10.48047/jocaaa.2026.35.06.20

The Sentinel Protocol: A High-Throughput, Privacy-Preserving Framework for Multi-Jurisdictional KYC Compliance

Sanjay Kumar Mishra†

†Independent Researcher, USA, sanjay.amu28@gmail.com

***Abstract*—Anti-money-laundering (AML) and know-your-customer (KYC) frameworks require institutions to verify identity, screen against sanctions lists, and retain auditable evidence of compliance. Prevailing implementations centralize personally identifiable information (PII), creating high-value breach targets and a compliance paradox: institutions must verify identity while minimizing data exposure under privacy regimes such as GDPR. This paper proposes the Sentinel Protocol, a privacy-preserving compliance framework for high-throughput, multi-jurisdictional financial systems. Sentinel combines zero-knowledge proofs, compact sanctions-list commitments, threshold-decryption escrow, and kernel-adjacent fast-path verification to decouple compliance verification from raw PII exchange. We evaluate Sentinel in a controlled, production-inspired simulation against a user-space baseline across latency, tail behavior, sanctions-list growth, and threshold recovery. In simulation, Sentinel reached a p99.9 verification latency of about 101 µs versus about 1069 µs for the baseline, a 10.5x p99.9 speedup, and held verifier latency stable as the sanctions registry grew from one thousand to one million entries. These are simulation results from a modeled fast path, not measurements from a production zk-SNARK deployment; replacing the modeled capsule with real proofs and a full AF_XDP implementation is left to future work.**

***Index Terms*—zero-knowledge proofs, AF_XDP, distributed systems, fintech, regulatory compliance, threshold cryptography, KYC, AML, sanctions screening, tail latency**

I. INTRODUCTION

The global financial system faces a structural compliance paradox. AML and KYC regimes require institutions to verify identity, screen customers, and preserve auditable evidence, yet the operational model still depends on collecting, duplicating, and retaining PII. This concentration creates high-value breach targets: in 2024 the Identity Theft Resource Center reported 3,158 publicly tracked U.S. data compromises and more than 1.35 billion victim notices [1].

At the same time, performance requirements are rising. FinCEN has emphasized effective, risk-based AML/CFT programs [2], and the EU's AMLA assumed AML/CFT mandates on January 1, 2026 [4]. Payment networks are moving toward richer ISO 20022 messaging, real-time screening, and near-instant settlement [8], [9]. Compliance checks must become more precise and auditable while also becoming faster and less dependent on raw PII.

This paper introduces the Sentinel Protocol, which decouples identity verification from identity disclosure. Sentinel combines zero-knowledge proofs, compact sanctions-list commitments, threshold-decryption escrow, and kernel-adjacent fast-path verification, so a customer can prove satisfaction of jurisdictional KYC predicates without revealing the underlying PII while institutions retain an auditable path for lawful unmasking. The central contribution is the design and simulation of a high-throughput architecture for distributed financial messaging. The remainder of this paper is organized as follows. Section II reviews related work. Section III presents the architecture, Section IV the implementation, Section V the simulation results, and Sections VI and VII the regulatory significance and conclusions.

II. RELATED WORK

Prior work on privacy-preserving identity shows that zero-knowledge proofs and anonymous credentials enable selective disclosure of attributes without revealing the underlying PII. Camenisch–Lysyanskaya-style anonymous credentials let users prove possession of certified attributes while preserving unlinkability [10]. More recent ZKP-KYC frameworks apply zk-SNARKs, Merkle commitments, and off-chain issuers to financial compliance, proving attributes such as age, residency, or prior verification status [11], [12].

Two gaps remain for regulated high-throughput systems. First, many prototypes optimize correctness and privacy rather than latency under payment-network workloads; user-space verification and proof-processing jitter create tail-latency behavior that is hard to reconcile with instant payments. We therefore evaluate p99.9 latency and burst behavior, not only the mean. Second, most designs do not resolve the lawful-access problem: pure non-disclosure can satisfy privacy but lacks a controlled recovery mechanism, while centralized escrow recreates the honeypot risk. Sentinel integrates threshold-decryption escrow requiring multi-party authorization, treating privacy-preserving compliance as a systems problem rather than only a cryptographic one.

III. THE SENTINEL ARCHITECTURE

Sentinel represents compliance as a cryptographic statement rather than an exchange of raw PII. A user proves they satisfy the relevant regulatory predicates, and the verifying institution receives only a proof, public policy commitments, and audit metadata. The protocol has three components: a zero-knowledge constraint model, a threshold-decryption escrow layer, and a kernel-adjacent fast-path verifier. Figure 1 shows how they connect.

10.48047/jocaaa.2026.35.06.20

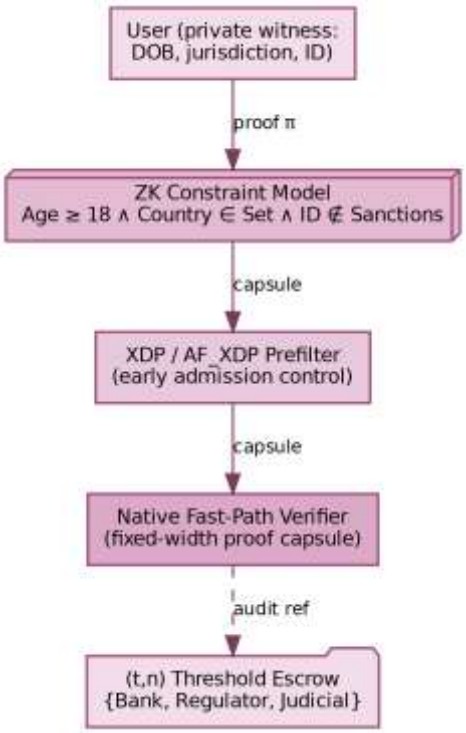

Fig. 1. Sentinel components: a ZK constraint model produces a proof that is admitted by an XDP/AF_XDP prefilter and checked by a native fast-path verifier, with a (t,n) threshold escrow governing lawful recovery.

A. The Constraint Model

Sentinel defines a KYC circuit, expressed in Circom in the prototype, that evaluates private user attributes against public regulatory constraints. It models three predicates: age verification (date of birth satisfies a minimum-age rule), jurisdictional residency (the user's jurisdiction belongs to an approved allow-list), and sanctions screening (non-membership in a sanctions registry represented by a compact Merkle root). The private witness holds the user's attributes; the public inputs hold only policy-level commitments. Formally, for private witness w and public statement x, the proof establishes that age(w) ≥ 18, country(w) is in the jurisdiction set of x, and the identity of w is not in the sanctions root of x, all without revealing w.

B. Threshold-Decryption Escrow

Regulated systems must still support lawful identity recovery. During enrollment, the user's identity is encrypted and the decryption authority is split across n independent stakeholders using a (t,n) threshold scheme [14]. No single party can unmask a user; recovery requires at least t valid shares. The prototype uses a 2-of-3 model with shares held by a bank, a regulator, and an independent judicial auditor. This provides conditional recoverability: privacy holds during ordinary flows, while identity can be recovered under valid legal process when the threshold is met. Requests presenting fewer than t shares are rejected.

C. Hybrid Verification Shard

The verifier is split into two stages for high-throughput environments. A lightweight kernel-adjacent prefilter validates packet structure, proof-capsule formatting, and routing metadata near the network boundary. A native fast-path verifier then processes fixed-width proof capsules using preloaded verification parameters. The design intentionally does not perform full zk-SNARK pairing verification inside eBPF; it uses eBPF/XDP-style placement for early admission control and routes well-formed capsules to a native verifier, which suits real-time messaging where p99 and p99.9 latency matter more than the average.

IV. IMPLEMENTATION AND OPTIMIZATION

The core systems contribution is the kernel-adjacent fast-path model, which separates packet admission, capsule extraction, and verification into distinct stages. An XDP-style prefilter rejects malformed or incomplete capsule requests as early as possible, validating capsule length, routing metadata, and admission rules rather than performing cryptographic verification, consistent with the practical role of eBPF/XDP in high-performance networking [16], [17].

After prefiltering, fixed-width capsules are forwarded to a native verifier implemented in C that processes memory-aligned records in batches. The benchmark compares this native path against a user-space baseline that performs JSON parsing, transcript reconstruction, and tag validation. In a production Linux deployment the fast path can be extended with AF_XDP sockets, which redirect ingress frames into user-space memory rings with reduced copying; Sentinel's fixed-width capsules are designed to align with this model. The reported results measure the native capsule verifier plus a modeled handoff budget; a full AF_XDP implementation is left as future systems work.

V. SIMULATION RESULTS

We evaluate Sentinel in a controlled, production-inspired simulation against a user-space JSON/HMAC baseline, measuring verification latency, p99.9 tail behavior, burst scalability, sanctions-list growth, and threshold-escrow rejection. All numbers below are simulation outputs, not production measurements.

A. Latency and Tail Behavior

Table I summarizes the latency comparison. The fast path reduces both average- and tail-case verification cost, and it narrows the p99.9 tail spread from about 250 µs to about 17 µs, a 14.7x reduction in jitter. In bursty financial messaging, this narrower tail implies more predictable behavior under load.

TABLE I
VERIFICATION LATENCY: BASELINE VS. SENTINEL

Metric	Baseline	Sentinel
Mean latency	839.01 µs	84.82 µs
p99 latency	1013.22 µs	100.45 µs
p99.9 latency	1069.22 µs	101.45 µs
p99.9 speedup	—	10.54x

10.48047/jocaaa.2026.35.06.20

B. Scalability Under Sanctions Pressure

Table II shows fast-path latency as the sanctions registry grows from one thousand to one million entries. Latency stays effectively flat (a p99.9 stability ratio of 1.0047x), because the registry is represented as a compact Merkle root and the verifier-facing capsule remains fixed-size. In a full deployment, list-update and proof-construction costs may scale with the tree, but the verifier path does not.

TABLE II
FAST-PATH LATENCY VS. SANCTIONS CARDINALITY

Sanctions Entries	p99.9 Fast-Path Latency
1,000	100.21 µs
10,000	100.18 µs
100,000	100.37 µs
1,000,000	100.65 µs

C. Throughput and Governance

Under the modeled fast path Sentinel reached an estimated 106,350 transactions per second. The threshold-escrow simulation rejected unauthorized one-share recovery attempts at a 100% rate, while authorized 2-of-3 recovery completed in sub-millisecond time (p99 ≈ 0.010 ms, p99.9 ≈ 0.014 ms). These results support the claim that privacy-preserving KYC can act as a low-latency primitive while preserving lawful-access governance.

VI. THREAT MODEL

Sentinel's security rests on stated assumptions, so it is worth naming the adversaries it does and does not stop. Table III lists the principal threats. The design's central move — proving predicates without disclosing PII — removes the breach honeypot that motivates much identity theft, but it shifts trust onto the proving system and the escrow stakeholders, which the threat model must account for.

TABLE III
THREAT MODEL AND MITIGATIONS

Threat	Mitigation	Residual
PII data breach	No raw PII retained; proofs only	Minimal
Unlawful unmasking	(t,n) threshold escrow	Needs t colluders
Escrow collusion	Cross-institution share split	If t parties collude
Proof replay	Nonce + policy commitment	Low
Verifier DoS	XDP prefilter drops malformed	Volumetric flood
Stale sanctions root	Signed, versioned Merkle root	Update latency

Two residual risks deserve emphasis. Threshold escrow converts unlawful unmasking from a single-point failure into a collusion problem: it is secure only while fewer than t of the n stakeholders collude, so the choice of t, n, and which institutions hold shares is a governance decision, not merely a cryptographic one. And the verifier prefilter stops malformed-capsule floods cheaply but does not by itself defeat a volumetric network flood, which remains a standard network-DoS concern handled upstream.

VII. WORKED EXAMPLE: A CROSS-BORDER KYC CHECK

Consider a customer initiating a cross-border payment that must satisfy the destination jurisdiction's KYC rules. Instead of transmitting a passport and address, the customer's wallet produces a single zero-knowledge proof over the private witness (date of birth, jurisdiction, identity commitment) against the public policy statement (minimum age, the jurisdiction allow-list commitment, and the current sanctions Merkle root). The proof establishes age ≥ 18, jurisdiction $\in$ allow-list, and identity $\notin$ sanctions root, and nothing else.

The proof capsule travels with the payment message. At the receiving institution, the XDP-style prefilter validates capsule structure and routing near the network boundary, then forwards the fixed-width capsule to the native verifier, which checks it against preloaded parameters and attaches an audit reference. The institution learns only pass/fail plus the policy commitments — never the underlying attributes — and retains the audit reference for later. If a court later compels identity recovery, the bank, regulator, and judicial auditor combine their 2-of-3 escrow shares to unmask that specific record; a request with a single share is rejected. The example shows the full lifecycle: privacy-preserving verification on the hot path, with lawful recovery available only under multi-party authorization.

VIII. REGULATORY AND PRACTICAL SIGNIFICANCE

Sentinel addresses the tension at the center of modern compliance: institutions must verify, screen, and preserve auditability while minimizing sensitive-data retention. FinCEN's 2026 AML/CFT modernization emphasizes risk-based programs [2], and the EU AMLA transition reflects coordinated, evidence-driven supervision [4]. By producing cryptographically verifiable compliance evidence without routine PII disclosure, Sentinel aligns with this direction. For ISO 20022 networks, a payment message can carry a compact compliance proof, policy commitments, and audit references instead of repeatedly transmitting identity attributes, reducing the liability of transporting and storing raw identity data while preserving demonstrable compliance. The escrow design shows that privacy-preserving compliance need not mean absolute opacity; it provides conditional transparency under multi-party authorization.

IX. CONCLUSION

Privacy and regulatory compliance need not be opposing goals. Sentinel shows that KYC and AML obligations can be represented as verifiable cryptographic statements rather than repeated transfers of raw PII. In simulation it achieved a p99.9 latency of about 101 µs versus about 1069 µs for the baseline, reduced tail spread by 14.7x, and held verifier latency stable as

10.48047/jocaaa.2026.35.06.20

the sanctions registry scaled to one million entries, while the escrow rejected unauthorized recovery and enabled authorized 2-of-3 recovery in sub-millisecond time. Future work should replace the simulated capsule with production zk-SNARK proofs, implement a full AF_XDP deployment, and evaluate the protocol under real payment-network traffic.

X. REFERENCES

[1] Identity Theft Resource Center, “2024 annual data breach report,” Jan. 2025.
[2] Financial Crimes Enforcement Network, “FinCEN proposes rule to reform financial institution programs designed to fight illicit finance,” Apr. 2026.
[3] Financial Crimes Enforcement Network, “Customer due diligence final rule.”
[4] European Banking Authority, “EBA and AMLA complete handover of AML/CFT mandates,” Jan. 2026.
[5] European Parliament and Council, “Regulation (EU) 2016/679, General Data Protection Regulation,” Official Journal of the EU, Apr. 2016.
[6] Commonwealth of Virginia, “Code of Virginia § 59.1-578: Data controller responsibilities; transparency.”
[7] Financial Action Task Force, “The FATF recommendations,” amended Oct. 2025.
[8] SWIFT, “ISO 20022.”
[9] SWIFT, “Instant payments.”
[10] J. Camenisch and T. Groß, “Efficient attributes for anonymous credentials,” ACM Trans. Information and System Security, vol. 15, no. 1, 2012.
[11] I. Solomka and B. Liubinskyi, “Zero-knowledge proof framework for privacy-preserving financial compliance,” Mathematical Modeling and Computing, vol. 12, no. 1, pp. 342–354, 2025.
[12] O. Kuznetsov, Y. Khavikova, V. Bushkov, D. Shchytov, and N. Mormul, “Performance analysis of Groth16 zkSNARK: Systematic benchmarking with Circom-snarkjs,” Int. J. Computing, 2026.
[13] J. Groth, “On the size of pairing-based non-interactive arguments,” in Advances in Cryptology — EUROCRYPT, pp. 305–326, 2016.
[14] A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.
[15] R. C. Merkle, “A digital signature based on a conventional encryption function,” in Advances in Cryptology — CRYPTO '87, LNCS 293, pp. 369–378, 1987.
[16] Linux Kernel Documentation, “AF_XDP.”
[17] Linux Kernel Documentation, “XDP_REDIRECT.”