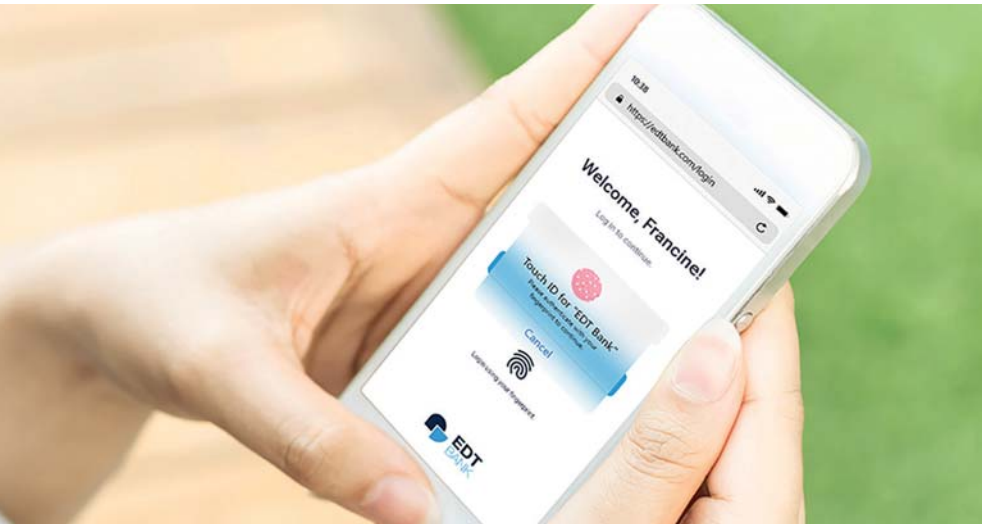
Passwortlose Zahlungsauthentifikation mit Fido – Zukunftsmusik oder Realität?

Von Uwe Härtel



Die Zeit der Passwörter ist definitiv vorbei, sagt Uwe Härtel – und die passwortlose Zukunft zum Greifen nah. Zum Game Changer werden könnte hier der Fido-Standard. Die europaweit erste Fido-basierte Lösung im Payment ist bereits bei Pluscard implementiert. Bis der Fido-Standard bei der Authentifizierung von Online-Zahlungen eine bedeutende Rolle spielen wird, wird es wohl noch eine gewisse Zeit dauern. Weil im neuen EMV 3DS 2.3 Protokoll der Einsatz der Secure Payment Confirmation (SPC) nun standardisiert ist, ist sich der Autor jedoch sicher: Spätestens, wenn 3D-Secure 2.3 umgesetzt ist und SPC zum Standard wird, wird Fido im Payment-Bereich nicht mehr wegzudenken sein. Red.

Heutzutage ist es bequem, mit der Kreditkarte schnell und einfach online einzukaufen. Um Betrug zu verhindern, muss jede dieser Zahlungen authentifiziert werden. Das heißt, bei jeder Transaktion wird geprüft, ob die Konto- oder Kartendaten tatsächlich vom Karteninhaber eingegeben wurden. Zur Legitimation sind Passwörter immer noch weitverbreitet. Sie werden mittlerweile jedoch als unsicher eingestuft, weil sie leicht abgefangen oder erraten werden können.

Zudem ist es für den Anwender sehr umständlich, sich unterschiedliche Passwörter für die zahlreichen verschiedenen Anwendungen zu merken. Die Zeit der Passwörter ist also definitiv vorbei. Aber wie kann eine sichere Authentifizierung von Online-Zahlungen ohne den Einsatz von Passwörtern aussehen?

Als Lösung mit Zukunftspotenzial kommt Fido ins Spiel. Mit Fido (Fast IDentity Online) ist bereits seit 2013 eine Alternative zur Abhängigkeit von Passwörtern verfügbar. Die Non-Profit-Organisation Fido Alliance wurde 2012 von den Unternehmen Agnitio, Infineon, Lenovo, Nok Nok Labs, Paypal und Validity Sensors gegründet. Ziel war die Entwicklung offener und lizenzfreier Industriestandards für die weltweite Authentifizierung im Internet.

Die aktualisierte Version Fido2 basiert auf den freien und offenen Standards der Fido Alliance und kombiniert zwei Standards des World Wide Web Consortiums (W3C): WebAuthn und CTAP2. Fido2 erfüllt die höchsten Sicherheitsanforderungen und adressiert verschiedene Einsatzszenarien für Authentifizierung. Darunter fallen passwortloses Login, passwortloses Multi-Faktor-Login mit Biometrie, delegierte Authentifizierung, digitale Registrierung und Identitätswiederherstellung. Sehr gut eignet sich Fido auch für die Authentifizierung von Online-Zahlungen.

Durchsetzung braucht noch Zeit

Mit der Einführung der Revised Payment Services Directive (PSD2) wurde die Verwendung von starker Multi-Faktor-Authentifizierung für Online-Zahlungen verpflichtend. Dadurch hat sich die Zahlungsverkehrslandschaft grundlegend verändert. Fido2 passt perfekt zu PSD2: Mit einem starken Faktor der Kategorie „Besitz" – also einem Smartphone oder Laptop – können sich die Fido-Nutzer selbst auf einer Webseite während des Step-up-Prozesses authentifizieren.

Neue Standards brauchen immer eine gewisse Zeit, bis sie sich durchgesetzt haben. Bei Fido ist das nicht anders. Obwohl die großen Player wie Microsoft, Google und Apple von Fido überzeugt sind, ist diese Anwendung (bis jetzt) in der Praxis zwar technisch mög-

Uwe Härtel,
Country Manager Central Europe,
Entersekt Europe Cooperatif U.A.,
Utrecht/München

lich, aber bislang kaum verbreitet. Hier könnte der Zahlungsverkehr in Zukunft eine wichtige Rolle spielen. Es ist davon auszugehen, dass Fido bei der Authentifizierung von Online-Zahlungen in Zukunft eine wichtige Rolle spielt und dadurch insgesamt dem Fido-Standard zu größerer Popularität verhilft.

Plattform-Authentifikatoren sind die Zukunft

Wenn man heute Fido für die Freigabe von Online-Zahlungen nutzen möchte, stehen dazu generell zwei technische Lösungen zur Verfügung:

– Roaming-Authentifikatoren (zum Beispiel ein Hardware-Token) und

– Plattform-Authentifikatoren (für mobile Geräte und Laptops/PCs).

Künftig werden neben den physischen Roaming-Authentifikatoren vermehrt sogenannte Plattform-Authentifikatoren zum Einsatz kommen. So unterstützen nun alle aktuellen Versionen der Betriebssysteme der großen Anbieter wie Apple, Microsoft und Google den Fido-Standard für sicheres Log-in sowohl für PC/Notebooks als auch mobile Endgeräte. Alle gängigen Webbrowser wie Edge, Firefox oder Chrome unterstützen Fido2/WebAuthn ebenso wie die mobilen Browser von Android ab Version 7.0 sowie iOS ab Version 13.3.

Zur Registrierung reicht im einfachsten Fall die Eingabe des Benutzernamens oder der Mailadresse aus. Anschließend wählt man die Registriermethode sowie den bevorzugten Authenticator-Type, also entweder das Notebook beziehungsweise Mobilgerät oder einen separaten Fido-Hardware-Token. Zum Abschluss der Registrierung berührt man dann den Sensor, zum Beispiel des eigenen Fido-Tokens.

Authentifikatoren in Kürze

Roaming-Authentifikatoren sind portable Hardware-Token, die mit jedem Computer oder Smartphone über USB, Bluetooth oder Near-Field Communication (NFC) verbunden werden können.

Plattform-Authentifikatoren sind in Laptops oder Smartphones integriert, sodass die Geräte selbst als Authentifikatoren fungieren.

Kartenherausgeber favorisieren 3D-Secure

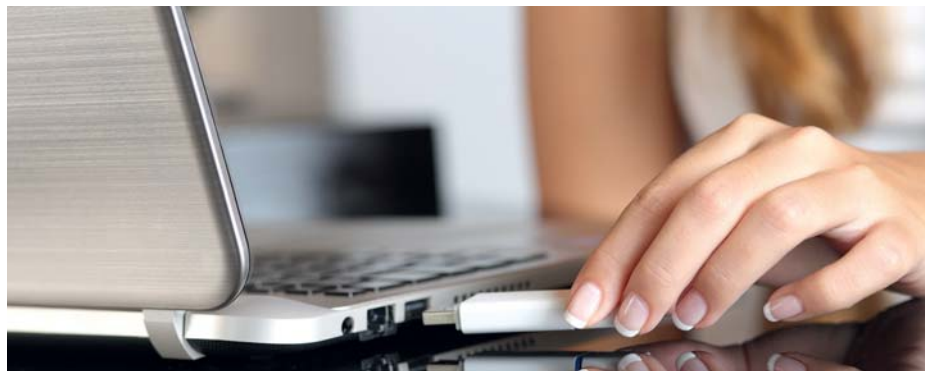
Für die Authentifizierung von Kartenzahlungen lassen sich drei Einsatzszenarien unterscheiden, bei denen Fido eingesetzt werden kann:

– Klassisches 3D-Secure-Verfahren,

– Delegated Authentication und

– Secure Payment Confirmation (SPC).

Bei 3D-Secure handelt es sich um einen weitverbreiteten Industriestandard, der einen Großteil des Marktes abdeckt und von den Kartenherausgebern gepuscht wird. In den Spezifikationen für 3D-Secure ist festgelegt, wie Fido für die Authentifizierung genutzt werden kann. 3D-Secure wird von manchen Händlern mit Skepsis betrachtet, da es im Checkout-Vorgang zu vermehrten Kaufabbrüchen kommen kann, wenn der Authentifizierungsschritt zu umständlich aufgesetzt ist. Je nahtloser und mit je weniger Schritten der Authentifizierungsprozess auskommt, desto besser ist die User Experience und damit die Akzeptanz durch die Nutzer.



Fido-Nutzung von Roaming-Authentifikatoren zur Authentifizierung – bei Pluscard bereits im Einsatz

Delegated Authentication für kleine Händler noch aufwendig

Im Zusammenhang mit der Einführung von Fido2 gewinnt ein weiterer Ansatz an Aufmerksamkeit, der die Situation der Händler deutlich verbessern könnte. Dieser Vorgang, der in der PSD2 beschrieben wird, ermöglicht es Online-Händlern, die Authentifizierung bei der Zahlung mit Kreditkarten selbst zu übernehmen. Normalerweise sind die Banken, die die Karten herausgeben, zuständig für die Authentifizierung der Konsumenten und ihrer Transaktionen. So wird der Zahlungswunsch des Kunden von der Webseite des Händlers zum Server der kartenausgebenden Bank weitergeleitet und nach Überprüfung wieder zurückgeschickt. Dabei kann es zu Reibungsverlusten bis hin zum Abbruch des Kaufs kommen.

Auf Basis detaillierter „Delegated Authentication"-Konzepte von Mastercard und Visa kann der Händler beantragen, die Authentifizierung selbst durchzuführen. Das macht den Vorgang schneller, einfacher und minimiert die Schnittstellen, die technische Probleme erzeugen können. Dazu müssen jedoch die technischen Voraussetzungen geschaffen werden, wobei Fido2 in Zukunft eine wichtige Rolle spielen könnte. Leider gibt es bisher für dieses Konzept noch keinen verbreiteten Industriestandard. Zudem wird es von den Kartenherausgebern nicht unbedingt favorisiert, weil sie damit einen Teil ihrer Kontrolle über den Authentifizierungsvorgang abgeben. Außerdem ist die Implementierung dieses Verfahrens wahrscheinlich für die Mehrheit der kleineren Händler zu aufwendig.

Das World Wide Web Consortium (W3C), das die Techniken im Internet standardisiert, hat bereits einen Entwurf für Secure Payment Confirmation (SPC) als neuen Standard veröffentlicht. Dieser soll die Authentifizierung bei Zahlungs-

transaktionen auf der Basis von Fido vereinfachen und beschleunigen. Somit ergänzen sich Fido und SPC ideal, um die Authentifizierung von Kartenzahlungen im Rahmen von 3D-Secure noch kundenfreundlicher zu gestalten.

Secure Payment Confirmation (SPC) als goldener Mittelweg

Bei Secure Payment Confirmation (SPC) handelt es sich um ein Web API (Application Programming Interface), das von der Web Payment Working Group innerhalb des World Wide Web Consortium (W3C) entwickelt wurde. Google hat es in seinem Browser Chrome 95 bereits implementiert. Zudem ist im neuen EMV 3DS 2.3 Protokoll der Einsatz von SPC nun standardisiert. Issuer, Händler und PSPs können also nicht umhin, sich mit dem Thema zu befassen und seine Chancen auszuloten.

Laut W3C unterstützt das API eine reibungslose Authentifizierung während einer Zahlungstransaktion. Es erbringt den kryptografischen Beleg dafür, dass der Nutzer die Daten des Bezahlvorgangs bestätigt hat. Ein wichtiges Merkmal der sicheren Zahlungsbestätigung ist, dass der Händler die Authentifizierung selbst einleiten kann. Hier kommt das oben beschriebene Konzept der „Delegated Authentication" zum Tragen. Sowohl bei der Registrierung als auch bei der Authentifizierung kommt Fido zum Einsatz und macht dieses neue Verfahren dadurch für den Nutzer so angenehm und unkompliziert. Experten erwarten deshalb, dass sich mit SPC die Konversionsraten signifikant steigern sowie die Transaktionszeiten deutlich verringern lassen.

Erste Fido-Implementierung im Payment-Bereich

Viele Konzepte für eine sichere Authentifizierung mit Fido befinden sich noch im Entwicklungsstadium. Bis auf eine Ausnahme: In einem gemeinsamen Projekt lancierten Pluscard, Full-Service Processor für zahlreiche kartenausgebende Institute deutschlandweit, Netcetera, Marktführer für digitale Bezahllösungen, und Entersekt, Spezialist für starke Kundenauthentifizierung, im Juni 2021 die erste Authentifizierungsalternative gemäß Fido-Standard in Europa. Diese verspricht sicheres, uneingeschränktes Zahlen mit der Kreditkarte im Internet, ohne den Einsatz eines mobilen Endgerätes.

Die Authentifizierung wird über einen physischen Token abgewickelt. Diesen Token bekommen die Kunden von der Bank für die Verwendung am Computer. Die Kunden registrieren den Token über eine eingerichtete Registrierungsseite. Der Token ist danach mit der Kreditkarte verknüpft und Kunden können damit ganz einfach ihre Online-Transaktionen authentifizieren.

Kunden ohne mobiles Endgerät haben nun die Möglichkeit, ihre Online-Zahlungen bequem und sicher über den Fido-Token freigeben zu können. Zusammen mit Netcetera und Entersekt wurde mit dem Fido-Standard eine zukunftssichere Lösung umgesetzt. Diese ist bisher eine einzigartige Alternative zur App-basierten Authentifizierung auf dem deutschen Markt. Da mittelfristig neben Roaming-Authentifikatoren auch Plattform-Authentifikatoren eine größere Rolle spielen werden und die Lösung von Pluscard auf die Nutzung beider Methoden ausgerichtet ist, hat diese Lösung viel Potenzial für die Zukunft.

Die passwortlose Zukunft ist zum Greifen nah

Für Unternehmen, die die geforderte Sicherheit mit einer guten Nutzererfahrung verbinden wollen und auf eine einheitliche Lösung setzen, die über alle Kanäle hinweg funktioniert, ist Fido bereits heute eine Authentifizierungslösung. Spätestens dann, wenn 3D-Secure 2.3 umgesetzt ist, wird die passwortlose, sichere und gleichzeitig nutzerfreundliche Authentifizierung im Bereich Payments nicht mehr wegzudenken sein.

Und wenn SPC zum neuen Standard wird, hat Fido das Potenzial, zum „Game Changer" für reibungslose, sichere Zahlungsvorgänge zu werden. Jedoch wird es noch einige Zeit dauern, bis alle Voraussetzungen am Markt geschaffen sind und sich alle relevanten Marktteilnehmer dem Standard angeschlossen haben. ■