The American Journal of Interdisciplinary Innovations and Research
ISSN 2642-7478 | Open Access

Type Original Research
PAGE NO. 82-88

Check for updates

Closing Enterprise Identity Assurance Gaps Through Combined FIDO2 and Certificate-Based Authentication Architectures

John R. Whitaker
Global Cybersecurity Institute, University of Edinburgh, United Kingdom

Abstract- The accelerating shift toward passwordless authentication, driven by technological advances in device-bound biometrics, platform authenticators, and standardized protocols, has created both opportunity and complexity for enterprise identity assurance. This article critically examines the integration of FIDO2-based passwordless mechanisms (including passkeys and CTAP/WebAuthn paradigms) with traditional certificate-based authentication to construct a hybrid, phishing-resistant, privacy-aware, and scalable identity architecture suited to modern enterprises. Drawing strictly from the provided literature, the paper synthesizes empirical and normative findings about mobile biometric advances, behavioral biometrics, FIDO2 usability and privacy implications, certificate lifecycle management, and data-protection regulation constraints (notably GDPR). The work articulates a detailed methodology for combining FIDO2 client- and server-side flows with enterprise Public Key Infrastructure (PKI), including trust anchoring, credential lifecycle orchestration, fallback and account recovery strategies, and privacy-preserving biometric handling aligned with regulatory obligations. Results are presented as descriptive analyses of anticipated security posture improvements, usability trade-offs, and operational complexity, supported by comparative studies of FIDO2 usability and biometric misconceptions. The discussion explores theoretical implications for identity assurance, counter-arguments regarding centralization and vendor lock-in, limitations in biometric entropy and behavioral approaches, and directions for future research including decentralized identifiers and semantic design patterns for passwordless applications. The article concludes with practical recommendations for phased enterprise

OPEN ACCESS

SUBMITTED 01 November2025
ACCEPTED 15 November 2025
PUBLISHED 29 November 2025
VOLUME Vol.07 Issue 11 2025

CITATION

John R. Whitaker. (2025). Closing Enterprise Identity Assurance Gaps Through Combined FIDO2 and Certificate-Based Authentication Architectures. The American Journal of Interdisciplinary Innovations and Research, 7(11), 82–88. Retrieved from https://theamericanjournals.com/index.php/tajiir/article/view/6970

adoption, governance controls, and technical blueprints aimed at realizing phishing-resistant, GDPR-compliant, and user-friendly authentication in heterogeneous enterprise ecosystems. (Abstract 238 words)

Keywords: FIDO2; passkeys; certificate-based authentication; passwordless; biometrics; GDPR; enterprise security

Introduction

The contemporary enterprise landscape confronts a paradox: while authentication mechanisms have evolved rapidly, risk exposure from credential-based attacks—particularly phishing, credential stuffing, and large-scale password leaks—remains persistent. Passwords, historically the dominant user authentication mechanism, suffer from inherent weaknesses: low entropy, reuse across services, susceptibility to social engineering, and mental overhead for users (Adams & Sasse, 1999). Against this backdrop, the FIDO2 suite (WebAuthn and CTAP) and the emerging passkeys paradigm represent a concerted industry effort to replace passwords with cryptographic and device-bound authenticators that resist phishing by design (FIDO Alliance, 2019; FIDO Alliance, 2025). Simultaneously, many enterprises maintain robust investments in certificate-based authentication and Public Key Infrastructure (PKI), which offer strong, well-understood properties for entity binding, device identity, and machine-level trust. There is a pressing need to reconcile these architectures into a coherent identity assurance strategy that preserves phishing resistance, scales across heterogeneous endpoints, and complies with regulatory regimes such as the European Union's GDPR (GDPR, 2016).

This paper addresses that need by proposing and elaborating on a hybrid identity architecture that integrates FIDO2 passwordless mechanisms with certificate-based authentication. The central problem statement is as follows: how can enterprises combine the user-centered phishing resistance and usability advantages of FIDO2/passkeys with the systemic device and machine trust capabilities of certificate-based PKI, while satisfying privacy, usability, and operational governance requirements? Existing literature offers pieces of the answer. Work on biometric advances for mobile devices and behavioral biometrics highlights both the maturation of device-bound identity modalities and their limitations (Das et al., 2018; Stragapede et al., 2022; Malik, 2024). Usability investigations into FIDO2 show strong acceptance and effectiveness but expose misconceptions about storage and recovery that impact deployment decisions (Lyastani et al., 2020; Lassak et al., 2021; Owens et al., 2020). Guidance from the FIDO Alliance and standards bodies provides the technical substrate for passkeys and CTAP flows (FIDO Alliance, 2019; FIDO Alliance, 2023; W3C WebAuthn, 2019). Yet, there is a literature gap in comprehensive, implementable frameworks that operationalize these advancements within enterprise PKI ecosystems and regulatory contexts. This article aims to fill that gap by presenting a detailed, publication-ready architecture, supported by rigorous theoretical elaboration and grounded in the specified references.

The contribution of this work is fourfold. First, it synthesizes technical, usability, and privacy literature to justify the hybrid approach. Second, it defines a methodology for integrating FIDO2 flows with certificate issuance, lifecycle management, and trust anchoring in enterprise PKI. Third, it provides a descriptive analysis of security, usability, and compliance outcomes anticipated from adoption. Fourth, it discusses counter-arguments, limitations, and future research avenues, ensuring a balanced and academically rigorous treatment of the subject matter. Every major claim in this article is linked to the provided references, ensuring traceability and fidelity to existing scholarship and standards.

Methodology

The methodology adopted in this paper is conceptual synthesis combined with methodical architectural design and normative analysis. Given the constraint to use only the provided references, the approach comprises four interlocking activities: literature synthesis, architectural decomposition, procedural orchestration, and evaluative projection. Each activity is described in detail below, explaining the logical steps, underlying assumptions, and the means by which the design aligns with cited sources.

Literature synthesis. The first activity consolidates empirical and standards-based knowledge from the supplied references. Key themes were identified: mobile

biometric technology maturity and privacy implications (Das et al., 2018; Malik, 2024), passive behavioral biometrics for continuous authentication (Stragapede et al., 2022), FIDO2 technical specifics and passkey ecosystem development (FIDO Alliance, 2019; FIDO Alliance, 2023; FIDO Alliance, 2025), GDPR privacy constrains affecting biometric and identity data (GDPR, 2016), usability and misconceptions around FIDO2 (Lyastani et al., 2020; Lassak et al., 2021), and pragmatic enterprise perspectives on certificate-based systems (multiple sources provided in the reference list addressing PKI and certificate lifecycles). Each theme was analyzed for relevance to the hybrid architecture's security, usability, and compliance goals.

Architectural decomposition. Building on the synthesized themes, the architecture was decomposed into canonical components: end-user authenticators (platform and roaming authenticators), credential brokers and passkey managers, enterprise PKI and certificate authorities (CAs), authentication and authorization servers, device identity agents, account recovery and key escrow systems, and privacy controls. The decomposition specifies interfaces, dataflow sequences, and trust boundaries inspired by FIDO2's client-to-authenticator model and standard PKI trust chains (FIDO Alliance, 2019; W3C WebAuthn, 2019). The decomposition pays particular attention to how device-bound biometric matching (Das et al., 2018) and behavioral biometrics (Stragapede et al., 2022) can inform multi-factor decisions without transmitting raw biometric data, consistent with GDPR principles (GDPR, 2016).

Procedural orchestration. For each component identified in the decomposition, procedural steps were articulated to operationalize integration. This includes certificate provisioning tied to a successful FIDO2 attestation, issuance of device or user certificates (for machine identity and mutual TLS) following passkey registration, binding of certificate lifecycles with FIDO2 key lifecycle events (creation, rotation, revocation), and account recovery protocols that avoid weakening phishing resistance. The orchestration explicitly references FIDO2 attestation and CTAP flows to ensure cryptographic authenticity and to utilize attestation statements where enterprise policy requires hardware-backed assurance (FIDO Alliance, 2019; FIDO Alliance, 2025).

Evaluative projection. Finally, the design's anticipated outcomes were projected across security, usability, privacy, and operational dimensions. This evaluative projection is descriptive rather than quantitative, drawing on the cited usability studies (Lyastani et al., 2020; Owens et al., 2020), empirical discussions of biometric misconceptions (Lassak et al., 2021), and GDPR guidance about personal and biometric data handling (GDPR, 2016). Scenarios were constructed to demonstrate how the hybrid system responds to phishing attempts, device compromise, and large-scale credential theft, and to illuminate trade-offs in usability, recovery complexity, and administrative overhead.

Throughout the methodology, two overriding assumptions were maintained to align with the references: (1) device-based biometrics and secure enclave-backed cryptographic keys provide stronger phishing resistance than passwords when correctly implemented and managed (Das et al., 2018; FIDO Alliance, 2019), and (2) enterprise PKI remains essential for device identity, machine trust, and integration with legacy systems, thus justifying a hybrid architecture that does not mandate wholesale replacement of certificates (Bridging Identity Assurance Gaps, 2025; W3C WebAuthn, 2019). Ethical and legal constraints from GDPR were treated as normative boundaries shaping data handling, retention, and consent flows (GDPR, 2016).

Results

This section presents a descriptive analysis of the outcomes of integrating FIDO2 passkeys with certificate-based authentication in enterprise environments. The results are narrative and evaluative, explicating security posture changes, usability effects, privacy implications, and operational impacts the hybrid architecture yields when implemented according to the procedural orchestration laid out in the methodology.

Security posture improvements. Integrating FIDO2 with PKI materially enhances phishing resistance by shifting the authentication model from shared secrets (passwords) to asymmetric key pairs bound to user devices and controlled by platform authenticators (FIDO Alliance, 2019; FIDO Alliance, 2025). The FIDO2 model ensures that credentials cannot be replayed on phishing sites because the origin-bound WebAuthn challenge/response prevents an attacker from

presenting a valid assertion without control of the private key on the correct origin. When FIDO2 attestation is leveraged during registration, enterprises gain hardware-backed proof that the authenticator is a genuine device, which when combined with PKI-bound device certificates, creates a layered trust model: user authentication attested by device-level keys and device identity asserted by certificate chains anchored to corporate CAs (FIDO Alliance, 2019; FIDO Alliance, 2025).

In addition, the hybrid model mitigates risks associated with device loss and server-side credential theft. Because FIDO2 private keys are ideally generated and retained within secure hardware (e.g., TPM, Secure Enclave) and never leave the device, server compromise alone cannot disclose private keys. Certificate-based authentication provides machine identity and mutual TLS capabilities that limit device impersonation even when network-level threats are present. By aligning certificate issuance to FIDO2 attestation events, certificate issuance can be made contingent upon verifiable device integrity, thereby reducing the chance of fraudulent certificate enrollment (FIDO Alliance, 2019; Bridging Identity Assurance Gaps, 2025).

Usability effects. FIDO2 passkeys reduce cognitive load and login friction relative to passwords (Lyastani et al., 2020; FIDO Alliance, 2025). Empirical usability studies show high acceptance of FIDO2 passwordless flows, especially when platform authenticators are used, because users interact with familiar device modalities (e.g., fingerprint, face unlock) rather than remembering complex secrets (Lyastani et al., 2020). However, the literature also underscores critical user misconceptions—particularly about where biometric data and credentials are stored—which can affect trust and adoption if not properly communicated by IT teams (Lassak et al., 2021). The hybrid model must therefore invest in clear user communications and UX design that explains local-only storage of biometric templates and the cryptographic separation between private keys and biometric sensors.

Continuity of access with certificate-based device identity also supports seamless machine-to-machine interactions and background synchronization tasks where userless authentication is required. Certificates provisioned in conjunction with FIDO2 registration can be used for device-to-service authentication, enabling single-sign-on experiences that reduce repeated user prompts while maintaining high assurance for service interactions. Thus, usability is improved across both interactive human access and automated machine interactions.

Privacy and regulatory compliance. The hybrid architecture allows enterprises to adhere to GDPR principles by minimizing biometric data transfer and by employing privacy-preserving attestation and data minimization strategies. The FIDO2 model typically matches biometric templates locally and transmits only cryptographic assertions, which reduces the risk of personal data flows that would trigger special category data concerns (GDPR, 2016; FIDO Alliance, 2018). The architecture must still ensure that attestation metadata and certificate identifiers do not inadvertently become personal data or enable tracking without consent; procedural controls for attestation statement minimization, pseudonymization of identifiers, and explicit user consent for device attestations are therefore integral to compliance (GDPR, 2016; FIDO Alliance, 2018).

Operational impacts and lifecycle considerations. Operationally, coupling FIDO2 events with certificate issuance imposes new dependencies on identity and device management systems. For example, when a user registers a passkey, a certificate issuance workflow can be triggered to provide the device with a short-lived certificate suitable for mutual TLS and V2X machine identity. Certificate lifecycle orchestration must accommodate passkey portability features (e.g., cloud-synced passkeys) and ensure that certificate revocation and key rotation semantics align with passkey revocation to avoid orphaned credentials or unauthorized device access. The literature advises careful handling of key recovery and backup: users' expectations of portability conflict with the security goal of keeping keys hardware-bound (Lassak et al., 2021; Mitra et al., 2023). The proposed hybrid architecture anticipates these trade-offs by recommending enterprise-managed escrow of certificates (not private keys) and by designing recovery flows that revalidate device and user identity via multi-step, out-of-band confirmation procedures tied to PKI revocation and reissuance events.

Comparative reflections. Compared to a pure FIDO2 deployment, the hybrid approach offers additional capabilities for machine identity, centralized policy enforcement via certificate lifecycle control, and better integration with legacy systems that rely on PKI. Compared to certificate-only systems, the hybrid model substantially improves resilience to credential phishing and user-targeted social engineering attacks by removing shared secrets from the primary authentication vector. However, the hybrid architecture does introduce added operational complexity and dependency on orchestration components that must be robustly designed and governed.

Discussion

This discussion explores theoretical implications of the hybrid integration, presents counter-arguments, considers limitations, and identifies future research directions. Each argument is tied to underlying references to maintain evidential integrity.

Theoretical implications for identity assurance. The hybrid model reflects a theoretical shift from reliance on single-layer, monolithic identity proofs to layered, origin-aware, and device-bound authentication. FIDO2's origin-binding model redefines the authentication threat model by ensuring that authorization assertions are cryptographically tied to the requesting origin. When extended with PKI-bound device identity, the enterprise gains a dual-axis assurance: user presence and consent verified by FIDO2; device trust and lifecycle enforcement verified by PKI. This conceptual layering resonates with zero-trust principles by minimizing implicit trust in network location or secret possession and requiring cryptographic proof at each interaction boundary (FIDO Alliance, 2019; Bridging Identity Assurance Gaps, 2025).

Privacy-first authentication. The literature emphasizes the privacy advantages achievable by keeping biometric templates local and using attestation sparingly (FIDO Alliance, 2018; GDPR, 2016). The hybrid architecture amplifies privacy-first design by ensuring that PKI elements do not become covert identifiers. By applying pseudonymization techniques to certificate subjects and by generating per-relying-party keys alongside enterprise certificates, organizations can balance auditability with privacy. This dual-key approach allows for per-service unlinkability while maintaining the enterprise's ability to authenticate and authorize devices at scale.

Counter-arguments and critique. Several counter-arguments warrant careful attention. First, critics may argue that passkey portability and cloud-synced FIDO2 credentials reintroduce centralization and vendor dependence, undermining the security and privacy benefits of local-only hardware keys (Lassak et al., 2021). The hybrid architecture addresses this by differentiating between user-centric passkey portability (which improves usability) and enterprise device identity (which must remain under corporate governance). Enterprises can adopt policies that restrict cloud-synced passkeys for high-assurance roles or require additional attestation for such accounts.

Second, some contend that biometric authentication—especially behavioral biometrics—suffers from insufficient entropy and is vulnerable to spoofing or adversarial examples (Das et al., 2018; Stragapede et al., 2022; Malik, 2024). The literature supports this caution: while mobile biometric sensors have become more sophisticated, no biometric is flawless. Consequently, the hybrid model avoids treating biometrics as standalone secrets; rather, biometrics unlock asymmetric keys (FIDO2), so the security depends primarily on the cryptographic keys rather than on biometric templates alone. Behavioral biometrics are used as an auxiliary signal for continuous authentication rather than the primary authentication factor (Stragapede et al., 2022), thereby reducing their exposure to adversarial manipulation.

Third, operational critics will point to the increased management burden of synchronizing passkey events with certificate issuance and revocation workflows. This concern is valid; integrating two cryptographic ecosystems demands rigorous orchestration. The architecture proposed here mitigates this by recommending short-lived certificates, automated provisioning pipelines, and tight coupling between identity events (e.g., joiners, leavers, role changes) and certificate management processes. Automation reduces human error and scales management but requires robust IAM (Identity and Access Management) integrations.

Limitations. The present work is bounded by the literature it references and by conceptual design rather

than empirical deployment data. Without large-scale field studies or direct measurement of attack incidence post-adoption, the projected benefits remain inferential—albeit grounded in standards, usability studies, and technical analyses. Another limitation is the treatment of edge cases such as jurisdictions with stricter biometric data laws than GDPR or organizations with constrained device inventories; the architecture must be adapted to local legal regimes and resource realities.

Future research directions. Several research trajectories emerge. First, empirical evaluation of hybrid deployments across sectors—measuring phishing incidence, login success rates, recovery times, and administrative overhead—would provide crucial validation. Second, exploring decentralized identity primitives, such as DID (Decentralized Identifiers) and verifiable credentials, in combination with FIDO2 and PKI could offer a path to reduce vendor lock-in and improve user agency. Third, advancing privacy-preserving attestation techniques (e.g., group attestations or selective disclosure) could enhance enterprises' ability to verify device authenticity without wide-scale personal data collection. Finally, in-depth study of behavioral biometrics' robustness and privacy implications is necessary before wide-scale adoption as a continuous authentication signal (Stragapede et al., 2022; Malik, 2024).

Conclusion

Enterprises seeking to eliminate phishing and modernize identity assurance face a strategic choice: adopt pure passwordless paradigms and reengineer legacy systems, or construct hybrid architectures that incrementally incorporate passwordless protections while preserving PKI-based machine identity. The analysis in this article, grounded in the supplied literature, advocates the latter: a deliberate integration of FIDO2 passkeys and certificate-based authentication yields a pragmatic path to phishing-resistant, GDPR-aware, and operationally viable identity assurance.

Key recommendations include: (1) adopt FIDO2 platform authenticators for primary human authentication, ensuring clear user communication about local biometric processing and key storage (Lyastani et al., 2020; Lassak et al., 2021); (2) bind certificate issuance to FIDO2 attestation events to ensure that device certificates are granted only to verified, hardware-backed devices (FIDO Alliance, 2019); (3) design recovery and portability policies that preserve phishing resistance—favoring certificate reissuance and multi-step recovery rather than private key escrow—while accommodating business continuity (Mitra et al., 2023); (4) implement privacy controls aligned with GDPR including data minimization, pseudonymization, and explicit consent for any attestation metadata that could be personal data (GDPR, 2016; FIDO Alliance, 2018); and (5) invest in automation for certificate lifecycle and identity event orchestration to maintain scale without compromising security.

In sum, integrating FIDO2 and certificate-based authentication reconciles the strengths of modern, user-centric phishing resistance with the structural assurances of PKI. While not without operational and conceptual challenges, this hybrid architecture offers a robust blueprint for enterprises committed to secure, usable, and privacy-respecting identity assurance in the evolving cyber threat landscape.

References

1. Das, A.; Galdi, C.; Han, H.; Ramachandra, R.; Dugelay, J.-L.; Dantcheva, A. Recent Advances in Biometric Technology for Mobile Devices. 2018. Available online: https://ieeexplore.ieee.org/document/8698587 (accessed on 26 June 2025).
2. Stragapede, G.; Vera-Rodriguez, R.; Tolosana, R.; Morales, A.; Acien, A.; Le Lan, G. Mobile Behavioral Biometrics for Passive Authentication. Pattern Recognit. Lett. 2022, 157, 35–41.
3. Malik, G. Biometric Authentication-Risks and Advancements in Biometric Security Systems. J. Comput. Sci. Technol. Stud. 2024, 6, 159–180.
4. Badal Bhushan. (2025). Bridging Identity Assurance Gaps: Integrating FIDO2 and Certificate-Based Authentication for Phishing-Resistant, Scalable Enterprise Security. International Journal of Data Science and Machine Learning, 5(02), 9-24. https://doi.org/10.55640/ijdsml-05-02-02
5. GDPR. General Data Protection Regulation—Official Legal Text. 2016. Available online: https://gdpr-info.eu/ (accessed on 9 June 2025).

6. FIDO Alliance. Passkeys. 2025. Available online: https://fidoalliance.org/passkeys/ (accessed on 2 August 2025).
7. FIDO Alliance. Passkeys: Specifications Overview. 2025. Available online: https://fidoalliance.org/specifications-overview/ (accessed on 2 August 2025).
8. FIDO Alliance. Client to Authenticator Protocol (CTAP). 2019. Available online: https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html (accessed on 9 June 2025).
9. FIDO Alliance. Sign in With Passkey. 2023. Available online: https://www.passkeycentral.org/design-guidelines/required-patterns/sign-in-with-a-passkey (accessed on 15 June 2025).
10. Lyastani, S.G.; Schilling, M.; Neumayr, M.; Backes, M.; Bugiel, S. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. 2020. Available online: https://ieeexplore.ieee.org/document/9152694 (accessed on 9 June 2025).
11. FIDO Alliance. FAQ on FIDO Relevance for the GDPR. 2018. Available online: https://fidoalliance.org/wp-content/uploads/FIDO_Alliance_GDPR_FAQ_September2018.pdf (accessed on 15 June 2025).
12. Zhidovich, A.; Lubenko, A.; Vojteshenko, I.; Andrushevich, A. Semantic Approach to Designing Applications with Passwordless Authentication According to the FIDO2 Specification.
13. Adams, A.; Sasse, M.A. Users are not the enemy. Commun. ACM 42(12), 40–46 (1999).
14. FIDO Alliance. FIDO2: WebAuthn & CTAP. Available online: https://fidoalliance.org/fido2/.
15. Parmar, V.; Sanghvi, H.; Patel, R.; Pandya, A. A comprehensive study on passwordless authentication. In: Proceedings 3rd International Conference on Smart Systems and Inventive Technology, Tirunelveli, India, pp. 991–997 (2020).
16. Singh, R.; Jain, Y.; Khawade, S.; Jinde, A.; Zanwar, S. Blockchain-based decentralized passwordless user authentication system: a Survey. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. 5(1), 478–485 (2019).
17. Lassak, L.; Hildebrandt, A.; Golla, M.; Ur, B. It's Stored, Hopefully, on an Encrypted Server: Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn (2021).
18. Owens, K.; Ur, B.; Anise, O. A Framework for Evaluating the Usability and Security of Smartphones as FIDO2 Roaming Authenticators (2020).
19. W3C Web Authentication Working Group. Web Authentication: An API for Accessing Scoped Credentials. W3C Recommendation (2019). Available: https://www.w3.org/TR/webauthn-1/.
20. Farke, F.M.; Lorenz, L.; Schnitzler, T.; Markert, P.; Dürmuth, M. "You still use the password after all"—Exploring FIDO2 Security Keys in a Small Company (2020).
21. Mitra, A.; Ghosh, A.; Sethuraman, S. TUSH-Key: Transferable User Secrets on Hardware Key (2023).