Whitepaper

Passkeys-Handbuch

Wie Sie mit Phishing-resistenter FIDO-Authentisierung die User-Experience verbessern und Account-Übernahmen verhindern.

Inhalt

Einführung

Technikhistoriker werden Passkeys – speziell Synced Passkeys – möglicherweise einmal als Wendepunkt in der Phishing-resistenten Web-Authentisierung und dem Übergang zu einem passwortlosen Paradigma betrachten.

Gerätegebundene Passkeys gibt es seit mehreren Jahren, aber einige der Aspekte, die zu starker Authentisierung beitragen (z. B. die Bindung an ein bestimmtes Gerät), standen ihrer breiten Akzeptanz bisher im Weg.

Synced Passkeys auf der anderen Seite:

- können über mehrere Geräte hinweg synchronisiert werden
- ermöglichen Multi-Faktor-Authentifizierung (MFA) in einem einzigen Schritt

Diese Eigenschaften tragen zu einer hochwertigen Experience bei, die die Attraktivität von Synced Passkeys für die breite Masse deutlich erhöhen dürfte.

Passkeys erhöhen auch die Kontosicherheit für die Mehrheit der Benutzer. So lassen sich Account-Takeover-Angriffe (ATO) eindämmen, was Benutzern und Service-Providern hohe Kosten und viel Mühe erspart.

Obwohl Passkeys keineswegs die perfekte Authentisierungslösung für alle Benutzeranforderungen in allen Szenarien sind, sind wir bei Okta überzeugt, dass sie eine praktikable, Phishing-resistente und bessere Alternative zu Passwörtern darstellen. Daher wollen wir Entwicklern die Einbindung von Passkeys in ihre Authentisierungsprozesse so einfach wie möglich machen.

Um die Akzeptanz zu fördern, bietet dieses Dokument eine Übersicht über:

- die Vorteile von Passkeys
- die Funktionsweise von Passkeys
- die verschiedenen Implementierungsmöglichkeiten von Passkeys

Passkeys sind FIDO-Zugangsdaten, die von Browsern erkannt werden können oder in nativen Anwendungen oder Security Keys zur passwortlosen Authentisierung enthalten sind. Basierend auf den Standards der FIDO Alliance und des World Wide Web Consortiums (W3C) ersetzen Passkeys Passwörter durch Paare kryptographischer Keys.

Passkeys gibt es in zwei Varianten:

- Synced Passkeys, die über einen Cloud-Service über alle Geräte eines Benutzers hinweg synchronisiert sind, ähnlich wie ein Betriebssystem oder Passwortmanager
- Gerätegebundene Passkeys, die auf einem bestimmten Gerät verbleiben; diese können mit FIDO-zertifizierten Authentisierungsfaktoren und Security Keys verwendet werden, einschließlich solcher, die eine Sicherheitszertifizierung erhalten haben

In der Praxis ersetzen Synced Passkeys die Kombination aus Passwörtern und Multi-Faktor-Authentifizierung (MFA) für Standard-Benutzerkonten, und gerätegebundene Passkeys können sogar noch mehr Schutz und Sicherheit bieten.

Die FIDO Alliance und Okta

Die 2012 gegründete und 2013 der Öffentlichkeit vorgestellte FIDO Alliance ist ein offener Branchenverband mit dem Ziel, Authentisierungsstandards zu entwickeln und zu fördern, die „dazu beitragen, die Abhängigkeit von Passwörtern weltweit zu reduzieren“.

Der Verband:

- entwickelt technische Spezifikationen, die offene, skalierbare und dialogfähige Mechanismen definieren, die die Abhängigkeit von Passwörtern zur Benutzerauthentisierung reduzieren
- führt Branchenzertifizierungsprogramme durch, um eine erfolgreiche weltweite Einführung der Spezifikationen sicherzustellen
- reicht ausgereifte technische Spezifikationen bei anerkannten Normungsorganisationen zur formalen Standardisierung ein

Okta ist ein Sponsor-Level-Mitglied der FIDO Alliance. (Eine Liste aller Mitglieder finden Sie hier).

Durch den Terminologie-Dschungel: Eine kurze Geschichte der „Passkeys“
Verwirrt von der Terminologie und ihrer Entwicklung? Sie sind nicht allein! Hier ist ein wenig historischer Kontext, um das Dickicht zu lüften.

Im April 2018 erreichte der W3C Web Authentication Standard Candidate-Recommendation-Status und FIDO2 wurde offiziell eingeführt. Das von der FIDO Alliance entwickelte FIDO2 spezifiziert den Web-Authentication-JavaScript-API-Standard – allgemein bekannt als WebAuthn – und das entsprechende Client-to-Authenticator Protocol (CTAP) der FIDO.

Mit Hilfe der JavaScript API können Entwickler entweder Hardware-Keys (so genannte Roaming Authenticators) oder sichere Hardware auf dem Gerät (so genannte Platform Authenticators) verwenden – wobei letztere häufig durch biometrische Sensoren flankiert werden –, um Benutzer passwortlos zu authentifizieren.

Durch das Abstrahieren der Informationen über den Speicherort von Public Keys und Private Keys, haben diese Spezifikationen zur breiten Verfügbarkeit Phishing-resistenter Authentisierungsfunktionen auf modernen Geräten beigetragen.

Im Mai 2022 kündigten die Tech-Giganten Apple, Google und Microsoft an, FIDO2 um die Möglichkeit zu erweitern, Platform-Authentisierungsfaktoren in einer neuen Synchronisierungsstruktur zu sichern. Diese erweiterte Palette an Funktionen soll es Websites und Apps erleichtern, FIDO Credentials anstelle von Passwörtern zu verwenden.

In der Pressemitteilung tauchte der Begriff „Passkey“ zwar einmal auf:

- „Passkey“ bezog sich zum damaligen Zeitpunkt allerdings ausschließlich auf FIDO Multi-Device Credentials
- FIDO Multi-Device Credentials war der bevorzugte Begriff

Später bezeichnete der Begriff „Passkey“ die FIDO Credentials im Allgemeinen.

Mit der zunehmenden Verbreitung und Akzeptanz von Passkeys auf den wichtigsten Plattformen hat sich die FIDO Alliance jedoch auf den Begriff „Passkeys“ geeinigt, der nun sowohl Synced Passkey als auch gerätegebundene Passkeys umfasst. Der Begriff „Multi-Device Credentials“ wurde damit obsolet.

Warum sind Passkeys so wichtig?

Die breite Akzeptanz von Passkeys aufseiten der Benutzer wäre ein wichtiger Schritt im Kampf gegen Phishing, Kontoübernahmen und andere Identity Threats.

Die gängige Meinung ist, dass sicherere Authentisierung stets zulasten der User-Experience geht. Passkeys haben aber das Potenzial, die Sicherheit zu erhöhen und gleichzeitig die User-Experience zu verbessern, weil sie Authentisierungsprozesse vereinfachen und beschleunigen.

Passkeys sind sicherer als Passwörter (und herkömmliche MFA-Verfahren)

Es ist kein Geheimnis, dass Passwörter eine schlechte Lösung für das Problem der Benutzerauthentisierung sind. Es ist sogar nicht übertrieben zu sagen, dass Passwörter und Passwortmanagement zu einem Witz geworden sind: Es gibt zum Beispiel nicht weniger als drei xkcd-Comics (Password Reuse, Password Strength und Encryptic) zu diesem Thema.

Was als einfaches, von Menschen ausgefülltes Login-Feld begann, hat sich im Laufe der Jahre dramatisch verändert:

- Da Angreifer immer geschickter darin wurden, schwache Passwörter zu erraten und die weit verbreitete Wiederverwendung von Passwörtern auszunutzen, stiegen die Anforderungen an die Komplexität, was zu immer längeren Passwörtern mit Sonderzeichen, Kombinationen aus Groß- und Kleinbuchstaben und Zahlen führte
- Dies zwang die Benutzer, sich mit mehr und komplexeren Passwörtern auseinanderzusetzen, und förderte die Verbreitung von Passwort-managern (entweder als Browser- oder separate Anwendung)
- Phishing wurde zu einer weit verbreiteten Bedrohung, riesige Password-Dumps tauchten im Netz auf, und MFA etablierte sich als effektive Strategie gegen ATO
- Heute sind viele MFA-Verfahren von einst gefährdet, da Angreifer skalierbare und kostengünstige Wege finden, diese wichtige Hürde zu umgehen
- Währenddessen – meist jedoch hinter den Kulissen – führten Workforce- und Customer-Identity-Systeme Sicherheitsebenen ein, um sich vor einer breiten Palette automatisierter Cyberangriffe zu schützen, die Unternehmen finanziellen Schaden verursachen und Kundendaten bedrohen

Viele dieser Änderungen haben die User-Experience getrübt, vor allem durch den Mehraufwand bei alltäglichen Vorgängen wie der Registrierung oder dem Login.

Glücklicherweise bieten Passkeys eine Phishing-resistente Alternative zu Passwörtern, inklusive eines zweiten, impliziten, Authentisierungsfaktors.

Probleme mit Passwörtern

Basierend auf einer Befragung von 21.512 Verbrauchern in 14 Ländern kommt der Okta Customer Identity Trends Report zu folgenden Ergebnissen:

- 65 % der Befragten sind mit der Anzahl an Benutzernamen und Passwörtern, die sie managen müssen, überfordert
- 33 % geben an, dass es sie frustriert, ein Passwort wählen zu müssen, das bestimmten Vorgaben genügt
- 25 % fanden es frustrierend, für jeden Online-Service ein neues Passwort erstellen zu müssen

Passkeys sind Phishing-resistent

Business-to-Consumer-Anbieter (B2C) können ihre Websites durch den Ersatz von Passwörtern durch FIDO-Standards gegen automatisierte, seitenübergreifende Passwortangriffe wie Password Spraying oder Passwort Stuffing schützen. Da die FIDO Public Key mit Verschlüsselung arbeitet, müssen Unternehmen nur den Public Key eines Benutzers speichern – dessen Diebstahl für Angreifer von geringem Wert ist. Der Private Key des Benutzers wird sicher auf seinem lokalen Gerät gespeichert. Er bleibt auf den vertrauenswürdigen Geräten des Benutzers und lässt sich ohne großen Aufwand innerhalb über das Ökosystem des jeweiligen Betriebssystems oder über einen vertrauenswürdigen Third-Party-Service synchronisieren. Die Passkey-Synchronisierung ist E2E-verschlüsselt, sodass sensible Daten während des gesamten Prozesses geschützt sind.

Neben der Verringerung des Risikos und der Angriffsfläche von Unternehmen kommt diese Resilienz auch den Benutzern zugute. Diejenigen, die sich für Passkeys entscheiden, sind weitaus seltener von Account-Übernahmen und deren Folgen betroffen, die von kleinen Unannehmlichkeiten bis hin zu Datenschutzverletzungen und Identitätsdiebstahl reichen können.

Passkeys können implizit starke MFA bieten

Multi-Faktor-Authentisierung (MFA) erfordert zwei oder mehr Authentisierungsfaktoren. Zum Beispiel:

- Ein Wissensfaktor → etwas, das Sie wissen, wie ein Passwort, eine PIN oder eine Sicherheitsfrage
- Ein Besitzfaktor → etwas, das Sie besitzen, wie ein registriertes Gerät
- Ein Inhärenzfaktor → etwas, das Ihnen eigen ist, z. B. Ihr Fingerabdruck

Da Passkeys auf den Geräten des Benutzers gespeichert werden (Besitzfaktor) und – falls eine Verifizierung erforderlich ist – nur vom Benutzer über Biometrie, Sicherheitscode oder eine andere FIDO-konforme Technik verwendet werden können (Inhärenz- oder Wissensfaktor), erfüllen sie implizit das Grundprinzip der MFA.

Die MFA in Zusammenhang mit Passkeys zählt zu den stärksten verfügbaren und stellt einen großen Fortschritt gegenüber dem Schutz dar, den die heute noch üblichen Magic Links und One-Time Passcodes (OTPs) bieten.

Für viele kundenorientierte Unternehmen sind die Sicherheitsvorteile allein schon Grund genug, Passkeys zu implementieren – Sicherheit ist aber nur ein Aspekt.

Passkeys für Use Cases mit mittleren Sicherheits-anforderungen

Alle Passkeys haben mehrere gemeinsame Sicherheitsmerkmale, sind in hohem Maße Phishing-resistent und verwenden eindeutige Key-Paare für starke Authentisierung. Es gibt jedoch wichtige Unterschiede zwischen Synced Passkeys und gerätegebundenen Passkeys, die sich auf ihre Eignung für Use Cases mit unterschiedlichen Sicherheitsanforderungen auswirken.

Um Unternehmen dabei zu unterstützen, fundierte Entscheidungen zu treffen, insbesondere im Zusammenhang mit den Authenticator Assurance Levels (AALs), des National Institute of Standards and Technology (NIST), hat die FIDO Alliance im Juni 2023 die FIDO Authentication for Moderate Assurance Use Cases veröffentlicht.

Das Whitepaper bietet eine Orientierungshilfe für Unternehmen bei der Analyse der Möglichkeiten und Eigenschaften von gerätegebundenen Passkeys und Synced Passkeys, um festzustellen, wie beide Credential-Typen in einer Umgebung mit mittleren Sicherheitsanforderungen – definiert als ein Unternehmen mit mehreren verschiedenen Authentisierungs-Use-Cases, die durch eine Kombination von AAL1- und/oder AAL2- sowie AAL3-Sicherheitsstufen abgedeckt werden können – eingesetzt werden können.

Bitte beachten Sie: Das NIST aktualisiert derzeit die Sicherheitsstufen im Zusammenhang mit Synced Passkeys. Behalten Sie also die einschlägigen NIST- und FIDO-Alliance-Ressourcen im Auge, um auf dem neuesten Stand zu bleiben.

Passkeys sind komfortabler als Passwörter

Durch das Ersetzen umständlicher Authentisierungsprozesse durch Fingerabdruck- und Gesichtsscan, PIN-Eingabe oder andere vertraute Verfahren zum Entsperren von Geräten reduzieren Synced Passkeys die Reibungsverluste, die Benutzer im Umgang mit Online-Services erleben.

Es ist bezeichnend, dass einige der Early Adopters von Passkeys – darunter Shopify, DocuSign und PayPal – eine sichere und *komfortable* User-Experience bieten.

Für viele Service-Provider könnte die hohe Benutzerfreundlichkeit von Synced Passkeys gar zu ihrem attraktivsten Merkmal werden. Während gerätegebundene Passkeys erfordern, dass sich die Benutzer mit jedem Gerät bei jeder Website oder App registrieren, erlauben Synced Passkeys:

- Benutzern den automatischen Zugriff auf ihre FIDO Sign-in Credentials auf mehreren (auch neuen) Geräten
- Benutzern die Wiederherstellung ihrer Passkeys, selbst wenn sie alle ihre Geräte verlieren

Im Privatkundengeschäft ist Mehraufwand – sprich: alles, was die Interaktion des Anwenders mit Ihrem Service verlangsamt – ein großes Hindernis für Konversionen und somit für den Umsatz. Der Okta Customer Identity Trends Report ergab, dass fast 60 Prozent der Befragten eher dazu bereit wären, Geld auszugeben, wenn Services einen einfachen, sicheren und reibungslosen Login-Prozess bieten würden. Diese Erkenntnis gilt dabei über alle Segmente und Branchen hinweg. Eine unkomplizierte und komfortable Interaktion ist also allen Kunden gleichermaßen wichtig.

Während es einige regionale Unterschiede gab, zeigen sich die größten Diskrepanzen bei den Altersgruppen: Jüngere Verbraucher geben etwa ein Drittel häufiger mehr Geld aus als ältere Verbraucher, wenn ihnen eine einfache, sichere und reibungslose Login-Erfahrung geboten wird (Abbildung 1).

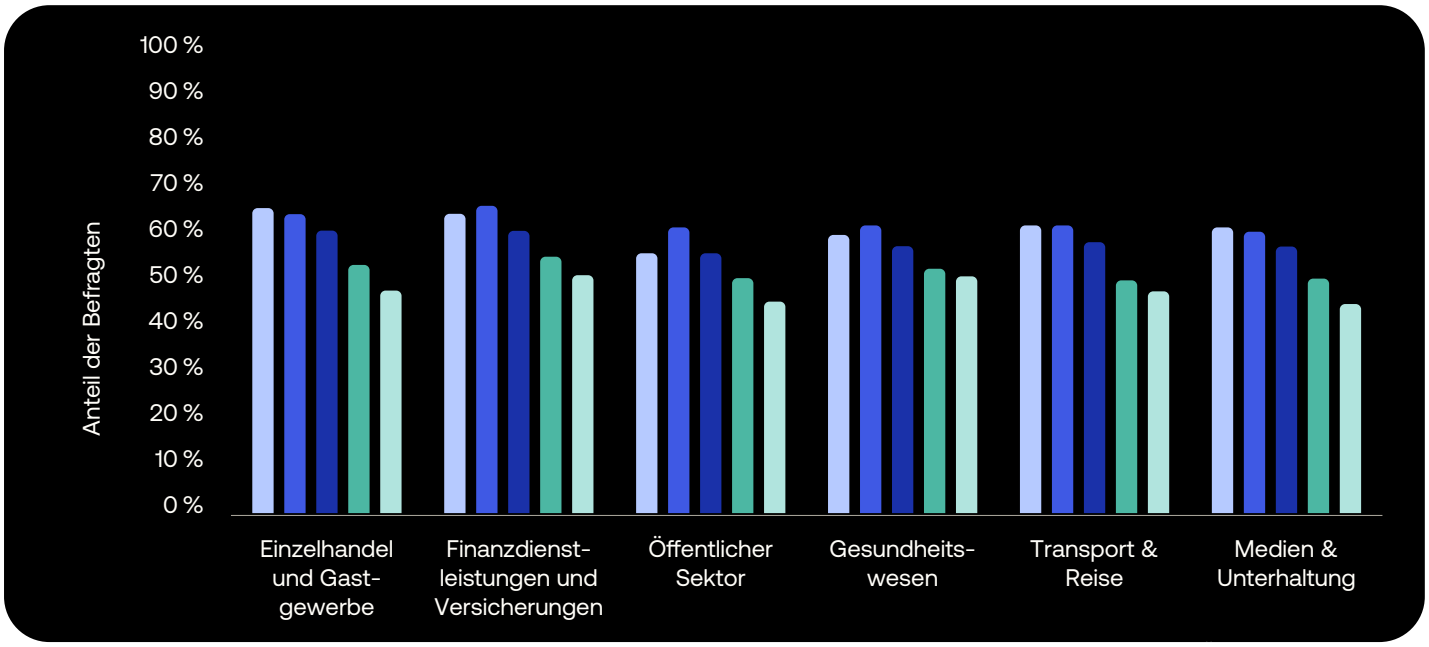


Abbildung 1: Wenn Sie online mit einem Unternehmen interagieren, wären Sie dann eher oder weniger geneigt Geld auszugeben, wenn Sie wüssten, dass der Login-Prozess einfach, sicher und reibungslos ist? Die Grafiken zeigen die Summe der Antworten „sehr wahrscheinlich“ und „eher wahrscheinlich“.

Natürlich ist ein gewisses Maß an Reibungsverlust notwendig, um Vertrauen zu schaffen und Sicherheit zu bieten. Allerdings kann die Reduzierung von Reibungsverlusten, wo immer dies möglich ist – bei jeder Kundeninteraktion –, die Konversionsraten erhöhen und somit den Umsatz sowohl kurz- als auch langfristig steigern.

Sehen wir uns nun an, wie Passkeys den Aufwand für die Benutzer im Vergleich zu Passwörtern reduzieren können.

Synced Passkeys lassen sich schneller verwenden als Passwörter

Untersuchungen zeigen, dass Synced Passkeys nicht nur einfacher zu verwenden sind als Passwörter, sondern auch deutlich schneller. In einem Post auf deren Security-Blog zeigte Google, dass der Login mit einem Passkey durchschnittlich 14,9 Sekunden dauert – 50 Prozent schneller als die 30 Sekunden, die man mit einem Passwort benötigt.

Im Blog heißt es weiter: „Vorläufige, qualitative Daten deuten auch darauf hin, dass dieser Komfort für Benutzer bereits jetzt den wichtigsten Mehrwert von Passkeys darstellt.“

Passkeys sind einfacher in der Handhabung als Passwörter

Während ein aufwändiges Handling für die meisten Verbraucher lediglich eine Unannehmlichkeit ist, können sie manche Verbraucher daran hindern, auf Ihre Services zuzugreifen.

Denken Sie an Seh- oder kognitive Beeinträchtigungen oder eingeschränkte motorische Fähigkeiten und stellen Sie sich vor, Sie müssten durch einen umständlichen Authentisierungsprozess navigieren, bei dem der Benutzer sich ein langes, komplexes Passwort merken und dann eingeben (oder es „einfach“ nachschlagen, kopieren und einfügen) muss. Oder stellen Sie sich vor, wie ein nicht technologieaffiner Benutzer auf eine Nachricht reagieren würde, in der er aufgefordert wird, eine Authenticator-App herunterzuladen.

Passkeys bieten eine barrierefreie Alternative zu diesen traditionellen Ansätzen.

Barrierefreiheit entlang der gesamten Customer Journey zu gewährleisten, hat auch einen finanziellen Anreiz. Mit Angeboten für jedermann können Unternehmen ihre Marktreichweite maximieren.

Synced Passkeys machen stärkere Authentisierung bequemer

Synced Passkeys bieten Komfort auch bei erhöhter Sicherheit, da sie sowohl die Identität als auch den Private Key eines Benutzers in einem einzigen Schritt (aus Benutzersicht) verifizieren – eine deutliche Verbesserung gegenüber anderen MFA-Verfahren.

Dieser erhöhte Komfort erlaubt es Service-Providern auch, erneute Authentisierungen in kürzeren Zeitabständen oder als zusätzliche Hürde in Betracht zu ziehen (z. B. für den Zugriff auf sensible Apps, für Konto-änderungen, für den Zugriff auf private Daten usw.). Beides sind wichtige Schutzmaßnahmen gegen Session-Hijacking-Angriffe. Dem **Okta Secure Sign-in Trends Report 2023** zufolge dauerten Authenticator-Abfragen mit WebAuthn durchschnittlich nur drei Sekunden – ein Vielfaches schneller als die Kombination aus Passwörtern und OTP-basierten Abfragen.

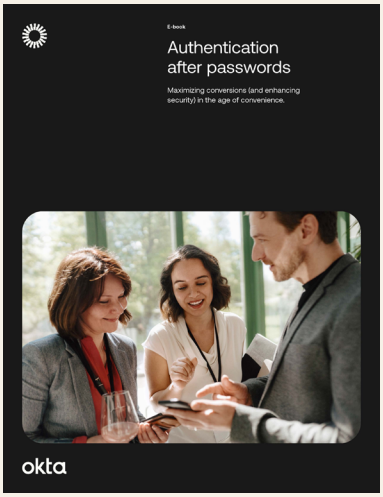
Synced Passkeys lassen sich einfacher ausrollen als Passwörter

All diese Annehmlichkeiten stehen Benutzern natürlich erst nach der Registrierung eines Synced Passkeys zur Verfügung, weshalb die Registrierung unkompliziert sein sollte. Die wiederholte Registrierung, die bei gerätegebundenen Passkeys erforderlich ist, wird häufig als einer der Hauptgründe für die geringe Akzeptanz von WebAuthn – insbesondere im Verbraucherkontext – angeführt.

Synced Passkeys lösen dieses Problem, indem sie es ermöglichen, dass sich die FIDO Credentials eines Benutzers einfach (aber sicher) über mehrere Geräte hinweg bewegen: Die Registrierung selbst ist unkompliziert und nur einmal pro Service notwendig.

Dem Secure Sign-In Trends Report zufolge beträgt die durchschnittliche Zeit für die Registrierung eines Passworts etwa 34 Sekunden – einschließlich der Zeit, die ein Benutzer für die Erstellung und Bestätigung (erneute Eingabe) eines neuen Passworts benötigt. Im Gegensatz dazu dauerte die WebAuthn-basierte Registrierung nur 19 Sekunden, was die Annahme widerlegt, dass stärkere Authentisierungsfaktoren während der Registrierung einen erheblichen Aufwand für die Benutzer bedeuten.

Am Ende des Tages werden Benutzer Synced Passkeys anfangs als ungewohnt, die Registrierung aber schnell als mindestens genauso intuitiv und viel schneller als andere Authentisierungsmechanismen empfinden.



Synced Passkeys sind ein wichtiger Schritt in Richtung einer passwortlosen Welt

Da sie im Vergleich zu Passwörtern sowohl einen besseren Schutz als auch eine komfortablere User-Experience bieten, haben Synced Passkeys gute Chancen, die passwortlose Authentisierung weit über den Kreis der IT-Administratoren (die die Sicherheit priorisieren) und Early Adopters (die die vielen Vorteile erkennen) hinaus salonfähig zu machen.

Holen Sie sich unseren detaillierten Guide **Authentication After Passwords** und erfahren Sie mehr über die passwortlose Zukunft, gängige Irrtümer – etwa, dass Sie, ohne es zu wissen, wahrscheinlich bereits passwortlose Prozesse etabliert haben – und darüber, was Sie jetzt tun können, um der Konkurrenz einen Schritt voraus zu sein (und zu bleiben).

Mehr über die Passwordless Journey von Okta erfahren Sie in **Warum wir bei Okta zu 100 Prozent passwortlos arbeiten**.

Wie funktionieren Passkeys?

Wie von der FIDO Alliance erläutert, verwenden die zugrundeliegenden FIDO-Protokolle Standard-Public-Key-Cryptography für starke Authentisierung. Um sich bei einem Online-Service zu registrieren, erzeugt das Gerät des Benutzers ein neues Paar kryptografischer Keys, bestehend aus:

- einem Public Key, der beim Online-Service registriert ist
- einem Private Key, der geheim gehalten wird

Die Keys werden sicher und eindeutig für jedes Konto generiert – Sie müssen sich keine Sorgen machen, dass Benutzer einen schwachen Private Key wählen, und die Private Keys werden nicht für mehrere Services wiederverwendet.

Um sich bei einem bestimmten Service zu authentisieren, weist das Client-Gerät den Besitz des zum Konto gehörenden Private Keys nach, indem es eine vom Service bereitgestellte Challenge signiert – der Service selbst sieht den Private Key zu keinem Zeitpunkt und muss diese Information daher auch nicht speichern oder schützen.

Entscheidend ist, dass der Private Key erst dann verwendet werden kann, wenn er vom Benutzer entsperrt wurde, wobei das lokale Entsperren normalerweise entweder über ein Zweitfaktor-Gerät oder den Entsperrmechanismus des primären Geräts erfolgt – in der Regel eine biometrische Authentisierung (z. B. Touch ID, Face ID, Windows Hello usw.) oder eine PIN.

Synced Passkeys unterscheiden sich insofern von früheren FIDO2-Implementierungen, als dass sie:

- Benutzern die Möglichkeit geben, Synced Passkeys auf jedem Gerät in einem bestimmten Ökosystem zu verwenden, in dem die Passkeys auf dem Gerät und in der Cloud gesichert sind
- Benutzern die Möglichkeit geben, Ökosystem-Grenzen dank geräte-übergreifender Authentisierung bequem zu verlassen, ohne dass die FIDO Credentials auf neuen Geräten registriert werden müssen

Weitere Informationen zur Funktionsweise von Passkeys finden Sie auf der Website der FIDO Alliance.

Wie integriere ich Passkeys in meine App?

Grundsätzlich haben Entwickler zwei Möglichkeiten, die Authentisierung um Passkeys zu erweitern:

- Passkeys über APIs und SDKs selbst implementieren; und
- einen Identity-Service-Provider beauftragen.

Weitere Informationen zum Einsatz von Passkeys

Die FIDO Alliance hat eine Reihe von Whitepapers für IT-Administratoren, Sicherheitsarchitekten und Vorstände veröffentlicht, die den Einsatz von FIDO-Authentisierung in ihrem Unternehmen in Betracht ziehen.

Der DIY-Ansatz

Aus Implementierungssicht sehen Synced Passkeys genauso aus wie zertifikatlose Platform-Authentisierungsfaktoren. Das heißt, wenn Ihre Web-App aus Protokollsicht bereits WebAuthn unterstützt und keine Zertifikatsantwort benötigt, unterstützen Sie Synced Passkeys de facto bereits. Mit Blick auf die User-Experience ist dies jedoch nicht ganz korrekt. Zum Beispiel:

- Die Eingabeaufforderungen und Formulierungen auf Ihren aktuellen Registrierungsseiten beziehen sich wahrscheinlich auf gerätebezogene Credentials (z. B. „Loggen Sie sich von diesem Gerät aus schneller ein“), was im Falle von Synced Passkeys nicht mehr ganz der Wahrheit entspricht.
- Wahrscheinlich verwenden Sie die Platform-Authentisierungsfaktoren nur als sekundäre Authentisierungsfaktoren, da Sie vor Synced Passkeys unmittelbar für die Kontowiederherstellung verantwortlich waren.

Keine der oben genannten Änderungen ist übermäßig komplex, zumal dann wenn Sie WebAuthn bereits implementiert haben – Sie müssen allerdings ein wenig Aufwand in eine gute Erfahrung stecken.

Um Entwickler zu unterstützen, haben die W3C WebAuthn Community Adoption Group und die FIDO Alliance im Oktober 2022 mit Passkeys.Dev eine Online-Ressource ins Leben gerufen, die (unter anderem) eine umfassende Dokumentation bereitstellt und die unterstützten Geräte trackt.

Identity Unlocked

Passkeys mit Andrew Shikiar und Tim Cappalli

Kurz nach der Ankündigung von Synced Passkeys (als geräte-übergreifende Credentials) sprachen Andrew Shikiar (Executive Director & CMO, FIDO Alliance) und Tim Cappalli (Digital Identity Standards Architect bei Microsoft) mit Host Vittorio Bertocci (Principal Architect bei Auth0) im Rahmen des **Identity Unlocked Podcasts**.

Hören Sie rein, um mehr über die Entwicklung von FIDO Credentials zu erfahren und weitere entwicklungsorientierte Einblicke in die Funktionsweise von Multi-Device Credentials zu erhalten.

Einbindung eines Identity-Service-Providers

Identity Management ist schwierig – selbst für erfahrene Experten ist es eine Herausforderung, effektive und effiziente Implementierungen bereitzustellen. Hinzu kommt, dass die Kundenerwartungen ständig steigen, da jeder Benutzer jede Erfahrung mit der besten vergleicht, die er bisher gemacht hat – was Unternehmen erheblich unter Druck setzt, ihre UX ständig weiterzuentwickeln.

Identitätsanforderungen müssen erfüllt werden, ohne wertvolle Engineering-Ressourcen zu binden, die für die Erweiterung der Kernkompetenzen benötigt werden – und beide Ziele müssen erreicht werden, ohne gesetzliche Anforderungen zu vernachlässigen oder Kompromisse bei der Sicherheit einzugehen.

Aus diesen Gründen halten es viele Unternehmen für effizienter und kostengünstiger, einen Identity-Service in ihre Anwendungen und ihren Tech-Stack zu integrieren. Darüber hinaus können Unternehmen durch die Zusammenarbeit mit einem Identity-Service-Provider eine Vielzahl von Anforderungen im Bereich Customer Identity & Access Management (CIAM) abdecken, darunter:

- Authentisierung
- Autorisierung
- User-Management

Etablierte Identity-Provider unterstützen Passkeys und bieten Anwendungsentwicklern damit eine bequeme Möglichkeit, ihre Authentisierungsoptionen zu erweitern und mit der sich dynamischen Authentisierungslandschaft Schritt zu halten.

Wenn Sie eine App beispielsweise so konfiguriert haben, dass sie die Okta Customer Identity Cloud zur Authentisierung verwendet, können Sie die Passkey-Authentisierung kurzfristig bereitstellen, ohne Ihren Code ändern zu müssen.

Unterschiedliche Identity-Provider bieten jedoch unterschiedliche Features, weshalb Due Diligence ein Muss ist. Hier sind einige Aspekte, die Sie auf Ihrer Einkaufsliste vermerken sollten:

- Unabhängig und neutral
  Ihre CIAM-Lösung sollte neue Wege öffnen, keine Barrieren schaffen. Sie sollte sich in Ihre bestehenden Lösungen einfügen und auf offenen Standards aufsetzen, um einen Vendor Lock-in zu vermeiden. Und sie sollte mit ihrem bevorzugten Cloud-Provider kompatibel sein.

- Vollumfänglich und individualisierbar
  Jeder Kunde ist einzigartig – und hat ganz eigene, komplexe Anforderungen. Ihre CIAM-Lösung sollte daher für jede Art von User eine hochwertige, konsistente und vertrauenswürdige User-Experience garantieren.

- Einfach zu entwickeln, zu warten und zu nutzen
  Ihre Teams achten bei jeder einzelnen Technologie-Komponente darauf, dass sie sich so einfach und schnell wie möglich integrieren konfigurieren und betreiben lässt. Das müssen Sie auch bei Ihrer CIAM-Lösung im Blick behalten.

- Zuverlässig
  Ein erfolgreicher Angriff, ein Compliance-Verstoß oder ein längerer Einbruch in der Verfügbarkeit und Qualität Ihrer Dienste kann ernsthafte Folgen haben und Strafzahlungen, Vertrauensverlust und wirtschaftliche Schäden nach sich ziehen. Die richtige CIAM-Lösung sollte diese Risiken nachhaltig minimieren.

Was kommt als Nächstes?

Auth0 (jetzt Okta Customer Identity Cloud) erkannte sehr früh das Potenzial von WebAuthn und übernahm es sowohl als zweiten Faktor für Administratoren, die auf unser Management-Dashboard zugreifen, als auch als Methode, die Entwickler zur Authentisierung ihrer Benutzer beim Schutz ihrer Web-Apps verwenden können.

Trotz der offensichtlichen Sicherheitsvorteile war die Akzeptanz der FIDO2-Authentisierung im Verbraucherkontext bisher jedoch verhalten. Unsere eigenen Beobachtungen deuten darauf hin, dass der größte Teil der Nutzung auf professionelle Anwender zurückzuführen ist, die ein hohes Maß an Sicherheit für den Zugriff auf die von ihnen verwalteten Ressourcen benötigen.

Es gibt viele mögliche Erklärungen, aber es besteht Konsens darüber, dass:

- Hardware-Keys in erster Linie ein Thema für Admins und privilegierte Mitarbeiter und weniger für den breiten Verbrauchermarkt sind
- Platform-Authentisierungsfaktoren einen höheren Komfort bieten. Aber da sie an ein einzelnes Gerät gebunden sind (was in Business-Szenarien durchaus ein Pluspunkt sein kann), ist die Benutzer-freundlichkeit für Verbraucher ein Problem, da die Benutzer oft viele Geräte besitzen und regelmäßig neue erwerben

Die Einführung von Synced Passkeys – und der beträchtliche Einfluss von Apple, Google, Microsoft und anderen – könnte jedoch einen wichtigen Wendepunkt darstellen. Einige Benutzer werden sie lieben, andere werden zögern, aber in den kommenden Monaten und Jahren werden Passkeys allgegenwärtig und vertraut werden.

Generell wird passwortlose Authentisierung angesichts der hochwertigen User-Experience und des besseren Schutzniveaus immer breitere Akzeptanz erfahren. Unternehmen, die ihren Kunden und anderen Benutzern Passkeys und andere passwortlose Authentisierungsmechanismen bieten, werden profitieren.

Allerdings sind noch einige Fragen offen. Zum Beispiel:

- Passkeys sind Phishing-resistent, aber das Onboarding eines neuen Benutzers mit dem Passkey und der Möglichkeit, diesen wiederherzustellen (z. B. das E-Mail-Konto, das mit dem Ökosystem des Betriebssystems verbunden ist), stellt eine potenzielle Schwachstelle dar.
- Bisher variiert die User-Experience je nach Plattform-Ökosystemen und Passwortmanager. Die FIDO Alliance arbeitet an einer Vereinheitlichung – zumindest kurzfristig wird es aber weiterhin zu inkonsistenten Experiences kommen, die bei einigen Benutzern zu Frustrationen führen können.
- Wie bereits erwähnt, ist die Einordnung von Synced Passkeys in das AAL-Framework des NIST eine unbeantwortete Frage – eine, die in einer Welt, in der viele Mitarbeiter ihre privaten Geräte nutzen, um auf geschützte Unternehmensressourcen zuzugreifen, von zentraler Bedeutung ist.
- Wie bei anderen neuen Technologien stellt die Aufklärung der Verbraucher auch im Zusammenhang mit Passkeys eine Herausforderung dar, insbesondere im Hinblick auf Sicherheit, Datenschutz und Usability.

Es ist wichtig, noch einmal zu betonen, dass Passkeys noch in den Kinderschuhen stecken und sich der gesamte Bereich im Zuge neuer und verbesserter Implementierungen weiterentwickeln wird.

Warum auf Perfektion warten, wenn es bereits heute schon besser geht?

Verglichen mit den Problemen, die mit Passwörtern einhergehen, wirken die Probleme im Zusammenhang mit Passkeys wohl verschwindend gering. Passwörter müssen verschwinden oder zumindest viel seltener werden, und jeder in der Identity-Branche sollte daran arbeiten, Wege zu finden, die Vorteile von Passkeys zu nutzen und gleichzeitig die Nachteile zu minimieren.

Wir bei Okta haben es uns zum Ziel gesetzt, unseren Teil dazu beizutragen, indem wir zeitnah modernste und entwicklerfreundliche Features bereitstellen, die Passkeys unterstützen – und indem wir uns aktiv an den Branchendiskussionen beteiligen, die die Zukunft dieser Technologie mitprägen.

Passwortlos zu arbeiten, wird einfacher werden, wenn sich Plattformanbieter und Gerätehersteller auf standardisierte Prozesse für Wiederherstellung, Ausgabe und Schutz einigen. Denjenigen, die die passwortlose Authentisierung einführen oder erweitern wollen, empfehlen wir, nach Authenticators Ausschau zu halten, die Folgendes bieten:

- Einfache Authentisierung
- Weniger Fehler beim Anmeldeprozess
- Einfaches Onboarding von Benutzern
- Phishing-resistente Technologie

Passkeys erfüllen alle diese Kriterien.