ZKBioVault: A Privacy-Preserving Biometric Authentication Framework for Fraud-Resilient Financial Identity Management

Izza Sohail Khan, Faisal Iradat
School of Mathematics and Computer Science, Institute of Business Administration (IBA), Karachi, Pakistan

Correspondence to: Izza Sohail Khan i.sohail.28996@khi.iba.edu.pk

1. Abstract

In the current times, biometric authentication has become the backbone of financial identity. From governing mobile banking access to digital onboarding and high-value payment authorization at scale, the integrity of these systems carries direct regulatory weight. GDPR Article 9 classifies biometric data as a special category demanding maximum protection, PSD2 mandates Strong Customer Authentication for transactions, and the EU AI Act introduces binding controls in biometric systems entering force in 2025-2026. However, at the same time, generative AI as made high-fidelity synthetic biometrics like deepfakes, replay attacks, printed artefacts, trivially accessible to adversaries, fundamentally shifting the attack surface [4].

Existing defences typically address either template protection or liveness verification, but rarely both in an integrated manner. Cryptographic approaches such as cancellable biometrics and fuzzy vaults secure the stored templates under the assumption that the presented biometric input given is authentic. Conversely, liveness detection mechanisms aim to filter synthetic or replayed inputs but operate independently of the cryptographic protection layer [4]. This separation creates an exploitable architectural gap. If liveness checks are bypassed, the template repository remains vulnerable; if templates are cryptographically protected, the system still lacks safeguards against synthetic inputs that successfully bypass liveness detection. To date, no framework systematically co-designs these two layers or integrates them within a unified compliance architecture aligned with ISO/IEC 24745, GDPR, and PSD2 requirements.

This paper introduces ZKBioVault, a novel methodology designed to close this architectural seam while simultaneously satisfying all applicable regulatory obligations. The design is structured around three core requirements. Firstly, no biometric data or derived secret ever leaves the user's device. Secondly, the server verifies identity without receiving, processing, or storing any biometric information. And lastly, the three ISO/IEC 24745 privacy properties which are irreversibility, unlinkability, and renewability, are guaranteed by architectural design rather than assumed through policy or post hoc safeguards.

ZKBioVault operates in two phases. During enrolment, an on-device deep neural network performs hierarchical liveness verification. Fast adapting layers detect frame-level anomalies, while slower, and more stable layers track evolving deepfake signatures without requiring centralized model updates. Only inputs that successfully pass liveness checks proceed further. A user-specific cancellable transformation encodes the extracted features in a non-invertible protected template, which is then bound to a cryptographic secret through a fuzzy vault construction using chaff data. This enables approximate matching while concealing genuine biometric features. Crucially, only a commitment hash and minimal metadata is transmitted to the server, never the protected template or the vault itself. During authentication, the device reconstructs the vault locally and generates a zero-knowledge proof (ZKP) attesting to the possession of the biometric derived key [1,3]. The server verifies this proof without ever receiving or accessing biometric information. Figure 1 shows the comprehensive flow within the unique systematic approach.

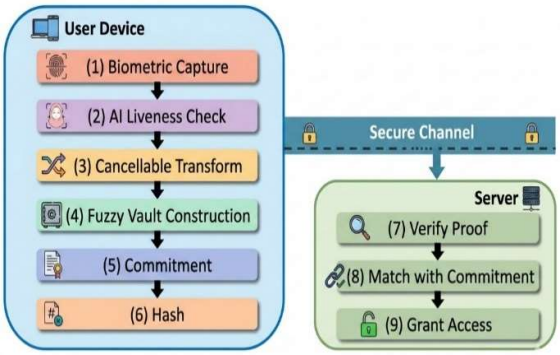

Figure1: Flow from user to server once the user is enrolled

Scenario-driven analysis within a retail banking deployment context yields three principal findings. First and foremost, the methodology struc-

turally satisfies all ISO/IEC 24745 privacy properties alongside two extended properties addressing AI-era threat models through architectural guarantees rather than policy assumptions as stated in Table 1. Secondly, by eliminating server-side biometric storage, the system removes GDPR Article 9 breach liability at the infrastructure layer there is no centrally stored biometric data to compromise. Thirdly, ZKP-based authentication satisfies PSD2 Strong Customer Authentication (SCA) requirements by cryptographically binding inherence and possession factors within a single proof [1,3], while exclusive on-device biometric processing positions the system to qualify for exemption from high-risk biometric identification classification under EU AI Act.

For financial institutions, ZKBioVault reduces three categories of risk in a single architecture: security risk through liveness-to-template seam, legal risk through compliance with GDPR, PSD2, and EU AI act, along with operational risk through instant biometric revocation which replaces costly re-enrolment which is analogous to reissuing a card number without changing the account. This removes the need for costly full re-enrolment while preserving system integrity. For researchers, the proposed methodology highlights a broader design principle with significant implications: liveness verification, template protection, and proof-based authentication are not modular or independent components [3]. Evaluating them in isolation obscures systematic vulnerabilities that only emerge at their intersections. For policy makers, the architecture demonstrates that ISO/IEC 24745 compliance and the EU AI Act's on-device processing exemption are not competing objectives. When privacy-by design is embedded from inception, these regulatory requirements become mutually reinforcing, illustrating that robust security engineering and data protection compliance can be achieved concurrently rather than through trade-offs.

Table 1: Properties and their importance

ISO/IEC 24745 Property	How ZKBioVault Achieves It	Why It Matters in Finance
Irreversibility	Non-invertible cancellable transformation using a user-specific random parameter	Original biometrics cannot be reconstructed even after a server breach
Unlinkability	Fresh randomised vault + per-session commitments across all authentications	Blocks cross-platform identity correlation; satisfies GDPR Art. 9
Renewability	Transform parameter replaceable on demand — no re-enrolment needed	Compromised identities revoked and reissued instantly
Anti-Spoofing	On-device hierarchical AI liveness filters deepfakes and replay attacks before cryptographic processing	Closes the liveness-to-template seam; meets PSD2 SCA inherence factor
Non-Disclosure	ZKP proves key possession without transmitting the key, template, or vault	Server receives proof only — qualifies for EU AI Act on-device exemption

References

[1] Mao, X., Zhou, X., Zhao, X., & Chen, Y. A ZKP-based anonymous biometric authentication scheme for the E-health systems. PLoS ONE, 20(6), e0324289, 2025.
[2] Hamm, D. et al. Always Authenticated, Never Exposed: Continuous Authentication via Zero-Knowledge Proofs. Lecture Notes in Computer Science, Springer, pp. 18–34, 2025.
[3] Rezaei, M. et al. Addressing deepfake issue in selfie-banking through camera-based authentication. https://arxiv.org/abs/2508.19714, 2025. Accessed: February 28, 2026.