End-to-End Post-Quantum Security at ACM: Securing Every Hop from the API Gateway to Key Management Against Harvest-Now, Decrypt-Later

ACM Global Tech

Abstract

ACM Global Tech licenses an end-to-end, post-quantum, regulatory-compliant infrastructure stack for regulated banking and digital securities. This white paper describes how ACM extends post-quantum protection beyond the ledger to *every off-chain hop*: client to gateway, gateway to backend services, services to key management, and key management to storage. The construction draws on the Hanzo end-to-end encryption and security architecture [1], the Hanzo KMS secrets-management platform with envelope encryption and per-environment rotation [2], and the Hanzo post-quantum migration that replaces classical algorithms with the NIST standards ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) [3]. The migration is *hybrid*: classical and post-quantum primitives run in parallel so the system stays secure as long as either assumption holds. The goal is that long-lived financial records—retained for years to decades by regulation—resist a "harvest now, decrypt later" adversary who records ciphertext today to decrypt once a cryptographically relevant quantum computer (CRQC) exists. The technical guarantees trace to the cited research; the stack ACM licenses and operates is built on Lux (blockchain, post-quantum cryptography, FHE), Hanzo (AI/data), and Zen (LLMs).

1 The Problem: Long-Lived Records, A Patient Adversary

A regulated financial platform encrypts data at many layers, but most of that protection assumes a *classical* adversary. Transport security (TLS) protects data in transit yet decrypts it at each service boundary, creating exposure windows [1]; key establishment, request signing, and identity tokens rest on elliptic-curve cryptography that Shor's algorithm breaks in polynomial time on a CRQC [3]. The danger is not only a future break but a present one: a "harvest now, decrypt later" adversary records encrypted traffic and on-the-wire key material today, then decrypts it once quantum hardware arrives [3].

For data whose confidentiality horizon T_D exceeds the year T_Q that a CRQC becomes available, today's encryption already fails. The source research places T_Q roughly a decade or two out and assigns *financial* records a T_D of 7–25 years (regulatory retention), making migration urgency *high*; blockchain signatures, recorded on-chain forever, have $T_D = \infty$ and urgency *critical* [3]. A platform that retains transaction records, audit logs, and custody material for that long must make every hop quantum-resistant now—not retrofit it after a break is announced.

2 ACM's Approach

ACM composes the three source layers into a single end-to-end posture in which each hop is protected by a NIST post-quantum primitive, deployed in hybrid mode during transition.

Client and inter-service transport (ML-KEM).
Key establishment for TLS—client-to-gateway and service-to-service—uses hybrid key exchange that combines X25519 with ML-KEM-768 (FIPS 203, NIST Level 3), derived as $K_{\text{hybrid}} = \texttt{HKDF-SHA256}(K_{\text{X25519}} \,\|\, K_{\text{ML-KEM}})$, so the session key is safe if *either* scheme holds [3]. The gateway implements TLS 1.3 with the `X25519MLKEM768` named group; application data is sealed with AES-256-GCM, which retains 128-bit security against Grover's bound [3]. Measured handshake overhead is 1.2 ms on a cold connection, within a single TCP segment and adding no round trip [3].

Authentication and request signing (ML-DSA).
Identity tokens, service certificates, and credential chains migrate from Ed25519/ECDSA to ML-DSA-65 (FIPS 204, NIST Level 3) [3]. IAM-issued JWTs follow a three-phase path: dual-sign with both algorithms, then issue ML-DSA-only while still verifying both, then remove classical verification—so tokens stay valid across the cutover. Internal service-to-service calls use mTLS with ML-DSA-65 certificates; delegated credentials preserve the chain structure Root → Org → Agent under ML-DSA with cross-signed certificates bridging old and new roots [3].

Long-lived roots of trust (SLH-DSA).
Root certificates—verified rarely and trusted longest—use SLH-DSA-SHA2-192s (FIPS 205), whose security rests only on hash-function second-preimage resistance, an assumption believed to hold against quantum adversaries up to Grover's quadratic factor [3]. The conservative hash-based root anchors the lattice-based ML-DSA chains beneath it.

Key management and storage (PQ envelope encryption).
Secrets and data-at-rest are protected by KMS envelope encryption: a per-project data encryption key (DEK) seals values with AES-256-GCM, and the DEK is wrapped by a key encryption key (KEK) held in an HSM/TPM, limiting the blast radius of any single compromise to one project [2]. Where DEK wrapping previously relied on ECDH-derived keys, the post-quantum migration derives the wrapping key via ML-KEM encapsulation, keeping the same envelope pattern and key hierarchy; existing secrets are re-wrapped on the next rotation cycle (within 90 days per KMS policy) [3]. The same defense-in-depth hierarchy—master key, per-tenant key, per-object key—protects objects in the S3-compatible store so a storage breach yields only ciphertext [1].

The composition works because the original key-management abstraction was built with *algorithm agility*: the KMS API surface stays fixed while the underlying primitive is swapped, which is exactly what let ML-KEM replace X25519 in envelope encryption without changing callers [1].

ACM positioning. ACM is a W3A (w3a.foundation) member that licenses this end-to-end post-quantum stack—built on Lux (blockchain, post-quantum cryptography, FHE), Hanzo (AI/data), and Zen (LLMs)—and partners to resell and co-build it for regulated institutions. Beyond the cryptographic core, ACM operates a real-time AI/ML AML and transaction-monitoring engine and ships a Stripe-class payment service provider together with a full Banking-as-a-Service product, so regulated institutions adopt post-quantum security as part of a complete, compliant platform.

3 Cryptographic Foundation

The technical guarantees trace directly to three Hanzo research papers.

- **End-to-end encryption architecture.** *End-to-End Encryption and Security Architecture for Cloud-Native Applications* [1] specifies defense-in-depth encryption for data at rest, in transit, and in storage—Age (X25519 + ChaCha20-Poly1305) file encryption, per-message envelope encryption, and a three-tier master/tenant/object key hierarchy—and explicitly notes that TLS alone is insufficient and that the KMS abstraction was designed for algorithm agility, enabling ML-KEM to replace X25519.
- **KMS secrets management.** *Hanzo KMS: Secrets Management with Per-Environment Rotation and Audit Trail* [2] specifies two-layer envelope encryption (per-project DEK wrapped by an HSM/TPM-held KEK with AES-256-GCM), RBAC scoped to project and environment, automatic rotation for database credentials, API keys, and TLS certificates, an append-only audit trail, and a Kubernetes operator that delivers secrets to running workloads.
- **Post-quantum migration.** *Hanzo Post-Quantum Cryptography: Migration Path for AI Infrastructure* [3] deploys ML-KEM-768 for key exchange (TLS, KMS wrapping), ML-DSA-65 for signatures (IAM JWTs, mTLS, agent credentials), and SLH-DSA-192s for root certificates; defines the harvest-now/decrypt-later threat model with per-data-class confidentiality horizons; specifies hybrid classical+PQ transition; and reports the performance and key-size impact (e.g. a 1.2 ms hybrid-handshake increase and negligible KMS storage growth).

4 Outcomes

The intended outcomes, as supported by the cited research, are:

1. **Every hop is quantum-resistant.** Key establishment (ML-KEM), authentication and signing (ML-DSA), long-lived roots (SLH-DSA), and key wrapping/storage (ML-KEM envelope encryption) are each protected by a NIST post-quantum primitive, so no single hop remains a classical-only weak link [3, 2, 1].
2. **Harvest-now, decrypt-later is defeated for records that matter.** Because session keys and stored DEKs are derived under post-quantum encapsulation, traffic and ciphertext recorded today cannot be decrypted by a future CRQC, protecting records across their multi-year regulatory retention horizon [3].
3. **Non-disruptive, fail-safe migration.** Hybrid key exchange and dual-signed tokens let classical and post-quantum schemes run in parallel; the system stays secure if either holds, and clients migrate without a flag-day cutover [3].
4. **Bounded blast radius and accountability.** The per-project DEK / HSM-held KEK hierarchy confines a key compromise to one project, and an append-only audit trail records every secret access, preserving least privilege and traceability through the migration [2, 1].

References

[1] Z. Kelling. *End-to-End Encryption and Security Architecture for Cloud-Native Applications.* Hanzo Industries. Source: `hanzo:hanzo-encryption-security/hanzo-encryption-security.tex`.

[2] Z. Kelling. *Hanzo KMS: Secrets Management with Per-Environment Rotation and Audit Trail.* Hanzo Industries. Source: `hanzo:hanzo-kms-secrets.tex`.

[3] Z. Kelling. *Hanzo Post-Quantum Cryptography: Migration Path for AI Infrastructure*. Hanzo Industries Inc. Source: `hanzo:hanzo-pq-crypto/hanzo-pq-crypto.tex`.