Upgrade to FIPS 140-3 — Without Disruption

SafeCipher: the vendor-neutral partner for regulated HSM migrations

SafeCipher · Innovative Cryptography Solutions for Enterprises · safecipher.com

FIPS 140-2 modules are being retired across CMVP listings. Auditors now expect 140-3 for new deployments. SafeCipher delivers governed, low-risk migrations: blue/green cutovers, M-of-N ceremonies, and audit-ready evidence—without downtime.

Why act now

- Reduce audit exposure and procurement friction tied to 'Historical' 140-2 modules.
- Strengthen resilience and support posture with modern, validated firmware.
- Position for post-quantum (ML-DSA/ML-KEM) with agile crypto patterns.

What SafeCipher delivers

- Governance-first migration plan aligned to CP/CPS and Key Management Standards.
- Key ceremonies with evidence (M-of-N, immutable logs, firmware attestations).
- Hybrid architecture: offline roots on-prem; fit-for-purpose issuing (on-prem/cloud) with HA/DR.
- Zero-outage execution: blue/green issuance, canary renewals, rollback runbooks.
- Audit-ready artifacts: CMVP certs, OCSP/CRL SLOs, traceability to ISO/NIS2/PCI.

Why SafeCipher

- Vendor-neutral across Thales Luna, Entrust nShield, Utimaco, Azure Managed HSM, AWS CloudHSM, GCP Cloud HSM.
- Deep PKI/CLM expertise (AD CS, EJBCA, Keyfactor, Venafi/CyberArk).
- Proven in finance, public sector, healthcare, payments, and defense.

Typical timeline (8–16 weeks)

- Week 1–2: Discovery, governance updates, inventory, CMVP validation.
- Week 3–5: 140-3 build, ceremonies, integration validation in pre-prod.
- Week 6–9: Blue/green cutover, canary cohorts, performance/resilience tests.
- Week 10–16: Decommission 140-2, finalize evidence pack, handover runbooks.

Call to action

Let’s modernize to FIPS 140-3 with confidence. Book a discovery call: safecipher.com · crypto@safecipher.com