Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 13, Issue. 4, April 2024, pg.103 – 106

Passwordless Login in the Financial Domain: A Practical Architecture and Industry Best Practices

Ajmal Ali Kannu

Chicago, IL, USA
ajmal004@gmail.com

DOI: https://doi.org/10.47760/ijcsmc.2024.v13i04.011

Abstract: Passwordless authentication is increasingly adopted in financial services to mitigate account takeover, credential phishing, and to enhance user experience. This article presents a pragmatic architecture for financial institutions—combining device-bound public-key credentials (FIDO2/WebAuthn), adaptive risk-based controls, and secure fallback and recovery flows. It further synthesizes industry-wide best practices for reducing account takeover fraud, including telemetry-driven anomaly detection, account behaviour analytics, and credential hygiene. Operational considerations such as enrollment, device lifecycle management, and regulatory compliance are discussed. The solution aims both to reduce fraud losses and to streamline authentication flows for large-scale financial user bases.

Keywords: passwordless authentication, financial services, WebAuthn, account takeover, fraud prevention, adaptive authentication

Introduction

Passwords remain a significant vulnerability within the financial services sector. Credential stuffing, phishing, reuse, and weak recovery flows allow a high proportion of account takeovers. Passwordless authentication, based on device-bound cryptographic credentials and strong authenticators, promises to eliminate shared secrets and reduce threat exposure. Financial institutions must maintain accessibility, compliance, and user convenience.

Background and Motivation

The FIDO2 and WebAuthn standards provide an asymmetric-key framework for phishing-resistant authentication. Regulatory bodies, such as NIST (SP 800-63), recommend phishing-resistant authenticators. Financial services benefit strongly from such frameworks due to the high value of transactions, stringent compliance, and demand for seamless customer experience.

System Design

The architecture includes a client-side authenticator layer, an authentication server with key store, and a risk and policy engine. Clients generate key pairs during enrollment and securely store private keys. The backend validates attestation and stores metadata. The risk engine evaluates telemetry and enforces adaptive policies.

Enrollment Flow

1. Verify user identity through strong existing methods.
2. Issue WebAuthn registration challenge; client returns attestation.
3. Validate attestation and store public key with metadata.

Authentication Flow

1. Server issues challenge.
2. Client signs challenge; server verifies signature.
3. Risk engine evaluates context and determines allow/step-up/block.

Fallback and Device Recovery

• Enroll multiple authenticators (primary + backup).
Provide offline one-time recovery codes.
Use in-branch or notarized verification for high-value recovery.
Log all recovery flows and maintain device revocation lists.

Industry-Wide Best Practices

Telemetry and Behavioural Analytics: Gather session telemetry, device fingerprinting, and geolocation data to detect anomalies.
Credential Hygiene and Threat Intelligence: Check for credentials in breach datasets. Subscribe to phishing and credential-stuffing intelligence feeds.

Multi-Factor and Step-Up Authentication: Adopt adaptive step-up mechanisms for high-value operations using biometrics, push confirmation, or device posture checks.
User-Centric Recovery Design: Limit recovery via email/Text alone; include device proof or ID verification.
Audit and Compliance: Maintain audit trails aligned with KYC and fraud-monitoring regulations.
Phased Deployment: Pilot early adopters, measure adoption, and plan password deprecation.
Device Lifecycle Management: Handle device de-registration robustly and remove lost-device credentials.
Continuous Threat-Model Review: Red-team authentication systems and update attestation trust stores regularly.

Implementation and Findings

Initial testing demonstrated smooth interoperability between device-bound authenticators and institutional security controls. The system successfully supported multiple user devices, handled attestation verification, and logged all authentication events in compliance with financial audit requirements.
Usability testing indicated that passwordless login provided a noticeably smoother experience for users once enrolled, with strong acceptance among participants familiar with biometric or device-based authentication. Early-stage deployment efforts highlighted operational areas requiring special attention—particularly user onboarding, recovery design, and device lifecycle management.
The findings affirm that passwordless authentication can be implemented without major architectural disruption to existing systems, provided sufficient planning, identity proofing controls, and phased rollout strategies are adopted. Further empirical validation in production-scale environments would provide richer insights into adoption rates, fraud mitigation impact, and customer satisfaction.

Security and Usability Trade-Off

The architecture is highly phishing-resistant, as private keys never leave devices. However, lost or compromised devices remain residual risks. Ensuring backup authenticators and effective user education minimizes these issues.

Conclusion

Passwordless authentication combined with adaptive risk and secure fallback provides a robust pathway for financial institutions to reduce fraud and enhance user experience. Future work will focus on longitudinal adoption metrics and cross-institutional federation of authenticators.

References

[1]. FIDO Alliance. FIDO2 and WebAuthn Specifications.
[2]. NIST SP 800-63B -Digital Identity Guidelines: Authentication and Lifecycle Management, 2023.
[3]. Authentication - OWASP Cheat Sheet Series.
[4]. Campbell M. Putting the Passe Into Passwords: How Passwordless Technologies Are Reshaping Digital Identity. Computer. 2020; 53(8):89–93.
[5]. Progonov D, Cherniakova V, Kolesnichenko P, Oliynyk A. Behavior-Based User Authentication on Mobile Devices in Various Usage Contexts. EURASIP Journal on Information Security.2022;2022(1):6
[6]. Mastercard Security Research (2022). Fighting Account Takeover Fraud Through Strong Authentication.
[7]. Bhargav, A., & Liu, Y. (2021). Passwordless Authentication in Cloud-Centric Enterprise Environments: A Case Study and Comparative Analysis. Journal of Information Security and Applications, 59, 102834
[8]. Tunde Oduguwa. A Review of Password-less User Authentication Schemes

