Whitepaper

Passkeys primer

How to improve user experiences and prevent account takeovers by enabling phishing-resistant FIDO authentication.

Contents

Introduction

Technology historians may regard passkeys in general — and synced passkeys in particular — as marking an inflection point in phishing-resistant web authentication and the broader transition to a passwordless paradigm.

Device-bound passkeys have been available for a few years, but some of the same aspects that contribute to strong authentication security (i.e., being tied to a single device) have limited their mainstream adoption.

In contrast, synced passkeys:

- Have the ability to be synchronized across multiple devices
- Allow for Multi-Factor Authentication (MFA) to be performed in a single step

These characteristics contribute to a convenient experience that is expected to vastly expand synced passkeys' mainstream appeal.

Passkeys also meaningfully increase account security for the majority of users — which will help to mitigate account takeover (ATO) attacks, saving users and service providers from a range of expensive consequences.

While passkeys aren't a perfect authentication solution for all user needs in all scenarios, we at Okta believe that they are nevertheless a viable, phishing-resistant, and better alternative to passwords and are committed to making it easy for developers to introduce passkeys into their authentication flows.

To help encourage adoption, this document:

- Reviews the benefits that passkeys offer
- Touches on how passkeys work
- Explores different ways of implementing passkeys

Passkeys are FIDO credentials that are discoverable by browsers, or housed within native applications or security keys for passwordless authentication. Based on FIDO Alliance and World Wide Web Consortium (W3C) standards, passkeys replace passwords with cryptographic key pairs.

Passkeys come in two forms:

- Synced passkeys, that are synced between user's devices via a cloud service, like an operating system ecosystem or password manager
- Device-bound passkeys, that never leave a single device; these can be used on FIDO Certified authenticators and security keys, including those that have achieved security level certification

In practice, synced passkeys replace the combination of passwords and Multi-Factor Authentication (MFA) for standard user accounts, and device-bound passkeys can provide even stronger protection and assurance.

FIDO Alliance and Okta

Founded in 2012 and publicly launched in 2013, the FIDO Alliance is an open industry association with a focused mission to develop and promote authentication standards that "help reduce the world's over-reliance on passwords."

To that end, the organization:

- Develops technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users
- Operates industry certification programs to help ensure successful worldwide adoption of the specifications
- Submits mature technical specification(s) to recognized standards development organization(s) for formal standardization

Okta is a Sponsor-Level Member of the FIDO Alliance (see all members here).

Untangling terminology with a brief history of “passkeys”
Confused by the terminology and how it has evolved? You’re not alone! Here’s a bit of historical context to help straighten things out.

In April 2018, the W3C Web Authentication standard reached candidate recommendation and FIDO2 was officially launched. Developed by the FIDO Alliance, FIDO2 specifies the Web Authentication JavaScript API standard — commonly referred to as WebAuthn — and FIDO’s corresponding Client-to-Authenticator Protocol (CTAP).

Using the Javascript API, developers can leverage either hardware keys (known as roaming authenticators) or secure hardware on the device (known as platform authenticators), the latter of which are often gated by biometric sensors, to authenticate users in a passwordless manner.

By abstracting away the details of where public and private keys reside, this set of specifications led to the widespread availability of phishing-resistant authentication features on modern devices.

In May 2022, the tech giants Apple, Google, and Microsoft announced plans to expand on FIDO2 by adding the ability to back up platform authenticators to a new sync fabric. The goal of this expanded set of features is to make it easier for websites and apps to adopt FIDO credentials instead of passwords.

While the press release included one instance of “passkey,” at that time:

- “Passkey” only referred to FIDO multi-device credentials
- FIDO multi-device credentials was the preferred name

Subsequently, “passkey” referred to discoverable FIDO credentials, in general.

But with widespread introduction and the embrace of passkeys by major platforms, FIDO Alliance has settled upon the term “passkeys” and the term now encompasses both synced passkeys and device-bound passkeys. The term “multi-device credentials” was then deprecated.

Why do passkeys matter?

Mass adoption of passkeys by everyday users would represent a major step in the fight against phishing, account takeovers, and other Identity threats.

While conventional wisdom is that more secure authentication comes at the expense of the user experience, passkeys have the potential to increase security while improving user experiences by simplifying and speeding up authentication flows.

Passkeys are more secure than passwords (and traditional MFA techniques)

It's no secret that passwords are a poor solution to the problem of authenticating a user. In fact, it's not a stretch to say that passwords and password management have become a joke: for example, there are no fewer than three xkcd comics (Password Reuse, Password Strength, and Encryptic) on the subject.

What started as a simple login box filled in by humans has changed dramatically over the years:

- As attackers became adept at guessing weak passwords and taking advantage of widespread password reuse, requirements about complexity evolved, leading to ever-longer passwords with special characters, combinations of upper and lowercase letters, and numbers
- This forced users to grapple with more passwords, greater password complexity and drove adoption of password managers (whether implemented in a browser or in a separate application)
- Phishing became a widespread threat and huge password dumps appeared online, MFA rose to prominence as an effective defense against ATOs
- Today, many earlier MFA techniques are under threat, with attackers finding scalable and economic ways to bypass this important barrier
- And all along — but largely behind the scenes — workforce and customer identity systems introduced layers of security to defend against a wide array of automated cyberattacks that both cost businesses money and that threaten the privacy of customers

Many of these changes have degraded the user experience, whether by adding friction to everyday actions like registering for a service or logging in to an account.

Fortunately, passkeys offer a phishing-resistant alternative to passwords that also implicitly provide a second authentication factor.

Problems with passwords

Based on a 14-country survey of 21,512 consumers, Okta's Customer Identity Trends Report found that:

- 65% of respondents feel overwhelmed with the number of usernames and passwords they have to manage
- 33% indicated feeling frustrated when they have to create a password that meets certain requirements
- 25% reported frustration with needing to create a new password for every online service

Passkeys are resistant to phishing

For business-to-consumer (B2C) brands, replacing passwords with the FIDO standards means that automated, cross-site password attacks like password spraying or password stuffing will not be successful when applied against their websites. Plus, FIDO's use of public key cryptography means that organizations only have to store a user's public key — the theft of which has negligible value to attackers. The user's private key is securely stored on their local device. It remains within the user's trusted devices, allowing seamless synchronization within the operating systems' ecosystem or through a reliable third-party service. Passkey syncing is end-to-end encrypted, safeguarding sensitive information throughout the process.

In addition to reducing risk and exposure for businesses, such resilience also benefits users. Those who opt to use passkeys are far less susceptible to account takeovers and the consequences — ranging from minor inconvenience to privacy violations and even identity theft — that can follow.

Passkeys can implicitly provide strong MFA

Multi-factor authentication (MFA) requires two or more authentication factors. For example:

- A knowledge factor → something you know, like a password, PIN, or security question
- A possession factor → something you have, like an enrolled device
- An inherence factor → something you are, like your fingerprint

Because passkeys are kept on a user's devices (a possession factor) and — when verification is required — can only be exercised by the user via biometrics, security code, or another FIDO-approved technique (an inheritance or knowledge factor), they implicitly satisfy the core principle of MFA.

The MFA provided by passkeys is among the strongest available, and is a major leap beyond the protection offered by the magic links and one-time passcodes (OTPs) that remain commonplace today.

For many customer-facing organizations, the security benefits alone are enough to justify implementing support for passkeys, but security is only half the story.

Passkeys for moderate-assurance use cases

All passkeys share several common security properties, are highly phishing resistant, and use unique key pairs to enable strong authentication. However, there are important differences between synced and device-bound passkeys that impact their suitability for different assurance use cases.

To help organizations make informed decisions, especially in the context of National Institute of Standards and Technology (NIST) Authenticator Assurance Levels (AALs), in June 2023 FIDO Alliance published FIDO Authentication for Moderate Assurance Use Cases.

The paper provides guidance for organizations as they analyze the abilities and features of both device-bound passkeys and synced passkeys to determine how both credential types can be utilized in a moderate assurance environment — defined as an organization that has several different authentication use case scenarios that can be met by a combination of AAL1 and/or AAL2 as well as AAL3 levels of assurance.

Note: There is currently work underway by NIST to update assurance levels in the context of synced passkeys, so be sure to seek out the latest NIST and FIDO Alliance resources for the latest information.

Passkeys are more convenient than passwords

By replacing cumbersome authentication processes with a finger swipe, facial scan, PIN entry, or other familiar device-unlocking act, synced passkeys dramatically reduce the friction users experience while engaging with online services.

It's telling that some of the earliest adopters of passkeys — including Shopify, DocuSign, and PayPal — deliver user experiences that are secure and *convenient*.

In fact, for many service providers, the enhanced user convenience of synced passkeys might be their most attractive feature. While device-bound passkeys require users to register with each website or app with each device, synced passkeys:

- Allow users to automatically access their FIDO sign-in credentials on multiple devices (even new ones)
- Recover their passkeys even if they lose all of their devices

For consumer businesses, friction — i.e., anything that slows down a person's interactions with your service — is a major obstacle to conversions and, by extension, to revenue. Okta's Customer Identity Trends Report revealed that nearly 60% of survey respondents indicated that they would be more likely to spend money when services offered a simple, secure, and frictionless login process. This finding is consistent across all sectors/industries, suggesting that users crave convenience in every interaction.

While there were some regional differences, age groups show the largest variation: younger consumers are about a third more likely than older consumers to spend more money when offered a simple, secure, and frictionless login experience (Figure 1).

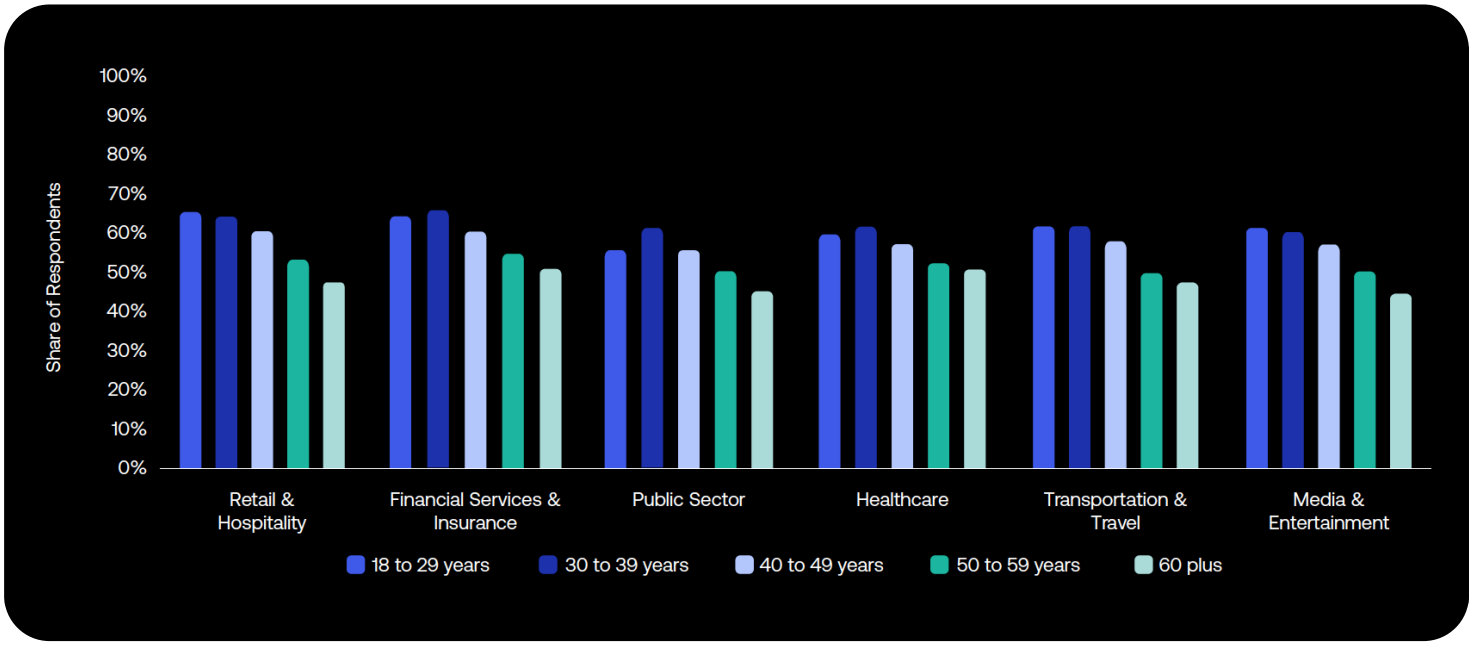


Figure 1: When interacting with a brand online, would you say you are more or less likely to spend money if you know the login process is simple, secure, and frictionless? The graphs show the sum of "Very likely" and "Somewhat likely" responses.

Of course, some amount of friction is necessary to establish trust and provide security controls, but lowering friction wherever practical — in any and every consumer interaction — can increase conversion rates and, accordingly, grow revenue in both the short and long term.

Let's now examine a few ways in which passkeys offer lower friction than passwords.

Synced passkeys are faster to use than passwords

Research shows that in addition to being easier to use than passwords, synced passkeys are also significantly faster. In a post on their security blog, Google showed that logging in with a passkey takes on average 14.9 seconds — 50% faster than the 30 seconds when using a password.

The blog also notes that, "Preliminary, qualitative data collected from user research also indicates that users already perceive this convenience as the key value of passkeys."

Passkeys are more accessible to use than passwords

While friction is an inconvenience for many consumers, it can completely prevent others from accessing your services.

Consider disabilities like vision or cognitive impairment, or limited motor function, and imagine trying to navigate a cumbersome authentication flow that requires the user to remember and then enter (or even 'simply' look up, copy, and paste) a long, complex password. Or give thought to how a user uncomfortable or unfamiliar with technology would respond to a message asking them to download an authenticator app.

Passkeys offer a much more accessible alternative to these traditional approaches.

Being intentional about designing accessibility throughout the customer journey also yields a financial incentive. By creating experiences for everyone, brands can maximize their market reach.

Synced passkeys make stronger authentication more convenient

Synced passkeys even make enhanced security more convenient, because they verify both a user's Identity and private key in a single step (from the user's perspective), a dramatic improvement upon other MFA techniques.

This increased convenience also empowers service providers to consider re-authentication at a higher frequency or as a step-up (e.g., for access to sensitive apps, to make account changes, to access private data, etc.), both of which are critical defenses against session hijacking attacks. As noted in Okta's **Secure Sign-in Trends Report 2023**, authenticator challenges using WebAuthn took an average of only three seconds to be completed — several times faster than combining passwords with OTP-based challenges.

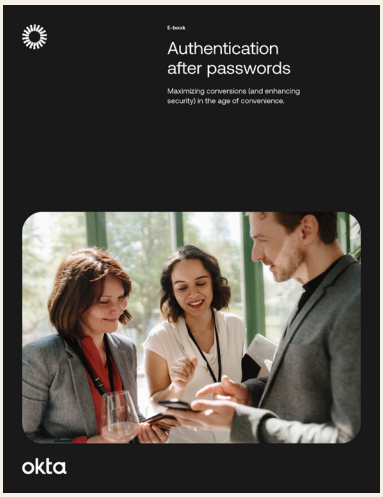
Synced passkeys are easier to enroll than passwords

Of course, all of these conveniences are only available to users after they have enrolled a synced passkey, so enrollment should be straightforward. Repeated enrollments required by device-bound passkeys are commonly cited as a major reason why WebAuthn has such limited adoption — especially within consumer scenarios.

By allowing a user's FIDO credentials to roam easily (but securely) across multiple devices, synced passkeys overcome this issue: enrollment itself is straightforward, and only happens once per service.

In fact, the Secure Sign-In Trends Report revealed that the median time to register a password is approximately 34 seconds, which includes the time for a user to create a new password and confirm (re-enter) the password. In contrast, WebAuthn-based registration took only 19 seconds, challenging the notion that higher assurance authenticators impose a significant burden on users during enrollment.

The likely reality is that users will initially be unfamiliar with synced passkeys, but will quickly find enrollment at least as intuitive as — and much faster than — other authentication mechanisms.



Synced passkeys are a significant step towards a passwordless world

By delivering both stronger account security relative to passwords, and more convenient user experiences, synced passkeys have a legitimate chance at popularizing passwordless authentication well beyond IT administrators (who prioritize security) and early adopters (who recognize the range of benefits).

Download our comprehensive guide, **Authentication After Passwords**, to learn more about the passwordless future, including common misconceptions — for example, you may think you don't already have passwordless flows, but you probably do — and what you can do now to get (and stay) ahead of the competition.

Learn about Okta's own passwordless journey, in **Why we're going 100% passwordless at Okta**.

How do passkeys work?

As explained by the FIDO Alliance, the underlying FIDO protocols employ standard public key cryptography techniques to provide strong authentication. To register with an online service, the user's device creates a new cryptographic key pair consisting of:

- A public key, which is registered with the online service
- A private key, which is retained as a true secret

Importantly, the keys are generated securely and uniquely for every account — you don't have to worry about users picking a weak private key, and private keys aren't reused across multiple services.

To authenticate with a particular service, the client device proves possession of the account's corresponding private key by signing a challenge provided by the service — the service itself never sees the private key and, by extension, never needs to store or protect this information.

Crucially, the private key can only be used after it is unlocked by the user, with the local unlock typically achieved either by inserting a second-factor device or via the primary device's unlock mechanism — usually a biometric authentication (e.g., Touch ID, Face ID, Windows Hello, etc.) or a PIN.

What makes synced passkeys different from earlier FIDO2 implementations is that they:

- Allow users to use synched passkeys on any device in a particular ecosystem where passkeys are backed up to the device and cloud
- Allow users to perform cross-device authentication to easily cross ecosystem boundaries without facing the friction of enrolling FIDO credentials on new devices

For more information on the underlying mechanics of how passkeys work, visit the FIDO Alliance's website.

How do I implement passkeys into my app?

Broadly speaking, developers have two approaches when it comes to extending authentication to support passkeys:

- Implementing passkeys yourself, via APIs and SDKs; and
- Leveraging an Identity service provider.

More information about deploying passkeys

FIDO Alliance has published a series of whitepapers for IT administrators, enterprise security architects, and executives considering deploying FIDO authentication across their organization.

The DIY approach

From the implementation perspective, synced passkeys look just like platform authenticators that do not provide an attestation statement. That means that from the protocol perspective, if your web app already supports WebAuthn, and as long as it doesn't require an attestation response, you technically already support synced passkeys. From the user experience perspective, however, that might not be entirely true. For example:

- The prompts and language you have in your current enrollment pages likely refer to device-bound credentials (e.g., "Sign in faster from this device"), which is no longer the whole truth with synced passkeys.
- Chances are that you are using platform authenticators to enable second authentication factors only, given that before synced passkeys, you were directly responsible for account recovery.

None of the changes above are particularly hard, especially if you already implemented WebAuthn, but you do need to do a bit of work to offer a good experience.

To help developers, in October 2022 the W3C WebAuthn Community Adoption Group and the FIDO Alliance launched passkeys.dev — an online resource that (among other things) contains documentation and tracks device support.

Identity Unlocked

Passkeys with Andrew Shikiar and Tim Cappalli

Shortly after synced passkeys were announced (as multi-device credentials), Andrew Shikiar (Executive Director & CMO, FIDO Alliance) and Tim Cappalli (Digital Identity Standards Architect at Microsoft) joined host Vittorio Bertocci, (Principal Architect at Auth0) on the **Identity Unlocked podcast**.

Tune in to learn about the evolution of FIDO credentials and to gain more develop-focused insights into how multi-device credentials work.

Using an Identity service provider

Identity is difficult — even seasoned professionals find creating effective and efficient implementations to be challenging. Plus, customer expectations are always increasing, with every user comparing each experience to the best ones they've encountered, placing businesses under considerable pressure to continually evolve the UX they deliver.

However, Identity needs must be satisfied without drawing heavily upon precious engineering resources that are needed to extend core competencies — and both of these goals must be satisfied without overlooking regulatory requirements or compromising on security.

For these reasons, many organizations find it both more efficient and cost-effective to integrate an Identity service into their applications and technology stack. Plus, partnering with an identity service provider helps businesses cater to a broader set of requirements in Customer Identity and Access Management (CIAM) including:

- Authentication
- Authorization
- User Management

It’s a certainty that established Identity providers will support passkeys, providing a convenient option for application developers to extend their authentication options and keep pace with a rapidly evolving authentication landscape.

For example, if you already have an app configured to use the Okta Customer Identity Cloud for authentication, you'll be able to flip that switch and enable passkey authentication without touching your code at all.

However, different Identity providers offer different features, so due diligence is strongly recommended. Here are a few things to look for as you make your short list:

- Independent and neutral → Your CIAM solution should enable you, not restrict you. That means it should integrate with your existing solutions, should leverage open standards to avoid vendor lock-in, and should work with your preferred cloud provider.
- Comprehensive and customizable → Every customer is unique with complex needs. Your CIAM solution should help you build seamless, consistent, and trustworthy experiences for every type of user.
- Easy to build with, maintain, and use → For virtually every piece of technology, engineering teams aim to reduce effort and time that it takes to deploy, configure, and operate it — and your CIAM solution should support this mission.
- Trusted → Having a serious security breach, failing to meet compliance requirements, or experiencing an unavailable or degraded service can result in significant brand, legal, and financial consequences. Your CIAM solution should cause you to worry less about these risks.

What happens next?

When WebAuthn debuted, Auth0 (now the Okta Customer Identity Cloud) immediately saw the value and adopted it both as a second factor for administrators accessing our management dashboard and as a method developers can use to authenticate their users when protecting their web apps.

However, despite its clear security advantages, adoption of FIDO2 authentication in consumer apps has so far remained low. Our own observations indicate that most of the use appears to be among professionals who need a high level of assurance when accessing the resources they manage.

There are many possible explanations, but the consensus indicates that:

- Hardware keys are mostly reserved for admins and key knowledge workers, rather than the wider consumer market
- While platform authenticators are more palatable, being tied to a single device (potentially a coveted feature in business scenarios) presents usability challenges in the consumer realm, where users frequently have many devices and regularly introduce new ones into the mix

But the arrival of synced passkeys — and the considerable influence of Apple, Google, Microsoft, and others — could represent an important inflection point. While some users will love them and others will be hesitant, in the coming months and years passkeys will become ubiquitous and familiar.

More broadly, passwordless authentication in general will become more common, with adoption driven by positive user experiences and security benefits. Organizations that make passkeys and other passwordless authentication mechanisms available to customers and other users will reap rewards.

Admittedly, some issues remain unresolved. For example:

- Passkeys are phishing-resistant, but onboarding a new user with both the passkey and the way to recover it (e.g., the email account associated with the operating system ecosystem) represents a potential vulnerability.
- So far, the user experience varies across different platform ecosystems and password managers. FIDO Alliance is working to create consistency, but — at least for the short term — inconsistent experiences will remain, and may cause frustration among some users.
- As noted earlier, where synced passkeys fit in the NIST AAL framework is an unanswered question — and one that has implications in a world in which many workers use their personal device to access protected organization resources.
- Finally and an ever-present challenge for new technology is consumer education on passkeys, particularly as it relates to the security, privacy, and convenience aspects of them.

And it's worth reiterating that passkeys are very new and the overall space will continue to evolve as implementations appear and are refined.

Don't wait for perfect when better is already here

Arguably, the issues surrounding passkeys are dwarfed by the problems associated with passwords. Passwords need to disappear, or at least become much less common, and everyone within the Identity industry should work to find ways to leverage the benefits of passkeys while minimizing the drawbacks.

We at Okta are committed to doing our part, both by providing timely, state-of-the-art, developer-friendly features enabling passkeys — and by actively participating in the industry discussions shaping the future of this technology.

Embracing passwordless will get easier as platform vendors and device manufacturers align on standardized flows for recovery, issuance, and non-proliferation. For those who want to introduce or extend passwordless authentication, we recommend looking for authenticators that support:

- Frictionless authentication
- Fewer sign-in errors
- Easy user enrollment
- Resistance to phishing attempts

For what it's worth, passkeys check all these boxes.