QUANTUM CORE INSTITUTE

PQC Remediation and Migration Providers

Who replaces what your QASI found, by cryptographic domain

Field	Value
Document ID	QCI-QS1-C2
Version	V1.4 – September 23, 2026. Clause references are QCI requirement identifiers from QCI-QS1 v2.3 (September 23, 2026).
Applies to	QCI-QS1 Clauses 6 and 7, QCI-4.5-01 to 4.5-04 (approved profiles), QCI-4.2-02 (roadmap decisions), Annex G
Status	Informative client handout. Nothing in this handout creates, modifies, or interprets a requirement. Where this handout and the standard differ, the standard governs.
Companion	QCI-QS1-C1, Cryptographic Discovery Tools; C3 to C5 for sector protocols, AI systems and identity
Endorsement	None. The providers listed are unranked. Quantum Core Institute does not endorse, resell, or certify any provider on this list and has not independently tested any product.
Review by	PQC support changes with every release. Review this handout quarterly or on any material vendor announcement.
License	Free. Attribution required. May not be modified and redistributed.
Publisher	Quantum Core Institute Inc.

1 Read this first

This is the companion to the discovery-tools handout. Once your QASI shows where quantum-vulnerable cryptography sits, these are the categories of provider that replace it. The chapters follow the cryptographic domains of QCI-QS1 Annex G, numbered as the standard numbers them, so a QASI row that records domain 6 points at chapter 6 here. Four rules precede every table.

1. **Remediation follows the inventory.** Do not buy a migration product before your QASI names the system, the owner, the data longevity and the algorithm. The provider category you need depends on the domain the finding sits in.
2. **Sequence by exposure, lead time and dependency, not by a fixed order.** QCI-4.2-02 requires each roadmap decision to weigh confidentiality and verification horizons, present capture exposure, consequences, dependencies, lead time, end-of-support and applicable deadlines, and forbids postponing all signature and hardware work until key exchange is done. Domains 3, 4 and 7 carry present-tense harvest exposure and usually move early; domains 5, 9, 11 and 13 have long lead times and often need parallel investment now.
3. **A profile is a decision.** Every production change uses an approved profile (QCI-4.5-01). A hybrid key-establishment profile can add resilience when its construction, authentication, negotiation and fallback policy are specified and verified (QCI-4.5-03); it does not upgrade signatures or authentication, and it carries complexity and a later transition to PQC-only. A PQC-only profile records the regime, such as CNSA 2.0, that requires it. Record the reasoning either way.
4. **Buy agility, not an algorithm.** Whatever you deploy, gate G80 (QCI-6.3-01) and the test rules of QCI-4.7 ask whether you can change it again without replacing the platform. A provider whose product hard-codes ML-DSA has repeated the mistake you are fixing.

> **WHY THIS HANDOUT EXISTS**
> Every provider on this list is a supplier under QCI-QS1 Clause 7 and should receive the Annex C request; new procurements are evaluated under QCI-7.1-02. A remediation purchase that does not come with a signed attestation has moved your exposure, not reduced it.

2 Domain 2: Crypto-agility and governance layer

These sit above every other domain. They manage which algorithm is used where, and let you change it without redeploying every application.

Provider	What it offers
SandboxAQ AQtive Guard	Inventory joined to policy enforcement and remediation workflow; used across defense, finance and telecoms
Keyfactor AgileSec Agility (formerly InfoSec Global)	An abstraction layer that lets applications switch algorithms by policy rather than by code change
QuSecure QuProtect	Orchestration overlay that negotiates hybrid sessions across existing networks without replacing endpoints

Provider	What it offers
Entrust Cryptographic Security Platform	CBOM import and export, Ansible-driven certificate automation, composite algorithms, machine and AI identity
IBM Quantum Safe Remediator	Deploys quantum-safe replacement patterns and hybrid schemes alongside IBM's discovery tools
PQShield	Migration consulting plus SDKs for products and devices
Systems integrators: IBM Consulting, Accenture, Deloitte, Capgemini, Thales	Programme-level migration for large estates

WHY THE REQUIREMENT EXISTS
An agility platform is not proof of agility. Gate G80 caps a Q-Risk Score at 80 until a critical trust pathway has passed a representative end-to-end test under QCI-4.7 within the last twelve months. Buy the platform, then run the test.

3 Domain 3: Data in transit, TLS edge, CDN and load balancers

The fastest win. Hybrid key exchange closes the harvest-now-decrypt-later gap on traffic without touching application code, and most of it is a version upgrade and a policy change.

Provider	What it offers
Cloudflare	X25519MLKEM768 on by default at the edge; over half of human traffic already uses it. ML-DSA authentication is experimental
AWS CloudFront and Elastic Load Balancing	Post-quantum TLS policies you must select; the default policy is usually classical
Google Cloud load balancing	BoringSSL-based edge with hybrid key agreement
Browsers: Chrome 131+, Firefox 132+, Safari 26+, Edge 131+	Post-quantum key agreement on by default. Your servers need only accept it
Web servers: NGINX with OpenSSL 3.5+, Caddy 2.10+, Traefik 3.4.2+	Hybrid key agreement once the linked library supports it
API gateways and service mesh: F5, Kong, Istio and Envoy	Depends on the TLS library underneath; verify the negotiated group, not the version
QuSecure QuProtect	Overlay for endpoints that cannot be upgraded

COMMON MISTAKE
Treating a TLS version as a verdict. TLS 1.3 over X25519 is quantum-vulnerable; TLS 1.3 over X25519MLKEM768 is not. Verify the negotiated group with a scanner from the discovery

> handout, and record the group, not the version, in the QASI.

4 Domain 4: VPN, IPsec, SSH and remote access

Covers both the key exchange on the tunnel and the authentication keys and certificates the tunnel relies on. Zero-trust access gateways belong here too.

Provider	What it offers
Cisco	IOS XE 26.1 ships ML-KEM in IPsec and 26.2 adds ML-DSA for IKEv2 on routers; Secure Firewall ASA 9.25 and FTD 10.5 bring ML-KEM in late 2026, with ML-DSA and SLH-DSA planned for 11.0 in 2027
Palo Alto Networks	PAN-OS supports RFC 8784 preshared keys and RFC 9242/9370 hybrid key exchange with up to seven additional KEMs including ML-KEM; both can be combined
Fortinet	FortiOS 7.6 implements RFC 9370 hybrid IKEv2 with ML-KEM-512/768/1024, plus RFC 8784 mixing
Juniper	Junos supports RFC 8784 postquantum preshared keys through the junos-ike package and Junos Key Manager; Junos OS Evolved 25.4 adds PQC features
strongSwan	Open-source IPsec with ML-KEM and RFC 8784 support
OpenSSH 10+	mlkem768x25519-sha256 is the default key exchange; 9.0 to 9.9 default to sntrup761x25519
American Binary Ambit Client	CNSA 2.0-only enterprise VPN on ML-KEM-1024 with a formally verified proprietary protocol; no hybrid mode; SaaS or on-premises. A replacement VPN, not an upgrade to an incumbent
QuSecure QuProtect	Commercial overlay that negotiates hybrid sessions across existing networks
Cloudflare Zero Trust	Post-quantum key agreement on access tunnels

A pure post-quantum mode, as CNSA 2.0 requires, is a legitimate choice for defence and federal-adjacent estates. Record it as an approved profile under QCI-4.5-01 with the regime named, and as a decision under QCI-T4.

5 Domain 5: PKI, certificates and code signing

Private PKI can move now. Public web PKI cannot: as of mid-2026 no browser trust store contains an ML-DSA root, and no browser negotiates ML-DSA server certificates by default. Plan private trust chains, code signing and machine identity first.

Provider	What it offers
DigiCert	ML-DSA and SLH-DSA certificates from DigiCert ONE and Trust Lifecycle Manager; HSM-backed issuance
Entrust	PQC-ready CA, composite certificates, and from September 2026 CBOM import and export in its Cryptographic Security Platform
Sectigo	Private PQC (ML-DSA) certificates issued and managed inside Sectigo Certificate Manager since April 2026, plus the PQC Labs sandbox
Keyfactor EJBCA	Open-source and enterprise CA with ML-KEM, ML-DSA and SLH-DSA
Microsoft AD CS	ML-DSA-44, -65 and -87 in Active Directory Certificate Services on Windows Server 2025 from May 2026
AWS Private CA	ML-DSA roots and issuing CAs since November 2025
Sigstore, HashiCorp Vault PKI, smallstep	Open-source signing and private CA tooling; PQC support varies by release, check before relying on it

For firmware and software signing, CNSA 2.0 requires the stateful hash-based LMS or XMSS of SP 800-208. Those need a signing service that never reuses a state, which is an operational control, not a library choice.

6 Domain 6: Key management and HSMs

Vendor firmware and product support here often gate progress in every other domain. The key-protection mechanism is what needs replacing, not the data, and a key-protection profile names the whole scheme: KEM, key derivation, symmetric wrap, recipient trust and bulk cipher (QCI-4.5-04).

Provider	Type	What it offers
Thales Luna	HSM	CAVP-validated ML-KEM and ML-DSA in firmware 7.8 and later; Luna 8 built for PQC
Entrust nShield	HSM	ML-KEM, ML-DSA and SLH-DSA native from Security World firmware v13.8 (August 2025); CAVP-validated
Utimaco	HSM	Q-safe loadable firmware extension adds ML-KEM, ML-DSA, LMS and XMSS to SecurityServer Se Gen2 and CSe over PKCS#11; retro-fittable
Crypto4A QxHSM, Securosys Primus, Fortanix DSM	HSM and KMS	All three FIPS PQC algorithms per the PKI Consortium matrix

Provider	Type	What it offers
AWS KMS	Cloud KMS	ML-DSA-44, -65 and -87 signing keys since June 2025 in FIPS 140-3 Level 3 hardware; ML-KEM hybrid TLS to the service
Google Cloud KMS	Cloud KMS	ML-DSA-44/65/87 and SLH-DSA signing keys generally available; ML-KEM key encapsulation in preview at time of writing
Azure Key Vault and Managed HSM	Cloud KMS	ML-KEM and ML-DSA for software-protected keys via SymCrypt; HSM-backed keys classical only in general availability as of April 2026 per third-party status reports. Confirm tier and region with Microsoft

WHAT THE ASSESSOR WILL ASK
Give me the CAVP certificate number covering the PQC algorithm, and the FIPS 140-3 certificate that lists it. A vendor roadmap slide is neither.

7 Domain 7: Data at rest, storage and backups

Sound AES-256 does not need replacement because of the quantum threat (QCI-4.6-03). The exposure is the asymmetric mechanism that wraps and distributes storage keys, and archives whose confidentiality horizon outlasts the threat. The decision to rewrap, rekey, re-encrypt, retain or retire is documented with its residual exposure, and a current rewrap is never reported as remediation of copies an adversary may already hold. This domain is remediated mostly through domain 6.

Provider	What it offers
Cloud storage: AWS S3 and EBS with KMS, Azure Storage, Google Cloud Storage	Key wrapping follows the provider's KMS. Once the KMS protects data keys with a KEM-based scheme, storage inherits it; confirm envelope encryption is in use rather than a static key
Databases: transparent data encryption in Oracle, SQL Server, PostgreSQL extensions	The master key wrap is the finding; check whether it sits in an HSM or KMS from domain 6
Endpoint disk: BitLocker, FileVault, LUKS	Symmetric at rest; the recovery key escrow and TPM sealing are the asymmetric dependencies
Commvault	ML-KEM, ML-DSA, FN-DSA and HQC available in the platform with a rule-based policy engine for applying PQC to workloads
Veeam	Post-quantum cryptography and hybrid FIPS support in v13.1; roadmap aligned to FIPS 203, 204 and 205

Provider	What it offers
Other backup and archive suppliers	Long-lived archives are the highest harvest-now exposure in this domain. Send the pack to each

For each archive, the QASI data-longevity field decides the urgency: an archive that must stay confidential past 2035 under a classical key wrap raises the QCI-5.3-01 exposure flag for vulnerable protection of long-lived confidentiality today.

8 Domain 8: Application cryptographic libraries

For code you own. Most remediation in application code is a library upgrade plus a configuration change, not a rewrite. Hard-coded algorithm choices are the exception and the agility finding.

Provider	Type	What it offers
OpenSSL 3.5+	Open source	Native ML-KEM, ML-DSA and SLH-DSA; hybrid X25519MLKEM768 in TLS 1.3. The default path for C, and for anything linked against OpenSSL
AWS-LC and s2n-tls	Open source (AWS)	ML-KEM and ML-DSA; AWS-LC is the first open-source module with ML-KEM inside its FIPS validation
BoringSSL	Open source (Google)	ML-KEM hybrid key agreement since 2024; ML-DSA support
Bouncy Castle	Open source	ML-KEM, ML-DSA and SLH-DSA for Java and C#; FIPS editions available
Botan	Open source	C++ library with all three FIPS algorithms
Microsoft SymCrypt	Open source (Microsoft)	ML-KEM and ML-DSA; the engine under Windows CNG; PQC APIs generally available in Windows Server 2025, Windows 11 and .NET 10
Go crypto/tls, Rust rustls and aws-lc-rs	Open source	Hybrid key agreement on by default in current Go; rustls via aws-lc-rs
liboqs and oqs-provider	Open source (Open Quantum Safe, Linux Foundation)	Every NIST candidate and standard, for prototyping and interoperability testing. Not intended for production
PQShield	Commercial	PQC software SDKs, firmware and hardware IP for embedded and constrained devices

WHAT THE ASSESSOR WILL ASK
Show me the FIPS 140-3 certificate, and show me that the PQC algorithm is on it. Few libraries carry a validation that covers ML-KEM or ML-DSA yet, and a validation that covers only the classical algorithms in the same module is not the evidence a regulated institution needs.

9 Domain 9: Identity and access, SSO, IAM and passkeys

Nearly all change here is in digital signatures and credential formats: SAML and OIDC assertion signing, JWTs, smart cards and PIV, FIDO2 passkeys, and the workload identities that authenticate services and agents. No identity provider has shipped post-quantum federation signing as a default; this domain is a vendor request, not a purchase. Handout C5 covers it in depth.

Provider	What it offers
Microsoft	PQC APIs generally available in Windows Server 2025, Windows 11 and .NET 10; ML-DSA in AD CS from May 2026. The Quantum Safe Program targets critical services by 2029 and the rest, including Entra and Microsoft 365, by 2033. Entra token signing on ML-DSA has no published date
Okta	Targeting 2026 to 2027 for initial PQC support, with administrative controls to move tenants to PQC-ready defaults
Ping Identity	Evaluating NIST PQC integration; publishing migration playbooks; no shipped PQC federation signing
FIDO Alliance	A PQC Study Group is scoping post-quantum extensions to WebAuthn; initial browser and authenticator support is expected late 2027 to 2028
Workload identity: SPIFFE/SPIRE, HashiCorp Vault, cloud IAM	Machine and agent identity; SPIRE-based PQC-capable identity is being built by Entrust and others. Where AI agents are in scope, this is where their identity sits
Yubico	ML-KEM and ML-DSA prototypes on security keys; not product-ready, new hardware required
IDEMIA	First complete PIV application running on a smart card with post-quantum cryptography, demonstrated June 2026
Thales SafeNet IDPrime PIV	Current cards are RSA and ECC only; ask for the PQC applet roadmap

COMMON MISTAKE
Running an identity modernization programme (passkeys, a new IAM platform, credential re-issuance) separately from PQC planning. The credentials get issued twice. One shared inventory, one re-issuance plan and one named owner for the seam, decided before the identity programme ships.

10 Domain 10: Messaging and collaboration

Secure email, enterprise messaging and end-to-end encrypted channels carrying long-lived content. Depends heavily on vendor and protocol support, and the consumer platforms are ahead of the enterprise suites.

Provider	What it offers
Apple iMessage PQ3, Signal PQXDH and SPQR	Hybrid post-quantum key establishment and ongoing ratcheting shipped in consumer messaging
Zoom	Post-quantum end-to-end encryption on Kyber-768 for Zoom Meetings since May 2024; Phone and Rooms followed
Microsoft 365	Covered by Microsoft's Quantum Safe Program: critical services by 2029, Microsoft 365 and data services by 2033
Google Workspace	PQC orchestration for client-side encryption and external key managers targeted by 2028
S/MIME and PGP	Signature and key-encapsulation formats are being revised by the IETF; deployable post-quantum S/MIME depends on domain 5 certificates

11 Domain 11: Devices, firmware, OT and hardware roots of trust

Endpoints, IoT and embedded devices, operational technology, TPMs, secure boot and firmware update chains. Long-lived, constrained and often unpatchable, so the plan is frequently replacement rather than upgrade, and procurement language for the next tender is the first control.

Provider	What it offers
PQShield	PQC hardware IP, firmware and SDKs for constrained devices
Infineon	OPTIGA TPM SLB 9672 with a post-quantum-secured firmware update path; next-generation OPTIGA TPM embeds ML-KEM and ML-DSA (June 2026)
NXP	i.MX 94 with EdgeLock Secure Enclave: post-quantum secure boot, debug and update; PQC services on secure elements and hardware security engines
BTQ QCIM	Crypto-agile compute-in-memory root of trust for chips, devices and secure enclaves
SEALSQ QS7001	Post-quantum secure element with ML-KEM and ML-DSA, plus the QVault TPM line; 2026 certification roadmap published

Provider	What it offers
OT and ICS vendors	Ask each for the firmware signing scheme (LMS/XMSS under CNSA 2.0) and the device certificate rotation path; the Handbook's substation example shows the pattern

Where cryptography cannot be changed on a fleet, segmentation and monitoring are the controls. Write them down as a decision with an owner and a review date under QCI-T4; an undocumented compensating control is an assumption with seniority.

12 Domain 12: Third-party, SaaS and cloud providers

Cryptography operated on your behalf. Addressed through vendor assessments, attestations, roadmap commitments and contract terms rather than direct technical change. Under the shared responsibility model, the provider secures its own endpoints and you must opt your resources in.

Provider	Key exchange in transit	Signatures and keys	Notes
AWS	ML-KEM hybrid TLS on KMS, ACM, Secrets Manager, S3, IAM and CloudFront	ML-DSA in KMS and Private CA	The most complete of the three; Kyber pre-standard endpoints retire during 2026
Google Cloud	X25519MLKEM768 on internal infrastructure TLS	Cloud KMS ML-DSA and SLH-DSA signing GA; ML-KEM preview	BoringSSL underneath; platform PQC roadmap published
Microsoft Azure	Windows and SymCrypt carry ML-KEM and ML-DSA	AD CS supports ML-DSA; Key Vault PQC for software keys only	Quantum Safe Program: critical services 2029, all by 2033; request the roadmap in writing
Cloudflare	Default at the edge and on Zero Trust tunnels	ML-DSA experimental	Largest production deployment on the public internet

For every SaaS provider in the QASI vendor field, the answer comes from Annex C section B, not from this handout. A supplier that has not answered is an exception, not a pending item.

13 Domain 13: Sector-specific protocols, payments, digital assets and custody

Industry protocols with their own standards bodies and timelines. Payment networks move on EMVCo, PCI SSC and SWIFT schedules. Digital-asset chains move on protocol upgrades you do not control, and on-chain public keys are already exposed, so signature migration cannot wait for key exchange. Handout C3 covers this domain in depth.

Provider	What it offers	Status
Futurex Excrypt	Payment HSM with native ML-KEM and ML-DSA; the first PCI HSM-validated platform supporting PQC, with no hardware refresh required	Shipping
Utimaco Atalla AT1000	First payment HSM with FIPS 140-3 (June 2025); PQC via Q-safe on the general-purpose line	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 payment protocol timelines; no post-quantum EMV specification is final	Track through the vendor pack and scheme bulletins
Algorand	Falcon signatures on mainnet; native PQ accounts and institutional PQ multisig on the roadmap	First PQ mainnet transaction November 2025; broad resilience targeted for 2027
Bitcoin BIP-360	Pay-to-Merkle-Root addresses with ML-DSA	Merged into the BIP repository February 2026; testnet only, not activated
Quantum Resistant Ledger	Hash-based XMSS signatures on every transaction since 2018	Live
BTQ	QSSN quantum-secure stablecoin network, Bitcoin Quantum, and QCIM silicon for signing devices	Commercial; verify deployment status directly
BitGo	Completed the first post-quantum MPC transaction simulation with Silence Laboratories	Simulation; not production
Coinbase	Independent quantum advisory board formed January 2026; position paper April 2026	Research and roadmap
Fireblocks, Anchorage Digital, Dfns	Reported work on quantum-resistant systems and Bitcoin migration research	Not documented by the firms; ask each for its roadmap

COMMON MISTAKE
Waiting for the protocol. For a client holding digital assets, the immediate controls are operational: no address reuse, minimal on-chain public key exposure, and a custody vendor request under Annex C section B. None of those depend on a mainnet activation.

14 Questions to ask any provider before you commit

These line up with Annex C sections A to F; the last two are section G, where the provider touches AI artifacts.

1. Which FIPS 203, 204 or 205 parameter sets do you support today, and in which product version? Not “Kyber” or “Dilithium”: the pre-standard names are a sign the implementation predates the standard.
2. Which of those are inside a CAVP or FIPS 140-3 validation, with the certificate number?
3. Do you support hybrid modes, and can the classical half be removed later without a product change?
4. Can the algorithm be changed by configuration, and have you tested rollback?
5. What are the performance costs: handshake latency, certificate size, signature size, memory on constrained devices?
6. What is your published deprecation timeline for RSA and ECC in your product, against NIST IR 8547’s 2030 and 2035 dates?
7. Will you provide a scoped CBOM for the product that meets QCI-5.4-03, and update it on material change?
8. Will an officer sign the attestation in the pack?
9. Where you sign, store or move AI artifacts: which signature scheme protects model provenance, and what is the complete key-protection scheme (KEM, KDF, wrap, recipient trust, bulk cipher) for AI artifact keys?
10. Where agents in your platform talk to each other or to ours: is the channel on hybrid key exchange, and can a downgrade be detected?

Sources

Provider capabilities are taken from each publisher’s own documentation, the PKI Consortium’s capabilities matrix and trade coverage, as of the date on the cover. Quantum Core Institute has not tested any product listed. PQC support changes with every release: confirm the version, the validation certificate and the licensing with the provider before you commit.

- PKI Consortium PQC Capabilities Matrix, a neutral, self-reported register of 50+ products
- AWS post-quantum cryptography · Cloudflare PQC support · Open Quantum Safe: TLS · Google Cloud PQC roadmap
- Cisco Secure Firewall PQC roadmap · Palo Alto Networks RFC 9370 hybrid keys · FortiOS 7.6 PQC for IPsec · Juniper quantum-safe IPsec · American Binary
- DigiCert ML-DSA issuance · Entrust CBOM announcement · Sectigo private PQC certificates · Microsoft AD CS ML-DSA
- Entrust nShield CAVP validation · Thales Luna firmware 7.9.0 · Utimaco Q-safe · Google Cloud KMS quantum-safe signatures · Azure Key Vault key types
- Commvault PQC · Veeam quantum readiness
- Microsoft PQC APIs GA · Microsoft Quantum Safe Program timeline · Okta on PQC · Ping Identity on PQC · FIDO and post-quantum passkeys · IDEMIA PQC PIV · Yubico PQC
- Zoom post-quantum E2EE · Apple iMessage PQ3
- Infineon OPTIGA TPM announcement · NXP post-quantum cryptography · SEALSQ QS7001 certification roadmap · BTQ

- Futurex PQC and PCI HSM · Utimaco payment HSM · Thales Luna 8 and payShield · Algorand post-quantum · Coinbase quantum advisory board · BitGo PQ MPC simulation
- QCI-QS1 Quantum Readiness and Post-Quantum Cryptography Governance Standard, v2.3 (September 23, 2026), at quantumcoreinstitute.com

Verification status: every named provider in this version was checked against its own documentation or press release, or trade coverage where noted, on September 23, 2026. The Azure Key Vault status rests on third-party reports and should be confirmed with Microsoft. The Thales SafeNet IDPrime PIV entry reflects the current product brief, not a roadmap statement.

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).