What is Passkey authentication?

Passkeys are a secure and robust alternative to passwords. They are specifically designed to protect against phishing attacks, simplify the login process, and eliminate the need to remember and manage multiple passwords.

Standardized by the FIDO Alliance, passkey authentication leverages public key cryptography and biometric authentication to verify a user. Unlike passwords that are stored on servers, passkeys are stored on user devices. This means that even in the event of a server breach, passkeys will not be stolen.

When a user registers on a passkey-enabled website, a unique passkey is generated and stored on their device. From that point forward, every login attempt to the website can be authenticated seamlessly using either a biometric sensor, such as facial recognition or a fingerprint scan, or by scanning a QR code.

Passkeys are cross-platform and cross-device, which means that you can use the same passkey to log in to a website or app from any device. For example, if you create a passkey for a website on your Mac, you can use the same passkey to log in on the website from your iPhone or iPad.

Passkey authentication vs. passwords

Passkeys and passwords are two fundamentally different methods of authentication. Let us explore their key differences:

1. The onus of creating and remembering

Passwords are created by the user, making the user responsible for remembering them. This can be difficult, especially if the user must remember multiple passwords for different apps. Based on company policies, passwords need to be updated regularly. Conversely, passkeys never need to be updated. Passkeys are generated by the service provider and remembered by the user's device, shifting the burden away from the user.

2. Security

While passwords are inherently insecure, passkeys are secure and phishing-resistant by design. Users often choose weak passwords or reuse them across different accounts (both corporate and personal), making them susceptible to compromise. Additionally, passwords can be intercepted, guessed or stolen through data breaches.

Passkey authentication uses encryption and device-bound storage to enhance security. Moreover, private keys are never shared with the application a user is logged into. By eliminating the need for users to remember passkeys, the risk of password reuse or misplacement is effectively eliminated.

3. User experience

Managing multiple passwords can be burdensome for users. Frequent password changes and complex requirements can be frustrating, and this may cause users to adopt unsafe practices, such as writing passwords down or storing them in insecure locations.

Passkey authentication is a more seamless, user-friendly and sustainable way to access applications. Users can log in to an application by scanning a biometric or entering a device PIN, regardless of the device they are using.

Is passkey authentication the same as passwordless authentication?

Passwordless authentication refers to any method that eliminates the need to use passwords for authentication. This can be done using different factors, such as biometrics, device PINs, physical security keys or passkeys.

Since passkey authentication replaces passwords with passkeys, passkey authentication is a type of passwordless authentication.

You might be interested in:

Elevating Security with Advanced Authentication

[GATED] Advanced Authentication offers a holistic solution that mitigates most AM challenges

Download Techbrief →

The difference between Advanced, Strong and Adaptive Auth

[INFOGRAPHIC] Learn the difference between Adaptive, Strong and Advanced auth, and how to deliver a seamless use...

Learn More →

Understanding the role of SSO in security

[GATED] Read why Single sign-on (SSO) is a key weapon in the battle for security in the enterprise.

Download Whitepaper →

How does passkey authentication work?

Here's a simplified overview of how the passkey creation process works:

Now let’s explore the passkey authentication workflow:

1. The user visits the login page of the website from a browser and selects the “Login with passkey” option.
2. When prompted, the user selects the device which contains the passkey for this website.
3. Once the user has selected the passkey, they are asked to verify their identity using a facial/fingerprint scan or a device pin.
4. The website uses the registered public key of the user to verify the passkey.
5. If the verification succeeds, the user gets access to the website.

Multi-factor authentication (MFA) vs Passkey authentication

MFA refers to any authentication mechanism that uses two or more factors for verification. For example, a password and a one-time password (OTP); or a password and a fingerprint scan.

Passkey authentication achieves MFA in a single step. While the user only needs to perform a biometric scan or enter the device pin, the underlying authentication process combines two factors: the passkey itself and the biometric/device pin. This streamlined approach enhances security without adding friction to the login experience.

Pros of passkey authentication

Passkey authentication offers several advantages for businesses:

- Passkeys are much less susceptible to password-related attacks, like phishing, credential stuffing, brute-force attacks and dictionary attacks.
- Passkeys reduce the risk profile of an organization by limiting the impact of a potential data breach. Even if a credential database is compromised, the attacker would only have access to public keys, which are not enough to gain unauthorized access.
- Passkey authentication makes the login process secure and convenient by verifying two authentication factors in a single step.
- Passkeys are designed to be cross-platform and cross-device. This interoperability ensures a consistent and user-friendly login experience.

Cons of passkey authentication

Passkey authentication has potential drawbacks and challenges that you should also consider.

- While passkey authentication is gaining traction, it is not as prevalent as other authentication methods. This means that users may not be able to use passkeys to sign in to all websites and applications. If the user's device is lost, stolen or compromised, it could grant unauthorized access to the passkey and the associated accounts.
- Passkey recovery is the weakest link as it usually relies on SMS OTP.
- Public key infrastructure (PKI) relies on large prime numbers that can be easily cracked with quantum computing.
- Some users may be hesitant to adopt passkey authentication because they are unfamiliar with the concept. Education and awareness are essential to promote user acceptance and drive adoption.

Conclusion

As passkey authentication becomes more prevalent, it is likely to become the new standard for authentication. It is a secure, convenient and cross-platform method that has the potential to replace passwords altogether.

Learn More