International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Transition to Password-Free and Phishing-Resistant Authentication in Enterprise Information Systems: A FIDO2/Passkey-Based Standards-Based Qualitative Assessment and Phased Implementation Framework

Oğuzhan Kilim

Lecturer Isparta Vocational School of Information Technologies, Database, Network Design and Management, Isparta University of Applied Science

Abstract

Password-based authentication is one of the most fundamental vulnerabilities of enterprise information systems. This vulnerability is exploited through phishing, credential stuffing, password reuse and real-time transmission attacks where an attacker intercepts data. With strong multi-factor authentication, the risk is minimized but human-mediated factors like SMS, time-based OTP, confirmation notifications may get affected through fake login pages and reverse proxy. In general, the paper presents an evaluation of the security, usability, recovery, governance and interoperability aspects of FIDO2/WebAuthn and passkey which to be used for enterprise authentication. As per standards and current research, the study is qualitative risk comparison of password, password+OTP, push MFA, device-bound passkey and synchronized passkey approach; it establishes threat-control mapping; and proposes Enterprises five-phase migration. Consequently, as the proof demonstrates, this passkey approach is distinctively architecturally more secure against phishing owing to its root binding, public-key cryptography and authenticator domain. Nonetheless, reliance on synchronization provider, account recovery processes, legacy applications, multi-user-device usage, loss of devices, and enterprise attestation requirements generate new clusters of risks. The framework will consist of the following phases: inventory and user segmentation; pilot implementation for high-risk accounts; rollout to the managed workforce; and recovery and telemetry optimisation towards a managed de-risking against passwords. According to the research, the deployment of passkeys should not merely be regarded as a new technology for logging in. When used, a passkey can be thought of as a comprehensive enterprise security programme that jointly transforms the identity lifecycle, help desk, device management, access policies, and incident response.

Keywords: FIDO2, WebAuthn, passkey, passwordless authentication, phishing, multi-factor authentication, enterprise security.

1. Introduction

In enterprise information systems, an authentication layer is the first step to access control. When a user

account is compromised, it does not just mean access to one application. Because of federation, single sign on, cloud services and remote work infrastructure, the account compromise can lead to secondary effects like lateral movement, data leak and privilege escalation. Nonetheless, password stays the most commonly used. Due to the attack surface created owing to human memory reliance, cross-service re-use, exposure in data breaches and the ability for users to enter into a fraudulent authentication interface. NIST states that multi- or single-factor phishing-resistant establishes cryptographic authentication. They argue that OTP and out-of-band, which rely on user entry of a code, is not phishing-resistant because they aren't cryptographically bound to the session or the authenticator [1]. This distinction is important: while classic MFA adds a second knowledge or possession factor to a password, FIDO2/WebAuthn links the authentication process itself to a specific web origin. In other words, because a signature cannot be produced using the private key associated with that origin on behalf of the actual service, the fake page will redirect users.

WebAuthn defines a standard API that enables web applications to create and use public-key credentials; these credentials are scoped to a relying party and used on the authenticator with the user's consent [2]. The concept of a passkey, on the other hand, enables discoverable FIDO credentials to be stored in platform authenticators, securely synchronized across devices in certain scenarios, and used by users to log in via device unlock mechanisms [3]. Such a structure eliminates the need to store a reusable password secret on the server. However, the term "passwordless" does not mean that all operational risks have been eliminated. Device loss, compromise of the credential synchronization account, weaknesses in the recovery channel, shared workstations, third-party users, browser and operating system compatibility, authentication policies, and legacy applications directly impact the success of the transition. Usability studies have shown that users may hold misconceptions about biometric WebAuthn and smartphone-based authentication; issues such as where biometric data is stored and whether it is visible to the service provider influence adoption [4], [5].

The aim of this study is to evaluate FIDO2/passkey-based authentication within the context of enterprise risk management, rather than merely explaining it at the protocol level. The study's contributions can be summarized under three headings. First, it presents a qualitative assessment comparing password-based and passwordless methods in terms of phishing, credential stuffing, user experience, and recovery. Second, a practical mapping is established between threats and technical and administrative controls. Third, a measurable, five-phase implementation framework is proposed to support organizations' controlled transition to passkey usage.

2. Conceptual Background and Related Work

2.1. Limitations of Passwords and Classical MFA

A password is a secret shared between the user and the authenticator. The fundamental problem with this architecture is the requirement that the secret be represented in a form that can be presented by the user and verified on the server side. Even if password hashes are protected by strong hash functions, weak or reused passwords remain vulnerable to offline guessing and credential stuffing attacks. At the user interface level, the browser cannot always prevent a password entered into a fake domain from being submitted to the "wrong authenticator."

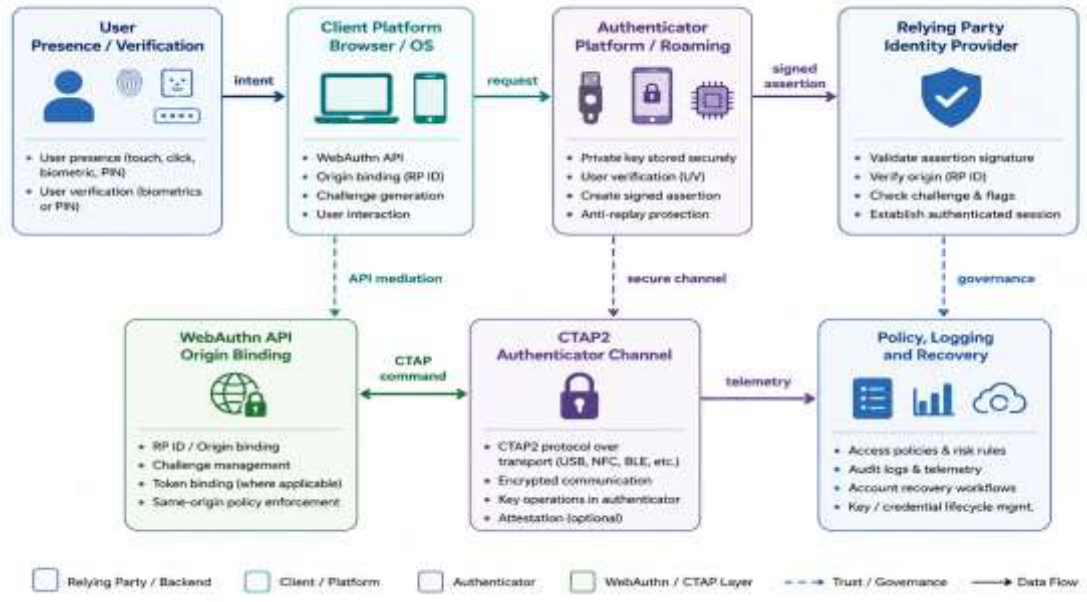
Classic MFA increases the attacker's cost by requiring a second factor even if the password is compromised. However, an SMS code, TOTP, or push notification can be inadvertently authorized by the user in the wrong context. The FIDO Alliance also notes that transitioning from the password+OTP

model to the passkey approach could provide benefits in terms of both security and user experience by reducing reliance on transferable codes [12]. Measurements of systemic 2FA usability show that security methods create varying levels of friction during processes such as lost device recovery, backup codes, setup, and re-authentication [6]. In particular, during real-time reverse proxy attacks, an attacker can obtain the session cookie by forwarding the password and OTP entered by the user to the legitimate service. Push notification fatigue attacks also aim to trick users into accidentally granting approval by sending a large number of notifications. Therefore, the fact that a method is multi-factor does not automatically mean it is phishing-resistant. Phishing resistance requires that the authentication output be tied to the target service and session. FIDO2 provides this feature by including the origin information and the relying party identifier within the client data under the scope of a cryptographic signature.

2.2. FIDO2, WebAuthn, and Passkey Architecture

The FIDO2 ecosystem relies on the interoperability of WebAuthn and the Client to Authenticator Protocol (CTAP) components. WebAuthn defines the API contract between the relying party and the client platform; CTAP defines the communication between the client platform and an external or platform-based authenticator. During registration, the authenticator generates a unique public/private key pair for the relevant relying party. The private key is not exposed from the authenticator; the public key and identity identifier are registered with the server. During login, the server's random challenge is responded to by signing the client data and authenticator data. Figure 1 shows the key actors in the FIDO2/WebAuthn architecture. User presence or user authentication can be established through biometrics, a device PIN, or physical contact with a security key. The purpose of biometrics is to grant local access to the private key; sending the biometric template to the relying party is not a requirement of the protocol. This distinction is critical for addressing users' misconceptions about biometric WebAuthn [4].

Figure 1. FIDO2 / WebAuthn authentication architecture and trust boundaries.



Passkeys can be implemented in either a device-bound or synced manner. With device-bound credentials, the private key remains on a single piece of hardware or within a secure execution environment. With synced passkeys, the credential can be transferred to the user's other devices via the

platform provider's end-to-end protected credential manager. While this architecture enhances usability and resilience against device loss, it shifts a portion of the trust to the passkey provider's account security and recovery mechanisms. This balance between device-bound and synchronized credentials is currently being debated in the literature in terms of security, usability, and accessibility [7].

2.3. Security and Usability Studies

According to early-stage surveys on the end-user acceptance of FIDO2, users consider passwordless authentication as secure and usable, but a proper explanation of setup, account recovery, and authenticators is necessary [8]. Research indicates that even though users may not understand the model of private keys and service-specific credentials when using their smartphones as roaming authenticators, they rated the login experience positive [5]. The study around WebAuthn, which made use of biometric data, showed that informative messages in the interface reduced some misunderstandings but the uncertainty about the storage of biometric data continued [4]. Challenges to enterprise deployment go beyond user awareness. According to research done with companies, the legacy system compatibility, cross-platform inconsistency, recovery, support costs, regulatory implications, and the reservations of decision makers about technology maturity are hindering the widespread uptake [9]. Besides, it is important to discuss what passkeys enable and prevent in person-to-person threat models and contexts outside the enterprise threat model such as coercive relationships, shared accounts and device access [10]. This study is based on 8 most influential standards and significant research area as indicated in Table 1. Despite a strong consensus in the literature that the protocol is resistant to phishing, analyses also show that its recovery, corporate governance and implementation in the real-world are key.

Table 1. Summary of key standards and related studies.

Ref.	Study / Standard	Main Focus	Implications for This Study
[1]	NIST SP 800-63B-4	Authentication Assurance Levels and Phishing Resistance	States that OTP is not phishing-resistant; cryptographic binding is required.
[2]	W3C WebAuthn Level 3	Public-key credential API and relying-party scope	Provides the technical foundation for origin binding and the signed challenge mechanism.
[4]	Lassak vd., 2021	Perception of Biometric WebAuthn	Demonstrates that user communication and privacy disclosures are necessary for adoption.
[5]	Owens vd., 2021	Smartphone-Based FIDO2 Usability	Notes that while the user experience is positive, the mental model may be lacking.
[6]	Reynolds vd., 2020	Systemic measurement of 2FA usability	Highlights friction related to setup, lost devices, and recovery.
[9]	Lassak vd., 2024	Barriers to enterprise passkey adoption	Identifies barriers related to legacy systems, recovery, support, and organizational decision-making.
[10]	Daffalla vd., 2025	Passkey misuse	Demonstrates that interpersonal and shared-device threats require additional policies.
[11]	Jannett vd., 2026	Passkey adoption and application security on the Web	Emphasizes the heterogeneity of real-world relying-party applications.

3. Research Methodology

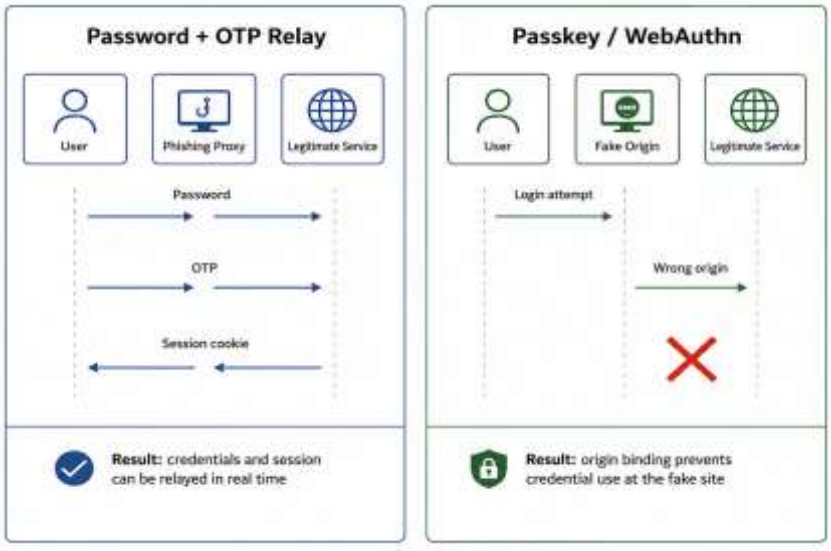
3.1. Scope and Analysis Approach

The research is a security analysis that does not create experimental user data and follows a standard, literature-based design science approach. The aim is not to evaluate a specific product's performance, but a comparative threat model and actionable roadmap to facilitate organizational migration decisions. The focus of the research will be limited to password, password+SMS OTP, password+TOTP, push MFA, device-bound passkey, and synchronized passkey methods in web and federated authentication scenarios. There were four steps to the analysis. The first step included defining four evaluation dimensions, namely phishing resistance, credential stuffing resistance, user convenience and recovery ease. In the second step, qualitative scoring of the methods on a scale of one to five was done, considering standard specification calculations and issues reported in user studies. These scores are not empirical measures of performance, rather analytical classification that exemplify the essential differences in architecture. During the third phase, threats were matched to preventive and detective controls. In the fourth phase, the outcome was presented as an enterprise migration framework using five phases.

3.2. Threat Model

The threat model assumes that an attacker may redirect a victim to a phishing login page, may have access to live password leaks, may set up an active reverse proxy infrastructure and may social-engineer the recovery channel. It is not assumed that the attacker can directly extract the private key from the secure hardware or break strong cryptography. However, the scenario does include the compromise of the device while it is powered on and unlocked, the bypassing of enterprise device management, the compromise of the synchronization account, and help desk manipulation. Figure 2 compares the attack flows in which the attacker intervenes in password+OTP and passkey scenarios. In the password+OTP flow, the fake relying party can forward the information obtained from the user to the legitimate service. In the passkey flow, however, since the credentials are not valid for the fake relying party, a usable signature cannot be generated on behalf of the legitimate relying party.

Figure 2. Conceptual comparison of credential relay in password-plus-OTP and passkey authentication.



3.3. Evaluation Criteria

Phishing resistance refers to the method's ability to prevent the reuse of credentials via a fake source or a real-time proxy. Credential Reuse Resistance it the probability that previously leaked credentials from one service may be used on other service. User convenience includes the need for memorization, number of steps required, integration with other platforms, and daily login experience. Recovery ease, on the other hand, is evaluated in terms of device loss, adding a new device, backup authenticators, and help desk workload. Table 2 compares the technical characteristics of the methods. Both types of passkeys eliminate password reuse due to service-specific public-key credentials. Device-bound passkeys provide strong key protection but increase the need for a backup authenticator in the event of device loss. Synchronized passkeys improve user continuity; however, the account security and recovery policies of the synchronization provider are incorporated into the risk model.

Table 2. Technical and operational comparison of authentication methods.

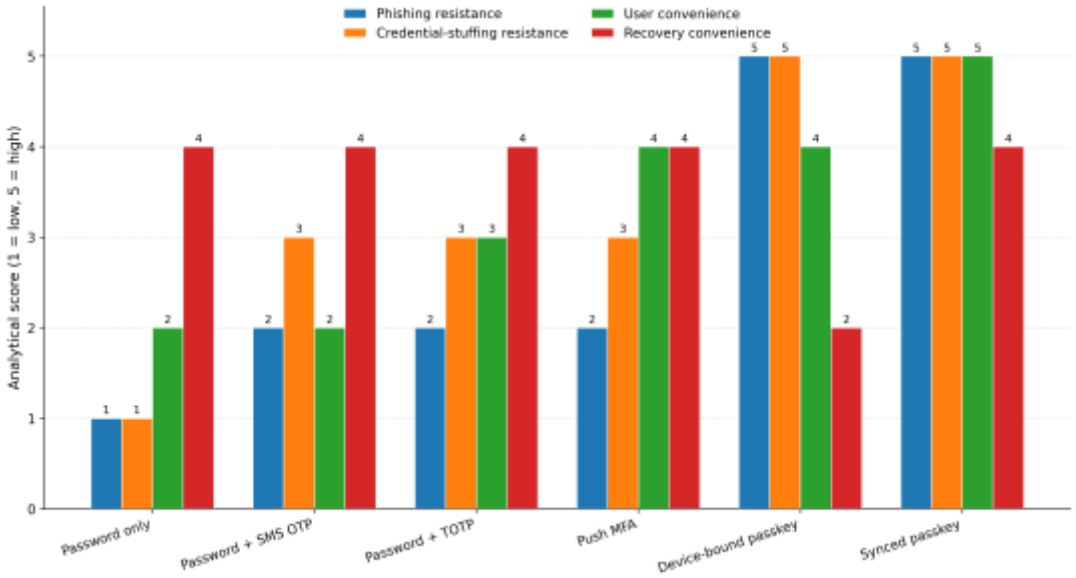
Method	Shared secret	Tying to origin	Resistance to real-time transfer	Core operational risk
Password only	Yes	No	Low	Reuse, data breach, phishing
Password + SMS OTP	Yes	No	Low-Medium	SIM swap, code transfer, coverage issues
Password + TOTP	Yes	No	Medium	Code transfer, setup and recovery burden
Push MFA	Yes	Limited / product-dependent	Medium	Push notification fatigue, incorrect approval
Device-bound passkey	No	Yes	High	Device loss, need for a backup authenticator
Synced passkey	No	Yes	High	Dependency on provider account and synchronization

4. Findings and Analytical Evaluation

4.1. Comparative Security Results

As shown in Figure 3, the qualitative scoring indicates that password-based approaches are the weakest in terms of phishing and credential stuffing. The fact that SMS and TOTP add a second factor to make it more difficult for an attacker to use the leaked password alone does not significantly impact phishing resistance, since the factor can still be entered into a fake interface. A push MFA that is less frictional in daily use may not provide sufficient contextual information and may cause users to approve alerts that are fraudulent. Passkeys that are device-bound and synchronized have a high analytical value for phishing and credential stuffing due to origin binding and service-derived key pairs. They differ in recovery and key portability or legacy issues. A device-bound passkey offers strong security at the hardware level by storing the key on a specific authenticator. However, in a single-device scenario, this raises an accessibility risk. Transparent cross-platform account recovery and delegated authorization with a synchronized passkey enhance user experience and continuity. On the contrary, it increases dependence on the identity provider's security architecture and account recovery [7].

Figure 3. Qualitative comparison of authentication methods across security and usability criteria.



The result suggests that a common passkey should not be selected for all users. Hardware-backed authenticators tethered to devices could be well-suited for privileged administrators, users approving financial transactions, and accounts with a high degree of impact. Nevertheless, for the usual working troop and end-user services, a coordinated passkey along with robust recovery policies and device integrity checks might support a greater balance.

4.2. Threat-Control Mapping

To maintain security enhancements accompanying the passkey transition, we must not focus only on the registration and sign-in steps. Table 3 Illustrates key threats, effects, and recommended controls. In particular, recovery mechanisms can serve as an alternative pathway that bypasses strong authentication. When the help desk only resets passkeys on the basis of knowledge-based questions, it makes protocol-level phishing resistance redundant. As such, proof of recovery should be multi-factorial and risk control delayed as appropriate to the authentication assurance level.

Table 3. Threat-control mapping for enterprise passkey deployment.

Threat	Potential Impact	Preventive Controls	Detection / Response
Phishing / AiTM	Account and session compromise	WebAuthn origin binding; reducing password/OTP fallback	Suspicious origin telemetry; session risk analysis
Credential stuffing	Mass account compromise	Service-specific keys; password disabling	Failed login anomalies; bot protection
Lost or stolen device	Unauthorized local use or lockout	Device lock, hardware protection, MDM, remote wipe	Device inventory; passkey revocation; event logging
Sync account compromise	Credential access across multiple devices	Strong MFA on provider account; restrict high-risk recovery	Alerts for new devices and sync events
Help-desk social	Account takeover via	Multi-channel authentication;	Reset logs; review of

engineering	passkey	separation of duties; waiting period	high-risk transactions
Legacy fallback abuse	Bypass via weak methods	Limit fallback scope by user and application	Fallback usage rate and anomaly monitoring
Shared-device misuse	Local access by the wrong user	Separate OS profiles; user authentication; session termination	Shared-device policy violation alert

4.3. Organizational Risks and Design Decisions

The initial choice relates to the type of authenticator and the assurance level. Relying on device management, platform-based authenticators can enhance user experience. Security keys designed to roam across multiple devices provide a high level of assurance but require managing the distribution, inventory, loss, and backup keys. Authenticator profiles should be tailored to user roles and business impact, and not a one-size-fits-all solution. Second decision is about verification vs privacy. In an enterprise context, the organization may want to ensure that the authenticator being used has particular security properties. Too much detail in verification might risk linking up the user/device across services, however. The policy should mandate no more authentication than required for the business–it should not impose unnecessary restrictions that would lessen interoperability for the wider workforce. Which third decision is account recovery? A passkey tied to a device needs to have at least two registered authenticators. To ensure compliance with organizational policy, the platform provider's recovery workflow must be assessed. Self-service recovery may not be available for privileged accounts, which may require an in-person process or a strong identity-verified process.

The fourth decision refers to legacy systems strategy. The transition may be delayed by thick clients that do not support WebAuthn, RDP/SSH scenarios, other network devices and legacy enterprise applications. The systems should be federated via an identity provider; if not supported, they should be isolated with risk acceptance or added to the modernization roadmap. Leaving a weak fallback method in place forever will always mean that an attacker will choose the easiest one. The fifth choice involves the measurement and reaction to incidents. The organization should create telemetry to monitor login success rates, the percentage of logins completed with passkeys, fallback use, account recoveries, help desk response times, failures, and device changes. A passkey event must link to the user, credentials, authenticator, device, application, and session context.

5. Proposed Five-Phase Enterprise Migration Framework

The proposed framework pursues a risk-informed and feedback-driven approach to migration, rather than implementing organization-wide rollout. According to Figure 4, the migration process is divided into phases as well as activities and responsibilities. Every phase of completion should not just be evaluated based on implementation of technology but also on the maturity of support from the organization through services, capabilities for recovery, measurement mechanism and governance policies.

Figure 4. Risk-based enterprise passkey migration roadmap.

- **Phase 1: Discovery, Inventory, and Segmentation:** The inventory of apps, identity providers, user groups, device ownership models, and existing MFA methods is created first. We categorize applications according to WebAuthn support, federation support, business impact, and fallback dependency. The users, for example, super administrators, standard users, field technicians, contractors, shared-device users and external customers, were put in groups. The threat model discussed in this paper is used to determine which type of passkey should be used where.
- **Phase 2: Pilot for High-Risk Accounts:** Technical support teams and volunteer members of high-risk user groups can launch the pilot group. For privileged accounts, enforce authenticator registration bound to two devices, a secure backup key, and controlled recovery. The pilot will not just be to show that the login works. The pilot will test scenarios including registration, adding new devices and lose devices, allowed browsers, work from home, help desk and so on. Short interviews and task observation are appropriate ways to collect user feedback to find misunderstanding.
- **Phase 3: Rollout to the Managed Workforce:** When pilot results are satisfactory, they will then scale out to managed devices and enterprise SaaS applications. Device compliance and passkey use can be evaluated together. Throughout the enrollment campaign, users must be made clear that the biometric data is not sent to the server, that the unlock lock of the device is taking place locally using a private key and how the fresh device acquisition process will work. Instead of being removed immediately, passwords are deprioritised for high-risk logins and fallback visibility is reduced.
- **Phase 4: Recovery, Telemetry, and Legacy System Optimization:** Once it is launched, recovery and exception management become the real bottlenecks. The processes of the help desk must be redesigned; permissions to reset passkeys must be restricted, and all operations must be subject to audit. By analyzing fallback usage across applications and user groups, the priority for modernization is established. New device registrations that seem suspicious, frequent recover attempts in a short time period, and sessions with geographic locations that are not normal have been escalated for incident response.
- **Phase 5: Controlled Reduction of Password Dependency:** In the last phase, password-based authentication is disabled for users and applications that have sufficient coverage and recovery maturity. Implementation need not happen at the same time across the organization but can be phased in. First, password-free high-maturity applications can be produced; legacy systems can have time-limited exceptions. Each exception must have a designated owner, a justification, compensating control, and an expiration date. According to the NIST approach, cryptographic authentications are to be used for high-assurance operations [1].

6. Performance Metrics and Governance

The transition programme's success should not only be determined to the extent of registered passkey. High registration numbers do not equate to security gains if users switch back to passwords for daily logins. Thus, metrics through coverage, usage, security, support and recovery dimensions should be balanced across. Table 4 provides recommended key performance measures and benchmark targets. Target values must be adjusted according to the starting point of your organisation; the thresholds in the table should not be seen as a universal standard but rather a sample for programme management.

Table 4. Recommended governance and performance indicators for passkey migration.

KPI	Definition	Sample Target	Management Objective
Enrollment coverage	The percentage of target users who have registered at least one passkey	Pilot > 90%; rollout > 80%	To monitor deployment coverage
Passkey sign-in share	The percentage of successful sign-ins completed using a passkey	> 75% in supported applications	To measure actual usage and password reduction
Fallback rate	The percentage of logins completed using a password or OTP	Monthly downward trend; < 10% in the mature group	Identify reliance on weak authentication methods
Recovery success time	Time for a legitimate user to securely regain access	Standard user < 30 min; privileged accounts based on policy	Measure the security-usability balance
Help-desk contacts	Authentication support requests per 1,000 users	Steady decline after the first month	Measuring operational load
Suspicious enrollment alerts	Investigation rate for risky devices or unusual enrollment events	100% investigation for high-risk events	Detecting enrollment and synchronization abuse
Legacy exception count	Number of password-dependent applications/accounts	Quarterly downward trend	Managing modernization and risk acceptance

Representatives from identity and access management, information security, endpoint management, help desk, legal/compliance, and application owners should be included in the governance structure. Authenticator profiles, the attestation policy, recovery requirements, and exceptions must be approved by the program committee. The incident response plan should have processes for revocation of passkeys, loss of devices, compromise of synchronization accounts, and suspicious recovery attempts. Security audits should also be carried out regularly. Relying party identifier, user authentication requirement, session binding, challenge uniqueness, and error message must be checked on WebAuthn calls. According to existing web metrics, passkey support and relying-party implementation formats are heterogeneous [11]. So, the phrase "standard supported" should not signal that secure configuration validation has taken place.

7. Discussion

The study shows that passkeys are not just an easier alternative to passwords. It shifts the threat model from a secret that is shared to a public-key credential for the service. The change prevents a data breach obtaining server side credentials and using it directly on another service. Also, it stops a user from presenting valid credentials to a spoofed origin. Thus, this security gain is structural as opposed to incremental improvements such as tightening password policies or larger OTPs. However, in enterprise security, it's not the core protocol which is weakest, but its lifecycle instead. If activities like user onboarding, device replacement, account recovery, exit, privilege escalation, and helpdesk support lack the same security design, an attacker will exploit those side channels instead of executing a broken passkey attack. Specifically, a synchronized passkey makes it easier to recover your device when it's lost, while it turns the platform account into a critical root of trust. One way in which this situation may centralize risk; however, the risk may be managed by strong provider account security, device authentication, and risk-based recovery. According to usability findings, user training needs to focus on constructing the correct mental model instead of committing understanding the correct model to memory. Users should be told the truth: do not tell them "you are sending your face instead of a password." The truth is that facial or fingerprint authentication allows locally granting permission to use the private key on the device only. A signed cryptographic response is sent to the service. Earlier work indicated that providing brief and accurate information can improve perceptions of biometric WebAuthn [4].

Another important point for organizations is to not view the passkey as a standalone replacement for zero-trust or conditional access. The user being in control of a specific authenticator is strongly suggested by the passkey but does not, on its own, signify that the device is malware free, that data was not exfiltrated at the conclusion of the session, or that the user performed the action voluntarily. As a result, it must be supplemented with device health, session risk, least privilege, and network and application telemetry. One limitation regarding the analytical scores is they weren't taken from controlled experiments. The scores represent the simplified concatenation of patterns and investment results for each decision item. Organizations should recalculate the scores using metrics such as task completion time, error rate, help requests, recovery success, and security incidents within their own users' group. Another limitation is that the passkey ecosystem is evolving fast. As WebAuthn Level 3 features, cross-platform flows, and enterprise management tools mature, the significance of some operational issues may shift [2].

8. Conclusion and Future Research

This research looked into the move toward enterprise information systems that use FIDO2/WebAuthn and passkey-based authentication in terms of its security, usability, recovery, and governance. The main line of defence against phishing attacks utilises a public-key architecture which ties credentials to the relying party's origin, irrespective of user training. This architecture has the distinct advantage against attacks where passwords and OTPs entered via manual entry will be transmitted in real-time. But, a properly functioning passkey program requires more than just taking out the password field. All the organization's device inventory, user segmentation, authenticator profiles, account recovery, help desk, legacy systems, telemetry and incident response must be redesigned together. The five-phase framework as proposed (discovery, pilot, expansion, optimization, and reduction of password dependency) allows this change to be controlled. In practice, a balance can be achieved using device bound hardware

authenticators for high risk and privileged accounts and passkeys for most of the workforce, with requirements for strong platform account security and managed device policies. Antifishing benefits of the primary method will not go far enough unless weak fallback and recovery paths are removed. In the future, it is possible to pilot the framework in organizations of different sizes and measure it quantitatively with parameters like user session length, error rate, support cost, number of successful recoveries and scores in a phishing simulation. Experimental studies should also focus on portability among passkey providers, enterprise proof-of-identity privacy, and shared-device scenarios.

Acknowledgement

To express our gratitude, this study thanks all researchers, standards organizations, and the open scientific community who made this work possible through their respective papers and technical specifications. The FIDO2 and WebAuthn developers and maintainers deserve special mention. The publicly available documentation of theirs offered valuable technical insights of great assistance to this particular research.

References

1. D. Temoshok et al., “Digital Identity Guidelines: Authentication and Authenticator Management,” NIST Special Publication 800-63B-4, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2025.
2. W3C Web Authentication Working Group, “Web Authentication: An API for Accessing Public Key Credentials—Level 3,” W3C Candidate Recommendation Snapshot, May 2026.
3. FIDO Alliance, “Passkeys: Passwordless Authentication,” FIDO Alliance, 2026. [Online]. Available: https://fidoalliance.org/passkeys/ (accessed Jul. 20, 2026).
4. L. Lassak, A. Hildebrandt, M. Golla, and B. Ur, “It’s Stored, Hopefully, on an Encrypted Server: Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn,” in Proc. 30th USENIX Security Symp., 2021, pp. 91–108.
5. K. Owens, O. Anise, A. Krauss, and B. Ur, “User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators,” in Proc. 17th Symp. Usable Privacy and Security (SOUPS), 2021, pp. 57–76.
6. J. Reynolds et al., “Empirical Measurement of Systemic 2FA Usability,” in Proc. 29th USENIX Security Symp., 2020, pp. 1275–1292.
7. A. Büttner and N. Gruschka, “Device-Bound vs. Synced Credentials: A Comparative Evaluation of Passkey Authentication,” arXiv:2501.07380, 2025.
8. S. G. Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel, “Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication,” in Proc. IEEE Symp. Security and Privacy, 2020, pp. 268–285.
9. L. Lassak, A. Hildebrandt, T. A. Büttner, and B. Ur, “Why Aren’t We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication,” in Proc. 33rd USENIX Security Symp., 2024, pp. 7309–7326.
10. A. Daffalla, A. Bhattacharya, J. Wilder, R. Chatterjee, and T. Ristenpart, “A Framework for Abusability Analysis: The Case of Passkeys in Interpersonal Threat Models,” in Proc. 34th USENIX Security Symp., 2025.

11. L. Jannett et al., “Studying the Adoption and Security of Passkeys on the Web,” in Proc. 35th USENIX Security Symp., 2026.
12. FIDO Alliance, “Displace Password + OTP Authentication with Passkeys,” FIDO Alliance White Paper, Sep. 2024.