JUNE 2026
APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

PAYMENTS EXTENSION

Card Networks, RTGS, SWIFT, Payment HSMs, and Terminal Infrastructure *— Industry-Specific Challenges and Framework Adaptations*

Version 2.1 — June 2026

Marin Ivezic
CEO, Applied Quantum
Author, PostQuantum.com

PQCFramework.com | PQCMigrationBrief.com | PostQuantum.com | SecureQuantum.com | AppliedQuantum.com | QuantumReady.com

"Start while it's a project, before it's a crisis."

COPYRIGHT AND LICENSE

DISCLAIMER

This extension is provided as professional guidance based on the author's and Applied Quantum's practitioner experience and publicly available standards, regulations, and industry research. It does not constitute legal, regulatory, financial, or compliance advice. Organizations should consult qualified legal counsel, auditors, and regulatory authorities for guidance specific to their jurisdiction, sector, and circumstances.

The regulatory timelines, vendor capabilities, algorithm parameters, and tool categories referenced in this document reflect the state of the PQC landscape as of June 2026. These references may become outdated quickly. Readers should verify current status against primary sources before making implementation decisions.

References to specific vendors, products, or tools are for illustrative purposes and do not constitute endorsement. The PQC tooling market is evolving rapidly; products mentioned may have changed in capability, licensing, or availability since publication. Organizations should conduct their own evaluation based on their specific requirements, regulatory environment, and procurement constraints.

NIST IR 8547, referenced throughout for deprecation and disallowance timelines, was an Initial Public Draft as of November 2024 with final publication expected in 2026. Federal agencies and their contractors should reference the final version when available.

ABOUT THIS DOCUMENT

Document type	Enterprise methodology and practitioner framework
Parent Document	The Applied Quantum PQC Migration Framework — Universal — v2.1 (June 2026)

Intended audience	Payment infrastructure engineers, card network architects, HSM operations teams, terminal fleet managers, payment security officers, CISOs and program managers with payment system responsibility
Assumed knowledge	Familiarity with the Universal PQC Migration Framework and its 8-phase lifecycle; working knowledge of card payment systems, RTGS/settlement infrastructure, SWIFT messaging, and payment HSM operations
Scope	Payment-infrastructure-specific PQC migration challenges and framework adaptations: card networks, RTGS systems, SWIFT/ISO 20022 messaging, payment HSMs, POS terminals, mobile payments, and cross-border correspondent banking. Companion to the Financial Services Extension. Not a standalone document: intended to be used alongside the Universal Framework and the Financial Services Extension.

VERSION HISTORY

Version 1.1 (March 2026): Payment-specific content was previously included in the Financial Services Extension v1.1 (March 2026). This v2.0 Payments Extension is the first dedicated publication.

Version 2.0 (June 2026): Initial publication as a dedicated Payments Extension, separated from the Financial Services Extension. Anchored by BIS Project Leap Phase 2 findings. Covers 10 payment-specific challenges, phase-by-phase adaptations, payments regulatory alignment map, maturity model supplement, KPI supplement, and recommended immediate actions. Aligned with Universal Framework v2.0 (two-track model, FIPS validation gap, MTC position).

Version 2.1 (June 2026): Aligned with Universal Framework v2.1. Six new alignment subsections: composite/dual signatures under payment message constraints; algorithm-specific vulnerability weighting and the EMV ECC transition; the payments identity stack (payment passkeys, 3DS, wallets, token signing) in Track B; SP 800-208 firmware signing for terminal, ATM, and HSM fleets; payment CBOM protection; verification and decommissioning in multi-party payment networks. Editorial corrections (Universal dimension count, duplicated passage in Challenge 2) and companion book cross-reference.

HOW TO USE THIS EXTENSION

This document is a companion to both the Applied Quantum PQC Migration Framework (Universal) and the Financial Services Extension. It does not replace either document but extends them with payment-infrastructure-specific guidance. The Financial Services Extension covers challenges common to all financial sub-sectors; this Payments Extension goes deeper into the transaction processing infrastructure itself. Readers should have the Universal Framework open alongside this document and cross-reference its phase definitions, maturity indicators, and templates.

WHAT'S NEW IN V2.1

Version 2.1 of the Payments Extension is a targeted alignment release tracking Universal Framework v2.1 (June 2026):

Alignment with Universal Framework v2.1. Six new alignment subsections map the v2.1 positions that require sector adaptation to payment infrastructure: composite and dual signatures under payment message size constraints; algorithm-specific vulnerability weighting and the EMV ECC transition; the identity stack in payments (payment passkeys, 3DS signing, wallet credentials, token signing); SP 800-208 stateful hash-based signatures as the deploy-now action for terminal, ATM, and HSM firmware signing; protection of the payment CBOM as a high-value intelligence target; and verification and decommissioning in multi-party payment networks. The remaining Universal v2.1 additions are sector-neutral and apply as written; the alignment section introduction lists them and the governing cross-references.

Editorial corrections. The Universal Framework dimension count in Phase 3 risk scoring was corrected, a duplicated passage in Challenge 2 was removed, and payment passkeys were added to the mobile wallet challenge. A cross-reference to the companion book, *Quantum Ready*, was added.

WHAT'S NEW IN V2.0

Version 2.0 of the Payments Extension reflects three developments since the March 2026 release:

Alignment with Universal Framework v2.0. The parent framework introduced a two-track migration model, deployment-environment classification addressing the FIPS 140-3 validation gap, and a position on Merkle Tree Certificates for public Web PKI. This

extension maps those changes to payment infrastructure: card networks, RTGS systems, SWIFT and ISO 20022 messaging, payment HSMs, terminals, ATMs, mobile wallets, and real-time payment schemes.

Dedicated payments scope. Payments-specific content has been separated from the Financial Services Extension and substantially expanded. This document covers transaction-processing infrastructure, payment message formats, payment HSMs, POS and ATM fleets, card and wallet ecosystems, tokenization, real-time payment systems, and cross-border payment dependencies.

Payments-sector evidence and coordination. BIS Project Leap Phase 2 provides the first production-grade payment-system PQC experiment. SwiftNet 8.0, PCI DSS 12.3.3, PCI PIN and PTS dependencies, EMVCo and X9 workstreams, and G7/Europol/FS-ISAC coordination are treated as external planning inputs.

ACCOMPANYING RESOURCES

Every aspect of this framework, from executive business cases and cryptographic inventory methodologies to CBOM architecture, hybrid deployment patterns, and vendor governance, has been analyzed in detail on PostQuantum.com over the past 10+ years through practitioner-grounded articles, deep dives, and sector-specific analyses.

The best starting point is the curated Getting Started with Quantum Security and PQC Migration page: https://postquantum.com/starting-pqc-quantum-security/, but readers should also use PostQuantum.com's Search function to surface additional relevant posts that may not be included in that curated list.

Key framework resources, templates, and supporting materials are also published on PQCFramework.com, a dedicated companion site for this framework, drawing on relevant content from PostQuantum.com.

This extension, like the framework it accompanies, is the execution methodology. For the complete treatment (the reasoning behind each phase, extended case examples, and guidance for leading the program from the first board conversation through closure), see the companion book, *Quantum Ready* (QuantumReady.com).

TABLE OF CONTENTS

WHY PAYMENTS REQUIRES ITS OWN EXTENSION

The Financial Services Extension addresses challenges common to banking, capital markets, insurance, and digital assets. Payments, however, concentrates several of these challenges to an extreme degree and introduces constraints that have no parallel elsewhere in financial services. A cross-border mobile banking payment triggers over 30,000 unique cryptographic function calls across nine independent parties. The authorization decision happens in under 300 milliseconds. The infrastructure executing that decision includes hardware that may remain in service for 15 years. And no single entity controls more than a fraction of the chain.

This section identifies the characteristics that make payment infrastructure a distinct PQC migration domain.

Cryptographic Density at Transaction Scale

A single mobile banking transaction invokes approximately 320 cryptographic function calls before the customer even initiates a payment. Extend that transaction to a cross-border payment through a correspondent banking chain, and the count rises to over 30,000 unique cryptographic functions spanning the cardholder's device, the merchant terminal, the acquirer, the card network, the issuing bank, one or more payment processors, SWIFT's messaging layer, correspondent banks, and the central bank RTGS system. Each function call represents a quantum-vulnerable dependency managed by a different organization with its own upgrade cycle. The cryptographic inventory challenge (Phase 1) for a payments organization dwarfs what a typical enterprise faces.

Multi-Party Coordination Without Central Authority

Payment chains lack a single coordinating authority for cryptographic upgrades. A domestic card payment involves at minimum the cardholder, the merchant, the acquirer, the card network, and the issuer. A cross-border payment adds correspondent banks, messaging networks, clearing houses, and central bank settlement systems. Each participant operates independently: different vendors, different certification timelines, different risk appetites, different regulatory jurisdictions. Migrating one node to PQC

protects the links and services that node controls, but does not make the end-to-end payment chain quantum-safe while counterparties and shared trust infrastructure remain classical. The chain's quantum safety is determined by its weakest link. This N-party synchronization problem has no equivalent in sectors where organizations control their own cryptographic estate.

Hardware Fleet with Decade-Long Replacement Cycles

Payment infrastructure runs on purpose-built, heavily certified hardware. Almost 20 billion payment cards are in circulation, most running 32-bit processors with 48 KB of RAM. Millions of POS terminals and ATMs are deployed globally, with typical replacement cycles of 7 to 15 years. Payment HSMs carry dual certification requirements (FIPS 140-3 and PCI PTS) with validation processes measured in years, not months. This hardware cannot be patched remotely on a software release cycle. It must be physically manufactured, distributed, certified, and installed, creating migration timelines that are constrained by logistics and certification bureaucracy.

Real-Time Performance with Zero Tolerance for Degradation

Payment authorization decisions operate within strict latency budgets. A contactless card transaction must complete within 300 milliseconds. RTGS settlement systems process trillions of euros daily with tight throughput guarantees. BIS Project Leap Phase 2 found that software-based PQC signature verification on T2 averaged 209.9 milliseconds compared to 28.1 milliseconds for RSA, a 7.5× slowdown. That overhead, applied to a system handling thousands of transactions per second at peak, creates capacity planning challenges specific to payment processing and absent from most other enterprise PQC migration contexts.

Message Format Constraints That Predate the Internet

ISO 8583, the binary format underpinning global card payment authorization, was designed when every byte was expensive. Its authentication data fields cap at approximately 256 bytes. An ML-DSA-44 signature is 2,420 bytes. It does not fit. ISO 20022 is more extensible, but BIS Project Leap Phase 2 found that PQC signatures in ISO 20022 Business Application Headers still exceeded expected buffer sizes in T2's message-handling logic. The problem extends beyond the wire format to every switch, gateway, parser, logging system, database schema, and archive built around current field size assumptions.

BIS Project Leap Phase 2: The First Real-World Proof Point

In December 2025, the BIS Innovation Hub, Banque de France, Deutsche Bundesbank, Banca d'Italia, Nexi-Colt, and SWIFT published the results of Project Leap Phase 2, the first production-grade payment-system PQC experiment, conducted on the Eurosystem's T2 test environment configured to reflect realistic operational scenarios. The experiment applied PQC digital signatures to liquidity transfer orders on T2 (the Euro area's RTGS system, successor to TARGET2 since March 2023), which processes over €2 trillion daily. All test scenarios passed: PQC-signed liquidity transfers were processed correctly.

The results confirmed that PQC works in settlement infrastructure, while simultaneously revealing the operational reality: a 7.5× signature verification slowdown, a 12.9× increase in signature payload size (pre-standard CRYSTALS-Dilithium category 3 at 3,293 bytes versus RSA-2048 at 256 bytes; the standardized ML-DSA-65 signature is 3,309 bytes per FIPS 204), and a missing digital certificate in T2's static reference data that blocked settlement until manually resolved. This last finding is especially instructive: the migration is not an algorithm swap. It requires parallel PKI infrastructure, updated static reference data, and end-to-end coordination that current systems were not designed to accommodate.

Payment Structural Advantages for PQC Migration

Despite severe migration challenges, payment infrastructure possesses structural advantages that organizations should recognize and use in their program design.

PCI Compliance Infrastructure as CBOM Accelerator

PCI DSS v4.0 Requirement 12.3.3 (effective March 2025) already mandates that PCI-scoped entities document all cryptographic cipher suites and protocols in use, with annual review. Most payment organizations are PCI-scoped across a broad swath of their infrastructure. The CBOM construction effort can be structured to satisfy PCI 12.3.3 as a standard output, producing both PQC readiness assessment and PCI compliance evidence from the same data collection. This dual-use approach makes the CBOM investment immediately justifiable in compliance terms, independent of quantum threat timelines.

ISO 20022 Migration as a Parallel Modernization Window

The global migration from SWIFT MT messages to ISO 20022 MX format is underway, with SWIFT's coexistence period extending through November 2025 and full adoption rolling out across markets on different timelines. This concurrent infrastructure modernization creates an opportunity: organizations redesigning message-handling systems for ISO 20022 can incorporate PQC payload accommodation into the same engineering effort, rather than retrofitting it later. Where ISO 20022 migration budgets

and teams are already funded, PQC requirements can be integrated at marginal additional cost.

Concentrated HSM Vendor Market

The payment HSM market is dominated by three vendors (Thales, Utimaco, Futurex), with Entrust holding significant general-purpose HSM share. This concentration simplifies Phase 7 vendor governance: fewer vendor relationships to manage, fewer PQC roadmaps to track, and greater leverage in driving certification timelines. Most payment organizations use one or two of these vendors, enabling focused engagement rather than the fragmented vendor management challenge that organizations with dozens of cryptographic dependencies face.

Existing Key Management Teams and Cryptographic Expertise

Payment organizations maintain dedicated key management functions within their security operations. These teams manage HSM estates, perform key ceremonies, handle PIN translation key hierarchies, and manage certificate lifecycles. They have institutional knowledge of the cryptographic estate that accelerates Phase 1 discovery: they know where the HSMs are, what applications use them, which key ceremonies are performed annually, and which DUKPT key hierarchies serve which terminal populations. This knowledge base provides a head start that organizations in less-regulated sectors typically lack.

Change Management Discipline

Payment organizations run formal change advisory boards with change freezes around month-end, quarter-end, and peak transaction periods (Black Friday, holiday seasons, fiscal year-end). PQC pilots fit naturally into this structure. The rollback requirements in Phase 5 align with existing change management practices: payment organizations already maintain rollback procedures, test in staging environments that mirror production, and schedule deployments in controlled maintenance windows.

PAYMENT-SPECIFIC CHALLENGES

This section details the technical and operational challenges specific to payment infrastructure PQC migration. Each challenge is presented with its technical basis, real-world evidence where available, and the Universal Framework phases it most directly impacts. The subsequent section maps these challenges to specific framework adaptations.

Challenge 1: The Signature Size Problem

PQC algorithms produce signatures and public keys that are orders of magnitude larger than their classical equivalents. This mismatch is a structural incompatibility with payment message formats engineered for minimal payload sizes.

ISO 8583: Hard Field Limits

ISO 8583 is the binary format underpinning global card payment authorization. Field 55 (ICC Related Data), Field 56 (Reserved ISO), and authentication data fields cap at approximately 256 bytes in most implementations. An ML-DSA-44 signature is 2,420 bytes (a 37.8× increase over the 64-byte ECDSA signature it replaces). An ML-DSA-65 signature is 3,309 bytes per FIPS 204 (3,293 bytes in the pre-standard Dilithium variant used in earlier testing). These signatures cannot be accommodated within ISO 8583's field structure without fundamental format revision.

The implications cascade across every switch, gateway, payment processor, middleware parser, logging system, database schema, and archive that assumes current field sizes. Payment processors that have spent decades optimizing ISO 8583 parsing logic (hardcoding field offsets to shave microseconds) will find those optimizations broken. The X9 Accredited Standards Committee has published a Post-Quantum Cryptography Financial Readiness Needs Assessment covering both ISO 8583 and ISO 20022, but the hard engineering of accommodating larger payloads across thousands of institutions remains ahead.

ISO 20022: Extensible but Not Free

ISO 20022's XML/JSON-based structure is more extensible than ISO 8583, and the industry migration from MT to MX messages is underway. However, extensibility does not

mean zero-effort accommodation. BIS Project Leap Phase 2 found that replacing the RSA-2048 signature (256 bytes) in the ISO 20022 Business Application Header with ML-DSA-65 (3,293 bytes) created a 12.9× payload increase at the BAH level. T2's message-handling logic encountered unexpected buffer sizes. Storage and archival systems that retain message copies for regulatory compliance face multiplicative increases in data volume.

Archive and Storage Multiplication

Payment message archives are among the largest data stores in financial institutions. Regulatory retention requirements (typically 5 to 10 years) mean that the signature size increase compounds across every stored message. A system archiving 10 million messages daily with an average PQC signature overhead of 3 KB per message adds approximately 30 GB of additional storage per day, or roughly 11 TB per year, for signature data alone. Certificate chains add further overhead. Organizations must model this storage impact during Phase 6 capacity planning.

> **Framework Impact:** Phase 1 (Discovery) must include message format analysis as a distinct inventory track, identifying every fixed-size field carrying cryptographic data. Phase 3 (Risk Scoring) must weight message-format-constrained systems separately. Phase 5 (Pilots) must include message-format-specific testing with realistic payload sizes. Phase 6 (Infrastructure) must model archive storage growth.

Challenge 2: Payment HSM Certification Bottleneck

Hardware Security Modules are the root of trust for every payment cryptographic operation: PIN translation, MAC generation and verification, key injection, card personalization, and transaction signing. Payment HSMs carry dual certification requirements that create a compounding bottleneck for PQC adoption.

The Double Certification Problem

Payment HSMs must satisfy two independent certification regimes. FIPS 140-3 Level 3 (or higher) validates the cryptographic module's security properties; SWIFT mandates FIPS 140-2 Level 2+ for its network participants. PCI PTS HSM v4 validates the module's suitability for payment-specific operations (PIN handling, key management). As of June 2026, no payment HSM product has completed a FIPS 140-3 Level 3 CMVP validation that includes PQC algorithms within the validated module boundary. Organizations should track validation status at the specific product, firmware version, and CMVP certificate level rather than relying on vendor marketing claims of PQC support.

HSM vendors ship firmware with PQC support (Utimaco's Quantum Protect firmware supports ML-DSA and LMS; Thales payShield offers PQC-enabled firmware), but running

PQC operations outside the FIPS-validated boundary creates a compliance gap that regulators and auditors may not accept. CMVP validation backlogs currently average 12 to 18 months. The earliest FIPS 140-3 validated PQC module is expected mid-2027 at the optimistic end. Adding PCI PTS certification extends the timeline further.

Payment HSM Vendor Concentration

The payment HSM market is concentrated among a small number of vendors, including Thales (payShield), Utimaco (Atalla, CryptoServer), Futurex (CryptoHub), and Entrust (nShield). This concentration simplifies vendor governance but also concentrates migration risk: a certification delay at one major vendor affects a significant fraction of the global payment infrastructure.

Utimaco's strategic partnership with Keyfactor (which acquired InfoSec Global and CipherInsights) provides an integrated path from cryptographic discovery to HSM-level remediation. The AgileSec Analytics platform integrates directly with Utimaco's u.trust HSMs for automated discovery and vulnerability analysis. Payment organizations using Utimaco should assess whether this existing vendor relationship provides Phase 1 discovery capabilities they have not yet activated.

> **Framework Impact:** Phase 6 (Infrastructure) must include HSM certification tracking as a gating dependency, with separate tracking for FIPS 140-3 and PCI PTS certification timelines. Phase 7 (Vendor Governance) must establish structured quarterly engagement with HSM vendors on certification timelines and early access to PQC firmware for lab testing.

Challenge 3: Terminal and Card Fleet Migration

The payment card and terminal fleet represents the most physically distributed PQC migration challenge in any sector.

Card Hardware Constraints

Almost 20 billion payment cards are in circulation worldwide, most running 32-bit processors at approximately 100 MHz with 48 KB of RAM and no hardware acceleration for PQC algorithms. Side-channel protection (essential for payment cards where physical attackers can probe power consumption) multiplies PQC execution time by 2× to 5.6×. Classic McEliece requires over 70 KB of RAM, exceeding the card's total memory. Only lattice-based algorithms (ML-KEM, ML-DSA) are theoretically feasible on current hardware, and EMV commands' 256-byte data transfer limits require new extended commands for PQC certificate and signature exchange.

FS-ISAC's payment card guidance explicitly notes that it is not known whether EMV can accommodate quantum-safe certificates. New 28nm smart card chips

(IDEMIA/GlobalFoundries, targeted for 2026 mass production) will provide more computational headroom, but the card replacement cycle is measured in years: the average card has a 3-to-5-year lifespan, and full fleet turnover takes longer.

Terminal Fleet Scale and the Mastercard Ecos Approach

Millions of POS terminals and ATMs are deployed globally, with replacement cycles of 7 to 15 years. Upgrading terminal firmware for PQC requires not just software development but re-certification under PCI PTS. Mastercard's Enhanced Contactless (Ecos) specification addresses the card constraint by using AES symmetric encryption for quantum resistance in the contactless interface, sidestepping asymmetric PQC on constrained hardware. This protects the contactless transaction channel but does not address offline data authentication (which relies on asymmetric signatures on the chip) or EMV certificate chains. EMVCo has established a quantum working group to assess PQC impact on EMV specifications, but no definitive updates have been published as of June 2026.

> **Framework Impact:** Phase 4 (Roadmap) must incorporate hardware refresh cycles for cards and terminals as hard constraints on migration timelines. Phase 5 must include a triage strategy separating online authentication (protectable with symmetric cryptography now) from offline data authentication (dependent on asymmetric PQC on constrained hardware). Phase 1 must inventory the card and terminal estate by chip generation, RAM capacity, and PQC feasibility.

Challenge 4: Settlement Latency and Performance

BIS Project Leap Phase 2 provided the first empirical evidence of PQC performance impact on production-grade settlement infrastructure.

BIS Project Leap Phase 2 Performance Data

Software-based PQC signature verification on T2 averaged 209.9 milliseconds compared to 28.1 milliseconds for RSA, a 7.5× slowdown. The test used pre-standard CRYSTALS-Dilithium category 3 signatures on ISO 20022 liquidity transfer orders. ML-DSA-65, the closest standardized NIST analogue, has a slightly larger signature (3,309 bytes versus the 3,293 bytes tested), but the performance implications are comparable. At peak throughput on a system processing thousands of transactions per second, each carrying an enlarged PQC certificate chain, the aggregate bandwidth and compute overhead is substantial. RTGS systems (T2, Fedwire, BOJ-NET, CHAPS), real-time payment networks (FedNow, TIPS, Faster Payments, UPI), and high-frequency trading venues all operate within tight latency budgets where PQC overhead must be engineered out through hardware acceleration or architectural changes.

Certificate Chain Overhead and Hardware Acceleration

PQC certificate chains compound the signature size problem. A three-level certificate hierarchy with ML-DSA-65 adds approximately 20 KB of overhead per chain validation. Hardware-accelerated PQC (via FPGA or ASIC in next-generation HSMs) will narrow the performance gap, potentially by an order of magnitude. However, hardware-accelerated PQC modules must themselves pass through FIPS/PCI certification before production deployment, adding the certification bottleneck to the performance optimization path.

> **Framework Impact:** Phase 6 (Infrastructure) must include settlement-system-specific performance benchmarking. Phase 5 (Pilots) should prioritize RTGS and real-time payment interfaces for early PQC testing.

Challenge 5: SWIFT Dependencies and Cross-Border Coordination

SWIFT is the backbone of cross-border payment messaging, connecting over 11,000 institutions in more than 200 countries. SWIFT's PQC migration timeline directly constrains every organization connected to the SWIFT network. This challenge section provides the detailed SWIFT dependency analysis that payment organizations need for planning.

SWIFT Customer Security Programme and PQC

SWIFT's Customer Security Programme (CSP) establishes mandatory and advisory security controls for all SWIFT-connected institutions. The CSP's mandatory controls include requirements for securing the local SWIFT infrastructure (operator workstations, Alliance Gateway/Lite2 software, HSMs used for message signing), managing credentials, and hardening the operating environment. As SWIFT transitions to PQC, these mandatory controls will likely be updated to include PQC requirements for message authentication and channel encryption. Organizations should monitor CSP updates for PQC-specific control additions and assess their current CSP architecture for PQC readiness.

SWIFT Alliance Architecture and PQC Readiness

SWIFT-connected institutions typically operate SWIFT Alliance Gateway (for larger institutions) or Alliance Lite2 (for smaller institutions). Both products handle message encryption, signing, and PKI certificate management. PQC migration for SWIFT connectivity requires updates at multiple layers: the Alliance software itself (SWIFT's responsibility to update), the HSMs used for message signing (the institution's responsibility, subject to HSM vendor certification timelines), the PKI certificates used for authentication (requiring coordinated certificate rotation with SWIFT's CA hierarchy), and the network connectivity layer (TLS for IP-based SWIFT access).

Organizations should inventory their SWIFT Alliance deployment model, identify the HSMs used for SWIFT message signing, verify the firmware's PQC capability, and assess the certificate management process for PQC certificate handling. For institutions using Alliance Gateway in a high-availability configuration, the PQC migration must be coordinated across primary and backup sites.

SwiftNet 8.0 Migration Planning

SWIFT has announced that SwiftNet 8.0 is being designed as PQC-enabled, with industry communications indicating a target introduction around 2027 and a migration window on the order of 12 to 18 months for member institutions. This provides a concrete external milestone. Key planning considerations include: whether the institution's current Alliance Gateway/Lite2 version supports PQC (or requires an upgrade), whether the institution's SWIFT-facing HSMs can generate and use PQC keys within the FIPS-validated boundary by 2027, and whether the institution's message-handling systems can process PQC-signed ISO 20022 messages with enlarged signature payloads. Organizations should register for SWIFT PQC pilot programs as they become available and conduct readiness assessments against the SwiftNet 8.0 requirements as soon as SWIFT publishes detailed specifications.

SWIFT PKI and Certificate Management

SWIFT operates its own PKI hierarchy for message authentication. Member institutions receive certificates from SWIFT's CA and use them for message signing and mutual TLS authentication. The transition from classical to PQC certificates in SWIFT's PKI requires coordinated action: SWIFT must update its root and intermediate CA certificates to PQC, member institutions must deploy the new PQC certificates on their Alliance infrastructure, and message verification logic must be updated to handle PQC signatures. BIS Project Leap demonstrated that this certificate provisioning is a real operational challenge: a valid PQC-signed message failed settlement because the corresponding PQC CA certificate was missing from T2's static reference data.

The Correspondent Banking Chain

Beyond SWIFT, cross-border payments traverse the originating bank, its correspondent bank, the receiving correspondent bank, and the beneficiary bank, with one or more central bank RTGS systems for settlement. Each entity operates independent cryptographic implementations with independent PKI hierarchies. Card networks (Visa, Mastercard) operate their own CAs and will set independent PQC migration timelines. Domestic payment schemes (ACH, SEPA, Faster Payments, BACS, UPI, PIX) operate under national governance with their own adoption timelines. No coordination mechanism exists to synchronize PQC migration across all of these independent entities.

> **Framework Impact:** Phase 0 (Executive Mandate) must establish cross-industry coordination mechanisms from the outset. Phase 4 (Roadmap) must map SWIFT, card network, domestic scheme, and central bank timelines as hard constraints. Phase 7 must include strategic-level engagement with SWIFT on SwiftNet 8.0 requirements and timeline.

Challenge 6: PCI Standards and Payment Security Requirements

The PCI Security Standards Council (PCI SSC) maintains several standards that intersect with PQC migration. While PCI SSC has not published standalone PQC guidance as of June 2026, multiple PCI standards create both compliance drivers and migration constraints for payment organizations.

PCI DSS v4.0 and Cryptographic Documentation

PCI DSS v4.0 Requirement 12.3.3 (effective March 2025) mandates that PCI-scoped entities document all cryptographic cipher suites and protocols in use, with annual review. This requirement already creates a compliance driver for Phase 1 (Discovery) and Phase 2 (CBOM), because a thorough PCI 12.3.3 assessment will surface the quantum-vulnerable algorithms in use. Organizations should structure their cryptographic inventory to satisfy both PCI 12.3.3 and PQC readiness assessment simultaneously.

Requirement 3.5.1 mandates that Primary Account Numbers (PANs) are secured with strong cryptography wherever stored. As quantum computing advances, the definition of “strong cryptography” will evolve. Organizations should anticipate that PCI SSC will eventually update its cryptographic guidance to reflect PQC requirements, and prepare accordingly.

PCI PIN Security and DUKPT Key Hierarchy

PCI PIN Security requirements govern the handling of cardholder PINs, including PIN block encryption, PIN translation between encryption zones, and the key management hierarchies that protect PIN data in transit. The Derived Unique Key Per Transaction (DUKPT) key management scheme, widely used for PIN encryption at the point of sale, derives per-transaction keys from an initial key loaded during terminal manufacturing. DUKPT uses TDEA (Triple DES) or AES as its underlying cipher. While AES-based DUKPT is quantum-resistant (symmetric cryptography is not vulnerable to Shor’s algorithm), many terminal populations still use TDEA-based DUKPT, which faces deprecation under PCI PIN Security requirements regardless of quantum considerations. Organizations must track the intersection of PCI’s TDEA deprecation timeline with their PQC migration timeline, as both require key hierarchy updates at the terminal and HSM layers.

PCI 3-D Secure and E-Commerce Authentication

3-D Secure (3DS) is the protocol used for cardholder authentication in e-commerce transactions (Visa Secure, Mastercard Identity Check, AmEx SafeKey). 3DS 2.0+ uses digital signatures and TLS for communication between the merchant, the card network's directory server, and the issuer's access control server. The cryptographic dependencies span multiple organizations: the card network operates the directory server, the issuer operates the ACS, and the merchant's payment service provider integrates the client-side SDK. PQC migration for 3DS requires coordinated action across all three parties, following the same N-party synchronization pattern as other payment channel migrations. Organizations should inventory their 3DS infrastructure during Phase 1 and include it in Phase 7 vendor governance.

PCI Point-to-Point Encryption (P2PE)

PCI P2PE solutions encrypt cardholder data at the point of interaction (the terminal) and decrypt it only in a secure decryption environment (the HSM), eliminating exposure of cleartext cardholder data throughout the payment chain. P2PE implementations use asymmetric cryptography for key distribution and symmetric cryptography for bulk data encryption. The asymmetric key distribution layer is quantum-vulnerable. Organizations operating validated P2PE solutions should assess whether the key distribution mechanism uses RSA or ECC (quantum-vulnerable) or AES key wrapping (quantum-resistant), and plan accordingly.

> **Framework Impact:** Phase 1 (Discovery) must include PCI-scoped systems as a priority inventory track, structured to satisfy both PCI 12.3.3 and PQC readiness. Phase 3 (Risk Scoring) must account for PCI compliance dependencies when prioritizing migration. Phase 7 (Vendor Governance) must include 3DS network providers and P2PE solution providers in vendor PQC readiness assessment.

Challenge 7: Real-Time Payment Systems

Real-time payment (RTP) systems have proliferated globally over the past decade: FedNow (United States, launched 2023), TIPS (Euro area), Faster Payments (UK), UPI (India, processing over 10 billion transactions per month), PIX (Brazil), and dozens of others. These systems operate 24/7/365 with settlement finality in seconds, creating specific PQC migration constraints.

Continuous Availability and Migration Windows

Unlike batch-settlement systems that have overnight processing windows, RTP systems run continuously. Traditional migration approaches that rely on scheduled downtime are not available. PQC migration for RTP must be executed through rolling upgrades with hybrid cryptography, maintaining backward compatibility throughout the transition. Any

performance degradation from PQC overhead is felt immediately and continuously, not just during batch processing windows.

Latency Sensitivity at Scale

RTP systems impose end-to-end processing time limits that are tighter than RTGS systems. UPI processes over 10 billion transactions per month with sub-second settlement. FedNow targets settlement in under 5 seconds. The PQC performance overhead observed in Project Leap (7.5× for software-based signature verification) would need to be reduced significantly through hardware acceleration before production deployment on high-volume RTP systems. Organizations participating in RTP schemes should benchmark PQC performance against their specific scheme's latency requirements.

> **Framework Impact:** Phase 5 (Pilots) should include RTP interface testing with PQC to measure real-world latency impact. Phase 6 (Infrastructure) must include RTP-specific hardware acceleration planning.

Challenge 8: Tokenization as Interim Quantum Defense

Payment infrastructure makes extensive use of tokenization, providing a structural advantage for quantum resilience that most other sectors lack.

Why Tokenization Reduces Quantum Exposure

Tokenization replaces sensitive data (card PANs, account numbers, personal identifiers) with cryptographically irreversible tokens. The token-to-value mapping is protected by AES symmetric cryptography, which is not vulnerable to Shor's algorithm (Grover's algorithm provides only a quadratic speedup, addressed by using AES-256). Tokenized data harvested for future quantum decryption yields only meaningless token values. However, the token vault, detokenization APIs, key-management layer, logs, and any systems that still process cleartext data remain in scope for PQC migration. Treat tokenization as a risk-reducing control and scope reducer, not a substitute for PQC migration. Card issuers, payment processors, and acquirers that have deployed tokenization broadly should quantify what percentage of their sensitive payment data is already quantum-defended. This assessment provides an immediate win for Phase 3 risk scoring.

Format-Preserving Encryption Caveat

Some tokenization implementations use format-preserving encryption (FPE) rather than true tokenization with a vault. FPE (typically based on FF1 or FF3-1, using AES as a building block) preserves the format of the original data. While AES itself is quantum-resistant, the security properties of FPE schemes under quantum attack are less well-

studied than AES in standard modes. Organizations using FPE should assess whether their specific implementation retains adequate security margins under quantum threat models.

> **Framework Impact:** Phase 3 (Risk Scoring) should incorporate tokenization coverage as a risk-reducing factor. Phase 5 should include a tokenization coverage assessment as an early action.

Challenge 9: Mobile and Digital Wallet Cryptography

Mobile payments and digital wallets introduce a distinct cryptographic surface. Mobile payment apps implement multiple layers of cryptography: TLS for API communication, certificate pinning for MITM prevention, local data encryption using the device keystore or secure element, biometric template protection, and application-level token generation. The TLS layer benefits from browser and OS-level PQC adoption, but application-level cryptography depends on the app developer's own migration.

Secure Element (SE) and Trusted Execution Environment (TEE) hardware used for payment credential storage faces similar constraints to payment cards: limited memory, limited processing power, and chipset vendor dependency (Qualcomm, Samsung, Apple). Certificate pinning configurations in mobile payment apps require updates when server certificates transition to PQC, creating a coordination requirement between server-side PQC deployment and client app updates.

Payment authentication itself is moving onto this surface: payment passkeys (FIDO credentials used in 3DS flows and Click to Pay) are replacing OTPs at scale, and each enrolled passkey is a long-lived ES256/P-256 credential. Universal Framework v2.1 places the identity stack explicitly in Track B; the Alignment section of this extension maps the payment-specific implications, including the credential re-enrollment question for ACS and wallet vendors.

> **Framework Impact:** Phase 1 must include mobile payment app cryptographic dependencies as a distinct inventory track. Phase 5 must coordinate server-side PQC deployment with mobile app update cycles. Phase 7 must include mobile platform vendors as dependencies for SE/TEE PQC support.

Challenge 10: ATM Network Security and Remote Key Loading

ATMs represent a distinct PQC challenge within the terminal estate. ATM networks use asymmetric cryptography for remote key loading (RKL), host-to-ATM communication authentication, and software update verification. TR-34, the certificate-based asymmetric remote key loading protocol, uses RSA or ECDSA for key transport and is

quantum-vulnerable. TR-31 is a symmetric key-block format for protecting keys in storage and transport; it is not an asymmetric protocol and should be inventoried separately under symmetric key management. The installed ATM base has a typical replacement cycle of 10 to 15 years, and many ATMs run on hardware platforms that cannot support PQC key sizes or computational requirements.

Organizations should inventory their ATM fleet by model, processor capability, and RKL protocol version during Phase 1. ATMs capable of firmware-based PQC updates should be identified and prioritized. For ATMs that cannot support PQC, the fallback strategy may include physical key injection (reverting from remote to manual key loading) or accelerated hardware replacement.

> **Framework Impact:** Phase 1 (Discovery) must include ATM network cryptographic dependencies and RKL protocol versions. Phase 4 (Roadmap) must incorporate ATM replacement cycles as hardware constraints.

ALIGNMENT WITH UNIVERSAL FRAMEWORK V2.1

The Universal Framework v2.0 introduced structural changes with specific implications for payment infrastructure, and v2.1 added positions and sections that payment organizations need to map onto their programs. This section covers both: the three v2.0 foundations below, followed by the v2.1 positions that require payment-specific adaptation. The remaining Universal v2.1 additions (the data-at-rest decision framework in Activity 5.6, the AI-assisted migration position in 5.7 with its Phase 1 tool category, cloud and SaaS shared responsibility in 7.7, the Accelerated Execution Profile in 4.7, the risk-weighted coverage KPI, algorithm sovereignty and standards fragmentation, crisis communications, the skills matrix, and Appendices G and H) are sector-neutral and apply to payment organizations as written. One cross-reference matters: the Universal's counterparty coordination pattern (Activity 7.6) is the general case of the scheme, network, and SWIFT coordination this extension already specifies; where the two overlap, this extension's guidance governs.

Two-Track Migration Model in Payments

Track A (Confidentiality / Key Exchange): SWIFT messaging channel encryption, correspondent banking host-to-host connections, payment API TLS endpoints, acquirer-to-processor connections, and card network management links. This track addresses HNDL.

Track B (Integrity / Signatures / PKI): ISO 20022 Business Application Header signatures, RTGS settlement instruction authentication, card network CA hierarchies, EMV offline data authentication signatures, and payment HSM root key signing. Note that symmetric MACs (including SWIFT message authentication), PIN translation keys, and DUKPT hierarchies are critical inventory items but should be tracked under symmetric key management rather than grouped with Shor-vulnerable public-key signatures. This track addresses TNFL.

Payment organizations should start Track A immediately (hybrid key exchange on SWIFT connections, payment APIs, and acquirer links) and launch Track B within 90 days. Both tracks should run as parallel workstreams with separate milestones, because their dependency profiles differ: Track A is largely within the organization's control, while Track B depends heavily on external parties (card networks, SWIFT, central banks).

FIPS Validation Gap Impact on Payments

Payment infrastructure operates predominantly in FIPS-required or FIPS-aware environments. The absence of FIPS 140-3 validated PQC modules (earliest expected mid-2027) directly constrains production HSM deployment timelines. Payment organizations should classify their systems using the Universal Framework's four-level environment classification (Unrestricted, FIPS-aware, FIPS-required, CNSA 2.0) and sequence migration accordingly. The FIPS 140-2 sunset on September 21, 2026 adds urgency: payment organizations must plan their FIPS 140-3 migration alongside their PQC migration, and the two timelines intersect at the HSM layer.

Merkle Tree Certificates for Payment Web Infrastructure

For public-facing payment portals, merchant-facing APIs, and consumer-facing digital wallet endpoints, Merkle Tree Certificates (MTCs) are the emerging preferred path for post-quantum authentication in Chrome-trusted public Web PKI. Chrome has indicated it has no immediate plan to add traditional PQC X.509 certificates to the Chrome Root Store, and is instead developing MTC-based HTTPS certificates. Let's Encrypt has announced plans for an MTC staging environment in late 2026, with production-ready deployment expected in 2027. Payment organizations should invest in ACME-based certificate automation now. Internal payment PKI (SWIFT mTLS, HSM certificate chains, card network CA hierarchies) will continue on X.509 with PQC algorithms.

Hybrid and Composite Signatures Under Payment Message Constraints

Universal v2.1 takes the position that composite or dual signatures (classical plus PQC) are the default for Track B wherever toolchains support them, with solo ML-DSA treated as a recorded risk decision. Payments is where that position meets its hardest constraint: a composite signature is larger than the ML-DSA signature that already breaks ISO 8583 field limits and strained T2's buffers in Project Leap. The resolution is sequencing, not exemption. Where message formats are being revised anyway (ISO 20022 buffer work, BAH accommodation), engineer for composite from the start: the format revision is the gating effort, and carrying the classical component alongside ML-DSA is marginal once

buffers are being resized. Where dual certificates are operationally simpler than composite structures (settlement message signing, where Project Leap showed static reference data is the fragile layer), parallel dual-signing achieves the same defense-in-depth. Where neither fits (constrained EMV offline authentication, legacy formats pending revision) solo PQC deployment should be documented as a risk decision per the Universal position, with the implementation-maturity exposure that motivates hybrid weighed explicitly.

Algorithm Weighting and the EMV ECC Transition

Universal v2.1 introduces algorithm-specific vulnerability weighting in Phase 3: quantum attack cost scales with key size, not classical strength, so 256-bit ECC keys are at least as exposed as RSA-2048 and considerably more exposed than RSA-3072. Payments must read this against its own modernization path. The EMV specifications' addition of ECC as the successor to RSA for offline data authentication, 3DS signing on ES256, and P-256 credentials in wallets and secure elements are classical-security and performance wins that increase relative quantum exposure. Organizations mid-transition from RSA to ECC in EMV and card network infrastructure should not book that work as quantum progress, and should not deprioritize ECC-protected payment systems behind RSA-legacy ones in Phase 3 scoring. Record algorithm and key size per entry in the payment CBOM so the weighting applies mechanically.

The Identity Stack in Payments (Track B)

Universal v2.1 brings the identity stack explicitly into Track B scope, and payments is further along this curve than most sectors. Payment passkeys (FIDO credentials replacing OTPs in 3DS flows and Click to Pay) assert with ES256 on P-256: long-lived classical credentials being enrolled at scale right now. 3DS directory server and ACS signing, OAuth/OIDC token signing in payment APIs, wallet device-bound keys in secure elements, and terminal and ATM device certificates belong in the same Track B inventory slice. Two payment-specific actions follow: include the issuer ACS, wallet platforms, and passkey infrastructure in the identity CBOM slice during Phase 1, and put the credential migration question (how enrolled passkeys and device-bound keys will be re-enrolled or migrated when signature algorithms change) into Phase 7 vendor governance for ACS providers, wallet platforms, and authentication vendors.

SP 800-208 Firmware Signing: The Deploy-Now Track B Action

Universal v2.1 foregrounds stateful hash-based signatures (LMS and XMSS, NIST SP 800-208) as the component of Track B that deploys now, and nowhere does that matter more than in payments. Terminal and ATM fleets carry 7-to-15-year replacement cycles; the firmware update verification keys provisioned into hardware shipping today must survive into the CRQC era. LMS and XMSS are standardized, conservative, required by CNSA 2.0 for firmware signing, and already supported in payment-relevant HSM firmware (Utimaco's Quantum Protect supports LMS alongside ML-DSA). The action: move terminal, ATM, and HSM firmware signing pipelines to SP 800-208 signatures now, dual-signed with classical during transition, operated from HSM-backed signing infrastructure. The state-management constraint that makes these schemes unsuitable for general-purpose use is precisely satisfied by the controlled signing ceremonies payment organizations already run.

Securing the Payment CBOM

Universal v2.1's Activity 2.5 (Secure the CBOM and Program Artifacts) lands with particular force in payments. A complete payment CBOM maps HSM locations and key hierarchies, DUKPT-to-terminal-population relationships, unmigrated external interfaces, and the certificate chains that authenticate settlement: target selection done for free, for adversaries ranging from payment fraud operations to nation-states. PCI workflows widen the exposure: 12.3.3 documentation, QSA assessments, and acquirer or network due diligence all create standing requests for exactly this data. Apply Activity 2.5's controls with a payments addendum: assessors and counterparties receive point-in-time extracts scoped to their assessment, not standing access to the queryable inventory, and the CBOM repository joins the SOC's high-sensitivity exfiltration watch list.

Verification and Decommissioning in Multi-Party Payment Networks

Universal v2.1 adds a Migration Verification & Program Closure section, and payments needs its discipline more than most because configuration and reality diverge across counterparty boundaries. Verification in payments means observed negotiation on the wire: SWIFT connections, card network links, and payment APIs showing hybrid or PQC algorithms in production traffic, not in configuration files; and, once schemes set classical-refusal dates, negative testing that classical-only counterparties are actually refused. Decommissioning carries a payments-specific sting: retired EMV CA certificates and superseded signing keys persist in terminal trust stores for years, and a key is only retired when nothing trusts it. Plan trust-store cleanup across the terminal and ATM

estate as an explicit migration wave, and log key destruction with certificates for HSM-held material per the Universal evidence standard.

PHASE-BY-PHASE FRAMEWORK ADAPTATIONS FOR PAYMENTS

This section specifies the adaptations required for payment infrastructure for each Universal Framework phase. Organizations should implement these alongside the Universal Framework and the Financial Services Extension.

Phase 0 — Executive Mandate & Business Case

Payment-Specific Business Case Arguments

1. **Settlement disruption risk:** Reference BIS Project Leap Phase 2 findings to demonstrate that PQC works but introduces measurable performance overhead. The 7.5× signature verification slowdown on a system processing trillions of euros daily makes the case concrete.
2. **Systemic cascading-loss scenario:** The Citi Institute/Hudson Institute analysis estimated $2.0–3.3 trillion in indirect economic losses from a quantum attack on a top-five U.S. bank's Fedwire access, with a six-month recession driven by cascading liquidity failures.
3. **Regulatory convergence:** Map PCI DSS 12.3.3 (effective March 2025), G7 CEG roadmap (2030–2032), EU roadmap (2030 critical-sector), and SWIFT SwiftNet 8.0 (2027) into a single timeline showing inevitable investment.
4. **Hardware lead times:** HSM certification cycles (12–24 months), card reissuance (3–5 years for fleet turnover), and terminal replacement cycles (7–15 years) mean decisions deferred today constrain options for years.

Governance Adaptation for Payments

Payment PQC governance must include representation from acquiring operations, issuing operations, terminal management, HSM operations, SWIFT administration, and settlement operations, in addition to IT security and compliance. The Financial Services Extension's recommended Quantum Readiness Working Group should include a dedicated payments sub-group.

Phase 1 — Discovery & Inventory

Payment-Specific Inventory Tracks

In addition to the Universal Framework's three parallel inventory tracks and the Financial Services Extension's broader sector tracks, payment organizations should add:

1. **Payment message format analysis:** Inventory every format in use (ISO 8583, ISO 20022, SWIFT MT/MX, domestic scheme formats). Map field-level cryptographic dependencies and identify fixed-size fields that cannot accommodate PQC payloads.
2. **Payment HSM estate mapping:** Inventory all payment HSMs by model, firmware version, FIPS/PCI certification status, and vendor PQC roadmap. Classify each as PQC-ready, PQC-upgradeable, or PQC-blocked.
3. **Card and terminal estate:** Inventory card platforms by chip type, RAM capacity, supported algorithms. Map offline versus online authentication reliance by card program. Inventory terminals by firmware version and PCI PTS certification status.
4. **SWIFT infrastructure:** Inventory Alliance Gateway/Lite2 deployment model, SWIFT-facing HSMs, PKI certificates, and CSP control compliance. Assess compatibility with SwiftNet 8.0 PQC requirements.
5. **Third-party payment interfaces:** Map every external cryptographic interface: SWIFT, card network links, clearing house integrations, correspondent banking channels, payment APIs, 3DS directory server connections.
6. **Certificate authority hierarchies:** Map all CA hierarchies: internal PKI, card network CAs, SWIFT PKI, domestic payment scheme CAs, EMV CA hierarchies.
7. **PCI-scoped system cryptography:** Structure the inventory to satisfy PCI DSS 12.3.3 simultaneously, producing both PQC readiness assessment and PCI compliance evidence from the same data collection.
8. **ATM and remote key loading:** Inventory ATM fleet by model, RKL protocol version (TR-34, TR-31), and PQC hardware feasibility.

Phase 2 — CBOM & Documentation

Payment CBOM Complexity

Build the payment CBOM in concentric rings. The first ring documents cryptography the organization controls directly: HSM key material, internal application encryption, owned certificate hierarchies. The second ring documents vendor-consumed cryptography: payment HSM firmware implementations, card platform SDK functions, SWIFT Alliance software. The third ring documents dependencies on counterparties and networks: card network CA certificates, SWIFT PKI, RTGS authentication, correspondent bank channel encryption. The third ring will be incomplete, and that is acceptable.

PCI DSS 12.3.3 as CBOM Accelerator

PCI DSS 12.3.3 already mandates documentation of all cryptographic cipher suites and protocols for PCI-scoped entities. The CBOM effort should be structured to produce PCI 12.3.3 evidence artifacts as a standard output. This dual-use approach makes the CBOM investment immediately justifiable in compliance terms.

Phase 3 — Risk Scoring & Prioritization

Payment-Specific Risk Scoring Dimensions

In addition to the Universal Framework's four dimensions and the Financial Services Extension's systemic criticality and multi-party dependency dimensions, payments adds:

1. **Settlement chain position:** Systems at the RTGS or clearing layer carry higher systemic risk than systems at the acquirer or merchant interface layer.
2. **Hardware constraint severity:** Is migration blocked by hardware limitations (card chip RAM, terminal processor, HSM certification status)? Hardware-constrained systems require different remediation strategies.

Algorithm-specific weighting: Apply the Universal Framework v2.1 algorithm weighting (Activity 3.1): quantum attack cost tracks key size, not classical strength, so ECC-protected payment systems score at least as urgent as RSA-2048 estates. See the Alignment section for the EMV ECC transition implications.

Payment Infrastructure Priority Tiers

Priority	System Category	Rationale
Tier 1	SWIFT interfaces, RTGS/settlement connections, payment HSM root key material, correspondent banking encryption	Highest HNDL exposure, systemic criticality, regulatory visibility. External-facing with cross-border traffic exposure.
Tier 2	Card network CA hierarchies, external payment APIs, acquiring platform TLS, payment gateway connections, 3DS infrastructure	High HNDL and TNFL exposure. Multi-party coordination required. Consumer-facing reputational risk.
Tier 3	Internal payment service mesh, payment databases, transaction monitoring encryption, fraud detection data stores	Internally controlled. Migrable on organizational timeline without external dependencies.

Tier 4	Smart card offline authentication, legacy POS terminal cryptography, ATM RKL (legacy), archival payment message stores	Hardware-constrained. Dependent on vendor hardware refresh cycles. Plan now, execute on hardware availability.

Phase 4 — Roadmap & Governance

External Dependency Timeline Map

Payment roadmaps must incorporate external timelines that the organization does not control:

1. **SWIFT SwiftNet 8.0:** Being designed for PQC enablement, with a target introduction around 2027 and a migration window on the order of 12 to 18 months.
2. **Card network PQC timelines:** Visa and Mastercard CA migration timelines (not yet committed as of June 2026). EMV specification updates from EMVCo quantum working group.
3. **HSM vendor certification:** FIPS 140-3 Level 3 CMVP validation with PQC. Track Thales, Utimaco, Futurex, Entrust individually. PCI PTS HSM v4 certification with PQC.
4. **FIPS 140-2 sunset:** September 21, 2026. Organizations must complete FIPS 140-3 migration for existing HSMs on this timeline, independent of PQC.
5. **Smart card silicon:** IDEMIA/GlobalFoundries 28nm PQC-capable chips (targeted 2026). Infineon SLC38 and equivalent next-generation secure microcontrollers.
6. **Central bank RTGS upgrades:** T2, Fedwire, BOE RTGS, BOJ-NET modernization timelines for PQC adoption.
7. **Domestic payment schemes:** ACH, SEPA, Faster Payments, BACS, UPI, PIX scheme-level PQC adoption decisions.
8. **PCI SSC PQC guidance:** Expected but not yet published. Payment organizations should anticipate and prepare for compliance requirements.

Recommended Year-1 Plan for Payments

1. **Q1:** Establish payment PQC governance sub-group. Begin PCI 12.3.3 aligned cryptographic inventory on PCI-scoped payment systems. Initiate payment HSM vendor engagement. Commission SWIFT readiness assessment for SwiftNet 8.0.
2. **Q2:** Expand inventory to payment message format analysis (ISO 8583/20022 field-level mapping), card/terminal estate, ATM fleet, and 3DS infrastructure. Begin CBOM construction for Tier 1 systems. Conduct tokenization coverage assessment.
3. **Q3:** Complete Tier 1 risk scoring with payment-specific dimensions. Produce initial Quantum Readiness Assessment for board consumption. Begin Tier 1 pilot design

(SWIFT test interface or external payment API with hybrid ML-KEM-768 + X25519).

4. **Q4:** Execute first Tier 1 pilot in test environment. Establish external dependency timeline map. Produce Year-2 roadmap with budget for HSM hardware refresh and expanded pilot scope.

Phase 5 — Pilots & Migration Execution

Payment Pilot Targets

1. **External payment API with hybrid TLS:** Enable hybrid ML-KEM-768 + X25519 on a non-critical external payment API. Lowest-risk, highest-learning pilot.
2. **SWIFT test environment:** Pilot PQC message signing in non-production SWIFT environment. Measure ISO 20022 BAH signature size impacts and certificate distribution requirements.
3. **Settlement performance benchmarking:** Replicate BIS Project Leap methodology on your own infrastructure. Benchmark ML-DSA verification throughput at peak volumes.
4. **Payment HSM PQC key generation:** Pilot PQC key generation on test HSMs (even outside FIPS boundary). Validate key ceremony procedures and dual-key management.
5. **Internal payment service mesh:** Enable PQC in internal TLS mesh between payment microservices for production-scale performance data.

Tokenization Coverage Assessment

Before designing data-at-rest migration pilots, conduct a tokenization coverage assessment identifying which payment data categories are already quantum-defended, which use FPE warranting further analysis, and which remain exposed to HNDL. Expanding tokenization scope may be faster and cheaper than end-to-end PQC for certain data stores.

Hybrid Architecture Planning

BIS Project Leap revealed that hybridization in settlement systems was not envisaged in the original cryptographic design and requires substantial system evolution. Plan for hybrid as an architectural change requiring duplicate PKI infrastructure, extended certificate handling, modified verification logic, expanded message format buffers, and updated static reference data at all counterparties. The hybrid period will last years and must be managed as a sustained operational state.

Phase 6 — Infrastructure Modernization & Performance

Payment HSM Modernization Strategy

1. **Firmware versus hardware replacement:** Classify the HSM estate. Newer HSMs (Thales payShield 10K with post-2024 firmware, Utimaco CryptoServer with Quantum Protect, Futurex CryptoHub) may be firmware-upgradeable. Older units require hardware replacement with 12 to 24 month lead times.
2. **FIPS/PCI certification gap management:** Document compliance risk of running PQC outside FIPS boundary. Prepare risk acceptance memos. Track FIPS 140-3 and PCI PTS HSM v4 certification as two independent dependencies.
3. **Key ceremony adaptation:** PQC key generation requires updated procedures for HSM root keys and PIN translation master keys. Rehearse in test environments before production.
4. **Dual-key management:** During hybrid transition, HSMs must manage both classical and PQC key material. This doubles key storage and complicates lifecycle management.

Settlement Performance Benchmarking

1. **Signature verification throughput:** Benchmark ML-DSA at peak volumes. Use Project Leap 7.5× as software baseline. Test with hardware acceleration.
2. **Certificate chain validation:** Test full PQC chain validation including OCSP/CRL with enlarged certificates.
3. **Network bandwidth impact:** Model bandwidth increase from PQC signatures and certificates at peak volumes. Include archive storage growth projections.
4. **End-to-end transaction timing:** Measure complete transaction lifecycle (authorization, clearing, settlement) with PQC at each stage.

Phase 7 — Vendor & Supply Chain Governance

Payment-Specific Vendor Classification

Vendor Category	Examples	Engagement Approach
Network operators	SWIFT, Visa, Mastercard, domestic schemes (ACH, SEPA, Faster Payments), central bank RTGS operators	Strategic C-suite engagement. Participate in forums and pilots. Align roadmap to published timelines.
Payment HSM vendors	Thales (payShield), Utimaco (Atalla, CryptoServer), Futurex (CryptoHub), Entrust (nShield)	Quarterly PQC roadmap reviews. Separate FIPS 140-3 and PCI PTS tracking. Early PQC firmware access.

Card and terminal vendors	IDEMIA, Thales, G+D, Ingenico/Worldline, Verifone, PAX Technology	Monitor PQC chip availability. Track EMVCo quantum WG. Plan terminal replacement cycles.
Payment processors	Fiserv, FIS, Global Payments, Adyen, Stripe, Worldpay, ACI Worldwide	PQC readiness questionnaires. Message format testing. Hybrid TLS interoperability validation.
Digital wallet platforms	Apple Pay, Google Pay, Samsung Pay, PayPal, regional wallets	Monitor platform PQC adoption. Coordinate certificate pinning updates.

Industry Coordination Forums

1. **BIS Innovation Hub:** Central bank PQC experiments (Project Leap successors). Early insight into RTGS timelines.
2. **EMVCo Quantum Working Group:** PQC specifications for EMV chip authentication and certificate hierarchies.
3. **X9 Accredited Standards Committee:** PQC in financial messaging (ISO 8583, ISO 20022 accommodation).
4. **SWIFT PQC program:** SwiftNet 8.0 preparation. Sandbox and pilot participation.
5. **PCI SSC:** Monitor for standalone PQC guidance (expected but not yet published).
6. **Europol QSFF / FS-ISAC:** Cross-sector coordination and prioritization frameworks.

PAYMENTS REGULATORY ALIGNMENT MAP

Payment infrastructure faces regulatory requirements from multiple overlapping bodies. The following table maps key requirements to framework phases. For the broader financial services regulatory map, see the Financial Services Extension.

Regulatory Body / Standard	Key Requirement	Timeline	Framework Phase(s)
PCI DSS v4.0 Req 12.3.3	Document and annually review all cryptographic cipher suites and protocols	Effective March 2025	Phase 1, Phase 2
PCI PIN Security	PIN block encryption and DUKPT key management requirements; TDEA deprecation	Ongoing; TDEA phase-out active	Phase 1, Phase 6
PCI PTS HSM v4	Payment HSM security requirements; PQC inclusion pending	Current; PQC timing TBD	Phase 6, Phase 7
SWIFT CSP / SwiftNet 8.0	PQC-enabled messaging; participant migration requirements	Target around 2027; 12-to-18-month migration window	Phase 5, Phase 7
G7 CEG Roadmap	Six-phase financial sector quantum readiness	2030–2032 target	Phase 0, Phase 4
EU Coordinated Roadmap	Critical financial infrastructure quantum-safe	End of 2030	Phase 0 through Phase 5

EMVCo Quantum Working Group	PQC for EMV chip authentication and certificates	Ongoing; no published timeline	Phase 4, Phase 5
BIS/CPMI	Central bank quantum readiness for payment systems	Ongoing (Project Leap model)	Phase 0, Phase 6
NIST IR 8547	Deprecate RSA/ECC at 112-bit after 2030; disallow after 2035	2030/2035	Phase 3, Phase 4
FIPS 140-2 Sunset	FIPS 140-2 certificates move to CMVP Historical List. New deployments should use FIPS 140-3; historical modules may still be used for existing systems per agency policy.	September 21, 2026	Phase 6
Europol QSFF	Prioritization scoring for financial services PQC migration	Published January 2026	Phase 3

PCI SSC has not published standalone PQC guidance as of June 2026. Requirement 12.3.3 mandates cryptographic documentation (which surfaces quantum vulnerability) but does not mandate remediation. Payment organizations should anticipate that PCI SSC PQC guidance will follow and build their processes to produce the evidence artifacts that future requirements will demand.

PAYMENTS MATURITY MODEL SUPPLEMENT

The Universal Framework's 5-level maturity model applies. The following table provides payment-infrastructure-specific indicators.

Level	Universal Indicator	Payment Infrastructure Indicator
1 — Aware	Quantum risk acknowledged; no formal program	No inventory of payment HSMs, card platforms, or message format cryptographic dependencies. No engagement with SWIFT, card networks, or EMVCo on quantum readiness. PCI 12.3.3 compliance may be ad hoc.
2 — Assessed	Cryptographic inventory underway; initial risk assessment completed	Payment HSM estate mapped by model, firmware, and certification status. Message formats analyzed for PQC payload constraints. SWIFT and card network PQC readiness assessed. Tokenization coverage quantified. Initial QRA produced.
3 — Planning	Roadmap established; pilots designed; governance operational	External dependency timeline map maintained (SWIFT, card networks, HSM vendors, central banks). Year-1 plan in execution. HSM vendor PQC reviews quarterly. Industry forum participation active.
4 — Migrating	Pilots in production; wave-based migration underway	Hybrid PQC on Tier 1 systems (SWIFT, external APIs). Payment HSM PQC in validated or risk-accepted mode. Card/terminal migration aligned to silicon availability. Settlement performance benchmarked.
5 — Resilient	Crypto-agility achieved; algorithm transitions routine	All payment channels quantum-safe or hybrid. Payment HSMs FIPS + PCI PTS validated with PQC. Card platforms PQC-capable. Full CBOM exchange with network operators. Algorithm rotation without program effort.

PAYMENTS KPI SUPPLEMENT

The following additional KPIs are recommended for payment organizations, supplementing the Universal Framework and Financial Services Extension KPIs.

Board-Level KPIs (Quarterly)

1. **Payment HSM PQC readiness:** Percentage of payment HSMs with PQC-capable firmware installed / total estate. Track separately for FIPS-validated and non-validated capability.
2. **External payment interface quantum exposure:** Number of external payment interfaces (SWIFT, card network, payment APIs) without PQC protection / total external interfaces.
3. **Settlement PQC performance baseline:** PQC signature verification latency as a multiple of classical baseline (target: converging toward 1× through hardware acceleration).
4. **HNDL data-at-risk volume:** Payment data in transit across external interfaces with >10-year confidentiality requirements, not yet PQC-protected or tokenized.

Operational KPIs (Monthly)

1. **Payment vendor PQC roadmap alignment:** Critical payment vendors with confirmed PQC roadmaps / total critical payment vendors.
2. **Message format PQC readiness:** Payment message formats analyzed for PQC accommodation / total formats in active use.
3. **Tokenization coverage:** Percentage of high-sensitivity payment data categories protected by tokenization.
4. **Card/terminal fleet PQC readiness:** Percentage of estate with PQC-capable hardware / total estate. Long-term fleet turnover metric.

RECOMMENDED IMMEDIATE ACTIONS

For payment organizations at Maturity Level 1 (Aware) or Level 2 (Assessed), the following actions can begin immediately and do not depend on external vendor readiness.

#	Action	Timeline	Phase
1	Map the complete payment HSM estate by model, firmware, FIPS/PCI certification status, and vendor PQC roadmap. Initiate vendor engagement on PQC firmware and certification timelines.	0–3 months	Phase 1/7
2	Inventory all payment message formats (ISO 8583, ISO 20022, SWIFT MT/MX, domestic formats) and map field-level cryptographic dependencies.	0–3 months	Phase 1
3	Conduct tokenization coverage assessment to quantify which payment data is already quantum-defended.	0–3 months	Phase 3/5
4	Assess SWIFT interface readiness for SwiftNet 8.0. Register for SWIFT PQC pilot programs. Review Alliance Gateway/Lite2 for PQC compatibility.	0–6 months	Phase 5/7
5	Inventory card/terminal estate by chip generation, RAM capacity, PQC feasibility, and replacement cycle.	0–6 months	Phase 1/4
6	Inventory ATM fleet by model, RKL protocol version, and PQC hardware feasibility.	0–6 months	Phase 1
7	Structure PCI 12.3.3 cryptographic inventory to simultaneously produce PQC readiness assessment.	0–3 months	Phase 1/2

8	Join BIS Innovation Hub, EMVCo quantum WG, X9, SWIFT PQC program, and FS-ISAC/Europol QSFF.	0–3 months	Phase 0/7
9	Enable hybrid PQC (ML-KEM-768 + X25519) on at least one external payment API endpoint.	3–9 months	Phase 5
10	Replicate BIS Project Leap settlement benchmarking on your own infrastructure.	3–9 months	Phase 6

FURTHER READING

The following PostQuantum.com articles provide detailed analysis supporting this extension:

1. **Payments and the Race to Quantum Safety — https://postquantum.com/post-quantum/payments-quantum-pqc/ —** Seven payments-specific PQC challenges with detailed technical analysis.
2. **BIS Project Leap Phase 2 — https://postquantum.com/security-pqc/bis-leap-2-pqc-payments/ —** Analysis of the first real-world PQC test on production payment settlement infrastructure.
3. **The Cryptographic Iceberg Inside a Mobile Banking Transaction — https://postquantum.com/post-quantum/cryptography-cbom-mobile-banking/ —** Layer-by-layer reconstruction of ~320 cryptographic function calls across 9 parties and 30,000+ unique functions.
4. **Cryptographic Stack in Modern Interbank Payment Systems — https://postquantum.com/post-quantum/cryptography-interbank-payment/ —** End-to-end cryptographic mapping from customer authentication through SWIFT to central bank settlement.
5. **Hybrid Cryptography for the Post-Quantum Era — https://postquantum.com/post-quantum/hybrid-cryptography-pqc/ —** Hybrid schemes in TLS, SSH, IPsec; standards alignment; pilot design.
6. **Infrastructure Challenges of Dropping In PQC — https://postquantum.com/post-quantum/infrastructure-challenges-pqc/ —** How PQC stresses real infrastructure: handshakes, cert chains, CPU/memory, middleboxes.
7. **Evaluating Tokenization in the Context of Quantum Readiness — https://postquantum.com/post-quantum/tokenization-quantum-readiness/ —** Tokenization as scope-reducer and blast-radius limiter.
8. **Rethinking CBOM — https://postquantum.com/post-quantum/rethinking-cbom/ —** Challenges the completeness model; proposes the Minimum Viable CBOM approach.
9. **120,000 Tasks: Why PQC Migration Is Enormous — https://postquantum.com/post-quantum/quantum-security-pqc-program-plan/ —** Why credibly planned programs reach six-figure task counts.

ABOUT

ABOUT THE AUTHOR

Marin Ivezic is a former Fortune Global 500 CISO/CTO, the Editor-in-Chief of PostQuantum.com, and the founder and CEO of Applied Quantum. He previously held cybersecurity partner and practice lead roles, including regional and global leadership positions, at IBM, Accenture, PwC, and KPMG. He is also the former CEO of Cyber Agency and the founder of Cryptosec, a cryptography advisory and engineering firm.

Marin has been involved in quantum technologies for over 25 years, having advised governments on the quantum threat since the early 2000s. He previously founded Boston Photonics and PQ Defense. He has led real-world quantum readiness programs for telecoms, financial institutions, and critical infrastructure operators, including programs exceeding 120,000 discrete migration tasks.

PostQuantum.com, his personal blog, reaches over 1 million monthly readers and is recognized as the premier quantum security publication for CISOs, CTOs, and security architects worldwide.

QUANTUM READY: THE COMPANION BOOK

Quantum Ready (QuantumReady.com) is the book-length companion to this framework, written by the same author. Where this document is deliberately methodology-grade (prerequisites, activities, outputs, decision logic). The book provides the complete treatment: the reasoning behind each phase, extended case examples from real migration programs, sector narratives, and guidance for leading the program from the first board conversation through closure. The two are maintained in alignment: the framework is updated as the field moves, and the book supplies the depth that a methodology document omits by design.

ABOUT APPLIED QUANTUM

Applied Quantum (AppliedQuantum.com) is a research-driven professional services firm focused entirely on quantum technologies and post-quantum security. Its dedicated security practice, Secure Quantum (SecureQuantum.com), focuses on quantum security

advisory and PQC migration. Services span Quantum Security & PQC Migration, Quantum Strategy & Sovereignty, Quantum Engineering & Implementation, and Quantum Commercialization.

If you need help: Applied Quantum provides advisory, program design, and hands-on migration execution support. Contact: contact@appliedquantum.com