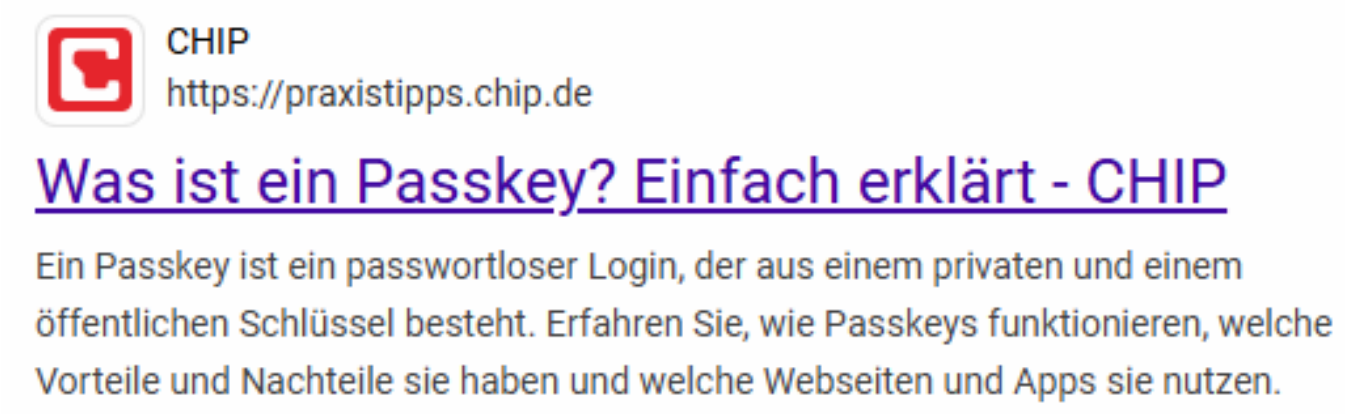

Ein Passkey ist ein passwortloser Login

Wer sich in Apps oder Websites einloggen möchte, der benutzt dazu in der Regel ein Passwort, um sich zu identifizieren.

Mit einem Passkey funktioniert der Login passwortlos.

In Zeiten von Cyber-Kriminalität wird nach Lösungen gesucht, um Logins in Webseiten und Apps sicherer zu machen. Passwörter haben den Nachteil, dass sie etwa durch Phishing in falsche Hände geraten und dann missbraucht werden können. Passkeys sollen als eine Art digitale Signatur Abhilfe schaffen.

Das Wort "Passkey" kann man mit "Schlüsselpaar" übersetzen. Ein Passkey besteht nämlich aus einem privatem und einem öffentlichen Schlüssel. Der private Kryptoschlüssel besteht aus einer langen Zeichenfolge. Er ist geheim und bleibt immer auf Ihrem lokalen Gerät (Authenticator), z. B. Smartphone. Das sorgt für mehr Sicherheit, da er nicht durch Phishing abgegriffen werden kann. Passkeys sind also geräte- und nicht personengebunden.

Wenn Sie sich bei einer Webseite anmelden, die die Passkey-Identifizierung anbietet, kommuniziert diese mit Ihrem lokalen Gerät mit dem Passkey. Sie sendet dazu eine Aufgabe (Challenge). Sie müssen sich dann per PIN oder mit Ihren biometrischen Daten (Gesichtserkennung (Face ID) oder Fingerabdruck (Touch ID)) ausweisen. Danach sendet Ihr Gerät eine digitale Signatur (öffentlicher Schlüssel) an die Webseite zurück und bestätigt sozusagen, dass es tatsächlich Sie sind, der sich einloggen möchte.

Das Ganze hat neben dem Mehr an Sicherheit einen weiteren Vorteil – nämlich, dass Sie sich bei dieser Art der Authentifizierung keine Passwörter mehr selbst ausdenken und merken müssen.

Das Passkey-Verfahren wurde von FIDO Alliance entwickelt. Apple, Google, Paypal, Amazon und Microsoft bieten zum Beispiel die Möglichkeit der Passkey-Nutzung an. Es gibt aber auch eine Reihe von Webseiten oder Apps, die dieses Verfahren noch nicht nutzen.
Passkeys sollen sicherer, bequemer und schneller sein. Es gibt aber auch Nachteile: So können Sie zum Beispiel Passkeys nicht einfach teilen. Nutzen Sie zum Beispiel einen Netflix-Account mit jemandem gemeinsam, **kann sich immer nur die Person, welcher das Gerät mit dem Passkey gehört, einloggen, da das Verfahren gerätegebunden ist.**

Passkeys sind auf meinem Smartphone gespeichert, die Anmeldung soll aber am PC erfolgen – Wie geht das?
Weil der Passkey unter anderem aus einem geheimen Schlüssel besteht, der beispielsweise auf Ihrem Smartphone hinterlegt ist, stellt sich die Frage, wie Sie sich dann etwa am PC in einen Account einloggen. Dazu gibt Ihnen der Dienst, bei dem Sie sich mit Ihrem PC anmelden möchten, die Möglichkeit, sich trotzdem mit dem Smartphone zu authentisieren. Sie wählen am Computer Ihr Smartphone als Anmeldegerät aus und erhalten die Aufforderung, einen QR-Code vom PC-Bildschirm zu scannen. Gleichzeitig müssen beide Geräte über eine eingeschaltete Bluetooth-Verbindung verfügen. Nun bestätigen Sie den Login als würden Sie sich auf Ihrem Handy einloggen, zum Beispiel per Fingerabdruck. Wurde der kryptografische Vorgang erfolgreich aufgelöst, gibt der Dienst Ihren Account auf dem PC frei.

Falls Sie bereits einzelne Funktionen oder das Gerätedisplay per Fingerabdruck oder Gesichtsscan entsperren, bedeutet das nicht, dass Sie bereits Passkeys nutzen. Denn Passkeys werden ausschließlich für das Einloggen bei einem Onlinedienst oder Account genutzt. Sie müssen einmalig eingerichtet werden und können ab dann den Login einfacher und trotzdem sicher gestalten. Zum Entsperren des Geräts können Sie weiterhin Ihre bisherige Methode verwenden.

Wo begegnen uns Passkeys schon jetzt?
Die Verbreitung von Passkeys nimmt täglich zu. Die meisten Betriebssysteme von Computern und Mobilgeräten unterstützen die Funktion bereits. Auch große Onlineshopping-Plattformen, Soziale Medien, Foren, Finanzportale oder Messengerdienste ermöglichen den Login mit Passkeys: Liste bekannter Dienste, die Passkeys verwenden

Passkeys sind auf meinem Smartphone gespeichert, die Anmeldung soll aber am PC erfolgen – Wie geht das?
Weil der Passkey unter anderem aus einem geheimen Schlüssel besteht, der beispielsweise auf Ihrem Smartphone hinterlegt ist, stellt sich die Frage, wie Sie sich dann etwa am PC in einen Account einloggen. Dazu gibt Ihnen der Dienst, bei dem Sie sich mit Ihrem PC anmelden möchten, die Möglichkeit, sich trotzdem mit dem Smartphone zu authentisieren. Sie wählen am Computer Ihr Smartphone als Anmeldegerät aus und erhalten die Aufforderung, einen QR-Code vom PC-Bildschirm zu scannen. Gleichzeitig müssen beide Geräte über eine eingeschaltete Bluetooth-Verbindung verfügen. Nun bestätigen Sie den Login als würden Sie sich auf Ihrem Handy einloggen, zum Beispiel per Fingerabdruck. Wurde der kryptografische Vorgang erfolgreich aufgelöst, gibt der Dienst Ihren Account auf dem PC frei.

Falls Sie bereits einzelne Funktionen oder das Gerätedisplay per Fingerabdruck oder Gesichtsscan entsperren, bedeutet das nicht, dass Sie bereits Passkeys nutzen. Denn Passkeys werden ausschließlich für das Einloggen bei einem Onlinedienst oder Account genutzt. Sie müssen einmalig eingerichtet werden und können ab dann den Login einfacher und trotzdem sicher gestalten. Zum Entsperren des Geräts können Sie weiterhin Ihre bisherige Methode verwenden.

Was, wenn mein Gerät verloren oder gestohlen wird?
Falls das Gerät, auf dem Ihre Passkeys hinterlegt sind, verloren gegangen ist oder gestohlen wurde, können Sie Ihre Zugänge dann wiederherstellen, wenn Sie entweder lokale Backups angelegt haben oder wenn Ihre Passkeys in einer Cloud synchronisiert werden. Sollten

Sie keine Sicherheitskopien Ihrer Passkeys besitzen, bieten einige Dienste weitere Möglichkeiten, Ihre Identität nachzuweisen und so beispielsweise einen neuen Passkey für Ihren Zugang zu erstellen. Falls Sie Ihre Passkeys mit einem FIDO2-Sicherheitsschlüssel verwalten, ist es ratsam, einen zweiten FIDO2-Stick anzuschaffen, um eine Notfalllösung bereitzuhalten. FIDO2-Sticks können nicht kopiert werden, weshalb Sie bei Ihren Online-Diensten für jeden Ihrer Sticks einzeln Passkeys generieren müssen. In seltenen Fällen kann es dennoch vorkommen, dass Sie sich nach dem Verlust Ihres Geräts nicht mehr einloggen können. Dann müssen Sie den Anbieter kontaktieren und den Account wiederherstellen.