Passkeys: When They Are (And Aren't) the Right Fit

February 21, 2024 • Adrian Castillo

FIDO | Identity Assurance | Identity Management | Security & Identity Trends

Subscribe

Forget passwords. Literally. That's the vision of the FIDO Alliance, an open industry association that launched in 2013 to "solve the world's password problem" and develop secure, global passwordless authentication standards based on public key cryptography.

It's not hard to see the attraction. Passwords are a pain — hard to remember, easy to steal or phish, and time-consuming for both users and IT teams to manage. Passwordless authentication, by contrast, is convenient for users and it removes the most common phishable element AKA "password" from the equation. For now, the public key cryptography on which passwordless techniques are based is significantly more difficult to breach.

Enter ... passkeys? The game-changing technology has made passwordless authentication significantly easier to adopt, especially now that major tech companies like Google, Apple and Microsoft support it in their products and devices. But it isn't the best fit for all authentication use cases.

In this article, we'll review what passkeys are and how they work — and discuss when they are (and aren't) a good fit.

What Is a Passkey — And How Is It Evolving?

A passkey is a credential that's based on FIDO protocols and can be used to access a digital account, whether it's your email or your digital banking app for example. Each passkey or private key can only be used for a single account; and you must prove that you own your passkey with a *user verification* method like those used to unlock your phone: PIN or biometrics, to be able to access your account.

Originally, passkeys could only be stored on dedicated hardware tokens known as security keys or smart cards, which users presented to a computer or phone in order to authenticate themselves.

> Now, thanks to expanded support from the high-tech ecosystem, passkeys can be stored on ordinary smartphones, offering a high level of trust and giving users options that best fit what they see as easier or more convenient to use.

There are two ways of storing passkeys:

- **Platform synchronized passkeys (synced passkeys)** are stored in a cloud, where they can be accessed on different customer devices. This enables users to access one account on multiple devices without having to re-enroll each device.
- **Device-bound passkeys** bind a specific sign-in credential to a specific device (like a Crescendo security key or a smart card). That means users always require that device holding the passkey to be connected to the phone or computer to access their account. When using device-bound passkeys, it is common practice to enroll more than one key as a backup.

How Passkeys Power Passwordless Authentication

To understand how passkeys power passwordless authentication, let's review how FIDO works:

1. Users register a device — either a computer or mobile phone that supports synced or device bound passkeys — to a FIDO compatible service or application.
2. The registered user device generates a cryptographic key pair (a passkey and a public key). Each passkey is unique to each service or application; the private key is stored on the device, while the public key is shared with the service.

3. The next time they access the service, they'll unlock their device, and a cryptographic protocol will be performed in the background to prove they still own the passkey
4. The process is simply repeated with the same mobile, security key or smart card next time you want to enroll to a new FIDO compatible service or application.

Passkeys — a type of private key that's discoverable by browsers and can be stored in native applications or devices, like the Crescendo cards or security keys — make this process simpler and more scalable.

Because passkeys are stored on individual user devices instead of on corporate servers, they can't be compromised through a network breach. Security can be further strengthened by requiring users to confirm that they own the device through a PIN or biometric — reducing the risk of theft or loss.

Passkeys in Action: Use Cases

Passkeys are now widely available on consumer facing web applications across many different industries, from healthcare to financial services.

Some companies, like PayPal and Best Buy, use passkeys to power completely passwordless log-ins. The use case is an obvious fit for companies with a younger customer base. In fact, studies suggest that nearly half of Gen Zers will abandon an online purchase if they forget their password! However, it's important to note that consumers of all ages are fed up with passwords — 93% of them told Oxford University researchers that they preferred biometric authentication.

Perhaps that's why several companies that have not yet gone fully passwordless have also been experimenting with passkeys. Bank of America and Vanguard, for instance, use device-bound passkeys to offer additional security, either as a multi-factor authentication (MFA) factor for log-in or for transactions above a certain threshold. These passkeys are only available in the form of device-bound passkeys.

A few enterprises, like AWS, support passkeys to authenticate B2B customers. Some use them for workforce applications access — usually device-bound passkeys that work via cards or security keys such as the Crescendo product line.

The Pros and Cons of Passkeys

Passkeys are convenient, flexible, and widely accepted. Yet it's important to understand both their strengths and their limitations.

Synced passkeys, for example, aren't crackable like passwords. They are highly user-friendly, because they don't require users to re-enroll every time they want to access an account on a new device. Yet synced passkeys can be shared with others using AirDrop and Nearby Share, threatening account integrity if they inadvertently fall into the hands of malicious actors.

Device-bound passkeys offer greater security and tend to be more optimal for enterprise or workforce use cases.

When Passkeys Fit — And When They Don't

Are passkeys the right fit for your organization?

To answer that question, you'll need to analyze the level of security you need, the workflow that's best for your users and how any passwordless authentication technologies might fit into your existing IT infrastructure.

For consumer applications, where convenience is key, synced passkeys are a great way to boost account security — especially since they enjoy broad support on the most popular smartphones and devices. HID's Authentication Platform enables web developers to add passkey support to digital properties with a flexible, scalable and highly secure architecture.

Smart cards and security keys, meanwhile, are an ideal fit for many workforce applications — and best-in-breed solutions support FIDO.

The Keys to Stronger Identity Assurance

Passkeys are an exciting step forward — and they're part of an even more exciting landscape of solutions and technologies. HID is a security industry leader and a member of the FIDO Alliance, and we're deeply invested in supporting a variety of paths to passwordless.

Have questions about passkeys, PKI or other identity technologies? Learn how HID can facilitate your path to passwordless.

RELATED POSTS

HID Connects S2E8: Security and Healthcare — Are We Taking Care of Those Who Are Taking Care of Us?

Patient and staff safety are paramount in the healthcare industry. In this podcast episode, we discuss the technology that can improve security for everyone.

May 15, 2024 • HID

Security & Identity Trends

How to Ensure the Cybersecurity of Your Access Control Systems

Cybersecurity of your access control systems protects sensitive data from credentials to readers, controllers, servers, software clients and more.

May 14, 2024 • Steven Commander

Access Control | Enterprise | Security | Security & Identity Trends

COMPANY

About

Blog

Careers

Events

Management Team

Newsroom

Sustainability

Values & Culture

SUPPORT

Customer Service

Technical Support

Return Merchandise Authorization (RMA)

Product Support Lifecycle

RESOURCES

Certifications

Document Library

Drivers & Downloads

CONTACT HID

(800) 237-7769

Check Order Status

Contact Sales

Corporate Offices

Security Center