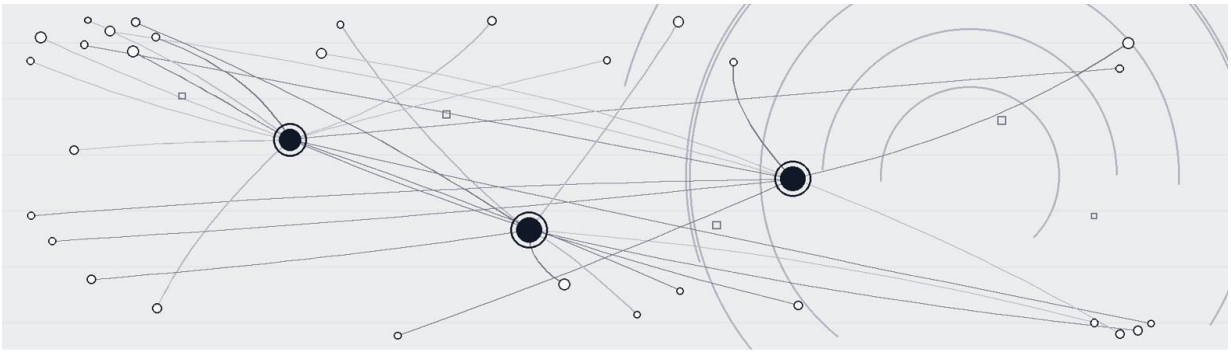
AUGUST 2026

APPLIED QUANTUM

THE APPLIED QUANTUM CRYPTOGRAPHIC CONCENTRATION FRAMEWORK

PAYMENTS EXTENSION



Card, interbank and settlement enumeration, with the worked example

Version 1.0-RC – August 2026

Steve Vaile and Marin Ivezic, Applied Quantum

Disclosure: Applied Quantum provides post-quantum migration advisory services. This work is published openly under CC BY 4.0 and is computable without engaging Applied Quantum.

"Switching vendors moves the contract, not the dependency."

COPYRIGHT AND LICENSE

DISCLAIMER

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

The regulatory instruments, certification records, standards and vendor capabilities referenced in this document reflect the state of the landscape as of August 2026, and that landscape moves. Readers should verify current status against primary sources (regulators and supervisory authorities, NIST, EMVCo and PCI SSC, the CycloneDX specification, public certification listings, vendor documentation) before making decisions.

References to specific vendors, products or tools are for illustrative purposes and do not constitute endorsement.

This is a v1.0 release candidate: v1.0 final publishes in November 2026 after a pilot cycle. Open items are public on the roadmap at CCFramework.org, and corrections are published as dated entries on its errata page.

ABOUT THIS DOCUMENT

Document type	Sector extension to the CCF Universal Framework
Parent document	The Cryptographic Concentration Framework – Universal – v1.0-RC (August 2026)
Intended audience	Risk analysts assessing card, interbank and settlement services, and the payments-infrastructure specialists supplying them with data
Assumed knowledge	The Universal Framework and its phase definitions; familiarity with payments infrastructure and scheme arrangements
Scope	Payments-specific enumerations for the six layers, the payments consequence-threshold template, and the card-authorisation worked example. Not a standalone document – used alongside the Universal

	Framework.
Status	Version 1.0-RC – release candidate; v1.0 final November 2026 after pilot

VERSION HISTORY

Version	Date	Changes
1.0-RC	August 2026	First public release, as a release candidate; drafted through four external review rounds and a family-wide line-edit pass.
1.0-RC	7 September 2026	Layer 4 and 6 notes aligned to Universal C.3; A.7 lists the unit counts behind every layer, computed by the reference implementation, and names all four counterparty routes. No figure changed.
1.0-RC	8 September 2026	A.7 reports the largest failure domain per layer, including standalone units, and states the layer-6 evidenced figure as the largest point's own design. Prose revised throughout. No figure changed.

HOW TO USE THIS DOCUMENT

This document is a companion to the CCF Universal Framework. It does not replace it: for each service family it enumerates what to examine and maps the findings onto the Universal's phases, units and determinations. Readers should have the Universal Framework open alongside this document and cross-reference its phase definitions, evidence standards and templates.

ACCOMPANYING RESOURCES

The framework family publishes at CCFramework.org: the Universal Framework, the Payments and Financial Services extensions, the payments whitepaper, the CBOM Conformance Statement, the Technical Companion and the instruments, together with the public roadmap, the errata and corrections page, the provenance survey and the frontier-census methodology.

Every canonical figure in the family comes from the reference implementation, with ten canonical test vectors that fix each one exactly. Both are open under Apache-2.0 on the Applied Quantum GitHub, and any implementation that reproduces the fixtures is conformant.

The Applied Quantum CBOM Profile, the input data contract, publishes at CBOMProfile.org. The Applied Quantum PQC Migration Framework, whose sector taxonomy the extensions follow, publishes at PQCFramework.org. Practitioner background and adjacent analysis sits on PostQuantum.com, as further reading rather than a normative source.

TABLE OF CONTENTS

Requires the CCF Universal Framework **v1.0-RC.** This extension names what to enumerate at each of the six layers for payments. It does not restate the computation, the interpretation bands, or the reporting rules, which are defined in the Universal Framework and do not change between sectors.

A.1 SERVICES IN SCOPE

The services in scope are card authorisation and clearing; PIN acceptance and translation; cross-border messaging; high-value settlement access; instant and batch credit transfer; tokenisation and credential provisioning; and merchant settlement.

An institution operating both payments and broader banking applies the Payments and Financial Services extensions to their own service lists without merging them. The four counterparty classes are common to both extensions, but their membership differs.

Use this extension for card issuers and acquirers, processors, payment service providers, payment gateways and payment-infrastructure functions. It identifies the assets, trust relationships, counterparties and operational questions commonly relevant to those services. It does not create different concentration equations or relax the Universal Framework's evidence and reporting requirements.

Define the service at a business-operational boundary. Card authorisation, merchant acceptance, payment submission, clearing and settlement can have different owners, dependencies and tolerances. A processor may include submission of settlement instructions in a wider service, but must not thereby imply that it operates the settlement system or determines legal finality itself.

The inventory should identify the relevant persistent keys, certificates, endpoint/configuration assets and issued estates. Select the counted classes explicitly and retain their relationships. A POS device, its unique key and a certificate are not automatically three independent exposures; nor is a shared certificate copied into every terminal automatically thousands of distinct certificates. Universal Annex 2 governs counting.

A.2 WHAT TO ENUMERATE AT EACH LAYER

Layer 1 – Algorithm

Include quantum-vulnerable public-key material only: RSA in EMV certificate hierarchies and issuer keys, elliptic-curve material on TLS and scheme links, Diffie–Hellman in key establishment, and asymmetric wrapping over symmetric key estates. Exclude TDEA

and AES in PIN-block and DUKPT operations from the layer-1 denominator and report them in the estate profile.

Layer 2 – Implementation lineage

Enumerate the cryptographic library executing in the authorisation switch, cryptographic modules inside HSM firmware, terminal libraries and payment SDKs, TLS stacks on acquirer, issuer and scheme links, and modules within processor and gateway platforms. Identify the executing family for each operation and resolve each implementation to its upstream ancestor. Keep the executing-family assignment distinct from the shared-code relationships used for reach.

Before migration, this measures classical lineage and establishes the baseline for later comparison.

Layer 3 – Trust root

Enumerate scheme certificate authorities operated by Visa, Mastercard, American Express, Discover, JCB and UnionPay; SWIFT PKI; the relevant central bank RTGS PKI; the institution's own issuing authorities; and public roots on externally facing paths. Establish which anchor is accepted for the specified function and distinguish withdrawal from compromise when determining its effect.

EMV key horizon. Visa has extended its production 1984-bit CA key to 31 December 2029, following EMVCo's annual RSA key-length assessments. EMVCo records that NIST will not support EMV's longest RSA key length, 1984 bits, after 2030.

Issuer keys minted now remain on cards for their multi-year life, including time beyond that horizon. Record expiry against the deprecation horizon. Every such asset triggers criticality test 4.

Planning horizons. EMVCo's published position is that quantum computing is not expected to threaten the EMV infrastructure until at least 2040. The G7 Cyber Expert Group, NIST and the UK NCSC work to horizons between 2030 and 2035. Record the horizon against which each service is planned.

EMVCo's ECC guidance describes the introduction of elliptic-curve support and states that EMVCo does not mandate the use of encryption standards. ECC remains a classical public-key approach for CCF's quantum scenario. Treat scheme requirements, product lifecycles and PQC targets as distinct planning inputs, with their actual scope and dates.

A PIN-management or issuer symmetric master key should not be described as certified by a scheme CA merely because both appear in the same payment estate. Establish the actual function and relationship. Other classical-security requirements remain relevant even where a symmetric mechanism is outside layer 1's specified quantum-vulnerable class.

Layer 4 – Key custody platform

Enumerate payShield, Atalla, nShield, Futurex, IBM Crypto Express and Securosys, together with cloud payment cryptography and HSM services. Resolve each platform to its firmware family. Record the relevant original manufacturer and shared components separately from product identity.

Module scope. Vendor post-quantum announcements frequently describe general-purpose modules rather than the payment HSMs in the PIN and key path. Record the module actually deployed.

Provenance disclosure. Payment HSM vendors publish algorithm support and certification status. None currently publishes the code lineage of its post-quantum implementation. PCI Security Standards Council device listings carry a post-quantum support flag and refer readers to the vendor for detail. Expect `UNDISCLOSED` at layer 2 for most custody platforms. Each undisclosed module is included in every reach bound from which it cannot be excluded, under Universal C.3.2.

Layer 5 – Protocol and negotiation

The unit is the negotiated profile. Record TLS protocol, version and key-establishment group on acquirer and issuer links; IPsec negotiated proposals on scheme connections; the EMV kernel's negotiated offline data authentication method per path; and 3-D Secure negotiated protocol versions. Identify the cryptographic method selected in operation, its path and function, and any fallback.

DUKPT and tokenisation are key-derivation and custody facts, mapped to layers 2, 4 and 6. For ISO 8583 and ISO 20022 message security, record the security profile negotiated per path, not the message standard as a dependency. A scheme name, an ISO 20022 message type or a protocol version alone is contextual information, not a sufficient cryptographic outcome.

Layer 6 – Key generation: entropy source and generation design

Enumerate the hardware RNG in each custody platform, secure-element RNG across the issued card estate, terminal RNG, host processor instructions, and key-generation libraries and generation-algorithm designs at each point. Identify the origin of persistent material, including imported keys. Record the design and certification profile rather than only the device.

Secure elements from several card vendors use ring-oscillator designs conforming to one certification profile. Conformance raises the likelihood of a shared design without establishing it. The shared profile is recorded as a bounded design node, with known reach at the largest conformant point and an upper bound spanning every conformant point, under the Universal's layer-6 determination and C.3.2. The known figure

represents the largest point's own design. It is a floor by construction, not evidence that separate points share a design.

A.3 EMV OFFLINE DATA AUTHENTICATION

EMV offline data authentication is assessed under layer 5, not as a separate layer. A card supporting combined data authentication that meets a terminal supporting only static data authentication falls back to the known-weak static method. This is the downgrade failure mode that layer 5 measures.

The reason to consider separate treatment is ownership: the issuer or acquirer does not control the terminal estate. Effective Coverage accounts for that external dependency. For each path, record the method negotiated in practice, the terminal population supporting each method and the share of transactions falling back. Retain the method's certificate and key relationships.

A.4 COUNTERPARTY CLASSIFICATION FOR PAYMENTS

Class	Payments members
Blocking	Card schemes; SWIFT; central bank RTGS operators; automated clearing house operators
Contractual	Corporate clients; downstream payment service providers; named merchant integrations
Peer	Correspondent banks; sponsor banks; other issuers and acquirers on shared rails
Population	Terminal and acceptance device estates; issued card estates; mass merchant populations under standard onboarding

Report terminal estates as a population percentage, not as an individual count. Their remediation route is a certification and refresh campaign.

These are illustrative classifications. A supplier is not blocking merely because it is large, and a contract does not guarantee practical substitutability. Record the route that governs the specific service change.

Establish the target for each function: a transport key-establishment upgrade does not automatically migrate payment-message signatures, card authentication or a trust chain. Read endpoint state with actual path outcomes, counterparties, intermediaries and fallback conditions. The first-class path records of the Applied Quantum CBOM Profile (v1.0-RC or later) and the supplementary topology prevent a platform's "hybrid deployed" status from being reported as complete service coverage.

For issued populations, record actual counts and joint state. Card readiness and terminal readiness measured as separate marginal percentages do not reveal the exact proportion of relevant card/terminal combinations at target. Use a defined combination population, observed compatible paths or explicit bounds. Do not multiply percentages or take their minimum without a justified relationship model.

A.5 CRITICALITY TEST 2 FOR PAYMENTS

The Universal Framework's test 2 covers material authorising an irreversible action or underwriting a finality or non-repudiation guarantee. For payments, this includes:

- Payment release and settlement instruction authorisation.
- Scheme and issuer certificate authority keys.
- Issuer master keys and derivation masters.
- Key encryption keys wrapping PIN and DUKPT estates.
- Any key whose compromise permits construction of a valid transaction.

Apply all five Universal criticality tests to the counted assets and their service context. Payment-signing and authorisation functions may qualify because they permit an irreversible instruction or support a finality guarantee. Master, derivation and wrapping keys may qualify because other keys depend on them. Terminal or issued-device material may qualify where replacement cannot be completed within the service's tolerance.

The assessment should identify the consequence rather than presume that every authorisation error is legally irreversible or every payment credential is a finality key. Distinguish a reversible authorisation, a submitted instruction, settlement and the institution's actual control over reversal. The service owner supplies that interpretation and the applicable threshold.

A.6 CONSEQUENCE-THRESHOLD TEMPLATE (NON-NORMATIVE)

Universal C.5.3 places the consequence threshold with the institution. This template provides a record for each in-scope service, owned by the service owner and reviewed with the tolerance.

Field	Prompt
Service	The important business service the threshold protects
Failure shape	Confidentiality exposure, forgery, or both – per the layer scenarios in Universal C.5.2
Threshold statement	The exposure or forgery consequence the service treats as intolerable, stated as a quantity or a named category. "Per risk appetite" is not a statement.
Anchored to	The obligation or harm that makes it intolerable – scheme rules, notification duties, finality guarantees, contract law
Owner	The named individual who defends it in challenge
Review	Date, aligned to the tolerance review

Two illustrative statements show how the threshold is tied to a consequence. "Any forged production authorisation is intolerable at any volume" is anchored to settlement finality. "Exposure of harvested cardholder traffic beyond the scheme's notification threshold is intolerable" is anchored to an existing obligation. An undefined threshold is Not assessable, never Pass.

For confidentiality and integrity, a short outage tolerance is not sufficient evidence of acceptable harm. Define the relevant consequence threshold and evaluate prior exposure, forged acceptance, revocation and recovery. Where the necessary threshold or operational facts are absent, record Not assessable rather than infer Pass from a low CCI.

A.7 WORKED EXAMPLE

A.7.1 Service and asset population

A mid-size acquiring processor assesses card authorisation over 4,200 cryptographic assets. Of these, 180 are flagged under tests 1, 3 and 4: issuer master keys and EMV certificates that derive other keys, cannot be revoked inside the tolerance because the cards are in the field, and remain valid past the migration completion date.

Estate profile (reported, not scored): 4,000 assets are quantum-vulnerable (95.2%), 200 are quantum-safe symmetric (4.8%), and there is no post-quantum public-key material. The layer-1 population is 4,000, not the full service population of 4,200.

The service boundary includes authorisation and the processor-operated settlement submission leg. This is why two central-bank rails appear among the blocking counterparties alongside four card schemes. An authorisation-only boundary would show four blocking counterparties and would change no layer figure.

The unit counts are synthetic. The reference implementation (`compute_ccf.py --payments-example`) computes every figure in the results table from them. These inputs are not observations of market share, a supplier estate or a published CBOM, and the example does not claim that a complete discovery, conformance or operational-validation process has been performed.

A.7.2 Dependencies and results

Layer 2. Three executing families carry 2,400, 900 and 900 assets. The last family's lineage is undisclosed. The disclosed ancestor reaches the 2,400-asset family, giving 57.1% evidenced reach. The second family is excluded from that ancestor's bound; the last cannot be excluded, giving a 78.6% upper bound. The three executing families remain separate primary units. The diversity ladder reads five brands observed, three families resolved and largest failure domain 78.6% bounded.

Layer 3. Five anchors carry 1,300, 1,000, 900, 800 and 200 assets. Of the 180 flagged assets, 150 are under the primary scheme authority and 30 under the institution's own issuing authority.

Layer 4. Two firmware families carry 2,900 and 1,300 assets. Every flagged asset is on the first family.

Layer 5. Three negotiated tuples cover 2,600, 1,100 and 500 paths.

Layer 6. Three generation points carry 2,650, 1,050 and 500 assets. They share one RNG certification profile, but no design is disclosed. The bounded design node has 63.1% known reach against a 100% upper bound. The 63.1% evidenced figure is the largest point's own design, a floor by construction. Every flagged key traces to the primary custody point.

Layer	Units (assets)	CCI	Largest share	Band	Flagged-only	Largest failure domain (bound)	Largest upstream node (bound)	Tolerance

Layer	Units (assets)	CCI	Largest share	Band	Flagged-only	Largest failure domain (bound)	Largest upstream node (bound)	Tolerance
1 Algorithm *(baseline, excluded from the reported figure)*	one class	10,000	100%	Single-source-equivalent	10,000	–	–	Fail
2 Lineage	2400/900/900	4,184	57.1%	Concentrated	–	57.1% evid. · 78.6% bound (reach node)	57.1% evid. · 78.6% bound	Fail, on the bound
3 Trust root	1300/1000/900/800/200	2,370	31.0%	Diversified	7,222	31.0% evid. (flagged 83.3%) (standalone unit)	31.0% evid. (flagged 83.3%)	Fail, flagged
4 Custody	2900/1300	5,726	69.0%	Highly concentrated	10,000	69.0% evid. (standalone unit)	–	Fail
5 Protocol	2600/1100/500	4,660	61.9%	Concentrated	–	61.9% evid. (standalone unit)	–	Pass
6 Key generation	2650/1050/500	4,748	63.1%	Concentrated	10,000	63.1% evid. · 100.0% bound (reach node)	63.1% evid. · 100.0% bound	Fail, on the bound

A flagged-only cell shows a dash where the illustration places no flagged material at that layer. An upstream-node cell shows a dash where no upstream node is named. Layers 4 and 5 report their standalone units in the largest-failure-domain column. The labels distinguish standalone units from reach nodes.

The reported service CCI is 5,726, the maximum across layers 2 to 6, at layer 4. Layer 1 is reported separately as the 10,000 baseline. The largest failure-domain reach is bounded at 100%, at layer 6: three generation points, one certification profile and no disclosed design. The disclosure programme is intended to narrow that bound. The trust-root cell's overall CCI is 2,370, while its flagged-only CCI is 7,222 and its largest flagged root share is 83.3%.

A.7.3 Operational determination

The service has a two-hour impact tolerance under rule 1. For the illustrative operational determination, assume an approved integrity threshold for the scoped instruction-signing function and the following service-owner recovery facts. These facts are additional scenario inputs; none is derived from the CCI or asset share.

Tolerance results come from the failure-impact determination in Universal C.5, applied to reach-defined domains.

Tested domain	Illustrative operational fact	Determination
Largest executing family	A tested isolated replacement can restore the affected function in 90 minutes	Pass for the isolated availability test; integrity assessed separately
Ancestor's upper-bound population	Coordinated replacement of all possible affected families takes at least six hours	Fail – upper-bound scenario; shared membership remains unconfirmed
Dominant flagged trust anchor	Revocation/reissuance and required verifier updates take at least four hours	Fail for the defined withdrawal scenario; integrity assessed separately
Largest custody family	The required alternate capacity and key redistribution cannot be made operational within two hours	Fail
Largest protocol outcome	The scoped controlled cutover is demonstrated in 60 minutes with compatible counterparties	Pass for the stated availability test; other consequences assessed separately
Whole-service bounded design	Replacement of all potentially affected generated material cannot meet the approved response/consequence thresholds	Fail – upper-bound scenario; no common design asserted as fact

At layer 2, emergency patch-and-rotate across the 3,300-asset bounded domain exceeds the two-hour tolerance, while the 2,400-asset evidenced domain passes. Layer 3 fails on the flagged view because revoke-and-reissue under the single authority anchoring the issuer master keys exceeds the tolerance. Layer 4 fails on the flagged view outright. Layer 6 fails against the consequence threshold on the design bound: re-keying the issued estate is a multi-year campaign, and keys already generated stay exposed.

Layers 1, 3, 4 and 6 fail the service's tolerance test. Layer 2 fails on the bound while passing on the evidenced domain; layer 5 passes.

The table demonstrates how operational facts change interpretation. The overall trust distribution appears dispersed, but the qualifying functions have a concentrated dependency and an impractical recovery period. The layer-2 point scenario can pass while the wider ancestor scenario fails. In a real assessment, missing recovery or integrity evidence would change the corresponding conclusion to Not assessable.

A.7.4 Coverage and counterparties

Effective Coverage is 0%. No path in the service operates at target state end to end. This is a computed result on the defined population, not an inference from the classical baseline, the CCI or an endpoint capability label.

The counterparty register contains 6 blocking, 12 peer and 340 contractual relationships after de-duplication, together with a terminal population at 0% at target state. The six blocking counterparties are four card schemes and two central bank rails. The twelve peers require bilateral outreach. The 340 contractual counterparties require a certification programme. The terminal population requires a refresh campaign. These are four problems on different timescales, which a single count of 358 would conceal.

These numbers and classifications are synthetic. The assessment must identify which path populations depend on which counterparties; it must not imply that all 4,200 assets require every one of the six blockers to change.

The resulting decision is more specific than "buy a third HSM". Investigate the unidentified generation designs, address the concentrated qualifying custody/trust functions, verify the ancestor's uncertain membership and coordinate the affected below-target paths. An additional vendor sharing the same relevant design could change the primary distribution without addressing the upper-bound scenario.

Key generation, absent from every vendor assessment the institution has run, is the service's largest failure domain at a design bound of 100%. The custody layer has two firmware families, with all 180 flagged assets on the first. Coverage stays at 0% until the six blocking counterparties specify how to reach target state.

A.8 IMPLEMENTATION PRIORITIES

Begin with the payment service boundary and its actual cryptographic functions. Existing HSM, PKI, gateway and issued-estate records can provide an initial population, but reconcile their overlap before calculating. Identify generation origin and externally governed paths early, because both can remain outside ordinary infrastructure inventories.

Use the Data Request to obtain the internal evidence and the Supplier Lineage Request for external provenance. Apply the Technical Companion to the engineering work. Record service effects and disputed relationships in the Determination Log, then report decisions through the Board Report.

Keep key-establishment and authentication/signature migration tracks visible. Where technical standards, scheme rules and institutional dates differ, record their purposes and applicability rather than collapse them into one deadline. Product refresh is an opportunity to reduce future transition cost, not proof that all counterparties or issued populations will migrate at the same time.

The Payments whitepaper provides the fuller strategic explanation and interpretation of this example. This extension remains the compact assessment guide; the Universal Framework remains the authority for the calculations and reporting rules.

Canonical source. Published at ccframework.org under CC BY 4.0. Cite as: *The Applied Quantum Cryptographic Concentration Framework, Payments Extension v1.0-RC, Steve Vaile and Marin Ivezic / Applied Quantum, ccframework.org.*