Quantum-Ready PKI for Constrained Devices

Why Now

- Adversaries can store encrypted traffic today and decrypt it later.
- Device lifecycles span 10-20+ years; crypto must survive the full journey.
- Boards and regulators expect a plan for post-quantum risk.

What We Deliver

- Hybrid PKI: classical + PQC algorithms, policy-driven and switchable.
- No-downtime migration for constrained devices and low-bandwidth links.
- Custody & compliance: FIPS 140-2 -> 140-3 alignment, BYOK/HYOK, audit evidence.
- Vendor-neutral KMS/HSM: Azure Key Vault/Managed HSM, AWS KMS/CloudHSM, Google Cloud KMS/Cloud HSM.

Outcomes That Matter

- Risk reduced: HN/DL exposure addressed for communications and firmware.
- Predictable rollout: staged cohorts with green SLO gates and safe rollback.
- Regulator-ready: CP/CPS, key ceremonies, revocation and evidence packs.
- No lock-in: open libraries (wolfSSL, mbedTLS, OpenSSL + liboqs) and portable formats (X.509/COSE, SUIT).

Our Staged Approach

- A) Discovery & Positioning (2-6 weeks): Crypto SBOM; executive roadmap with cost, effort, and KPIs.

- B) Governance & Design (4-8 weeks): CP/CPS updates; Root->PQC-capable intermediates->device profiles; BYOK/HYOK across Azure, AWS, Google.
- C) Lab & Pilot (8-16 weeks): Hybrid TLS; dual-signed firmware/manifests; rollback rehearsed; telemetry to SIEM.
- D) Wave Rollout & RunOps: Cohorts; rotation cadence; chain size optimisation and cost controls.

Proof & KPIs

- >=99.9% handshake success in pilot; <=0.1% classical fallbacks.
- >=99% OTA success first attempt; <=0.05% rollbacks.
- <=10% increase in boot-to-service time (targeted by device class).

What Changes (In Plain Terms)

- On Devices: hybrid crypto via policy; dual signatures for OTA; short-lived comms certs; strong firmware key custody.
- Back End & Gateways: PQC-capable issuing CAs; hybrid TLS support; FIPS 140-3 aligned KMS/HSM with BYOK/HYOK.

Why SafeCipher

- Deep PKI + HSM/KMS practice across Azure, AWS, Google; on-prem ceremonies & cloud custody.
- Open-stack first: wolfSSL, mbedTLS, OpenSSL + liboqs, liboqs, PQClean.
- Sector-ready governance: ISO/IEC 27001, IEC 62443, utility and mobility contexts.
- Runbooks and evidence your auditors will accept.

Typical Deliverables

- Executive deck; reference architecture; policy pack; implementation kits; operational playbooks.

Getting Started

- Begin with a 4-6 week assessment to size risk, quantify cost, and plan an achievable pilot.

Contact SafeCipher

Email: crypto@safecipher.co.uk | Web: https://www.safecipher.co.uk

SafeCipher Vendor-neutral cryptography, PKI, and key management consultancy.