Replacing Password-Only Authentication with Passkeys in the Enterprise

June 2023

Editors:

Khaled Zaky, Amazon Web Services

Abstract

This white paper describes the need for a more secure and convenient solution for authentication. Passwords have long been the standard for authentication, but the risks inherent to passwords reduce their efficacy as an authentication mechanism. Multi-factor authentication (MFA) solutions have been on market for some time, but their widespread adoption has been slow due to various barriers. Passkeys are an authentication solution that reduces the adoption barriers of traditional MFA mechanisms, while offering improved security, ease of use, and scalability over passwords and classic MFA solutions. Passkeys utilize on-device biometrics or PINs for authentication and provide a seamless user experience. This white paper outlines the benefits of passkeys, the user experience, and adoption considerations for enterprises.

Contents

1. Introduction

Passwords have long been the standard for authentication, but their inherent security flaws make them exploitable. Many passwords can be easily guessed or obtained through data breaches, and the reuse of passwords across multiple accounts only exacerbates the problem. This vulnerability makes them susceptible to credential stuffing attacks, which use leaked or commonly used passwords to gain unauthorized access to user accounts. In fact, passwords are the root cause of over 80% of data breaches, with up to 51% of passwords being reused. Despite these security concerns, many consumers and organizations continue to rely solely on passwords for authentication. According to a recent research by the FIDO Alliance, 59% of consumers use only a password for their work computer or account.

Traditional multi-factor (MFA) mechanisms, such as one time passwords (OTPs) delivered via SMS, email, or an authenticator app, are used by organizations to reduce the risk associated with a single-factor, password-based authentication system. Organizations using single-factor authentication with passwords, or those that have deployed OTPs to reduce phishing and credential stuffing, can implement passkeys as a password replacement to provide an improved user experience, less authentication friction, and improved security properties using devices that users already use—laptops, desktops, and mobile devices. For an introduction to passkeys and the terminology, please see the FIDO Alliance's passkeys resource page. In the following pages, we will focus on migrating existing password-only use cases to passkeys. For additional use cases, please see here.

2. Why Are Passkeys Better than Passwords?

Passkeys are a superior alternative to passwords for authentication purposes and offer improved usability over traditional MFA methods. They offer several benefits such as better user experience, reduced cost of lost credentials, phishing resistance, and protection against credential compromise.

Synced passkeys offer a consistent authentication experience for users across multiple devices. This is made possible by leveraging the operating system platform (or a third party synchronization fabric such as that from password managers) to synchronize cryptographic keys for FIDO credentials. This allows for quick and easy sign-in using biometrics or a device PIN. Synced passkeys also improve scalability and credential recovery. With synced passkeys users do not have to enroll a new FIDO credential on every device they own, ensuring that they always have access to their passkeys, regardless of whether they replace their device.

On the other hand, device-bound passkeys such as security keys can be used on multiple devices allowing for cross-device portability. Unlike synced passkeys that are accessible on any synchronized device, device-bound passkeys are tied to the specific physical security key.

In terms of security, passkeys are built on the FIDO authentication standards, providing strong resistance against the threats of phishing and credential stuffing. Additionally, passkeys rely on existing on-device security capabilities, making it easier for small and medium enterprises to adopt stronger authentication methods.

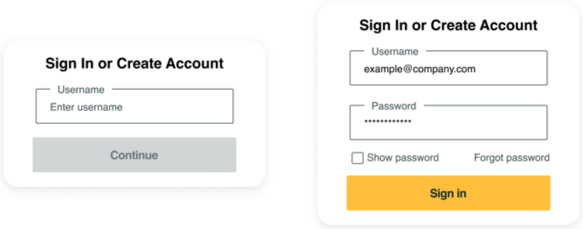
Finally, passkeys offer a comprehensive solution for secure and efficient authentication that is better than passwords and traditional MFA authentication methods. With a seamless user experience, improved scalability, and enhanced security, passkeys are a valuable solution for organizations of all sizes.

3. Passkeys User Experience

3.1 Create a passkey visual UX/UI

Note: This section will provide an overview of the passkey registration and sign-in process using examples. Note The FIDO Alliance User Experience Working Group has developed UX guidelines for passkeys that are available here.

1. In the passkey registration flow, users are first prompted to provide an email or username along with their password to authenticate.



Sign In or Create Account

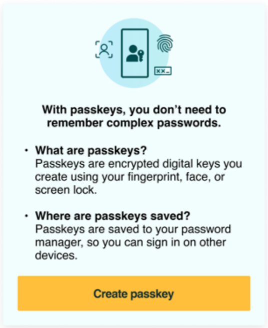
Username: Enter username

Sign In or Create Account

Username: example@company.com

Password: ••••••••••••

2. Then, users simply follow the prompts to provide their on-device biometric or PIN authentication.

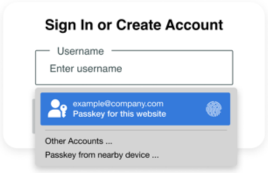


With passkeys, you don't need to remember complex passwords.

- What are passkeys?
  Passkeys are encrypted digital keys you create using your fingerprint, face, or screen lock.
- Where are passkeys saved?
  Passkeys are saved to your password manager, so you can sign in on other devices.

3.2 Sign in with a passkey visual UX/UI

1. To sign in with a passkey, a user just selects the email or username.
2. Available passkeys will be shown in the passkey autofill user interface.



Sign In or Create Account

Username: Enter username

4. Adoption Considerations for Enterprises

Within businesses large and small, there are systems and services dependent upon single factor authentication using passwords. We collectively refer to these use cases as "low assurance use cases." For low assurance use cases, technology leaders can displace password-only authentication mechanisms with passkeys, dramatically reducing the risk of phishing, and eliminating password reuse and credential stuffing. However, even for low assurance use cases, businesses must consider factors that will influence their choice of technology and implementation, which we outline below.

As a prerequisite to deploying passkeys in the enterprise, leaders must clearly define the set of use cases, users, and the suitability of passkeys for this set.

4.1 Does the relying party (RP) support passkeys?

At the time of writing (Q2 2023), passkeys are a relatively new technology, and as such broad-based support is not guaranteed. As organizations review their systems to identify candidates for migration to passkeys, leaders must start by identifying where passkeys are supported within their ecosystem.

First, for in-house developed/managed applications, how can passkey support be added to the application(s)? If a single-sign on (SSO) mechanism is used to federate multiple applications and services, adding passkey support to the Identity Provider (IdP) can propagate support for passkeys to numerous federated applications, creating a rich ecosystem of services supporting passkeys with engineering efforts focused on the SSO IdP. Conversely, if the environment uses multiple independent applications, each of which uses password-based authentication, organizations will have to prioritize FIDO implementation across their suite of applications to leverage passkeys, or consider migrating to a federated authentication model where the IdP supports passkeys.

Second, third-party developed or hosted applications may or may not support passkeys. If an organization's service provider does not support passkeys today, inquire when support is expected. Alternatively, if the organization is pursuing a federated identity model, does the service provider support inbound federation? If so, end users can authenticate to the IdP with a passkey before federating to the service providers' systems.

4.2 Which devices are used to create, manage, and authenticate with passkeys?

After identifying a set of targeted applications or IdPs, identify the users of the applications and the devices they use to access the same. Generally speaking, users on modern operating systems, browsers, and hardware will have broad support for passkeys registered on a platform device, using a credential manager, or with a hardware security key. There are tradeoffs with each mechanism.

Today, passkey providers allow users to register passkeys that are synchronized to all of the devices the user registered with the sync fabric. Passkeys providers may be part of the operating system, browser, or a credential manager which stores and manages passkeys on behalf of the user. If the user loses or replaces their device, the passkeys can be synchronized to a new device, minimizing the impact on users. Typically, this is a good solution for users who use a small number of devices on a regular basis.

Conversely, hardware security keys create device-bound passkeys; they never leave the device. If a user loses their hardware key, they must have a backup or perform account recovery for all credentials stored on the device. Passkeys may be shared with other users if they are not hardware bound.

Hardware security keys require connectivity to the user's computing device through USB, Bluetooth, or NFC whereas providers are always available on the user's devices once bootstrapped. Platform credentials may be used to authenticate on nearby devices using the FIDO Cross-Device Authentication. Enterprises should consider whether users who move between a number of shared devices should synchronize passkeys across all the shared devices, use hardware keys, or use the hybrid flow to best support their work style.

When users operate on shared devices using a single account (or profile), passkeys registered to the platform or credential managers are not a good fit. Device bound passkeys on a hardware key are recommended for this scenario. If the user carries a mobile device, consider registering a passkey on the device and using the cross device authentication flow to authenticate users.

Unlike passwords, all of the passkey solutions reviewed above provide strong phishing resistance and eliminate credential theft from the RP and reuse.

4.3 Registration & Recovery

If there are no restrictions on which device(s) or platform(s) the user can register their passkeys, users may self-provision passkeys by bootstrapping a new credential from their existing password using the device(s) of the user's choice. If using hardware security keys, organizations should provide two per user to allow for a backup credential.

As long as a password remains active on the user account, the user can recover from credential loss following the self-provisioning described above. This step is only required if the user is unable to restore their credentials from their passkey provider.

5. Conclusion

Passkeys offer a significant improvement in security compared to traditional passwords, but it is important to carefully evaluate and understand the adoption considerations before proceeding with an implementation. Organizations should ensure its technical requirements, security, and management preferences align with the passkey solution. Not all use cases are suitable for a passkey-only implementation. For additional deployment patterns, see the other white papers in this series here.

6. Next Steps: Get Started Today

Organizations should upgrade their authentication method and take advantage of the stronger security that passkeys provide. Based on the FIDO authentication standards, passkeys offer a robust solution to the growing threat of phishing attacks. Look for the passkey icon on websites and applications that support it, and take the first step towards a more secure future. Don't wait. Make the switch to passkeys today!

For more information about passkeys, visit the FIDO Alliance site.

7. Acknowledgements

We would like to thank all FIDO Alliance members who participated in the group discussions or took the time to review this paper and provide input, specifically (in alphabetic order):

- Jerome Becquart, Axiad
- Vittorio Bertocci, Okta
- Greg Brown, Axiad
- Tim Cappalli, Microsoft
- Matthew Estes, Amazon Web Services
- John Fontana, Yubico, Co-Chair FIDO Enterprise Deployment Working Group
- Rew Islam, Dashlane
- Jeff Kraemer, Axiad
- Karen Larson, Axiad
- Sean Miller, RSA
- Dean H. Saxe, Amazon Web Services, Co-Chair FIDO Enterprise Deployment Working Group
- Tom Sheffield, Target Corporation
- Johannes Stockmann, Okta
- Shane Weeden, IBM
- Monty Wiseman, Beyond Identity
- FIDO Enterprise Deployment Working Group Members