Apple kommt eine weitere Besonderheit hinzu: Diese speichern die Passkeys in ihren eigenen Cloud-Diensten. Einmal eingegeben sind sie auf allen Geräten nutzbar, die dasselbe Konto benutzen.

- Bei einem Mac also beispielsweise auf jedem iPhone, iPad, MacBook etc., auf dem ihr euch mit derselben Apple ID

So geht's leichter | Passkeys: Online-Konten sichern

anmeldet. Einzige Voraussetzung: Die Synchronisation des Schlüsselbundes über iCloud muss aktiviert sein.

- Das könnt ihr über **Einstellungen** > **Kontobild** > **iCloud** > Passwörter und Schlüsselbund und das Aktivieren des Schalters neben **iPhone synchronisieren** erreichen. Für die anderen Geräte und Dienste läuft dies sehr ähnlich.

Sind Passkeys wirklich sicherer als herkömmliche Passwörter?

Die einfache Antwort: Ja. Das wäre aber natürlich ein wenig kurz gegriffen, darum hier die Gründe dafür:

Passkeys ersetzen Passwörter komplett. Und damit automatisch auch deren Schwächen:

- Benutzer tendieren dazu, einfache, leicht merkbare Passwörter zu verwenden und diese auch noch über mehrere Dienste gleich zu wählen. Das macht Passwörter angreifbar, riesige Datenbanken aus gestohlenen Kombinationen aus Benutzernamen und Passwörtern sind für wenig Geld im Darknet zu bekommen. Passkeys hingegen sind gar nicht direkt für den Anwender wählbar oder zugänglich, damit besteht das Problem nicht.

So geht's leichter | Passkeys: Online-Konten sichern

- Eine große Gefahr bei Passwörtern sind Phishing-Angriffe oder Social Engineering, bei denen der Benutzer seine Passwörter gut meinend auf einer Fake-Webseite eingibt und diese damit offenbart. Das funktioniert bei Passkeys nicht, denn damit diese funktionieren, muss die Webseite ja den echten öffentlichen Teil des Schlüssels kennen, was bei einer Fake-Webseite nicht der Fall ist.
- Die Aufteilung zwischen privatem und öffentlichem Schlüssel hat einen weiteren Vorteil: Sie ist so umgesetzt, dass niemand aus dem einen Schlüsselteil den anderen erzeugen kann. Ein Angreifer braucht also auf jeden Fall beide Schlüsselteile.

Hinzu kommt, dass Passkeys deutlich komfortabler sind: Gute Passwörter wollen gewechselt werden, sollen lang und nicht einfach sein. Das bedeutet, dass ihr eine Menge an Zusatzaufwand betreiben müsst:

- Passwörter wollen behalten werden.
- Da das nicht so einfach ist, nutzt ihr Passwort-Safes als Apps oder Webdienste, die wollen gefüttert werden.
- Bei der Anmeldung müsst ihr euch das Passwort aus dem Passwort-Safe (oder der Erinnerung) herauskramen und eingeben, auch das kostet Zeit.

Diese Aufwände sorgen schnell dafür, dass ihr es euch einfach macht und an der Qualität der Passwörter spart. Das passiert bei einem Passkey nicht: Der ist komplex, die Verwaltung wird euch aber komplett abgenommen. Damit erhöht sich automatisch die Sicherheit!

So geht’s leichter | Passkeys: Online-Konten sichern

Ausblick und Zukunft von Passkeys

Die Zukunft der Passkeys verspricht, deine digitale Erfahrung grundlegend zu verändern. Stell dir vor, du wachst morgens auf und greifst nach deinem Smartphone. Mit einem kurzen Blick oder einer sanften Berührung deines Fingers öffnet sich nicht nur dein Gerät, sondern du erhältst gleichzeitig Zugang zu all deinen Online-Konten – sicher, schnell und ohne ein einziges Passwort einzugeben.

In den kommenden Jahren werden Passkeys voraussichtlich allgegenwärtig werden. Immer mehr Dienste und Plattformen werden sie als primäre Authentifizierungsmethode anbieten, sodass du dich schon bald fragen wirst, wie du jemals ohne sie ausgekommen bist. Die Technologie wird sich dabei stetig weiterentwickeln und noch benutzerfreundlicher werden.

Biometrie wird dabei eine zunehmend wichtigere Rolle spielen. Neben Fingerabdruck und Gesichtserkennung könnten in Zukunft auch dein Herzschlag, deine Stimme oder sogar dein Gang als einzigartige Identifikatoren dienen. Diese Entwicklung wird die Sicherheit weiter erhöhen und gleichzeitig den Authentifizierungsprozess noch natürlicher und nahtloser gestalten.

Stell dir vor, du betrittst einen Raum und deine persönlichen Geräte erkennen dich automatisch. Dein Smart Home passt sich an, dein Computer startet deine bevorzugten Anwendungen, und deine Online-Dienste sind sofort verfügbar – alles dank fortschrittlicher Passkey-

So geht’s leichter | Passkeys: Online-Konten sichern

Technologie, die dich anhand einer Kombination aus Umgebungsfaktoren und biometrischen Daten identifiziert.

Die Integration von Passkeys in verschiedene Geräte und Systeme wird voranschreiten. Von deiner Smartwatch über dein Auto bis hin zu öffentlichen Terminals – überall wirst du sicher und bequem auf deine persönlichen Daten und Dienste zugreifen können. Dies wird nicht nur dein digitales Leben vereinfachen, sondern auch neue Möglichkeiten für personalisierte Dienste und nahtlose Interaktionen in der physischen Welt eröffnen.

Trotz dieser spannenden Entwicklungen wird der Schutz deiner Privatsphäre weiterhin im Mittelpunkt stehen.

Zukünftige Passkey-Systeme werden noch robustere Sicherheitsmaßnahmen implementieren, um sicherzustellen, dass deine biometrischen Daten und digitalen Identitäten sicher bleiben. Du wirst mehr Kontrolle darüber haben, welche Informationen du teilst und wie sie verwendet werden.

So geht’s leichter | Passkeys: Online-Konten sichern

Die Reise in diese passwortlose Zukunft hat gerade erst begonnen, und du stehst an der Schwelle zu einer sichereren, bequemeren und intelligenteren digitalen Welt. Bist du bereit, den nächsten Schritt zu machen?

Erwartete Entwicklungen und Verbreitung

Passkeys sind zum Zeitpunkt des Erscheinens dieses E-Books noch in der Startphase. Das heißt nicht, dass die Technologie noch nicht ausgereift ist, es hängt eher an der Verbreitung.

In den folgenden Wochen und Monaten werden wir eine immer schneller zunehmende Unterstützung von Passkeys sehen. Dadurch, dass diese von einer großen, mitgliederstarken Organisation wie der FIDO entwickelt und vorangetrieben werden, besteht nicht die Gefahr, dass alternative, von der Umsetzung her abweichende Alternativen entwickelt werden.

Wer als Webseite oder Dienst etwas von sich hält, der wird sich nicht dauerhaft verweigern können, die Anmeldung per Passkey zu unterstützen.

Am Ende ist hier auch der Benutzer am längeren Hebel: Die großen, oft alternativlosen Anbieter unterstützen Passkeys schon und haben es angekündigt. Die kleinen Anbieter, die eher abwarten und die Investition scheuen, werden irgendwann von Nutzeranfragen und irgendwann auch Abwanderungen dazu gezwungen werden.

Abschließende Gedanken und Empfehlungen

Werden Passkeys Passwörter komplett ablösen? Nahezu, aber nicht vollständig. Während Betriebssysteme und Webseiten ohnehin einem steten Wandel unterliegen und sich im Handumdrehen an neue technische Entwicklungen anpassen, gibt es immer noch Nischenanwendungen, bei denen das nicht der Fall ist.

Besonders IoT-Geräte wie Rauchmelder, IP-Kameras, Konsolen haben einen eingeschränkten Funktionsumfang. Die wenigen Updates, die es dafür – wenn überhaupt – gibt, sind meist sehr fokussiert auf die Behebung von Sicherheitslücken. Deren eingeschränkte Betriebssysteme erlauben oft nicht das Hinzufügen von komplexen Funktionalitäten wie Passkeys sie erfordern.

Mit zunehmender Gefährdung durch Hackerangriffe und Phishing ist jeder Erhöhung der Sicherheit von Benutzerkonten wichtig und begrüßenswert. Die Tatsache, dass Passkeys gerade noch in der Anfangsphase sind, sollte kein Grund sein, diese nicht zu nutzen oder skeptisch zu betrachten.

Da, wo Passkeys schon verfügbar sind, aktiviert sie. Und haltet die Augen auf: Bei vielen Diensten kommt ohne separate Ankündigung eine Schaltfläche „Mit Passkey anmelden" hinzu. Gerade bei den häufig genutzten Konten lohnt sich also ein regelmäßiger Blick in die Sicherheitseinstellungen des Dienstes!

Unabhängig davon aber verliert die Passwortsicherung nicht an Bedeutung. Solange ihr also nur ein einziges Konto verwendet, das noch „nur" mit einem Passwort geschützt wird, lasst nicht nach darin, dieses zu schützen.