SPOTLIGHT ON CYBERSECURITY

The Rise Of Advanced Passwordless Authentication

A Spotlight on the Transition from Traditional Authentication to Passwordless Authentication Methods

StratisAdvisory

RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT

Going Passwordless

The transition from password-based security to advanced passwordless methods is apparent, prioritizing enhanced security and user convenience. Traditional authentication, while useful, faces increased threats such as phishing and social engineering. Given the escalating cyber risks, adopting a passwordless approach is essential, underscoring the evolution towards advanced passwordless authentication. Below is a comparison between two (2) forms of passwordless authentication:

ONE-TIME PASSWORD

A one-time password (OTP) is a unique, automatically generated set of characters used for authentication. OTP is produced using standard algorithms that combine a static seed or secret key, established when an account is created, with a moving factor that changes with each code generation, ensuring synchronization with the authentication server.

- Becomes invalid in minutes, but still needs to be keyed in, making it vulnerable to phishing, theft, or interception.
- Relieves the sharing or reusing of credentials on multiple accounts or systems.
- Has multiple delivery channels and can be sent to a user via text message, email, phone call, authenticator app, or a push notification.
- More widely supported and used by services today and has global reach through mobile devices.
- Can be generated using hardware, software, or on-demand and can be built into apps and products using verification Application Programming Interfaces (APIs).

COMPARATIVE ANALYSIS

- RISK OF FRAUD
- USER EXPERIENCE
- ACCESSIBILITY
- ADAPTABILITY
- INTEROPERABILITY

PASSKEY

A passkey is a passwordless authentication method linking a user's account to an application or website, which consists of a unique cryptographic key used for authentication, consisting of a public key registered with the service provider and a private key securely stored on the user's device, often safeguarded by biometrics or screen lock mechanisms.

- Unphishable and does not require anything that can be lost, intercepted, or stolen since the private key never leaves the device.
- There is no need to type or enter codes or information and is relatively automatic.
- Passkeys are associated with a device or proximity to a device through biometrics, or a non-visible PIN, or a swipe pattern.
- Since this is a newer technology, adoption has yet to expand compared to other passwordless authentication methods.
- Single implementation enables a passwordless experience across operating systems or browsers and can be built into apps and products using verification APIs.

	ADVANTAGES	DISADVANTAGES
ONE-TIME PASSWORD	• Considered as an identity verification tool to authenticate users when logging into an account, a network or a system. • More secure than a static and user-created password, which have the potential of getting reused, forgotten or stolen. • May replace logging in with username and password information or may be used as another layer of security or Two Factor Authentication (2FA). • OTP can be sent to a customer's preferred delivery method, either through text message, email, phone call, authenticator app or a push notification. • Familiar, compatible, and scalable due to its wide usage today with global access to mobile devices. • OTPs can still be shared, which may be useful for emergency situations.	• There is a time-drift factor, which is the lag between the creation and the use of the OTP, that may cause interception and security issues. • Relies on internet or mobile data signal that may sometimes be weak or intermittent. • Usually requires the need to copy from the receiving device or window into the log in form or page, making it inconvenient to have to switch user interfaces. • Susceptible to online identity theft such as phishing, sim swapping, keyboard logging and man in the middle attacks. • OTPs can be shared that can facilitate remote access scams.
PASSKEY	• Considered as an identity verification tool to authenticate users when logging into an account, a network or a system. • More secure than a static and user-created password, which have the potential of getting reused, forgotten or stolen. • May replace logging in with username and password information or may be used as another layer of security or 2FA. • Promoted by international organizations such as the FIDO Alliance and the World Wide Web Consortium. • Passkeys cannot be shared or reused and can only exist on a user's device, making it more resistant to phishing or interception • Passkeys are not stored on servers, which makes them less prone to data breaches and hacks. • Passkeys are standardized and enables a passwordless experience across all of a user's devices and even with different browsers or operating systems.	• It is a newer technology and adoption is not yet widely supported by services, applications and websites. • Passkeys rely heavily on the security and availability of features on a user's device to store and process cryptographic keys. Older devices, browsers or operating systems may not be able to use passkeys yet due to incompatibility. • The recovery process may be more complex if lost or compromised compared to traditional authentication or OTP. • Currently not an advisable solution for accounts that employees or families need to share.

Discover what Stratis Advisory can do for you

Customer Experience Analysis

The customer experience is critical to customer acquisition and retention, understanding the balance between ease of use versus risk mitigation is an ongoing process seeking harmony. Stratis can execute a customer experience analysis comparing passwordless authentication techniques that focus on usability, security perception, and user satisfaction across methods like passkeys, biometrics, one-time passwords (OTP), and magic links.

Fraud Risk Assessment

Legacy and new methods of authentication are still subject to fraud risk. As such, undertaking a fraud risk assessment for passwordless authentication techniques should focus on identifying vulnerabilities, assessing potential attack vectors, and evaluating mitigation strategies across methods such as passkeys, biometrics, OTP, and magic links. Stratis can analyze each technique's exposure to phishing, credential theft, and device compromise to enhance fraud detection, reduce attack surfaces, and strengthen the overall security posture for passwordless authentication methods.

Passwordless Authentication Implementation

Implementing passwordless authentication requires a strategy and evaluation on current infrastructure, compatible solutions, and identifying the most effective passwordless methods such as passkeys or biometrics. Stratis can assess compliance with security and privacy regulations, design a transition plan for users, and provide training to ensure the passwordless solution is effective and scalable.

Stratis Advisory | 1.415.352.1060 | www.stratisadvisory.com | info@stratisadvisory.com