Journal of Information Systems Engineering and Management
2026, 11(1s) e-ISSN:
2468-4376
https://www.jisem-journal.com/

Research Article

Post-Quantum Security Enhancements for WebAuthn and FIDO2 Protocols

Hirenkumar Patel

Mastercard Inc, USA

ARTICLE INFO

Received: 13 Jan 2026

Revised: 16 Jan 2026

ABSTRACT

Advancements in quantum computing create substantial risks for classical cryptographic systems, particularly RSA and Elliptic-Curve Cryptography, that underpin FIDO2 and WebAuthn authentication protocols. Shor's algorithm can compromise these systems by extracting private keys from their public counterparts when sufficiently powerful quantum computers exist. Passwordless authentication has grown increasingly prevalent, with FIDO2 and WebAuthn serving as core trust elements within digital identity architectures. Quantum-enabled attackers present serious challenges to both credential security and attestation validation processes. Organizations must adopt post-quantum cryptographic methods proactively to sustain authentication integrity while maintaining existing trust structures. The harvest-nowdecrypt-later paradigm presents urgent risks where malicious entities intercept and store authentication traffic for future decryption upon quantum computer maturation. FIDO2 credentials embedded within authenticators or bound to user devices maintain long lifespans, often synchronized across cloud ecosystems as passkeys, creating extended vulnerability windows. Post-quantum migration represents both cryptographic enhancement and essential lifecycle management spanning authenticators, browsers, servers, and attestation authorities. This framework proposes a crypto-agile hybrid WebAuthn architecture integrating classical and postquantum algorithms. Embedding ML-DSA for digital signatures and ML-KEM for key encapsulation within WebAuthn registration and authentication flows enables progressive credential rotation without disrupting trust chains. The architecture aligns with CBOR Object Signing and Encryption identifiers and emerging IETF postquantum WebAuthn specifications, ensuring standards compliance.

Keywords: Post-Quantum Cryptography, WebAuthn, FIDO2, Quantum Computing Threats, Cryptographic Agility, ML-DSA, ML-KEM, Passwordless Authentication, Attestation Framework, Hybrid Cryptography

1. Introduction: Quantum Threats to Authentication Systems

Quantum computing advancement has accelerated substantially, exposing critical weaknesses in cryptographic systems protecting global authentication infrastructure. FIDO2 and WebAuthn protocols, widely implemented across platforms and enterprises, rely fundamentally on RSA and Elliptic-Curve Cryptography [1]. Security for these cryptographic approaches depends on mathematical problems that classical computers cannot practically solve. Quantum algorithms eliminate this protective barrier. Shor's algorithm allows quantum machines to perform integer factorization and discrete logarithm operations efficiently, breaking the mathematical foundations that secure authentication credentials.

Organizations need cryptographic upgrades immediately, not after quantum computers become operational threats. Post-quantum methods offer protection against attacks from both current and quantum systems. Shifting authentication to quantum-resistant approaches keeps credentials secure as attacker tools improve. Companies must move fast while avoiding service disruptions, updating security systems, and handling billions of logins daily.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s) e-ISSN:
2468-4376
https://www.jisem-journal.com/ Research Article

1.1 Evolution of Passwordless Authentication Standards

Password authentication creates persistent security and usability challenges across digital services. Users struggle to manage unique passwords for numerous accounts, resulting in reused credentials and predictable patterns that attackers exploit. Fake websites mimicking real services enable phishing campaigns, capturing login details. Data breaches regularly expose millions of passwords despite hashing and salting protections. The FIDO Alliance developed standardized cryptographic authentication to eliminate shared secrets [1]. FIDO Universal Second Factor introduced a hardware token, supplementing passwords through cryptographic challenge-response. This improved security by requiring physical device possession with password knowledge, complicating remote attacks. However, retaining passwords as primary authentication left many vulnerabilities intact.

WebAuthn shifted fundamentally toward passwordless authentication, making cryptographic credentials the primary authentication method [2]. The World Wide Web Consortium established WebAuthn as a browser standard allowing websites to register and verify users through public key methods. Users demonstrate identity through private keys stored in authenticators such as hardware tokens, smartphones, or built-in security components. Biometric sensors enable convenient verification without sending biometric information to servers. The protocol creates strong cryptographic links between credentials and specific websites, blocking phishing attempts and redirecting users to fraudulent sites.

Technology platforms adopted WebAuthn quickly after standardization. Operating systems integrated platform authenticators supporting fingerprint or face recognition for website login. Browser implementations enabled consistent authentication across different browsers and devices. Enterprises embraced the technology, recognizing security gains and cost savings. Banks deployed WebAuthn for transaction approval. Government agencies implemented passwordless authentication for public services.

1.2 Quantum Computing Risks to Classical Cryptography

Quantum computers utilize superposition and entanglement principles to solve problems that conventional computing systems cannot practically address. Traditional bits maintain fixed values of zero or one, whereas quantum bits exist across multiple state combinations concurrently. This allows quantum algorithms to search vast solution spaces efficiently for particular problem types. Shor's algorithm uses these capabilities to factor large integers and compute discrete logarithms in polynomial time—problems requiring exponential time classically [3]. RSA relies on factoring difficulty for large prime products.

The harvest-now-decrypt-later attack model intensifies migration urgency. Adversaries intercept and archive encrypted authentication traffic now, storing it until quantum computers capable of decryption exist. Long-lived credentials prove especially vulnerable. FIDO2 authenticators maintain cryptographic keys for years, synchronized across cloud platforms as passkeys. Retroactive key compromise enables unauthorized account and system access. Attestation certificates and trust chains persist similarly long, creating retroactive attack opportunities. Organizations cannot postpone postquantum migration, awaiting practical quantum cryptanalysis demonstrations. Transitions must happen while classical cryptography remains effective, ensuring uninterrupted protection as adversary capabilities evolve.

Threat Type	Impact on Authentication
Shor's Algorithm	Efficiently breaks RSA and ECC foundations
Harvest-Now-Decrypt-Later	Archives encrypted traffic for future quantum decryption
Key Extraction Attacks	Derives private keys from public key material
Retroactive Compromise	Threatens long-lived credentials and synchronized passkeys

Table 1: Quantum Threats to Authentication Cryptography [3,4]

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s) e-ISSN:
2468-4376
https://www.jisem-journal.com/ **Research Article**

Figure 1: Hybrid WebAuthn Authentication Flow [1], [4]

2. Problem Statement and Motivation

Quantum computing advancement creates immediate security concerns for authentication systems, despite quantum computers remaining years away from practical cryptanalytic capabilities. The harvest-now-decrypt-later threat model presents urgent risks where adversaries intercept and archive encrypted authentication traffic today with intentions to decrypt captured data once quantum computers achieve sufficient computational power [3]. This paradigm particularly threatens FIDO2 credentials because authentication keys embedded within hardware tokens, mobile secure enclaves, and trusted platform modules maintain extended operational lifespans often spanning multiple years before rotation or replacement occurs.

Passwordless authentication deployments increasingly synchronize credentials across cloud-based ecosystems as passkeys, enabling seamless user experiences across multiple devices and platforms. This synchronization extends credential exposure windows because compromising a single synchronized credential potentially affects authentication security across entire device ecosystems rather than isolated authenticator instances.

Traditional cryptographic migration strategies prove inadequate for authentication systems because credential replacement requires coordinated updates across distributed components, including user authenticators, browser implementations, relying party servers, and attestation authority infrastructure [1]. Users cannot simply generate new credentials without comprehensive ecosystem support enabling quantum-resistant algorithm registration and validation throughout the authentication chain. Legacy authenticators lacking post-quantum capability create long-term vulnerabilities as organizations

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

cannot force immediate hardware replacements across large user populations due to cost constraints and operational disruption concerns.

Algorithm	Standardization Status
ML-DSA (FIPS 204)	Lattice-based digital signature scheme
ML-KEM (FIPS 203)	Key encapsulation mechanism for secure sessions
Computational Overhead	Larger keys and signatures than classical ECC
Security Foundation	Module lattice mathematical hardness problems

Table 2: NIST Post-Quantum Algorithm Standards [5,6]

Attestation frameworks present additional migration complexities because trust chains depend on cryptographic signatures from authenticator manufacturers, certificate authorities, and metadata services that must all transition to quantum-resistant algorithms simultaneously [2]. Partial migrations create gaps where quantum-vulnerable components undermine overall system security despite individual component upgrades. The lengthy credential lifecycle typical in enterprise environments, where hardware tokens remain deployed for five to seven years, creates extended vulnerability windows during which archived authentication traffic remains at risk from future quantum cryptanalysis capabilities.

Post-quantum migration represents more than simple algorithm substitution because it requires fundamental rethinking of credential lifecycle management, trust chain validation, and backward compatibility preservation [5]. Organizations must balance security requirements against operational realities, including hardware constraints, user experience considerations, and infrastructure upgrade timelines that prevent immediate wholesale replacement of existing authentication systems. The challenge involves designing transition frameworks enabling progressive adoption of quantumresistant cryptography while maintaining authentication service continuity and interoperability across mixed deployments containing both classical and post-quantum capable components during extended migration periods [6].

3. Post-Quantum Cryptographic Foundations

The National Institute of Standards and Technology completed extensive evaluation processes spanning multiple years to identify quantum-resistant cryptographic algorithms suitable for standardization and widespread deployment across diverse security applications [5]. NIST selected lattice-based cryptographic schemes as primary post-quantum standards due to their strong security foundations, computational efficiency characteristics, and mathematical properties resisting known quantum algorithmic attacks.

Table 3: Hybrid WebAuthn Architecture Components [1,4]

ML-KEM, designated as FIPS 203, delivers key encapsulation functionality enabling secure session key establishment resistant to quantum cryptanalysis through lattice-based mathematical hardness assumptions. These algorithms address fundamental authentication requirements, including credential signing during registration, assertion generation during authentication, and secure channel establishment for sensitive data transmission [7]. Integrating post-quantum primitives into existing authentication frameworks requires careful consideration of performance implications because lattice-based algorithms typically generate larger keys and signatures compared to classical ellipticcurve alternatives.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Designing crypto-agile hybrid WebAuthn frameworks enables integration of both classical and postquantum algorithms within unified authentication flows, ensuring forward-compatible security while maintaining interoperability across legacy infrastructure deployments [4]. Embedding ML-DSA for digital signatures and ML-KEM for key encapsulation within WebAuthn registration and authentication processes supports progressive credential rotation without disrupting established trust chains or requiring immediate wholesale system replacements. This hybrid approach provides quantum resistance for new credentials while preserving backward compatibility with existing authenticators and relying party implementations during extended transition periods.

Framework alignment with updated CBOR Object Signing and Encryption identifiers and emerging IETF post-quantum WebAuthn specifications ensures standardization compliance, enabling interoperable implementations across diverse vendor platforms [1]. Hardware authenticators, including secure elements, trusted platform modules, and mobile secure enclaves, must support postquantum algorithm execution within constrained computational environments while maintaining acceptable performance characteristics for responsive user experiences [5]. Software authenticators implemented within operating system keystores and browser-managed credential stores face fewer resource constraints but require careful implementation, preventing side-channel vulnerabilities and ensuring cryptographic operation integrity.

Post-quantum algorithm integration extends beyond simple cryptographic primitive replacement because it necessitates updates to attestation statement formats, credential public key representations, and authentication assertion structures throughout WebAuthn protocol flows [2]. Migration strategies must account for varying capabilities across authenticator generations, where newer devices support hybrid post-quantum operations while legacy hardware remains limited to classical cryptography during transition periods spanning multiple years.

4. Hybrid WebAuthn Framework Design

Hybrid WebAuthn architectures integrate classical and post-quantum cryptographic primitives within unified credential structures, enabling quantum-resistant authentication while preserving backward compatibility with legacy system components. Protocol mapping modifications address WebAuthn registration flows where authenticators generate dual credential pairs combining traditional ellipticcurve keys with lattice-based post-quantum alternatives during credential creation ceremonies [4]. Registration responses include both classical and post-quantum public keys encoded within attestation objects using extended CBOR structures that maintain compatibility with existing relying party implementations while enabling quantum-resistant validation for upgraded servers.

Authentication assertion flows require corresponding modifications where authenticators generate signatures using both classical and post-quantum private keys, producing hybrid assertion responses containing dual signature values [1]. Relying parties validate both signature types during authentication verification with configurable policies determining whether classical signature validation alone suffices for legacy compatibility or both signatures must validate successfully for quantum-resistant assurance. This flexible validation approach enables progressive migration where organizations gradually enforce post-quantum requirements as authenticator populations upgrade without immediately breaking authentication for users with legacy hardware.

Credential pairing strategies must address synchronization challenges when passkeys replicate across cloud-based ecosystems because hybrid credentials contain significantly larger key material compared to classical alternatives [2]. Cloud synchronization protocols require updates accommodating expanded credential sizes while maintaining encryption protection for credential private keys during transmission and storage across distributed infrastructure. Authenticator identifier schemes must distinguish between classical-only, post-quantum-only, and hybrid credential types, enabling relying parties to request appropriate credential formats based on their current implementation capabilities and security requirements.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s) e-ISSN:
2468-4376
https://www.jisem-journal.com/ Research Article

Authenticator hardware constraints present significant challenges for post-quantum algorithm implementation because secure elements and trusted platform modules operate within strict memory, computational power, and energy consumption budgets [5]. Performance benchmarking reveals MLDSA signature generation requires substantially more computational cycles compared to ECDSA operations, potentially impacting user experience during authentication flows where responsiveness expectations demand sub-second completion times. Hardware token implementations must carefully optimize post-quantum algorithm execution through efficient mathematical library implementations and potential hardware acceleration for lattice-based operations.

Figure 2: Post-Quantum Migration Timeline [2], [5]

5. Implementation and Migration Strategy

Hybrid attestation frameworks extend existing FIDO metadata service architectures to incorporate post-quantum trust anchors, enabling relying parties to validate authenticator attestation statements containing both classical and post-quantum signatures [4]. Attestation certificate chains require updates where manufacturer root certificates include dual signature capabilities, allowing attestation intermediate certificates to inherit quantum-resistant validation properties throughout the trust hierarchy. Metadata statements distributed through FIDO Alliance repositories must specify authenticator post-quantum algorithm support, enabling relying parties to determine device cryptographic capabilities before initiating registration ceremonies requiring quantum-resistant credentials.

Attestation statement formats extend CBOR encoding structures to accommodate additional signature values and expanded public key representations associated with lattice-based cryptography [1]. Privacy-preserving attestation mechanisms, including anonymization and batch attestation techniques, require corresponding updates, ensuring post-quantum implementations maintain privacy properties

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

equivalent to classical attestation approaches. Relying party validation libraries need comprehensive updates supporting hybrid attestation verification, where software development kits provide simplified interfaces abstracting cryptographic complexity from application developers implementing WebAuthn integration.

Figure 3: Attestation Chain Architecture [1], [4]

Credential survivability analysis evaluates authentication service continuity during mixed-fleet deployments where user populations contain combinations of legacy classical-only authenticators, transitional hybrid devices, and future post-quantum-only implementations [5]. Fallback authentication mechanisms require careful design, ensuring quantum-vulnerable fallback paths don't undermine overall security postures while maintaining service availability for users unable to immediately upgrade authenticator hardware. Policy enforcement frameworks enable organizations to define progressive quantum-resistance requirements where initial permissive policies accept classical credentials during the early migration phase, while subsequent stricter policies mandate postquantum validation as authenticator upgrade penetration reaches acceptable thresholds.

Failure mode analysis identifies critical vulnerabilities during partial migration states, including trust chain gaps where quantum-resistant user credentials remain vulnerable due to classical attestation authority signatures [6]. Recovery procedures address scenarios where post-quantum algorithm vulnerabilities emerge, requiring rapid algorithm substitution without complete credential reenrollment across entire user populations. Automated monitoring systems track migration progress, providing visibility into quantum-resistance adoption rates across distributed authenticator fleets, enabling data-driven policy decisions regarding enforcement timeline acceleration or extension based on observed upgrade velocity and operational impact metrics [7].

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Strategy Element	Implementation Approach
Credential Rollover	Progressive rotation across mixed authenticator fleets
Policy Enforcement	Gradual transition from permissive to strict validation
Failure Mode Analysis	Identifies trust chain gaps during partial migration
Automated Monitoring	Tracks quantum-resistance adoption rates across deployments

Table 4: Migration Strategy Elements [2,7]

6. Standardization and Industry Adoption Roadmap

Transitioning passwordless authentication infrastructure toward quantum-resistant cryptography requires coordinated industry efforts spanning standards organizations, browser vendors, authenticator manufacturers, and relying party implementations. The FIDO Alliance continues evolving specifications to accommodate post-quantum algorithms within existing WebAuthn frameworks while maintaining backward compatibility with legacy deployments [1]. Standards bodies, including IETF and W3, actively develop protocol extensions that enable hybrid credential formats combining classical and post-quantum primitives without disrupting current authentication workflows.

CBOR Object Signing and Encryption specifications require updates to accommodate new algorithm identifiers for ML-DSA and ML-KEM within attestation statements and credential public keys. The COSE algorithm registry must incorporate standardized identifiers enabling interoperable implementations across diverse authenticator platforms and relying party ecosystems [4]. These registry modifications enable consistent interpretation of post-quantum credentials across different vendor implementations while preserving the cryptographic agility necessary for future algorithm transitions.

Browser vendors play critical roles in supporting post-quantum WebAuthn through navigator. Credentials API enhancements that handle larger signature sizes and extended key material associated with lattice-based cryptography [2]. Implementation timelines must account for performance optimization requirements, ensuring responsive user experiences despite increased computational overhead from post-quantum algorithms. Collaborative testing initiatives between browser developers and authenticator manufacturers validate protocol implementations while identifying integration challenges requiring specification clarification.

Authenticator manufacturers face hardware constraints when embedding post-quantum algorithms within secure elements, trusted platform modules, and mobile secure enclaves. Industry adoption depends on cost-effective hardware designs supporting both classical and post-quantum operations within existing form factors and power budgets [5]. Reference implementations demonstrating viable post-quantum authenticator architectures accelerate vendor adoption by proving technical feasibility and establishing performance benchmarks.

Relying party readiness requires backend infrastructure upgrades supporting hybrid credential validation and attestation verification, incorporating post-quantum signatures. Migration playbooks must address phased rollout strategies enabling progressive credential rotation across large user populations without service disruptions [3]. Enterprise identity providers need guidance on credential lifecycle management policies that balance security requirements against operational complexity during extended transition periods where mixed classical and post-quantum deployments coexist. Future standardization efforts will incorporate formal verification methodologies validating security properties of hybrid cryptographic constructions combining classical and post-quantum primitives.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Conclusion

Authentication systems require cryptographic transformation to counter emerging quantum computing threats targeting existing security foundations. Frameworks integrating both classical and post-quantum algorithms provide forward-compatible protection while preserving compatibility with established authentication infrastructures. Integrating ML-DSA for digital signatures and ML-KEM for key encapsulation within WebAuthn flows supports progressive credential rotation without disrupting trust chains. Performance evaluation confirms modern post-quantum algorithms maintain computational efficiency suitable for deployment across hardware tokens, mobile secure enclaves, and trusted platform modules.

Future enhancements include formal verification of hybrid cryptographic constructions, ensuring security holds when combining classical and post-quantum primitives. Side-channel resilience analysis of post-quantum algorithms in secure hardware requires continued investigation. Automating quantum-safe credential lifecycle management through dynamic attestation rotation and zero-trust recovery mechanisms remains a priority. Collaboration with browser vendors, authenticator manufacturers, and standards organizations facilitates experimental implementations informing WebAuthn Level 3 specifications and COSE algorithm registry updates. The framework establishes foundations for quantum-resilient digital identity infrastructure, securing authentication against future cryptanalytic capabilities. Post-quantum cryptography emerges as essential infrastructure for passwordless authentication operating under quantum threat models. Addressing these challenges positions authentication systems to withstand increasingly sophisticated adversarial environments as quantum computing capabilities mature and become accessible to threat actors.

References

[1] Hsia-Hung Ou, et al., "Decentralized Identity Authentication Mechanism: Integrating FIDO and Blockchain for Enhanced Security," MDPI, April 2024. https://www.mdpi.com/2076-3417/14/9/3551

[2] Rahul Kondakrindi, "FIDO2: A NEW ERA IN SECURE WEB AUTHENTICATION," International Journal of Computer Engineering and Technology (IJCET), July-August 2024.

https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_15_ISSUE_4/IJCET_15_04_074.pdf

[3] Barinder Pal Singh, M A Augie, Harpreet Singh, and Tuhin Banerjee, "Strengthening Modern IAM Authentication with Quantum Cryptography and Anti-Phishing Techniques," ResearchGate, October 2025. https://www.researchgate.net/publication/396692547_Strengthening_Modern_IAM_Authentica tio n_with_Quantum_Cryptography_and_Anti-Phishing_Techniques

[4] Nina Bindel, Cas Cremers, and Mang Zhao, "FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation," IEEE Symposium on Security and Privacy (SP), ResearchGate, May 2023. https://www.researchgate.net/publication/372551866_FIDO2_CTAP_21_and_WebAuthn_2_Provable_Security_and_Post-Quantum_Instantiation

[5] Manish Kumar, "Post-quantum cryptography Algorithm's standardization and performance analysis," ScienceDirect, August 2022.
https://www.sciencedirect.com/science/article/pii/S2590005622000777

[6] Ritik Bavdekar, et al., "Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations," IEEE Xplore, February 2023. https://ieeexplore.ieee.org/document/10048976

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[7] Ritik Bavdekar et al., "Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations," 2023 International Conference on Information Networking (ICOIN), ResearchGate, January 2023. https://www.researchgate.net/publication/368727573_Post_Quantum_Cryptography_A_Review_of_Techniques_Challenges_and_Standardizations

[8] Taniya Hasija, et al., "Exploring the landscape of post quantum cryptography: a bibliometric analysis of emerging trends and research impact," Springer Open, September 2025. https://journalofbigdata.springeropen.com/articles/10.1186/s40537-025-01269-5

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.