WHITE PAPER

**Banking & Financial Services | IoT Security**

# ZipIPS™

## Quantum-Secure IoT Authentication with NanoTimestamp Power

*Quantum-Secure Authentication for Financial Infrastructure, Transactions, and the Systems That Move Money*

**Helene E. Schmidt, Inventor | Creative Synergies LLC**

synergies.com | US10171465B2 | US10348729B2

May 2026

## Executive Summary

Financial infrastructure is a high-value target. Every point-of-sale terminal, every ATM, every online banking session, every blockchain transaction represents an authentication event — a moment when something must prove it is what it claims to be. The authentication systems protecting most of these events were designed before quantum computing was a practical threat, before AI agents began executing transactions autonomously, and before the scale of modern financial infrastructure made human-supervised security operationally impossible.

Admiral Grace Hopper famously demonstrated the nanosecond in the 1960s by handing admirals an 11.8-inch piece of wire — the distance light travels in one nanosecond — to make delays in satellite communications tangible. If nanosecond precision mattered enough to hold in your hand fifty years ago, it is more than justified as an authentication boundary today, when modern hardware measures it routinely and adversaries may soon operate at quantum speed.

ZipIPS™ (Zip Intrusion Prevention System) addresses the financial authentication problem with a single mechanism: one-time timestamp credentials derived from pre-shared tables that never cross the network during authentication, unpredictable by any outside party. Every timestamp has exactly one use. No mathematical puzzle for quantum computers to solve. No Certificate Authority to compromise. No clock synchronization required.

This White Paper describes the authentication problem specific to banking and financial services, explains how ZipIPS™ addresses it, and identifies the deployment categories where quantum-secure on-demand authentication is not just useful — it is essential. Grok 4 (xAI) first determined that ZipIPS™ exceeds current NIST post-quantum and lightweight cryptography standards in both security level and credential efficiency. Claude (Anthropic) subsequently reached the same conclusions independently — two separate analyses, the same result.

ZipIPS™ is available for licensing. Creative Synergies LLC welcomes inquiries.

# 1. The Financial Authentication Problem

## 1.1 Why Financial Systems Are a Target

Money moves through networks. Every point where money changes hands digitally is an authentication event — a moment when a device, a user, or a system must prove it is authorized to participate in that transaction. The scale is staggering: billions of card transactions daily, millions of ATM sessions, continuous high-frequency trading, real-time interbank settlement, and an expanding universe of IoT-connected payment devices from smart meters to connected vehicles.

Attackers follow the money. Financial infrastructure attracts the most sophisticated adversaries — nation-state actors, organized criminal enterprises, and increasingly, AI-driven automated attack systems that can probe authentication mechanisms at machine speed. The authentication systems protecting most of this infrastructure were not designed for that threat environment.

## 1.2 Three High-Risk Surfaces

The authentication risk in financial services concentrates at three points.

| Surface | Why It Is High Risk |
|---|---|
| **Point-of-sale and payment terminals** | Card terminals, ATMs, and payment kiosks are distributed, often physically accessible, and authenticate millions of transactions daily. A compromised terminal that accepts fraudulent authentication can skim card data, authorize unauthorized transactions, or serve as an entry point into broader financial network infrastructure. |
| **Online and mobile banking** | Online banking sessions rely on certificate-based PKI (Public Key Infrastructure — the system of certificate authorities and digital certificates underlying TLS) and session tokens that are valid for extended periods. A Man-in-the-Middle who intercepts a session can execute transactions for its duration without re-authentication. |
| **Algorithmic trading and AI financial agents** | AI agents executing trades, managing portfolios, and interacting with market infrastructure operate at speeds and frequencies that make human oversight impossible. A compromised trading agent — one receiving fraudulent instructions — can execute unauthorized transactions before any monitoring system detects the anomaly. |

## 1.3 The Quantum Threat to Financial Infrastructure

Financial systems face a specific and well-documented quantum threat. The “harvest now, decrypt later” attack is already in practice: adversaries capture encrypted financial sessions today, expecting to decrypt them when capable quantum computers are operational. Transaction records, authentication sessions, and interbank communications captured now may be exposed in the future.

Shor’s algorithm breaks RSA and elliptic curve cryptography — the mathematical foundations of most financial authentication today. PCI DSS v4.0, FFIEC guidance, and Executive Order 14028 all signal the regulatory direction: quantum-resistant authentication is not optional, it is the coming requirement. The time to implement it is before the threat matures, not after.

# 2. How ZipIPS™ Works

## 2.1 The Core Mechanism

Here is what happens. Both devices — the financial terminal, trading system, or banking application and whatever system is authenticating it — hold identical copies of two lookup tables, loaded when the devices were provisioned. During authentication, the requesting device checks its own clock, takes the timestamp at that exact moment, and uses it as a key to look up a set of character strings from its table. It assembles those strings into a single credential and sends three things across the network: its device ID, the timestamp, and the credential.

The receiving system does the same lookup independently, using the timestamp it just received and its own identical copy of the tables. If the two credentials match: authenticated. If they do not match, the attempt is blocked and permanently logged with its timestamp and device ID. That exact moment is gone — no window, no retry, no second chance.

The lookup tables never travel across the network during authentication. An attacker who intercepts the transmission — device ID, timestamp, and credential — gains nothing useful. That timestamp was valid for exactly one guess.

There is no way to predict what the next credential will be, because there is no way to predict the exact nanosecond at which the next request will be made.

But authentication doesn't stop there. At any point during a session, the financial system or device can issue a ZipIPS™ challenge to the host to prove it is still the authorized system — not an impersonator who has taken over the connection. The host must answer correctly, or the communication is ignored and permanently logged for review. The device remains open to valid communications.

## 2.2 The Handshake at a Glance

The table below summarizes what each round accomplishes:

| Round | What It Proves |
|---|---|
| **Round 1 — Device presents credential** | The device holds the right tables and can produce the correct credential for this exact timestamp. |
| **Round 2 — Host challenges device with new timestamp** | The device can answer an unpredictable ZipIPS™ challenge it has never seen before — proving it holds the real tables, not a captured credential. |
| **On demand — Device challenges host** | At any point during a session, the device generates a fresh timestamp from its own clock and issues a ZipIPS™ challenge to the host. The host must produce the correct credential, or the communication is ignored and permanently logged for review. The device remains open to valid communications. |

## 2.3 Key Properties for Financial Systems

| Property | Why It Matters for Financial Services |
|---|---|
| **No persistent credential to steal** | Static API keys, session tokens, and certificates are standing vulnerabilities — once compromised, they remain valid until rotated. ZipIPS™ generates a fresh credential for every exchange. There is nothing persistent to steal. See Figures 1 and 2 in the next section. |
| **No clock synchronization required** | One side generates and transmits the timestamp. The other uses it as a lookup key. No shared time infrastructure, no NTP dependency, no synchronization attack surface. |
| **Every timestamp has exactly one use** | Succeed or fail, a timestamp is gone. No iterative search. No replay within a window. No brute force, classical or quantum. |
| **Permanent audit log** | Every authentication attempt — successful or failed — is logged with its exact timestamp and device ID. PCI DSS v4.0, SOC 2, FFIEC guidance, and FIPS 140-3 all require tamper-evident authentication records. ZipIPS™ provides them by design. |
| **Compact credentials** | 95 bytes (ms precision) to 157 bytes (ns+ precision). For high-frequency transaction environments processing millions of authentications daily, credential size and overhead matter. See Figures 1 and 2 in the next section. |
| **Quantum-secure by architecture** | No mathematical structure for Shor's or Grover's algorithm to exploit. Financial infrastructure deployed today remains protected against the quantum threat emerging tomorrow. |

# 3. Security Performance

ZipIPS™ is a licensable architecture — licensees write their own implementation code and configure the system for their environment. The following table illustrates representative security levels the architecture achieves. There is no upper limit: security increases without bound as string length, character set size, or the number of time units increases.

| Configuration | Entropy | Payload | Characteristics |
|---|---|---|---|
| **ms original ★** | 381 bits | 95 bytes | Millisecond-precision timestamps. 8-character alphanumeric strings. 8 time units. Original patent embodiment. Strong baseline for high-frequency transaction authentication. |
| **ns standard ★** | 476 bits | 117 bytes | Nanosecond-precision timestamps. 8-character alphanumeric strings. 10 time units. Appropriate for online banking, algorithmic trading, and sensitive financial API authentication. |
| **ns+ high security ★** | 735 bits | 157 bytes | 10 time units with 12-character strings from a 70-character set including non-control special characters. For interbank settlement, central bank infrastructure, and high-value financial operations. |

*★ All three entropy figures were independently calculated by both Grok 4 (xAI) and Claude (Anthropic) — separate analyses reaching identical results in each case.*

The figures below show how ZipIPS™ compares to current NIST standards in both security level and credential size — two dimensions that matter equally for high-frequency financial transaction environments.

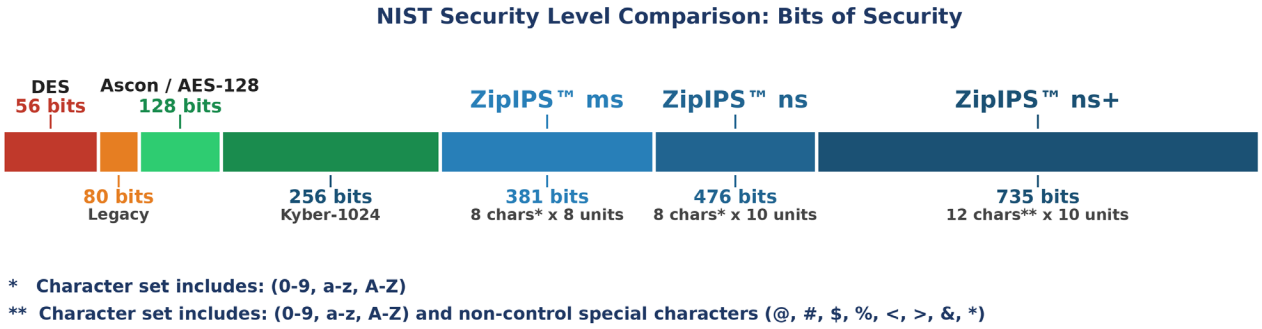


*Figure 1: NIST Security Level Comparison — ZipIPS™ illustrative implementations vs. reference points*

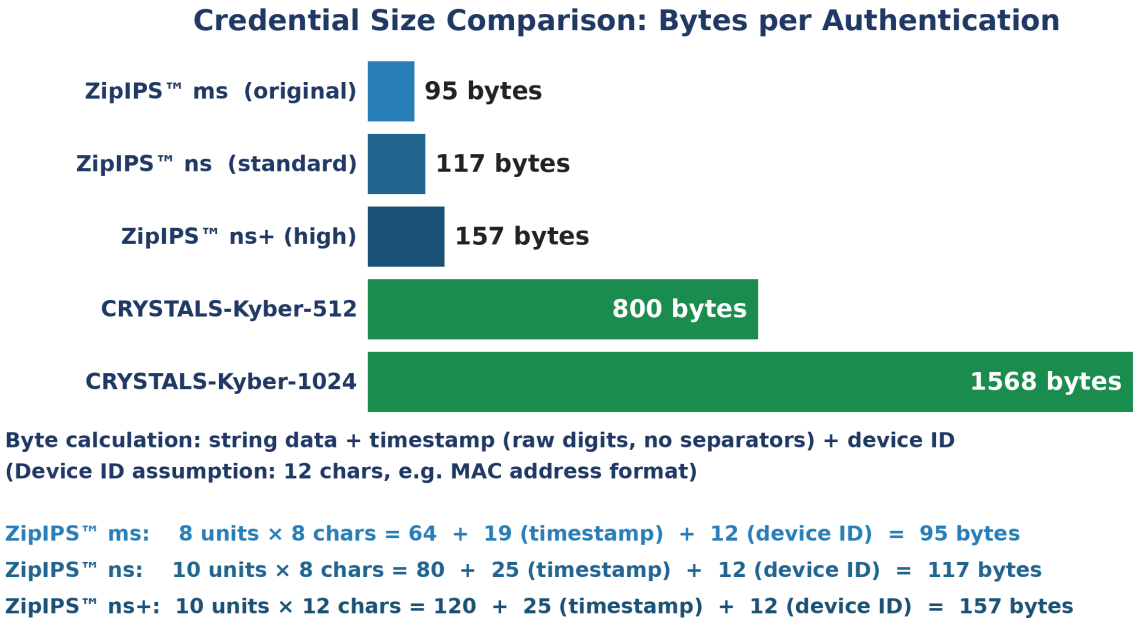


*Figure 2: Credential Size Comparison — ZipIPS™ illustrative implementations vs. CRYSTALS-Kyber*

CRYSTALS-Kyber-512 provides approximately 128 bits of security in an 800-byte credential. Kyber-1024 provides approximately 256 bits in 1,568 bytes. Ascon (NIST SP 800-232), the lightweight cryptography standard for constrained IoT devices, provides 128-bit classical security — reduced to approximately 64 bits against a quantum adversary using Grover's algorithm.

ZipIPS™ exceeds all three at every configuration level, in a credential compact enough for high-frequency transaction environments, with no quantum vulnerability. The classical and quantum security levels are the same number — because ZipIPS™ has no mathematical structure for quantum algorithms to exploit.

# 4. Financial Services Applications

## 4.1 Point-of-Sale and Payment Terminals

Credit card terminals and payment kiosks are among the most widely distributed authentication devices in existence. They are physically accessible, often in unsupervised environments, and authenticate millions of transactions daily. Skimming attacks, terminal substitution, and network interception are all documented threat vectors.

ZipIPS™ provides per-transaction authentication that eliminates the standing credential attack surface. Every transaction authentication generates a unique credential tied to a single nanosecond-precision timestamp. A skimmed credential from a previous transaction is worthless for any subsequent one. A substituted terminal that cannot produce a valid ZipIPS™ challenge response fails immediately. The attempt is logged with its device ID and timestamp.

## 4.2 ATMs and Banking Kiosks

ATMs authenticate both the user and the network connection to the financial institution. A compromised network connection — one where an attacker has substituted a fraudulent banking host — can intercept transaction data or authorize fraudulent withdrawals while the ATM believes it is communicating with the legitimate bank.

ZipIPS™ allows the ATM to issue a ZipIPS™ challenge to the host banking system before executing any transaction. A substituted host cannot produce a valid credential. The transaction is refused. The attempt is permanently logged with its precise timestamp and device ID — providing the tamper-evident audit trail that financial regulators require.

## 4.3 Online and Mobile Banking

Online banking sessions rely on TLS and session tokens that remain valid for minutes or hours. A Man-in-the-Middle who intercepts an established session can execute transactions for its entire duration without re-authentication. The user believes they are talking to their bank. They are not.

ZipIPS™ provides continuous session authentication. At any point during an online banking session, the client can issue a ZipIPS™ challenge to verify the host is still the authorized banking system. A substituted host cannot answer. The session is flagged and logged. For mobile banking operating over cellular networks where session interception is a known threat, this per-exchange verification closes the gap that TLS alone leaves open.

## 4.4 Algorithmic Trading and Financial AI Agents

AI agents executing trades, managing portfolios, and interacting with exchange infrastructure operate at speeds that make human oversight impossible in real time. A compromised trading agent — one receiving fraudulent instructions from a hijacked command source — can execute unauthorized transactions before any monitoring system detects the anomaly. The financial damage can occur faster than the detection.

ZipIPS™ provides command-level authentication for financial AI. Before executing any trade instruction or market interaction, the agent issues a ZipIPS™ challenge to the commanding source. A hijacked instruction source cannot answer. The fraudulent instruction is blocked. Every failed attempt is permanently logged — providing the audit trail that regulators and compliance teams require and that existing AI authentication systems were not designed to produce.

### 4.5 Blockchain and Cryptocurrency Systems

Blockchain networks depend on the integrity of the nodes participating in consensus and transaction validation. A node that has been compromised — one that is participating in consensus while actually under adversarial control — represents a structural threat to network integrity.

ZipIPS™ provides node-level authentication for blockchain infrastructure. Every interaction between nodes can be authenticated with a credential tied to a single timestamp. A compromised node that cannot produce a valid ZipIPS™ challenge response is identified before it participates in consensus. For cryptocurrency exchanges and custodians managing high-value digital assets, per-transaction authentication eliminates the static API key attack surface that represents one of the most common entry points in exchange compromises.

### 4.6 Interbank Settlement and Central Bank Infrastructure

Interbank settlement systems and central bank infrastructure represent the highest-value targets in financial services. The SWIFT network alone processes trillions of dollars in transactions daily. A compromised authentication event at this level is not a retail fraud incident — it is a systemic financial event.

ZipIPS™ ns+ configuration provides 735-bit quantum-secure authentication in a 157-byte credential — substantially exceeding any current NIST standard, with no quantum vulnerability. For institutions operating under DORA (Digital Operational Resilience Act), FFIEC guidance, and emerging CNSA 2.0 requirements, ZipIPS™ provides a quantum-secure authentication foundation that is deployable today.

## 5. Why Existing Approaches Are Insufficient

Legacy authentication was designed for supervised sessions over trusted networks with human-scale transaction frequencies. Modern financial infrastructure operates at machine speed, across untrusted networks, with AI agents executing millions of transactions without human oversight. Every approach below has a structural failure mode that ZipIPS™ resolves by design.

| Approach | Failure Mode / ZipIPS™ Resolution |
|---|---|
| **Static API keys** | Failure: Never expire. A compromised key gives permanent access to trading systems, payment APIs, or banking infrastructure. Exchange compromises involving static API keys are among the most common and costly incidents in financial services. Resolution: No static credential. Every exchange generates a unique, time-bounded credential. A compromised key from a previous exchange is immediately worthless. |
| **Session tokens / JWT** | Failure: Trusted for the duration of the session. A Man-in-the-Middle who intercepts an online banking or trading session can execute transactions for its entire lifetime without re-authentication. Resolution: No persistent session trust. Any device or system can issue a ZipIPS™ challenge to the commanding source at any point, independently verifying the connection is still legitimate. |
| **Certificate-based PKI / TLS** | Failure: Relies on PKI (Public Key Infrastructure — the system of certificate authorities and digital certificates underlying TLS) that can be compromised. Quantum computers will break RSA and ECC signatures underlying most financial authentication. Resolution: No CA required. Tables provisioned at deployment. Quantum-secure by architecture. |
| **TOTP / HOTP** | TOTP (Time-based One-Time Password) generates codes valid for a time window — typically 30 seconds. HOTP (HMAC-based One-Time Password) uses a counter instead of a clock. Both have an exploitable window and both rely on shared secrets that can be compromised. Resolution: ZipIPS™ credentials are tied to a single nanosecond-precision timestamp. Every timestamp has exactly one use. Succeed or fail, it is gone. |

## 6. Regulatory Alignment

ZipIPS™ was not designed to comply with specific financial regulations — it predates several of the most relevant ones. However, its architectural properties align directly with the direction regulators are moving in response to quantum threats and AI-driven financial infrastructure.

| Framework | ZipIPS™ Alignment |
|---|---|
| **PCI DSS v4.0** | Requires strong cryptography for cardholder data protection and authentication. ZipIPS™ provides quantum-secure authentication with tamper-evident logging for every transaction authentication attempt. |
| **FFIEC Authentication Guidance** | Requires layered security and risk-based authentication for online banking. ZipIPS™ provides per-session and per-transaction verification with no persistent credential to compromise. |
| **FIPS 140-3** | Cryptographic module standards for financial systems handling sensitive data. ZipIPS™ authentication derives from randomly generated lookup tables rather than mathematical structures, eliminating quantum attack vectors. |
| **NIST PQC FIPS 203/204/205** | Post-quantum cryptography standards now required for federal systems and their supply chains. ZipIPS™ exceeds NIST security baselines at every configuration level: 381 bits (ms), 476 bits (ns), 735 bits (ns+). |
| **Executive Order 14028** | Mandates quantum-resistant cryptography across federal financial systems and their contractors. ZipIPS™ provides a quantum-secure authentication layer deployable now, ahead of regulatory deadlines. |
| **DORA (EU Digital Operational Resilience Act)** | Requires financial institutions to demonstrate operational resilience against cyber threats including advanced persistent threats. ZipIPS™ eliminates the static credential attack surface and provides continuous authentication throughout financial sessions. |

*Note: These alignments are architectural observations, not certifications or legal compliance determinations. Organizations should consult qualified compliance counsel regarding their specific regulatory obligations.*

## 7. Implementation Considerations

ZipIPS™ is a licensable architecture — not a product. Licensees write their own implementation code, configured for their specific financial infrastructure and security requirements. Two implementation responsibilities rest with the licensee:

- Table generation: String tables and sequence tables are generated by the licensee. Independently and randomly generated tables provide a security foundation whose properties are well within the licensee's control to establish and verify.
- Secure provisioning: The initial provisioning of tables to authenticating devices and host systems is the licensee's responsibility. For financial infrastructure, this maps naturally to existing secure device provisioning workflows for payment terminals, ATMs, and trading systems.

For financial services specifically, the most effective integration builds ZipIPS™ authentication into the transaction flow: every authentication event — session initiation, transaction execution, and on-demand re-verification — uses a fresh ZipIPS™ credential. This pattern eliminates the session hijacking and replay attack surfaces that legacy authentication leaves open.

Implementation requirements will vary by institution and are the licensee's responsibility to evaluate. Creative Synergies LLC makes no representation regarding specific integration requirements for any particular financial system.

## 8. Patent Foundation

ZipIPS™ is protected by two issued United States patents, both assigned to Helene E. Schmidt of Creative Synergies LLC.

| Patent | Issued \| Scope |
|---|---|
| **US10171465B2** | Jan. 1, 2019 — Method patent covering the authentication process: timestamp generation, character string retrieval and sequencing, initiating string construction and transmission, host-side verification, second timestamp generation, client-side verification, and the on-demand re-verification loop. |
| **US10348729B2** | Jul. 9, 2019 — System patent covering the authentication architecture: host device with sequence tables and string tables at variable security levels, client device with mirrored table architecture, device identifier, and the system configuration for the complete double two-way handshake with on-demand re-verification. Continuation of US10171465B2. |

Both patents cover the core architecture — the method and the system. The claims establish broad protection for timestamp-based authentication using independently-derived, never-transmitted sequence ordering, across device pairs with mirrored table structures. The architecture applies directly to payment terminal authentication, ATM network security, online banking session verification, algorithmic trading command authentication, and blockchain node authentication. Prospective licensees are encouraged to review the patents directly and consult qualified patent counsel regarding scope.

## 9. Licensing

Creative Synergies LLC welcomes inquiries from qualified organizations interested in exploring licensing opportunities for ZipIPS™. No terms are presented in this White Paper — the right licensing structure is best arrived at through direct dialogue between technically and legally informed parties.

ZipIPS™ is available for licensing. Please visit synergies.com and Contact Us if you have any questions.

Helene E. Schmidt, Inventor | Creative Synergies LLC | synergies.com | zipips@synergies.com