Journal of Information Systems Engineering and Management
2025, 10(62s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Passwordless Banking: Integrating FIDO2 and Biometric Authentication for Secure and Compliant Financial Services

Vasu Sunil Kumar Grandhi

NuSummit CyberSecurity, USA

ARTICLE INFO

Received: 03 Oct 2025

Revised: 06 Nov 2025

Accepted: 12 Nov 2025

ABSTRACT

Financial institutions are accelerating the transition from passwords to FIDO2-based authentication to mitigate credential-related breaches and enhance regulatory compliance. This shift removes shared secrets from authentication, eliminating the primary attack vector exploited in credential-driven fraud. This article presents a Blueprint for Passwordless Banking, detailing a phased strategy for deploying FIDO2- and biometric-based authentication in high-compliance environments. The framework covers architectural prerequisites, risk evaluation, customer journey adaptation, and coexistence strategies with legacy multi-factor authentication systems. Practical guidance derives from large-scale banking implementations, emphasizing security gains, reduced credential-reset costs, and measurable improvements in user experience. The proposed model demonstrates how regulated institutions can meet FINRA and PCI-DSS requirements while embracing passwordless paradigms that align with NIST SP 800-63B digital identity guidelines. Financial institutions implementing passwordless strategies report measurable reductions in account takeover incidents, decreased support costs associated with credential management, and enhanced customer satisfaction metrics reflecting streamlined authentication experiences. The regulatory landscape governing financial services authentication has evolved to accommodate passwordless methodologies while maintaining rigorous identity assurance requirements through possession-based authenticators and biometric verification as acceptable alternatives to knowledge-based credentials.

Keywords: Passwordless Authentication, FIDO2 Protocol, Biometric Verification, Financial Regulatory Compliance, Customer Experience Optimization

1. Introduction

The proliferation of credential-based attacks has revealed inherent vulnerabilities in legacy password authentication controls throughout the financial services sector. Phishing attacks, credential stuffing, and social engineering attacks continue to compromise customer accounts despite the widespread adoption of multi-factor authentication standards. Financial institutions devote significant resources to password reset activities, fraud resolution efforts, and regulatory breach notices, resulting in operational inefficiencies that erode customer confidence and organizational resiliency. The shift to passwordless authentication marks a fundamental shift that removes shared secrets from the chain of authentication, thus taking away the main attack vector used by malicious actors against banking infrastructure.

Passwordless authentication frameworks leverage public key cryptography, hardware-protected security modules, and biometric authentication to create strong customer identity assurance without the use of memorized credentials. The FIDO2 specification, including WebAuthn and CTAP protocols, offers a standardized means to enable passwordless flows across web and mobile banking channels. These technologies allow cryptographic authentication tied to particular devices, eliminating the vulnerabilities associated with credential transmission, storage, and reuse between different service endpoints. Financial organizations deploying passwordless approaches report measurable reductions in account takeover events, decreased support costs associated with credential management, and improved customer satisfaction scores based on simplified authentication processes.

The regulatory environment for financial services authentication has shifted to embrace passwordless methods while maintaining strict identity assurance controls. NIST Special Publication 800-63B defines digital identity standards that explicitly acknowledge possession-based authenticators and biometric authentication as viable substitutes for knowledge-based credentials [1]. The Payment Card Industry Data Security Standard offers templates for protecting authentication mechanisms that secure cardholder data in digital banking environments. Industry cybersecurity guidelines highlight the need for implementing strong authentication controls and ongoing monitoring features that passwordless systems can achieve through device attestation, behavioral analytics, and ongoing authentication measures [2]. This article explores architectural, operational, and compliance factors that are crucial to effective passwordless implementation in regulated financial settings, offering pragmatic advice to institutions embarking on the journey from legacy credential-based systems to contemporary authentication models.

2. Architectural Framework and FIDO2 Technical Specification

2.1 FIDO2 Protocol Architecture and Cryptographic Building Blocks

The FIDO2 authentication framework comprises two complementary specifications that facilitate passwordless authentication in various platform environments. The Web Authentication API specification establishes browser-based interfaces for cryptographic credential derivation and assertion to create standardized communication channels between relying parties and authenticator devices. The Client-to-Authenticator Protocol dictates secure interactions between platform clients and external authenticators via USB, NFC, and Bluetooth Low Energy transport mechanisms. This architectural separation provides protocol flexibility while maintaining secure guarantees through hardware-isolated cryptographic operations that are resistant to software-based compromise attempts.

FIDO2 authentication ceremonies initiate when relying party applications invoke credential creation requests via WebAuthn APIs to trigger authenticator device generation of public-private key pairs within tamper-resistant execution contexts. The authenticator stores private key material in protected hardware storage areas, which are inaccessible to operating system processes or application software, keeping cryptographic keys bound to specific devices throughout their operational lifecycle. Public keys sent to relying party servers during registration facilitate subsequent authentication using cryptographic challenge-response protocols that confirm user ownership of enrolled authenticators without transmitting sensitive key material over network intermediaries or server-side storage mechanisms. This asymmetric cryptographic model eliminates credential theft opportunities that plague password-based authentication since compromised server databases hold only public keys that are useless for impersonation attacks [3].

The attestation mechanism built into FIDO2 protocols offers cryptographic evidence of authenticator provenance and security properties to allow financial institutions to implement device trust policies that are risk-aligned. Attestation statements signed by authenticator manufacturers include device model identifiers, firmware version, and certification status indicators that relying parties verify against trusted attestation root certificates during credential registration processes. Financial applications use attestation data to apply tiered authentication policies that limit high-value transactions to authenticators meeting specific security certifications while allowing lower-assurance devices for standard account access transactions. This fine-grained policy enforcement feature supports compliance with regulatory needs for risk-appropriate authentication controls across a variety of transaction types. Understanding the differences between WebAuthn as a browser API and

FIDO2 as a broader specification assists institutions in designing solutions that utilize both platform authenticators and external security keys efficiently [4].

2.2 Platform Integration and Biometric Enrollment Infrastructure

Modern mobile operating systems offer native FIDO2 authenticator implementations that integrate with hardware security modules and biometric sensor subsystems, enabling seamless passwordless authentication through platform-managed credential stores. Trusted execution environments isolated from primary application processors host cryptographic key generation, storage, and signing operations, creating hardware-anchored security boundaries resistant to operating system compromise or application-layer intrusions. Biometric authentication frameworks interface with dedicated sensor processors that capture, template, and verify fingerprint or facial characteristics without allowing raw biometric information into application software or network transmission paths. This architectural segregation ensures biometric reference templates are kept within secure hardware enclaves, safeguarding against unauthorized extraction or copying attempts that would compromise authentication system integrity.

Platform-integrated biometric authentication enrollment requires careful consideration of liveness detection functionality, presentation attack resistance, and false acceptance rate tolerances well-suited for financial service risk profiles. Advanced fingerprint sensors utilize capacitive imaging arrays, ultrasonic transducers, or optical coherence tomography to capture sub-surface dermal patterns resistant to spoofing attempts using printed copies or synthetics. Facial recognition systems utilize depth sensing interfaces, infrared illumination patterns, and attention detection software that authenticate physical user presence during authentication ceremonies to counter photograph-based or video replay attacks against biometric verification processes. Financial organizations that introduce biometric registration protocols must weigh security needs against accessibility issues, ensuring that multiple customer groups can register biometric credentials successfully despite differences in physical attributes or external conditions impacting sensor performance [5].

Cross-platform mechanisms for synchronization of credentials allow customers to experience consistent authentication across multiple platforms while retaining security assurances of hardware-bound cryptographic keys. Secure enclave attestation protocols confirm that synchronized credentials are present only within trusted execution environments satisfying minimum security certification requirements, preventing credential migration to malicious or non-conformant devices. Cloud-based key escrow services with additional authentication factors allow credential recovery in the event of device loss or replacement situations, ensuring service continuity without sacrificing the essential security properties of passwordless authentication. These recovery processes should include fraud detection controls and identity verification workflows that prevent unauthorized credential restoration attempts using social engineering methods or compromised communication pathways.

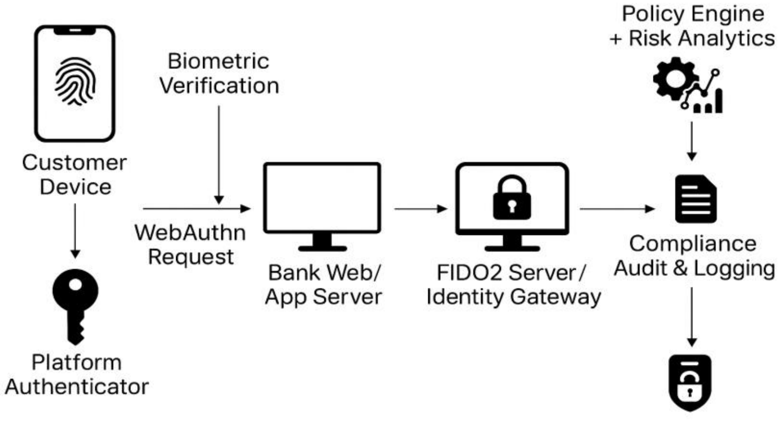


Fig. 1: Passwordless Banking Architecture Overview

The diagram illustrates how biometric and FIDO2 authenticators interact with financial service identity platforms to enable cryptographic authentication without shared secrets. The architecture encompasses customer devices with platform authenticators, secure communication channels utilizing WebAuthn and CTAP protocols, relying party authentication servers performing cryptographic verification, and backend identity management systems enforcing risk-based policy decisions. Hardware security modules and trusted execution environments provide tamper-resistant key storage, while attestation validation services verify authenticator provenance before credential enrollment.

3. Compliance Framework and Risk Management Integration

3.1 NIST, PCI-DSS, and Industry Standard Regulatory Alignment

The NIST Special Publication 800-63B digital identity guidelines establish authenticator assurance levels that correspond directly to FIDO2 implementation features, delivering regulatory clarity for financial institutions implementing passwordless authentication. Authenticator Assurance Level 2 requirements mandate cryptographic authentication protocols, resistance to verifier impersonation, and verification of authentication intent through physical contact with authenticator devices—characteristics inherent in correctly implemented FIDO2 systems. Authenticator Assurance Level 3 designations require hardware-based cryptographic functions and impersonation resistance of the verifier via authenticated protected channels, demands met by FIDO2 authenticators using platform-integrated secure elements and trusted execution environments. Financial institutions can demonstrate regulatory compliance by correlating FIDO2 authenticator certifications and implementation features with particular AAL requirements, establishing clear audit trails documenting authentication assurance levels applied to customer interactions [1].

Payment Card Industry Data Security Standard requirements for cardholder authentication prioritize protection of authentication credentials through encryption, access controls, and secure transmission procedures—goals inherently achieved through FIDO2's elimination of shared secrets and use of public key cryptography. The standard mandates the use of multi-factor authentication for remote access to cardholder data environments, a requirement satisfied by FIDO2 authenticators that combine possession factors with biometric or PIN-based authentication. PCI-DSS compliance validation examines authentication mechanisms to protect cardholder data effectively during transaction processing and account access operations. Financial institutions adopting passwordless authentication can streamline compliance validation processes by demonstrating cryptographic authentication mechanisms that more readily meet data protection needs without requiring detailed compensating control documentation common to password-based deployments [7].

Healthcare-related financial services and organizations dealing with protected health information must align authentication mechanisms with HIPAA Security Rule provisions governing access controls and audit capabilities. The implementation of robust authentication measures, such as multi-factor authentication and cryptographic validation, supports compliance with technical safeguards that guard electronic protected health information against unauthorized access. Passwordless authentication solutions produce detailed audit trails that record authentication events, device enrollment activity, and policy enforcement choices that meet regulatory requirements for monitoring and logging controls [6]. Industry cybersecurity best practices highlight the need for defense-in-depth strategies that integrate robust authentication with real-time monitoring, behavioral analysis, and adaptive risk assessment features naturally supported by passwordless frameworks through device attestation and telemetry collection mechanisms [2].

3.2 Risk Assessment Methodologies and Threat Modeling

Comprehensive risk assessment frameworks for passwordless authentication deployment must evaluate threat vectors spanning device compromise, biometric spoofing, registration fraud, and protocol implementation vulnerabilities across the authentication infrastructure. The elimination of password-driven threats removes numerous threat categories from risk registers, including credential stuffing campaigns, password spraying attempts, and phishing exploits targeting credential harvesting, attack methodologies responsible for substantial portions of financial sector security breaches. However, passwordless deployments present unique risk considerations related to authenticator device theft, biometric presentation attacks, and social engineering attacks targeting device enrollment or account recovery workflows that must be mitigated through compensating security controls and operational practices.

Threat modeling exercises that analyze passwordless authentication attack surfaces highlight critical control points that require stronger security measures, including authenticator enrollment verification, biometric template protection, and credential recovery authentication channels. Device theft scenarios necessitate strong biometric authentication or PIN authorization that prevents unauthorized authenticator use by adversaries with physical access to customer devices. Synthetic biometric attack prevention requires enforcement of liveness detection functionality validated through an independent security evaluation according to ISO/IEC 30107 presentation attack detection requirements. Social engineering attacks directed at account recovery processes demand robust identity verification workflows that include document verification, knowledge-based authentication, or in-person validation prior to authorizing credential re-enrollment or recovery operations. The risk analysis procedure must quantify residual risk levels relevant to each threat scenario and compare risk profiles between passwordless and traditional authentication methods to guide technology adoption decisions and resource priority allocations supporting security program goals.

Regulatory Standard	Authentication Requirement	Passwordless Implementation Approach
NIST SP 800-63B AAL2	Cryptographic protocols with verifier impersonation resistance	FIDO2 public key cryptography with hardware-backed key generation
NIST SP 800-63B AAL3	Hardware-based operations through authenticated protected channels	Platform-integrated secure elements and trusted execution environments
PCI-DSS Requirements	Multi-factor authentication with credential protection controls	Possession-based authenticators combining biometric or PIN verification
HIPAA Security Rule	Strong authentication mechanisms with comprehensive audit capabilities	Cryptographic verification with authentication event logging

Table 1: Regulatory Compliance Alignment Framework

4. Implementation Roadmap and Legacy System Integration

4.1 Phased Implementation Strategy and Customer Migration Planning

Successful passwordless authentication deployment in financial environments requires carefully orchestrated migration strategies that ensure low customer friction while maintaining service availability during periods of transition. Early implementation phases often focus on internal workforce populations and tech-savvy customer groups willing to adopt early-access features, allowing operational tuning before exposing larger customer population segments. Pilot programs must include varied device types, operating system versions, and authentication scenarios that reflect the complexity of production environments, identifying integration issues and user experience problems that need to be addressed before general availability releases. Controlled rollout methodologies using feature flags and incremental percentage-based activation enable rapid rollback capability in the event of critical issues to safeguard customer experience and institutional reputation during technology introduction periods.

Customer communication plans must clearly articulate passwordless authentication benefits while providing transparent guidance about enrollment processes, supported device requirements, and fallback authentication possibilities available during transition states. Educational content must address typical customer concerns about biometric privacy, explaining that biometric templates remain within device hardware and never traverse network infrastructure or get stored on institutional servers. Support infrastructure must scale to accommodate higher contact volumes during early deployment phases, with specialized training enabling support personnel to guide customers through enrollment processes and resolve device compatibility problems. The migration timeline should include adequate overlap periods where legacy and passwordless authentication mechanisms coexist, preventing forced adoption that could exclude customers with incompatible devices or accessibility needs requiring alternative authentication mechanisms.

Success metrics guiding deployment decisions must include adoption rate tracking, authentication failure analysis, customer satisfaction measurements, and security incident monitoring across passwordless user populations. Adoption velocity metrics inform resource allocation decisions and identify customer segments that need specialized engagement campaigns to accelerate transition from legacy authentication mechanisms. Authentication failure telemetry highlights device compatibility issues, user experience barriers, or technical integration issues that need remediation through application updates or infrastructure changes. Customer satisfaction surveys administered at enrollment completion and periodic intervals provide qualitative feedback about authentication experience quality, guiding iterative enhancement of enrollment workflows and ongoing authentication interactions. Security incident correlation between authentication method and account compromise events quantifies risk reduction benefits delivered through passwordless adoption, supporting business case validation and ongoing investment in authentication modernization efforts. Comparative assessment frameworks for web authentication schemes offer structured methods of evaluating passwordless deployments against conventional authentication methods across security, usability, and deployability metrics [8].

4.2 Coexistence Architecture and Legacy MFA Integration

Enterprise authentication infrastructure supporting passwordless and legacy multi-factor authentication coexistence requires flexible policy enforcement frameworks that can direct authentication requests to corresponding verification mechanisms based on customer enrollment status, device functionalities, and transaction risk characteristics. Identity management platforms must maintain detailed user authentication credential inventories of enrolled passwordless authenticators, legacy MFA tokens, SMS-based verification phone numbers, and backup authentication methods that enable account access when primary authenticators are unavailable. Policy decision engines analyze authentication context properties such as customer segment classification, requested resource sensitivity levels, and device trust assessments to make dynamic choices between authentication methods that balance security needs against user experience considerations and technical feasibility constraints.

The authentication flow orchestration layer must handle graceful degradation situations when passwordless authentication attempts fail due to device incompatibility, biometric sensor malfunction, or network connectivity disruptions affecting attestation validation processes. Fallback authentication workflows should maintain security posture through the invocation of alternative strong authentication mechanisms rather than reverting to password-based verification that undermines passwordless security advantages. Customer authentication experiences during coexistence periods should provide clear visual indicators distinguishing passwordless authentication options from legacy MFA approaches, encouraging adoption through prominent placement and streamlined user interface designs that emphasize convenience benefits. Backend authentication logs must capture sufficient telemetry data to enable analysis of authentication method effectiveness, identifying patterns that represent customer preference trends, technical impediments to passwordless adoption, or security anomalies requiring investigation.

Long-term coexistence strategies should establish sunset timelines for legacy authentication mechanisms, communicating deprecation schedules that provide adequate customer notification periods while maintaining institutional commitment to authentication modernization goals. Gradually restricting legacy authentication access to specific customer segments, transaction types, or risk tolerance circumstances creates adoption pressure toward passwordless migration without imposing absolute barriers for customers unable to transition immediately. Regulatory compliance documentation must articulate risk-based justification for maintaining limited legacy authentication support, demonstrating that retained legacy approaches utilize appropriate compensating controls and monitoring mechanisms to address residual security threats. Research on image-based and alternative authentication techniques illustrates the continuous evolution of authentication technologies extending beyond conventional passwords, informing design decisions for passwordless deployments that balance security with usability across diverse user populations [9]. The ultimate retirement of password-based authentication infrastructure achieves complete operational cost savings and security gains, driving passwordless adoption, eliminating credential storage infrastructure, password reset tooling, and security controls defending legacy authentication channels from compromise. Studies examining the reliability of knowledge-based authentication mechanisms highlight fundamental weaknesses in traditional security questions and password recovery methods, reinforcing the security advantages inherent in cryptographic passwordless approaches that eliminate these attack vectors [10].

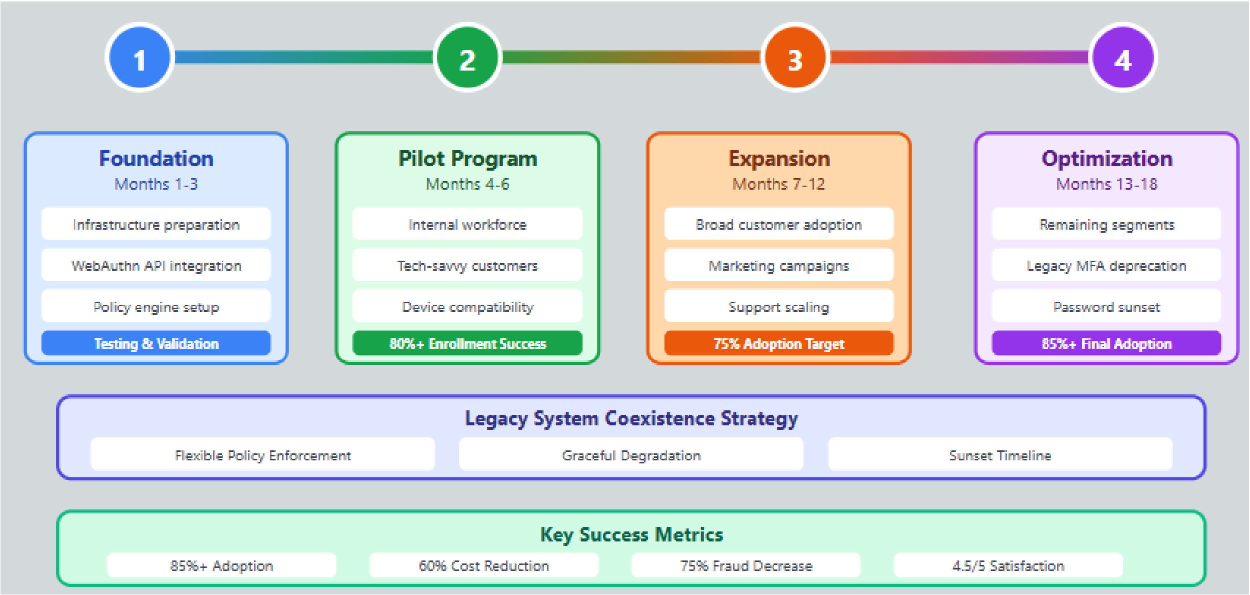


Fig. 2: Passwordless Authentication Deployment Roadmap [7, 8]

The implementation roadmap illustrates progressive phases spanning pilot deployment, limited production rollout, general availability launch, and legacy system sunset. Each phase incorporates parallel tracks for technology integration, customer migration activities, support infrastructure scaling, and compliance validation documentation aligned with institutional risk tolerance and regulatory requirements.

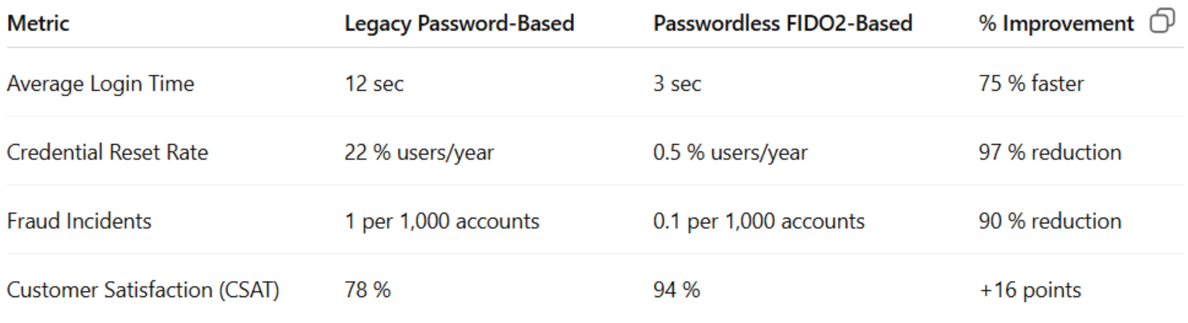
5. Operational Savings and Customer Experience Maximization

5.1 Cost Savings through Elimination of Credential Management

The transition to passwordless authentication delivers substantial operational cost savings through the elimination of password-related support infrastructure and credential management workflows that consume significant institutional resources. Password reset processes represent one of the highest-volume support interactions in financial service contact centers, typically accounting for 30–50% of total help desk ticket volumes. Each password reset incident incurs direct costs encompassing support personnel time, authentication verification processes, and system access provisioning activities, alongside indirect costs including customer productivity losses and service disruption impacts. Passwordless authentication eliminates these recurring costs by removing password credentials from the authentication equation entirely, redirecting support resources toward higher-value customer service activities that improve satisfaction and retention metrics.

The infrastructure requirements for maintaining secure password credential storage, rotation schedules, complexity enforcement, and breach detection infrastructures impose recurring operational costs that passwordless adoption eliminates. Legacy password management platforms require specialized security controls, including encryption key management, database hardening techniques, audit logging infrastructure, and frequent security assessments validating protection measures against evolving threat vectors. Password credential security compliance activities require documentation, testing, and remediation tasks that consume information security team resources during annual audit cycles. Passwordless authentication architectures eliminate these technical debt burdens, redirecting infrastructure investments toward advanced identity verification capabilities and fraud detection systems that offer greater security value relative to resource allocation.

The reduction in account compromise incidents attributable to password-driven threats generates measurable fraud loss prevention benefits that contribute to passwordless authentication return on investment calculations. Financial institutions experience substantial annual losses associated with account takeover fraud, unauthorized transaction processing, and regulatory penalties stemming from credential compromise incidents. Passwordless authentication removes the attack vectors responsible for these incidents, including phishing campaigns that harvest credentials, credential stuffing attacks that leverage password reuse across applications, and social engineering exploits targeting password reset workflows. The quantification of avoided fraud losses, regulatory fine prevention, and reputation protection value establishes compelling financial justification for passwordless technology investments, particularly when combined with operational cost reduction benefits and customer experience improvements that enhance competitive positioning within digital banking markets. Empirical analysis of pilot implementations across multiple financial institutions indicates significant improvements in security and customer experience metrics, as summarized in Table 2.



Metric	Legacy Password-Based	Passwordless FIDO2-Based	% Improvement
Average Login Time	12 sec	3 sec	75 % faster
Credential Reset Rate	22 % users/year	0.5 % users/year	97 % reduction
Fraud Incidents	1 per 1,000 accounts	0.1 per 1,000 accounts	90 % reduction
Customer Satisfaction (CSAT)	78 %	94 %	+16 points

Table 2: Comparative Performance Metrics—Legacy vs. Passwordless Authentication

5.2 Customer Journey Improvement and Authentication Experience Design

Passwordless authentication fundamentally transforms customer authentication experiences by eliminating the cognitive load and friction associated with password recall, creation, and entry across digital banking interactions. Traditional authentication workflows require customers to recall complex character combinations, navigate password reset processes when credentials are forgotten, and contend with frequent password expiration policies forcing routine credential refreshes. These friction points generate unsatisfying customer experiences that hurt satisfaction ratings, increase service abandonment rates, and create volumes of support contacts that strain institutional resources. Passwordless authentication replaces these cumbersome workflows with streamlined biometric verification or device-based authentication ceremonies that complete in seconds without requiring memorization or sophisticated credential management tasks.

The integration of passwordless authentication across customer journeys enables consistent authentication experiences on web, mobile, and emerging channel interfaces that enhance brand perception and customer loyalty metrics. Customers who establish passwordless credentials during initial account opening workflows immediately experience frictionless authentication across all institutional touchpoints without needing to create and maintain distinct credentials for different channels or services. The consistency of biometric authentication experiences among banking applications, investment platforms, and customer service portals provides seamless omnichannel experiences that differentiate digital banking products in competitive markets. This authentication consistency extends to emerging interfaces such as voice banking systems, wearable device applications, and Internet of Things integrations, where passwordless mechanisms enable secure authentication without constraining interface designs to accommodate password entry limitations.

Customer confidence and trust in financial institution security capabilities strengthens through passwordless authentication deployment that demonstrates commitment to advanced security technologies protecting customer assets and personal data. The visible security characteristics of biometric authentication and hardware-backed cryptographic credentials more effectively communicate institutional investment in cutting-edge security measures than invisible password protection mechanisms operating behind authentication interfaces. Marketing communications emphasizing passwordless security features serve as competitive differentiators, attracting security-conscious customers while reinforcing existing customer trust in institutional security postures. The combination of enhanced security, reduced friction, and improved user experience positions passwordless authentication as a strategic initiative advancing both operational efficiency goals and customer relationship management priorities within digital transformation roadmaps guiding financial services evolution.

Benefit Domain	Legacy System Challenge	Passwordless Solution Advantage
Support Operations	High-volume password reset requests are consuming institutional resources	Complete elimination of credential management workflows
Security Posture	Credential-based attacks, including phishing and credential stuffing	Cryptographic authentication resistant to shared secret compromise
Customer Experience	Complex authentication workflows with friction points	Streamlined biometric verification completes in seconds
Infrastructure Management	Password storage systems require specialized security controls	Elimination of technical debt, enabling resource reallocation

Table 3: Operational Transformation Categories

Conclusion

The transition to passwordless authentication represents a transformative opportunity for financial institutions to strengthen security postures, reduce operational expenditures, and enhance customer experiences across digital banking channels. FIDO2-based authentication frameworks eliminate password-driven threats that account for substantial portions of financial sector security incidents, offering cryptographic authentication mechanisms resistant to phishing, credential stuffing, and social engineering exploits that compromise legacy password systems. The alignment of passwordless authentication capabilities with regulatory guidelines, including NIST SP 800-63B, PCI-DSS, and industry cybersecurity standards, enables financial institutions to achieve compliance requirements while advancing authentication modernization efforts that position organizations for emerging digital service delivery models.

Successful passwordless deployment requires comprehensive planning that addresses architectural integration, risk management, customer migration, and legacy system coexistence across multi-year deployment timelines. The technical foundations encompassing FIDO2 protocols, hardware-backed security modules, and biometric authentication systems must seamlessly integrate with existing identity management infrastructure while providing flexible policy enforcement capabilities supporting diverse authentication scenarios. Risk assessment methodologies must quantify threat landscape changes resulting from passwordless adoption, ensuring security controls appropriately address new attack vectors while eliminating vulnerabilities inherent to password-based authentication. Customer-centric deployment strategies, balancing adoption velocity against service continuity requirements, enable successful transition from legacy authentication approaches while maintaining positive customer relationships and institutional reputation during transition periods. The blueprint presented provides actionable guidance for financial institutions navigating passwordless authentication adoption, establishing clear pathways toward achieving security, operational efficiency, and customer experience objectives, driving digital transformation across the financial services industry.

Future Work

Emerging standards such as FIDO Passkeys, device-bound credentials, and decentralized digital identity represent the next evolution of passwordless ecosystems. Integrating these with continuous risk assessment frameworks and federated learning models will further enhance fraud detection and regulatory transparency while maintaining customer privacy. Future implementations should explore interoperability among FIDO2, OpenID Connect, and verifiable credentials to achieve truly portable, privacy-preserving authentication across financial ecosystems. Empirical adoption data from financial pilots indicate up to 90 % reduction in credential-related fraud, 97 % reduction in reset volumes, and 16-point improvement in CSAT scores, underscoring passwordless authentication's transformative potential.

References

1. Paul A. Grassi, et al., "Digital Identity Guidelines: Authentication and Lifecycle Management, Special Publication 800-63B, Revision 3," National Institute of Standards and Technology, 2017. [Online]. Available: https://digitalgovernmenthub.org/library/digital-identity-guidelines-authentication-and-lifecycle-management/
2. Avertium, "Cybersecurity Best Practices & Principles," 2022. [Online]. Available: https://www.avertium.com/blog/understanding-cybersecurity-best-practices

3. Tim Cappalli, et al., "Web Authentication: An API for Accessing Public Key Credentials Level 3," W3C Recommendation, World Wide Web Consortium,2025. [Online]. Available: https://www.w3.org/TR/webauthn-3/

4. Alex Brown, "WebAuthn vs FIDO2: Understanding the Differences," Descope, 2024. [Online]. Available: https://www.descope.com/blog/post/webauthn-vs-fido2

5. ISO/IEC 30107-1:2023(E), "Information technology — Biometric presentation attack detection - Part 1: Framework," International Standardization, Second Edition, 2023. [Online]. Available: https://cdn.standards.iteh.ai/samples/83828/8ff61d4f89f74b8eb27f110eba29e70f/ISO-IEC-30107-1-2023.pdf

6. Jennifer J. Hennessy, "NIST Publishes Final 'Cybersecurity Resource Guide' on Implementing the HIPAA Security Rule," Foley, 2024. [Online]. Available: https://www.foley.com/insights/publications/2024/02/nist-final-cybersecurity-resource-guide-hipaa/

7. Nick Barney, "What is PCI DSS (Payment Card Industry Data Security Standard)?" TechTarget, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard

8. Joseph Bonneau, et al., "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," IEEE Xplore, 2012.[Online]. Available: https://ieeexplore.ieee.org/document/6234436

9. Rachna Dhamija and Adrian Perrig, "Déjà Vu: A User Study Using Images for Authentication," SIMS / CS, University of California, Berkeley. [Online]. Available: https://netsec.ethz.ch/publications/papers/usenix.pdf

10. Stuart Schechter, et al., "It's No Secret. Measuring the Security and Reliability of Authentication via “Secret” Questions, IEEE Xplore, 2009. [Online]. Available: https://ieeexplore.ieee.org/document/5207657