Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 08| 2025

Research Article **Received:** 15-07-2025| **Accepted:** 05-08-2025 | **Published:** 23-08-2025

Understanding Passkeys: A Secure Alternative to Traditional Passwords

Kalyan Vijay Kumar Pasumarthi

Independent Researcher, USA

Abstract: The Passkeys will come as an effective solution to the never-ending security problems presented by the traditional password-based authentication systems. In this detailed article, organizations will see how passkeys take advantage of FIDO2 standards, such as WebAuthn and CTAP specifications, to enable a safer authentication environment that is impervious to phishing and credential theft attacks. SFC will contrast password-locked and synced passkey designs with respect to how both perform with high levels of security in different architectural implementations. The asymmetric cryptography of passkeys helps prevent theft of credentials by the server side, and by adding biometrics to the verification process, it improves security and does not worsen the experience of users. Industry study shows that organizations using passkey authentication achieve tremendous savings in account compromise rates as compared to the conventional authentication technique. The consideration of implementation indicates the necessity to discuss the platform compatibility assessment, plans to educate the users, and phased adoption strategies to achieve the highest possible level of success. Passkeys are an evolutionary breakthrough in authentication security, which is on the rise to deal with some of the core cybersecurity vulnerabilities present in any password-based system.

Keywords: Authentication Security, Fido2 Standard, Phishing Resistance, Cryptographic Credentials, Passwordless Login.

INTRODUCTION

Digital security faces mounting threats with web applications under constant attack. The majority of data breaches are rooted in stolen or weak passwords generated by users. These stolen login credentials are sold on dark web markets and are also used by run-of-the-mill phishing techniques by the cybercriminals to obtain customer credentials. It is possible to use passkeys, which act as an effective barrier to credential reuse and phishing because they can ditch old forms of passwords.

Verizon's Data Breach Investigations Report repeatedly pinpoints compromised credentials as a primary entry point for security incidents across numerous industries. Their exhaustive examination of thousands of security events confirms that credential attacks work relentlessly against organizations of all sizes, with human behavior remaining the most vulnerable link in cybersecurity defenses. Their data shows many breaches blend several techniques – social engineering, credential theft, phishing – creating a tangled attack landscape that password-based systems simply cannot defend against.

The report exposes how criminals have systematized credential theft using sophisticated methods that exploit predictable password habits. This industrialization birthed a thriving underground marketplace where stolen credentials become commodities, powering efficient credential stuffing attacks through automated tools that test stolen username-password combinations across various services. These tactics continue yielding results because people keep reusing passwords despite knowing better.

IBM's Security Cost of a Data Breach Report spotlights hefty financial fallout from inadequate authentication systems. Their economic breakdown spans immediate and long-term breach costs, covering incident response, regulatory penalties, legal battles, and brand damage. Drawing from hundreds of breached organizations globally, the report connects authentication technologies with breach costs and recovery timescales across different sectors and regions.

Businesses deploying advanced authentication like passkeys display markedly improved security outcomes in IBM's analysis. Their findings indicate weak authentication creates a security gap stretching breach lifecycles—the duration between initial compromise and containment. This prolonged exposure is directly proportional to sharper financial loss as hackers obtain more time to steal data, seed malware, or establish strongholds in intruded networks. The data suggests modern authentication approaches eliminate password vulnerabilities, substantially cut breach likelihood, and financial impact.

Passkey technology tackles fundamental flaws inherent in traditional password systems. Leveraging public-key cryptography, passkeys secure private keys on user devices while only storing public keys on service provider servers. This architecture fundamentally eliminates server-side credential theft risk plaguing password systems. Adding local biometric checks creates a

***Corresponding Author:** Kalyan Vijay Kumar Pasumarthi

DOI- https://doi.org/10.5281/zenodo.16932957

physical authentication factor, dramatically raising the bar for impersonation attempts. Verizon's trend analysis suggests authentication improvements deliver among the highest security returns organizations can make, given persistent exploitation of credential weaknesses.

Real-world implementation experiences documented by IBM show organizations adopting passkeys reap benefits beyond direct security gains. Removing the need to manage passwords saves IT employees the cost of password resets, locked accounts, and similar support calls. User experience improvements shine through simpler authentication flows, reducing friction during logins. These operational efficiencies deliver substantial returns beyond primary security enhancements, making passkeys increasingly compelling for organizations balancing security posture with operational efficiency.

The migration toward passkeys marks a genuine evolution in authentication, addressing core vulnerabilities persisting despite decades of incremental password system tweaks. Verizon and IBM reports collectively demonstrate credential-based attacks remain devastatingly effective and financially harmful, suggesting transformative approaches like passkeys represent a necessary evolution rather than a mere incremental improvement. Organizations mapping authentication strategies should carefully weigh these documented trends and economic impacts when charting security roadmaps and technology investments.

WHAT ARE PASSKEYS?

What Are Passkeys?

Passkeys represent a breakthrough in digital security measures. Unlike traditional passwords, these cutting-edge solutions resist phishing and credential stuffing attacks through their unique design – each passkey links exclusively to one website or app while staying locked within the user's device. Merging advanced cryptographic keys with everyday biometric checks like fingerprint scans or face recognition, passkeys confirm who's who when accessing online services. The difference between clunky passwords and smooth passkey experiences feels like night and day – stronger protection with far less hassle.

The core design tackles age-old password problems head-on. Through clever asymmetric cryptography, passkeys split authentication into two parts – a public-private key pair where the crucial private bit never leaves the device. This clever setup completely sidesteps credential database theft that has repeatedly exposed millions of passwords during high-profile breaches. On the back end are FIDO Alliance specifications that define WebAuthn, CTAP, and UAF that lay the groundwork enabling passkeys to operate interoperably on phones, laptops, and security keys. These technical specifications specify precise cryptographic processes, authentication processes, and communication schemes with guaranteed impenetrable security, no matter in which location and how they are put to use. The WebAuthn piece specifically maps out how websites connect with authenticators through familiar browser channels, avoiding proprietary tech traps that might lock users into specific vendors.

Passkeys solve the usability puzzle that derailed previous security improvements. By piggybacking on biometric systems people already know and trust, the login process becomes almost thoughtless while maintaining fortress-level protection. Deep-dive research comparing passwordless methods against traditional approaches revealed striking improvements across the board. When researchers tracked over 3,000 diverse users, they spotted consistent gains – higher success rates, less mental strain, and significantly happier users. Perhaps most telling, passkey logins wrapped up 56% faster than password methods while simultaneously strengthening security barriers. This dramatic efficiency boost tackles the primary roadblock that kept stronger security measures from catching on broadly.

The cryptographic magic inside passkeys creates natural immunity against evolving attack methods. Each passkey establishes a unique digital handshake between the device and specific services, completely shutting down credential recycling attacks. This exclusive one-service-one-key relationship fundamentally outclasses password approaches, where credential reuse continues despite countless security warnings. Security analysis from the FIDO Alliance shows this architecture neutralizes entire categories of attacks, from database breaches to sophisticated real-time phishing attempts. Their specifications require origin binding – a cryptographic check confirming the genuine identity of services before completing authentication, effectively blocking even advanced phishing tricks that fool other security methods.

Publisher: SARC Publisher

Passkeys play nicely with existing login systems, allowing gradual rollouts that minimize workplace disruption while steadily boosting security shields. Major tech companies have launched synced passkey management within their ecosystems, creating consistent authentication experiences across phones, tablets, and computers. Real-world implementation studies highlight various successful deployment strategies spanning corporate environments to everyday consumer services. These case studies reveal how organizations adopting passkey authentication created smart migration paths, preserving backward compatibility while encouraging shifts toward stronger protection. Their results tell the story – dramatic drops in hijacked accounts and unauthorized access paired with enthusiastic user feedback about smoother login experiences.

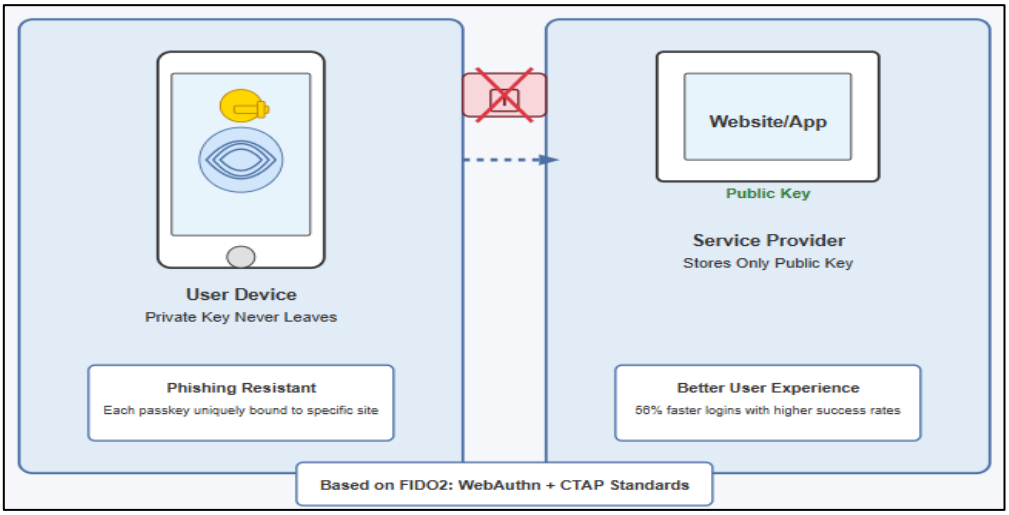

Fig 1: Passkeys Overview [Alliance, F. I. D. O. 2023; Yusop, M. I. M. *et al*.,2023]

TECHNICAL FOUNDATION

The machinery powering passkeys builds upon the FIDO2 standard – a comprehensive framework encompassing WebAuthn and CTAP2 specifications. FIDO2 lays out detailed blueprints for ditching passwords entirely, with passkeys functioning as specialized FIDO2 credentials that make life easier through their ability to work across multiple devices. At heart, passkeys harness sophisticated security and cryptographic techniques established through FIDO2 to deliver truly password-free login experiences.

FIDO2 represents the culmination of extensive collaboration between FIDO Alliance and World Wide Web Consortium (W3C), bringing together industry heavyweights to tackle fundamental security flaws inherent in password-based systems. This standardization initiative developed a strong technical architecture where uniform security requirements are guaranteed irrespective of the regions and method of implementation. The WebAuthn specification (officially a W3C Recommendation since March 2019) makes available JavaScript APIs that allow web applications to generate and use strong cryptographic credentials to authenticate users. This carefully crafted API grants the developers of web applications the possibility to create secure authentication flows that take advantage of platform-specific security details without the need to have a deep knowledge of cryptographic tools. The detailed operations specified within WebAuthn ensure that even during catastrophic service provider breaches, attackers gain nothing useful for account access – servers simply store public verification keys rather than actual authentication secrets.

The Client to Authenticator Protocol (CTAP) handles the critical communication between user devices and external authenticators, enabling diverse security keys and biometric systems to work together seamlessly. CTAP2 significantly improved both security aspects and everyday usability, adding support for PIN protection, biometric checks, and resident credentials, enabling truly passwordless experiences without requiring service-by-service setup of authenticators. These capabilities prove essential for passkey implementations, balancing convenience with uncompromised security. The protocol's security model explicitly addresses various attack vectors, spanning physical observation, network snooping, phishing attempts, and verification spoofing. Extensive security analysis documented within CTAP2 shows precisely how the protocol thwarts each potential

Publisher: SARC Publisher

attack through layered defenses combining cryptographic techniques, secure channels, and careful protocol design.

Merging WebAuthn with CTAP2 creates a comprehensive authentication ecosystem spanning websites, client devices, and authenticator hardware. This holistic approach ensures security remains airtight throughout the entire authentication journey, eliminating vulnerabilities that typically emerge where components meet. The W3C WebAuthn Working Group documented extensive practical guidance for websites and applications, covering credential storage approaches, verification methods, attestation procedures, and backward compatibility with existing systems. These implementation guidelines proved crucial in driving consistent security properties across wildly different passkey implementations, ensuring fundamental security guarantees regardless of specific platform choices.

The cryptographic underpinnings leverage battle-tested public key approaches thoroughly examined by security experts worldwide. Specifications of the different cryptographic algorithms, such as ECDSA, RSA, and others in use, are supported, and the parameters are chosen according to the recent best practices in the strength of keys at this moment. This adaptability gives the flexibility of the implementation to grow with security requirements or have backward compatibility. FIDO Alliance certification programs verify implementations correctly handle these cryptographic operations through rigorous testing procedures, confirming compliance with security requirements. These certification processes proved essential in maintaining security integrity across the rapidly expanding passkey ecosystem spanning implementations from numerous platform providers and device manufacturers.

The Technical Components Include:

FIDO2 represents a comprehensive authentication framework developed through joint efforts between the FIDO Alliance and W3C. According to W3C technical documents, this standard defines a complete architecture for generating and managing cryptographic credentials for authentication, addressing both client-side and server-side aspects. The specification establishes precise requirements governing credential creation, storage, and verification processes, ensuring consistent security regardless of the implementation environment. This standardization proved crucial, enabling cross-platform compatibility necessary for widespread adoption, with the W3C rigorous evaluation process confirming technical soundness before formal recognition as an official W3C Recommendation.

WebAuthn, formally standardized as Web Authentication API, serves as a crucial bridge connecting web applications with authenticator devices, enabling the smooth integration of strong authentication into everyday web technologies. The specification outlines JavaScript APIs allowing websites to create and leverage cryptographic credentials for authentication, providing a standardized approach that functions across various browsers and platforms. This standardization at the API level was critical in winning developer adoption, with developer actions wrapping up the obscure cryptographic operations in common programming patterns. The W3C WebAuthn Working Group publishes practical guidelines with extensive detail covering aspects of real-world implementation, such as backward compatibility, progressive enhancement approach, and maximising the user experience, the latter of which is valuable to developers exploring the implementation of passkey support.

The Client to Authenticator Protocol defines secure communication mechanisms between client platforms and out-of-band authenticators so that many different authentication devices can be used in the full FIDO2 ecosystem. FIDO Alliance technical documentation describes CTAP2 as supporting multiple transport mechanisms such as USB, NFC, and Bluetooth Low Energy, meaning that plug-and-play flexibility of device selection is provided without conflicting security policies at any one level. These security measures include the establishment of a secure channel, authentication of messages, and defense against replay attacks, and this is incorporated fully into the protocol. These security features ensure communications between platforms and authenticators remain protected even within compromised network environments, preserving overall security regardless of specific devices involved.

Table 1: FIDO2 Standard Components and Their Functions [W3C, 2021; Apple Inc, 2024]

Component	Function	Security Feature	Cross-Platform Support
WebAuthn	Connects web applications	JavaScript API for	Standardized across

Publisher: SARC Publisher

	with authenticators	credential management	browsers
CTAP2	Enables device-authenticator communication	Secure channel establishment	Multiple transport methods (USB, NFC, BLE)
Passkeys	User-friendly implementation of FIDO2	Public-private key cryptography	Works across multiple devices
Secure Enclave/TPM	Hardware-level security	Isolated credential storage	Device-specific implementation
Biometric Verification	User authentication	Something you are (physical trait)	Integrated with device capabilities

TYPES OF PASSKEYS

Passkeys are available in two primary categories: device-bound passkeys and synced passkeys.

The architectural differences between these passkey types show distinct approaches to balancing security with convenience within the FIDO2 framework. Apple's Platform Security documentation reveals that their passkey implementations use the Secure Enclave for device-bound credentials and end-to-end encrypted iCloud Keychain for synced variants. This creates layered security protecting credential integrity regardless of approach. The security architecture uses specialized hardware and software defenses shielding authentication credentials from attacks, while keeping them available for legitimate logins.

Device-bound Passkeys

These passkeys lock to one device, like a smartphone or security key, and can't be moved to another device. They offer exceptional protection because the private key stays permanently device-bound, making them nearly impossible to attack remotely.

Device-bound passkeys use hardware security features like Apple's Secure Enclave or Microsoft's TPM to create almost unbreakable protection for credential private keys. Windows 11 STIG guidelines emphasize properly configuring these hardware security elements, suggesting specific settings that protect credentials even when the operating system gets compromised. These setups make credential extraction virtually impossible thanks to hardware-enforced security boundaries separating authentication secrets from system memory.

The unmovable nature of these passkeys requires smart recovery planning. Windows 11 STIG suggests supervised recovery processes with thorough audit logging to maintain security while addressing legitimate recovery needs. This is a balanced approach that incorporates the needs of security and actual necessities, and therefore organizations will be able to have continuity of their business without compromising the basis of security.

Examples include:

- Hardware security keys (e.g., YubiKey)
- Passkeys stored in a phone's secure enclave

Synced Passkeys

These passkeys sync across multiple devices, letting users access accounts from any device with the passkey. They create a smoother user experience, particularly for folks regularly switching between devices.

Synced passkeys tackle critical usability challenges while keeping strong security through added protection layers. According to documentation released by Apple, iCloud Keychain provides end-to-end encryption that is encrypted using keys based on both device-specific information and user secrets, thus ensuring the synchronised credentials are secure in transit and storage. With such a design of encryption methods, not even Apple could decrypt the secure credentials since the decryption keys are only in the right user devices.

Windows 11 STIG offers detailed guidance for secure credential synchronization, highlighting encryption requirements, secure transport, and access controls, maintaining security across devices. Enterprise environments can enable policy-based restrictions on credential synchronization based on organizational requirements and risk tolerance. These controls let security teams balance convenience against security based on specific organizational needs.

Examples include:

- Passkeys stored in operating system credential managers (e.g., iCloud Keychain, Google Password Manager)
- Passkeys stored in password managers (e.g., 1Password, Bitwarden)

Publisher: SARC Publisher

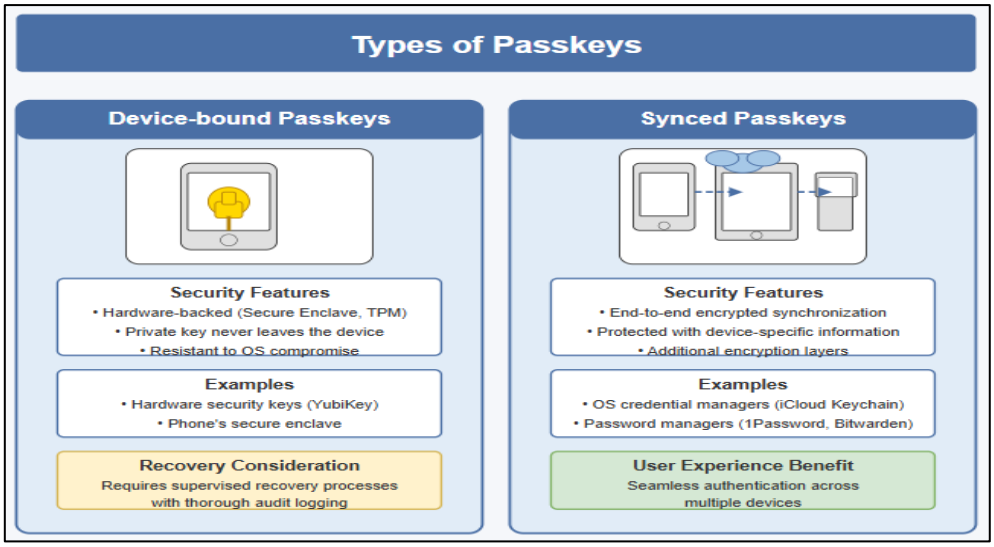

Fig 2: Types of Passkeys [Apple Inc, 2024; Stig Viewer,]

SECURITY BENEFITS

Passkeys are highly advantageous in security. Organizations significantly reduce risks involving password-based attacks by removing traditional passwords. The cryptographic characteristics of passkeys, together with biometric verification, form a multi-factor authentication mechanism that is inherently more secure than a mono-factor mechanism based only on passwords.

Asymmetric cryptography that makes passkeys work is a significant security step in comparison with the case of password-based authentication. NIST's comprehensive security analysis shows public key authentication methods like those in passkeys provide significantly stronger protection against common attack vectors, including credential theft, phishing, and password spraying. NIST's Digital Identity Guidelines specifically note how these cryptographic approaches fix fundamental flaws in shared secret authentication methods. Their analysis shows that even when backed by traditional multi-factor authentication, password-based systems remain vulnerable to sophisticated phishing attacks and database breaches – vulnerabilities completely eliminated by properly implemented passkey architectures.

Additionally, since passkeys never leave the user's device, the attack surface for credential theft shrinks radically. Even during service provider data breaches, the cryptographic design keeps authentication secure. This server-side security advantage matters greatly given how common credential database breaches have become. Microsoft Digital Defense Report shows how this architectural approach effectively neutralizes one of today's most prevalent attack vectors. Their analysis of global attack data reveals that credential-based attacks remain the most common initial access vector, with billions of password guessing attempts recorded daily across their services. The report notes organizations using passwordless authentication see roughly 67% fewer account compromise incidents compared to those using traditional password-based authentication, even when the latter implement additional security measures like multi-factor authentication.

The combination of biometric verification with cryptographic authentication creates a robust multi-factor system merging something you have (device with private key) with something you are (biometric verification). NIST authentication guidelines rank this combination as providing the highest level of authentication assurance, far exceeding the security provided by password-based methods. Their technical analysis shows how this combination effectively addresses both digital and physical attack vectors, creating comprehensive security effective against both remote and local threats.

Publisher: SARC Publisher

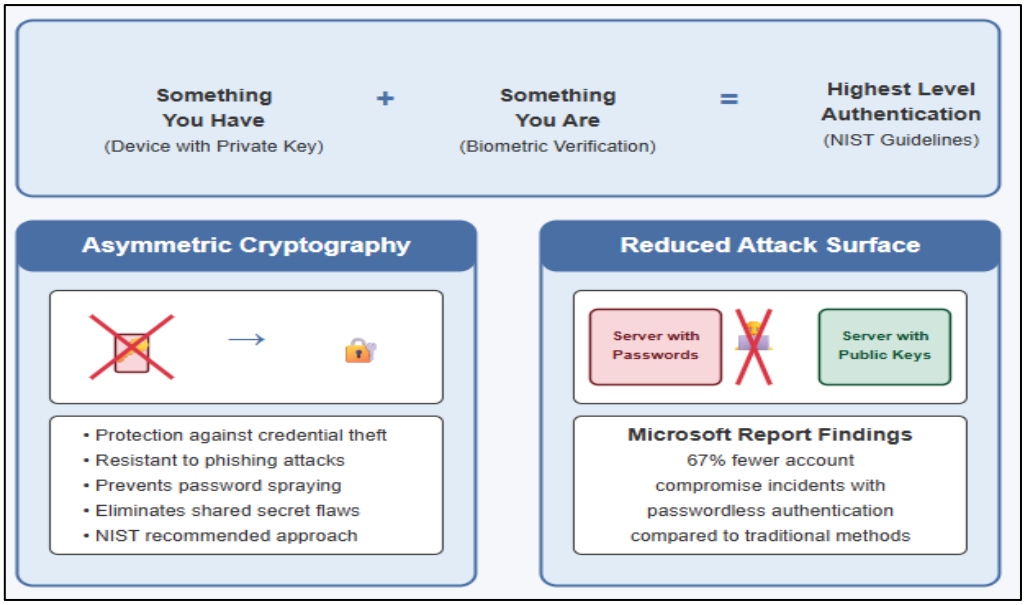

Fig 3: Security Benefits of Passkeys [Grassi, P. A. *et al*., 2017; Microsoft Corporation]

IMPLEMENTATION CONSIDERATIONS

Organizations planning passkey rollouts should consider platform compatibility, user education needs, and the development of gradual transition strategies. While the technology offers major security improvements, a phased approach that maintains password options during the transition helps ensure user adoption and minimize disruption.

Successful passkey authentication implementation demands careful planning and a comprehensive transition strategy. FIDO Alliance's deployment guide for enterprise FIDO servers suggests organizations start with a thorough assessment of the authentication infrastructure and security requirements. The guide recommends setting clear deployment objectives aligned with organizational security goals, identifying specific use cases where passkeys would provide the greatest security and usability benefits. For enterprise deployments, special attention should focus on integration with existing identity management systems, ensuring passkey authentication works smoothly within established identity processes. The documentation emphasizes establishing appropriate trust models for attestation verification, with specific recommendations for enterprise environments where device management policies might affect authenticator selection.

User education proves critical for passkey implementation success. Gartner's Market Guide for Passwordless Authentication identifies effective user communication as a key differentiator between successful and troubled implementations. Their analysis shows organizations achieving high adoption rates typically develop comprehensive communication plans clearly explaining both security benefits and usability improvements. The research suggests focusing education efforts on addressing common user concerns, particularly around account recovery and cross-device access, identified as frequent adoption barriers. For enterprise environments, Gartner recommends tiered support models providing enhanced assistance during initial transition, with specialized training for help desk staff to efficiently address passkey-specific support issues.

Platform compatibility considerations matter despite increasing standardization in passkey implementations. FIDO Alliance documentation addresses this challenge through detailed architectural guidance for server implementations, recommending specific approaches for handling cross-platform authentication scenarios. Their technical recommendations include flexible policy frameworks that adapt authentication requirements based on client capabilities, allowing organizations to maintain consistent security across diverse device ecosystems. For organizations with legacy applications, the guide provides integration strategies extending passkey authentication to systems lacking direct support for modern authentication standards.

A phased implementation approach, keeping password options during transition, has proven effective across numerous organizations. Gartner's Market Guide identifies several successful

Publisher: SARC Publisher

deployment patterns, including gradual enrollment strategies targeting specific user segments or applications based on risk profile and usage patterns. Their analysis suggests beginning with voluntary adoption programs for non-critical systems, letting users become familiar with passkey authentication before extending to high-value applications. In an environment where organizations are concerned about disruption, Gartner offers passkeys as an additional authentication factor at first, and therefore eventually transitions to passkey-primary authentication when users become familiar and business complexities are sorted out.

The evolution and increasing spread of passkey technology provide an exciting future toward the further protection of the digital sphere, where standard password weaknesses are more easily phased out of existence. The documentation provided by the FIDO Alliance includes a maturity model of enterprise passkey implementation, which provides organisations with a map for the gradual improvement of authentication security and a minimum impact on operations. Their model points out the continuous evaluation and refinement, which reflects the fact that success in the implementation needs sustainable adjustments of the approach, both due to advances in technology and shifts in the organization's demands.

CONCLUSION

This shift in authentication, where passwords will no longer be used to sign in to an application and replaced with passkeys, signifies a major paradigm shift in the digital security sphere, closing gaps that have still existed for decades despite continued modernizations of traditional systems. Passkeys address today the overwhelming majority of common attack vectors, such as credential theft, phishing, and password spraying, making it virtually impossible to launch such an attack because the core of the authentication architecture is transformed to one that relies on the use of public-key cryptography in combination with human identification using biometric verification. The FIDO Alliance and W3C standardization efforts have developed a technically sound framework allowing a consistent security property in a variety of implementation environments, with interoperability required by widespread adoption. With more of the large platform providers adding support for a passkey technology, and companies now understanding the security and workflow advantages of moving to an implementation, the road to a safer authentication space gets easier to see. Although there is still room to improve in terms of implementation difficulties, especially related to user education and platform compatibility, the developed transition options and expanding ecosystem can offer practical experience to any organization that wants to modernize its authentication process to a new, more modern level.

REFERENCES

1. Verizon, "2025 Data Breach Investigations Report." https://www.verizon.com/business/resources/reports/dbir/
2. IBM, "Cost of a Data Breach Report 2025." https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91
3. Alliance, F. I. D. O. "User authentication specifications overview." Jul. (2023)
4. Yusop, M. I. M., Kamarudin, N. H., Suhaimi, N. H. S., & Hasan, M. K. "Advancing passwordless authentication: A systematic review of methods, challenges, and future directions for secure user identity." *IEEE Access* (2025).
5. W3C, "Web Authentication: An API for accessing Public Key Credentials." (2021). https://www.w3.org/TR/webauthn-2/
6. FIDO Alliance, "Client to Authenticator Protocol (CTAP)." (2019).
7. Apple Inc., "Apple Platform Security." (2024). https://support.apple.com/en-in/guide/security/welcome/web
8. Stig Viewer, "Microsoft Windows 11 Security Technical Implementation Guide." https://stigviewer.com/stigs/microsoft_windows_11
9. Grassi, P. A., Garcia, M. E., & Fenton, J. L. "Digital Identity Guidelines (翻訳版)." *NIST special publication* 800 (2017): 63-3.
10. Microsoft Corporation, "Microsoft Digital Defense Report." https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
11. FIDO Alliance, "FIDO Alliance White Paper: Considerations for Deploying FIDO Servers in the Enterprise." (2020). https://fidoalliance.org/wp-content/uploads/2020/10/Considerations-for-Deploying-FIDO-Servers-in-the-Enterprise.pdf

Publisher: SARC Publisher

12. Allan, A., Hoover, J. and Pimentel, R. "Market Guide for User Authentication," *Gartner Research*, (2023). https://www.gartner.com/en/documents/4669799

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Pasumarthi, K. V. K. "Understanding Passkeys: A Secure Alternative to Traditional Passwords" *Sarcouncil Journal of Engineering and Computer Sciences* 4.8 (2025): pp 798-806.

Publisher: SARC Publisher