HYPR Info Brief

Security Implications of Apple's Passkeys

With the delivery of iOS 16, the much anticipated "Apple is killing the password" mantra is finally becoming a reality. By implementing passkeys, Apple is advancing consumer acceptance of a password-free life. It is also a logical progression considering that on Apple devices such as the iPhone, biometric capture was already in place for several years to log into the device rather than using a password.

Apple is not the only tech giant that recognizes that the days of the password are numbered. Both Microsoft and Google are developing their own version of passkeys. The actualization of "passwordless" as mainstream is an important tipping point in the approach and adoption of the technology that HYPR has been developing and educating about for years.

Apple Passkeys Are Consumer, Not Enterprise, Focused

Apple's passkeys use Touch ID or Face ID for biometric verification, and iCloud Keychain to sync across iPhone, iPad, Mac, and Apple TV. Passkeys are based on FIDO2 WebAuthn, providing a phishing-resistant login to websites and apps. iOS 16 is a tremendous step forward in furthering adoption of passwordless authentication. Apple's passkeys and other consumer-targeted passwordless options, however, carry challenges when attempting to apply it for enterprises.

Does Not Support SCA and Other Regulatory Requirements

These challenges include environments which are heavily regulated or are required to meet specific compliance objectives, such as SCA requirements. The current implementation of passkeys does not meet the possession requirement noted within SCA standards. This rings true for other compliance requirements as well. The FIDO2 working group has this in review to potentially evolve the specification, but it will not be completed by the release of Apple's passkeys.

Security Control Implications

Security teams and CISOs must consider the organizational control of authentication. For enterprises, the use of passkeys means acceptance of Apple's security controls and iCloud access. CISOs need to consider their level of confidence in Apple's security protections for iCloud. CISOs must also understand the security and auditability of keychain — giving Apple the "keys to the kingdom" can create a significant point of vulnerability.

OS and Environmental Limitations

Any application which supports WebAuthn will natively support passkeys and users will be able to access these applications from their iOS 16-enabled devices. However, passkey access to apps on a desktop or laptop requires running macOS Ventura — which will not be broadly deployed in most enterprises.

As noted earlier, regulated environments are currently not candidates for implementation of passkeys due to the lack of confidence in its possession factor. CISOs also have to consider the feasibility of deployment and cross-platform support, which applies both to those who use non-Apple PCs but also to those whose preferred phone is Android.

Security Siloes

Cooperation and interoperability between an organization's different security technologies is essential to keep pace with the rapidly changing threat landscape. The exchange of information between security systems can make the difference between effective threat response and missing an attack architected to evade point security products. It remains to be seen if passkeys will be fully interoperable with existing security investments or will follow Apple's typical "walled garden" approach.

Phishing Resistance by Design?

More than 80% of attacks include compromised passwords and failed authentication. The recent 0ktapus attacks and phishing services like EvilProxy highlight the degree to which traditional multifactor authentication is easily bypassed. This effectively is the collapse of traditional authentication methods. Eliminating passwords fundamentally changes the economics of attack and mitigates the risk of phishing, AitM and other credential-targeting attacks.

With passkeys, Apple delivers an advancement in driving users to adopt passwordless authentication. Based on the FIDO2 specification, passkeys help mitigate phishing on the client side. However, full phishing protection requires third-party app and service providers to adopt and implement FIDO2 specifications as well. Apple's delivery of passkeys only addresses part of the equation and thus does not offer a fully phishing-resistant, passwordless MFA solution.

The Bottom Line

The advancement of passwordless authentication by Apple and others brings wide-scale visibility to the problem of authentication security and serves as a clear endorsement of FIDO standards as the way forward. However, organizations and CISOs must understand that the current offering is not architected, nor does it have the comprehensiveness, feature functionality or forward compatibility to scale for businesses.

Organizations cannot wait and hope that such offerings will evolve to the type of enterprise-grade solution they require now. Whether businesses deploy for their workforce, their customers, or both, the execution of a successful passwordless MFA strategy must be done at scale to address authentication risk today as well as into the future.

Ensure Secure Passwordless MFA with HYPR

HYPR makes it easy to implement True Passwordless™ MFA for organizations across all verticals. It turns an ordinary smartphone into a FIDO-certified security key for frictionless authentication. This means less hassle for your team, increased productivity, cost savings and — most importantly — a more secure authentication system for your workforce and applications.

Apple Passkeys vs. HYPR Passwordless MFA (PMFA)

Description	Apple Passkeys	HYPR PMFA
Private Key Storage	Stored in iCloud Keychain.	Stored with the user in the device Secure Enclave or TPM.
Desktop to Cloud Coverage	Website apps that are WebAuthn compliant only. Does not apply to desktops or remote access.	Single authentication flow that begins at desktop login and carries through to connected applications. Protects remote access points — VDI, VPN, RDP.
Multi-Factor Authentication Possession Requirement	Does not meet definitions and regulatory requirements for an independent "possession" factor.	Meets or exceeds SCA and other regulatory requirements.
FIDO2 Certified End-to-End	Apple passkeys are not certified by FIDO	FIDO Certified on all solution components
Cross-Platform Support	Only works on iOS 16 and macOS Ventura.	Supports all major platforms including iOS, Android, macOS, Windows, Linux.
Integrates With Existing Security Investments	No current integrations.	Integrates with APIs and direct integrations with other security vendors.
Use Case	Individual	Enterprise – Workforce & Strong Customer Authentication

To find out how HYPR can make your systems more secure, **talk to our team** or **arrange a demo**.