HYPR Tech Brief

An Enterprise Guide to Passkeys

In September of 2022 Apple released iOS 16, which included the much anticipated rollout of passkeys. Google followed a few months later, with passkey support on Chrome and Android. By implementing passkeys, Apple and Google help significantly advance consumer acceptance of a password-free life. It's a logical progression considering that Apple and Android devices have used biometric capture instead of passwords for device login for years.

With support of passkeys by the top two mobile platforms, consumers no longer have to ever write, generate or remember a password (shared secret). The entry of passwordless into the mainstream is a pivotal moment in the history of computing and the internet. It's also an important signifier to businesses that remained on the fence about implementing passwordless technologies.

Passkeys Are Currently 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. Similarly, Google passkeys are created on an Android device and synced through the Google Password Manager. To sign in on a Windows or Mac system, the user scans a QR code. Passkeys are based on FIDO2 WebAuthn, providing a phishing-resistant login to websites and apps. They are a tremendous step forward in furthering adoption of passwordless authentication. Passkeys and other consumer-targeted passwordless options, however, carry challenges when attempting to apply them 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 evolve the specification.

Security Control Implications

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

While the security controls are something to evaluate, the use of passkeys does move toward a phishing-resistant form of authentication and will remove the password reset use case that has been a challenge of password-based authentication systems.

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 or Chrome on Android devices. However, Apple 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.

These specifications will evolve over time, and support for passkeys cross platform is a stated goal of Apple , Google and Microsoft and the FIDO Alliance. However, it does not yet meet these specifications nor is there an established timeframe to do so.

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 the typical "walled garden" approach.

It is critical that Relying Parties that offer passkey support share data insights with SIEMs and other Log Management systems, thereby delivering the insights of user authentication behavior to the security team and business.

Phishing Resistance by Design?

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

The Bottom Line

The advancement of passwordless authentication by Apple, Google 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.

Recommendations for End Users

If you have any service providers you interact with that offer passkeys as a login option, we recommend you take

advantage of it and enroll. Benefits include:

- No more password and no more “forgot password” links to click
- If your service provider is breached, the password is rendered useless
- If you lose or damage your device, you can move your service provider access to a new one

Recommendations for Service Providers

As passkeys gain traction and end user demand increases, practitioners and providers need to be prepared. Passkey support will need to be circumscribed and hardened with security measures. Much of what we had control over during either a registration event or authentication event will change.

- Passkeys are shared across devices
- Passkey enrollment UI is controlled and driven by the platform vendors
- Passkey authentication UI is controlled and driven by the platform vendors. Note that **Webauthn Conditional UI** is part of the the Webauthn standard and is only currently supported by Safari.

Recommendations for Enterprises

Organizations cannot wait and hope that passkey 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.

The adoption of passkeys does not need to be an all or nothing implementation. Depending on the type of service or industry regulation requirements you must adhere to, passkeys can be implemented in conjunction with strong authentication and security technologies to meet specific requirements.

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. That means less hassle for your team, increased productivity, cost savings and — most importantly — a more secure authentication system for your workforce and applications. It also opens up the possibility of offering passkeys as an authenticator option to your users in defined circumstances, while retaining control and management.

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