FAQ

Passwort-Nachfolger FIDO2

Das neue Login-Verfahren FIDO2 hat das Zeug, das Passwort abzulösen. In c't 18/2019 haben wir es ausführlich vorgestellt. Das Thema ist bei unseren Lesern auf großes Interesse gestoßen, und wir haben zahlreiche Rückfragen hierzu erhalten. Diese möchten wir an dieser Stelle gesammelt beantworten.

Von Jürgen Schmidt und Ronald Eikenberg

Das ist FIDO2

FIDO2 klingt interessant, aber auch kompliziert. Können Sie noch mal kurz und knackig erklären, was es damit auf sich hat?

FIDO2 ist ein neues Verfahren, mit dem Sie sich bei Webdiensten registrieren und einloggen können. Es kann entweder anstelle eines Passworts zum Einsatz kommen oder zusätzlich, als zweiter Faktor. Sie benötigen dafür einen sogenannten Authenticator: Solche gibt es zum Beispiel in Format eines USB-Sticks, den Sie am Schlüsselbund befestigen können.

Beim Login stecken Sie den Stick einfach in den Rechner und drücken die Taste auf dem Stick, um sich gegenüber dem Dienst zu authentifizieren. Unter Windows, Android und eingeschränkt auch unter macOS klappt es sogar ohne Zusatz-Hardware, da die Betriebssysteme selbst als virtuelle Authenticatoren arbeiten.

Je nachdem, wie der Dienst FIDO2 implementiert hat, genügt der Stick zum Einloggen (Ein-Faktor-Authentifizierung) oder Sie müssen zusätzlich noch eine PIN oder ein Passwort eingeben (zwei Faktoren). Beide Varianten sind erheblich sicherer, als sich allein auf das Passwort zu verlassen.

Begriffsklärung

FIDO2-Stick, Authenticator, Token, Sicherheitsschlüssel, geheimer Schlüssel: Was hat es damit auf sich?

Der FIDO2-Stick hat viele Namen. Wenn man vom Authenticator, Token oder Sicherheitsschlüssel spricht, ist das Gerät gemeint, mit dem Sie sich gegenüber den Diensten authentifizieren. Es kann sich dabei um ein externes Gerät handeln, das Sie per USB, NFC, Bluetooth oder Lightning mit Ihrem PC oder Smartphone verbinden. Diese Geräte haben meist den Formfaktor eines USB-Sticks oder Schlüsselanhängers.

FIDO-Sicherheitsschlüssel gibt es in allen Formen und Farben. Hier zu sehen (von links nach rechts): Digipass SecureClick, Feitian Multipass FIDO U2F Security Key, Yubico Security Key (Version 2), SoloKeys Solo USB-C und YubiKey 5C Nano.

Der FIDO2-Stick arbeitet als externer Authenticator. Darüber hinaus gibt es interne Authenticatoren. Damit ist eine Software gemeint, die den Krypto-Chip Ihres PCs, Smartphones oder Tablets für FIDO2 nutzt. Den Kauf eines externen FIDO2-Sticks können Sie sich damit sparen. Als internen Authenticator können Windows 10 und Android ab Version 7 arbeiten, unter macOS klappt es in Kombination mit Google Chrome.

Der geheime Krypto-Schlüssel ist das Geheimnis, das in Ihrem Token gespeichert ist. Sie können es sich wie eine zufällige Zeichenfolge vorstellen, die nur Ihr Token kennt. Dieses Geheimnis lässt sich nicht auslesen oder kopieren.

In der Praxis

Wo kann ich FIDO2 jetzt schon nutzen?

Das Einloggen ohne Passwort funktioniert bereits bei Microsoft.com und den daran angeschlossenen Diensten wie Outlook.com, Office 365 und OneDrive, sofern Sie Edge nutzen. Bei vielen weiteren Diensten können Sie FIDO2 als zweiten Faktor einrichten. Dann profitieren Sie von dem Schutz gegen Phishing & Co., müssen jedoch weiterhin Ihr Passwort eingeben. Das klappt etwa bei Google, GitHub, Dropbox, Twitter und BoxCryptor. Ausprobieren können Sie das Ganze zum Beispiel auf der Demo-Seite WebAuthn.io.

Mehrfachnutzung

Kann ich bei einem Dienst auch mehrere solcher Sicherheitsschlüssel registrieren?

Ja, das ist möglich und sogar sehr empfehlenswert. Denn falls Sie einen

davon verlieren, haben Sie immer noch einen zweiten, mit dem Sie sich anmelden und den verlorenen Sicherheitsschlüssel sperren können.

Diebstahl

Kann man mir so einen USB-Sicherheitsschlüssel nicht einfach klauen?

Ja, das ist prinzipiell möglich. Genauso wie jemand Ihren Auto- oder Wohnungsschlüssel klauen könnte. Dann gilt es, möglichst schnell den Zugang zu den damit verwendeten Accounts zu sperren. Ein entscheidender Vorteil gegenüber Passwörtern ist, dass ein Diebstahl nicht mehr virtuell möglich ist.

Es reicht nicht mehr, wenn die Cybermafia mit einem Trojaner oder durch Einbruch auf einem Server Millionen von Passwörtern ergattert. Es muss jemand direkt vor Ort einen Sicherheitsschlüssel klauen und dann auch missbrauchen. Letztlich ist das für Cybercrime unattraktiv.

Zusätzliche Sicherheit

Kann ich mich irgendwie vor dem Diebstahl meines Sicherheitsschlüssels und einer anschließenden Übernahme meiner Accounts schützen?

Ja, das ist im FIDO2-Standard explizit vorgesehen. So sind die eingebauten virtuellen Schlüssel in Windows und Android immer durch einen zweiten Faktor, also etwa einen Fingerabdruck oder eine PIN geschützt, die eine Nutzung durch Fremde verhindern.

Es gibt auch USB-Token, die einen solchen zweiten Faktor erfordern. So kann man die Yubikeys von Yubico mit einer zusätzlichen PIN sperren, die man eingeben muss, um den Sicherheitsschlüssel zu verwenden. Und von Feitian gibt es USB-Token mit eingebautem Fingerabdruck-Scanner.

Wiederherstellung

Wie komme ich an meine Konten, wenn ich meinen Stick verliere oder er geklaut wurde?

Sie haben den Schwachpunkt des aktuellen Konzepts erkannt. In diesem Bereich sind noch viele Fragen offen. Insbesondere hängt viel davon ab, wie die Dienste das konkret umsetzen. Es kristallisieren sich zwei Varianten heraus.

1) Accounts für hohe Sicherheitsanforderungen (Payment, E-Mail usw.): Hier müssen Sie sich beim Verlust des Sticks anderweitig sicher „ausweisen“. Also entweder mit einem zweiten Schlüssel, den Sie vorsorglich registriert haben, mit einem Backup-Code, über einen Code an die hinterlegte Handynummer eventuell in Kombination mit einer E-Mail-Autorisierung oder ähnlichem.

2) Accounts mit nicht so hohen Ansprüchen (Foren, Shops & Co.): Da wird dann wohl ein einfacher Reset über eine hinterlegte E-Mail-Adresse oder Handynummer möglich sein. Das ist auch durchaus vernünftig, denn man muss ja nicht jeden Foren-Account wie Fort Knox absichern. Da steht dann eher der Komfort und der niedrige Wartungsaufwand des Betreibers im Vordergrund.

Mechanische Probleme

Diese Token sehen mir nicht sonderlich stabil aus. Gehen die nicht schnell kaputt?

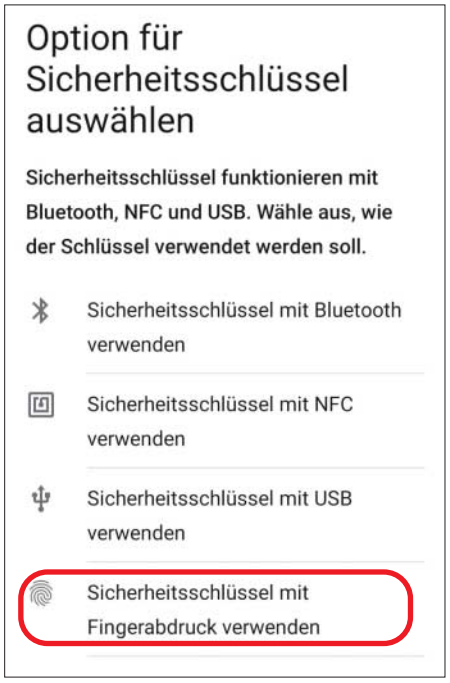
Die Token sind für das Tragen am Schlüsselbund ausgelegt. Wir haben etwa mit den Yubikeys diesbezüglich bereits sehr gute Erfahrungen gemacht. Die überleben auch mehrere Jahre rauen Einsatz am Schlüsselbund und zeigen danach zwar deutliche Abnutzungsspuren, funktionieren aber immer noch problemlos.

Backup

Kann ich ein Backup meines Tokens erstellen?

Nein, das ist explizit nicht möglich – und das ist auch gut so. Die FIDO2-Token sind nicht kopierbar und der darauf gespeicherte geheime Krypto-Schlüssel lässt sich auch nicht auslesen. Ein FIDO2-Sicherheitsschlüssel ist immer ein Unikat. Das ist auch der Grundgedanke der FIDO-Alliance hinter FIDO2.

Dadurch sind die Token viel sicherer als Passwörter: Ein Trojaner kann zwar Ihr Passwort abgreifen, jedoch nicht den geheimen Krypto-Schlüssel Ihres FIDO2-Token. Damit Sie im Fall eines Verlusts oder Hardware-Defekts weiter auf Ihre Accounts zugreifen können, müssen Sie eine zweite Authentifizierungsmöglichkeit einstellen, zum Beispiel, indem Sie ein zweites Token anlernen oder Backup-Codes ausdrucken.



Mit der untersten Option kann man FIDO2 unter Android ohne Zusatz-Hardware nutzen. Ist kein Google-Account eingerichtet, fehlt diese Funktion möglicherweise.

Android-Geräte

Ich möchte FIDO2 auf meinem Android-Smartphone nutzen, allerdings fehlt mir die dafür benötigte Option „Sicherheitsschlüssel mit Fingerabdruck verwenden“. Ich kann nur externe Schlüssel nutzen. Was läuft da falsch?

Sie benötigen Android 7 oder höher. Zudem müssen die Google-Play-Dienste auf dem aktuellen Stand sein, da Google die gewünschte Funktion über ein Update der Dienste auf die Geräte verteilt. Damit Sie das Update erhalten und die Dienste ordnungsgemäß arbeiten, müssen Sie einen Google-Account eingerichtet haben. Falls es dennoch nicht klappt, fehlt Ihrem Android-Gerät womöglich ein „Secure Element“, das den für FIDO2 genutzten Krypto-Schlüssel verwalten würde.

Smartphone als Schlüssel

Kann ich das Smartphone auch als Sicherheitsschlüssel für den PC hernehmen?

Theoretisch ja, praktisch derzeit nein. Aus technischer Sicht können nahezu beliebige Geräte über Bluetooth, NFC oder USB als FIDO2-Token fungieren, solange sie sich um die sichere Aufbewahrung des geheimen Schlüssels kümmern. Ein Smartphone wäre dafür ideal, da es meist nicht nur mit Bluetooth, sondern auch mit einem Secure Element für die Krypto-Operationen ausgestattet ist. Auch Smartwatches wären gut geeignet. Bislang mangelt es jedoch an der passenden Software.

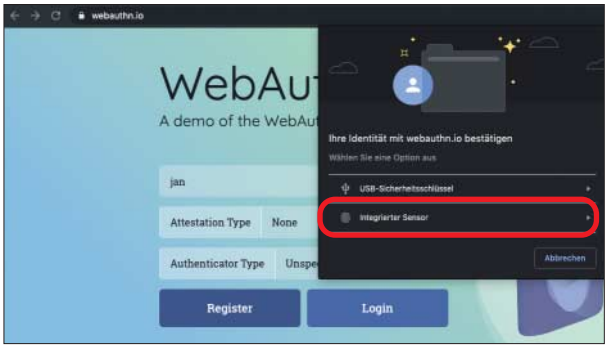
Google experimentiert bereits mit dieser Idee. Wenn man den Google-Account entsprechend konfiguriert, verbindet sich die auf dem PC geöffnete Google-Site beim Login über Bluetooth mit dem Smartphone. Die Krypto-Operationen finden anschließend auf dem Smartphone statt. Langfristig ist es denkbar, dass Google diese Funktion in Android einbaut und das Smartphone auch für andere Dienste als externer Authenticator nutzbar wird.

Apple-Nutzer

Wie ist da der Stand bei Apple? Kann ich FIDO2 inzwischen mit macOS und iPhone nutzen?

Als Nutzer von macOS können Sie FIDO2-Sticks mit Chrome oder Firefox problemlos einsetzen. Safari unterstützt den Webstandard nur mit rudimentärer FIDO2-Funktionalität. Die Sticks funktionieren damit zwar, es fehlen in der Bedienoberfläche jedoch noch die dazugehörigen Dialoge. Google Chrome ist da unter macOS schon weiter: Wer ein MacBook mit Fingerabdrucksensor (Touch ID) hat, kann darüber sogar den Rechner als Sicherheitsschlüssel einsetzen.

Unter iOS gibt es bisher nur den Umweg über den FIDO2-Stick YubiKey 5 Ci von Yubico. Er hat einen USB-C- und einen Lightning-Anschluss. Die Auswahl der Browser ist aber extrem eingeschränkt: Aktuell kann nur der Browser „Brave“ (Open-Source-Software) den Stick für WebAuthn nutzen. Einen Test des YubiKey 5 Ci finden Sie in c’t 20/2019 auf Seite 84.



Dank Google Chrome kann man Touch ID unter macOS auch als FIDO2-Authenticator nutzen.

Linux-Nutzer

Und wie sieht es mit Linux aus?

Unter Linux können Sie Ihren FIDO2-Stick genauso wie unter allen anderen Betriebssystemen verwenden. Entscheidend ist, dass der Browser das Webauthn-API unterstützt. Die meisten aktuellen Browser wie Firefox und Google Chrome sind bereits FIDO2-tauglich. Falls es nicht klappt, sollten Sie überprüfen, ob Sie die aktuelle Browserversion installiert haben.

Es gibt bereits erste Versuche, auch unter Linux das TPM-Modul des Rechners als internen Authenticator nutzbar zu machen. Damit könnten Sie dann auf den Einsatz eines externen FIDO2-Tokens verzichten. Derzeit gibt es allerdings noch keine stabile Implementierung.

Tracking

Kann man mich nicht leicht tracken, wenn ich überall den gleichen Sicherheitsschlüssel verwende?

Bei der Entwicklung des Standards wurde darauf geachtet, dass genau das nicht möglich ist. Der Sicherheitsschlüssel generiert für jeden Dienst ein eigenes Schlüsselpaar, basierend auf der Domain des Gegenübers. Somit können etwa Ebay und Google nicht feststellen, welche ihrer Nutzer den gleichen Sicherheitsschlüssel einsetzen.

Es gibt zwar einen optionalen Mechanismus zum Wiedererkennen, bei dem der Server dann den Schlüssel bittet, zusätzlich seine Seriennummer zu übermitteln. Der Nutzer muss dieser Bitte aber in einem separaten Dialog zustimmen. Heimliches Tracking ist damit also nicht möglich. Die Funktion ist etwa fürs Unternehmensumfeld gedacht, wenn zum Beispiel nur Sicherheitsschlüssel eines bestimmten Herstellers eingesetzt werden sollen.

Fingerabdrücke

Es ist praktisch, dass man sich per Fingerabdruck-Scan anmelden kann, aber wird dabei nicht mein Fingerabdruck an Google & Co. übertragen?

Nein, das passiert nicht. Weder PIN, noch Fingerabdruck oder Gesichts-Scan werden für die eigentliche Anmeldung bei einem Dienst benutzt. Diese Daten bleiben strikt lokal auf dem Sicherheitsschlüssel. Man beweist damit lediglich dem Sicherheitsschlüssel, dass man tatsächlich der richtige Anwender ist (User Verification).

Eigenbau

Ich betreibe eine Website. Wie kann ich meinen Nutzern das Einloggen über FIDO2 anbieten?

Das klappt mit überschaubarem Aufwand und ohne Investitionen. Es gibt zahlreiche Open-Source-Implementierungen von WebAuthn, die Sie mit etwas Geschick in Ihren Webdienst einbauen können. Als Grundlage können Sie zum Beispiel unser in Go geschriebenes Projekt nehmen, das Sie unter https://github.com/jamct/webauthn-start finden (siehe c’t 18/2019, S. 26). *(rei@ct.de)* c't