QUANTUM CORE INSTITUTE

Sector-Specific Protocols

Payments, digital assets and custody under QCI-QS1 Annex G domain 13

Field	Value
Document ID	QCI-QS1-C3
Version	V1.2 – September 23, 2026. Clause references are QCI requirement identifiers from QCI-QS1 v2.3 (September 23, 2026).
Applies to	QCI-QS1 Annex G domain 13; Clause 7 and Annex C (Vendor Roadmap Request Pack). Companions C1 and C2.
Status	Informative client handout. Nothing in this handout creates, modifies, or interprets a requirement. Where this handout and the standard differ, the standard governs.
Endorsement	None. Providers named are unranked. Quantum Core Institute does not endorse, resell, or certify any provider and has not independently tested any product.
License	Free. Attribution required. May not be modified and redistributed.
Publisher	Quantum Core Institute Inc.

1 Read this first

Domain 13 is different from the other twelve in one way that changes the governance: the organization does not control the protocol. Payment networks move on the schedules of EMVCo, PCI SSC, SWIFT and the card schemes. Blockchains move on protocol upgrades that require consensus the organization does not hold. In both, the QASI row is complete, the owner is named, and the migration date belongs to someone else.

Three consequences follow. The Vendor Roadmap Request Pack is the primary control, not a supporting one. Decisions to wait are the normal state and must be recorded under QCI-T4 with revisit conditions tied to the external body's milestones. And operational controls that reduce exposure without changing the protocol matter more here than anywhere else.

> **COMMON MISTAKE**
> Treating "the scheme has not published a PQC specification" as a reason to leave the row blank. The row records the dependency, the data longevity, the flag and the decision to wait. A blank row is a system the organization has not looked at; a recorded wait is a system it has.

2 Payments

2.1 Where the cryptography sits

Function	Cryptography today	Quantum exposure	Who controls the change
Card authorization (EMV)	RSA for issuer and ICC certificates; symmetric for cryptograms	Signature forgery on card and issuer certificates; long card lifetimes (3 to 5 years)	EMVCo, card schemes, card manufacturers
PIN and key management	Symmetric (TDES, AES) under key blocks; RSA for key transport	Key transport (harvest-now on RSA-wrapped keys); TDES weakness independent of quantum	PCI SSC (PCI PIN, PCI HSM), HSM vendors
Interbank messaging (SWIFT, ISO 20022)	TLS, PKI-based signing of messages and files	Message authenticity and non-repudiation	SWIFT, national infrastructures
Real-time payment rails	TLS, API signing, mutual TLS	Key exchange (HNDL) and API signature forgery	Rail operator, participant banks
Tokenization and 3-D Secure	RSA and ECC in token service providers; TLS	Token service key exchange and signing	Schemes, token service providers

2.2 Providers with shipped post-quantum capability

Provider	What it offers	Status, as of the cover date
Futurex Excrypt	Payment HSM with native ML-KEM and ML-DSA; the first PCI HSM-validated platform supporting PQC, no hardware refresh required	Shipping
Utimaco Atalla AT1000	First payment HSM with FIPS 140-3 (June 2025); PQC available on the general-purpose line via the Q-safe firmware extension	Shipping; ask for the payment-line PQC date
Thales payShield 11K	PQC support planned through future Luna 8 releases	Roadmap
EMVCo, PCI SSC, SWIFT	Own the protocol timelines; no post-quantum EMV or PCI PIN specification is final	Track scheme bulletins; record under QCI-T4

2.3 What to do now

1. Put the payment HSM, the key-transport mechanism and every scheme dependency in the QASI with data longevity set by regulation and contract (PCI DSS retention, dispute windows), not by the transaction lifetime.
2. Send the pack to the HSM vendor, the token service provider and the scheme relationship owner. Ask specifically for the PCI HSM certificate and the PQC roadmap together; a PQC-capable HSM without PCI HSM validation cannot be deployed in a payment estate.
3. Move key transport off RSA wrapping where the HSM supports ML-KEM; this is the harvest-now exposure in payments and it is in the organization’s control.
4. Record the EMV and PIN waits under QCI-T4, with revisit conditions tied to EMVCo and PCI SSC publications, and put procurement language for PQC agility into the next card and terminal tender.

3 Digital assets and custody

3.1 Why this is the urgent half

On a public blockchain the public key is exposed the moment an address is reused or a transaction is signed, and the private key becomes derivable once a cryptographically relevant quantum computer exists. Unlike TLS, there is no session to protect and no key exchange to hybridize: the exposure is the signature scheme itself, and the migration is per address, voluntary, and dependent on a protocol upgrade the organization does not control.

Protocol	Post-quantum status	What an asset holder can do now
Bitcoin	BIP-360 (Pay-to-Merkle-Root with ML-DSA) merged into the BIP repository February 2026; on an independent testnet; not activated on mainnet	No address reuse; move balances off exposed-key addresses; custody policy that forbids reuse
Ethereum	Research and roadmap; Ethereum Foundation post-quantum work in progress; no activated PQ signature scheme	Same address hygiene; smart-contract wallets that can rotate signing keys
Algorand	Falcon signatures on mainnet since November 2025; native PQ accounts and institutional PQ multisig on the 2027 roadmap	Adopt PQ accounts as they ship
Quantum Resistant Ledger	XMSS signatures on every transaction since 2018	Live
Solana	PQ signatures on testnet	Watch for mainnet activation

3.2 Custody and signing infrastructure

Provider	Reported post-quantum work	Status
BitGo	First post-quantum MPC transaction simulation, with Silence Laboratories, preserving distributed key control and policy enforcement	Simulation, not production
Coinbase	Independent quantum advisory board formed January 2026; position paper April 2026; roadmap covers address handling, key management and PQ signature research	Research and roadmap
Fireblocks, Anchorage Digital, Dfns	Reported work on quantum-resistant systems and Bitcoin migration research	Not documented by the firms; ask each
BTQ	QSSN quantum-secure stablecoin network, Bitcoin Quantum, and QCIM silicon for signing devices	Commercial; verify deployment status directly
SEALSQ QS7001	Post-quantum secure element positioned for wallet and signing hardware	Shipping; certifications on a 2026 roadmap

> **WHAT THE ASSESSOR WILL ASK**
> Show me the address-reuse policy and the evidence it is enforced. For a digital-asset estate that is the compensating control that matters, it costs nothing, and it does not wait for any protocol.

3.3 What to do now

1. Inventory every address, wallet and signing key as a QASI row with the chain, the signature scheme (secp256k1 ECDSA, Ed25519, BLS, Schnorr) and whether the public key is already

on-chain. Exposure type is authenticity; harvest-now risk is High wherever the key is exposed.
2. Enforce no address reuse and sweep balances from exposed-key addresses to fresh ones on a schedule. Record the policy under QCI-T4 as the compensating control, with an expiry tied to the chain's PQ activation.
3. Send the pack to every custodian and wallet vendor. Ask for the PQ signing roadmap, the MPC or HSM key-protection mechanism, and whether keys can be rotated to a PQ scheme without moving funds.
4. For validators and long-lived keys (staking, multisig signers, bridge keys), treat the key lifetime as the data longevity and exposure flag under QCI-5.3-01 (signature or trust dependency with a long verification horizon) where it exceeds the planned migration date.

4 Questions for domain 13 suppliers

In addition to sections A to F of the Vendor Roadmap Request Pack:

1. Which external standards body governs your protocol's post-quantum transition, and what is its published timeline?
2. For a payment HSM: which PCI HSM version is validated, and does that validation cover the PQC firmware?
3. For a custodian: which signature scheme protects client keys today, and can a client's key be rotated to a post-quantum scheme without an on-chain transfer of funds?
4. What operational controls do you enforce on behalf of clients: address reuse, key rotation, exposure of public keys?
5. Will you provide a CBOM for the signing path that meets QCI-5.4-03?

Sources

- Futurex: PQC and PCI HSM validation · Utimaco payment HSM · Thales Luna 8 announcement
- Bitcoin and post-quantum cryptography, 2026 · Algorand post-quantum · Quantum-resistant blockchains overview
- Coinbase quantum advisory board · BitGo post-quantum MPC simulation · BTQ · SEALSQ QS7001
- QCI-QS1 v2.3 (September 23, 2026), Annex G; QCI-M1; QCI-T4

The payment-function table in chapter 2 describes protocol cryptography in general terms and was not sourced to a scheme publication for this version; confirm against the client's scheme documentation. Fireblocks, Anchorage and Dfns entries rest on trade reporting.

Independent assessment against QCI-QS1 is performed by the Quantum Core Institute. Scope one at quantumcoreinstitute.com/independent-assessment. An independent assessment is not QCI certification (QCI-1.2-03).