ENCRYPTION CONSULTING

CASE STUDY

CUSTOM PKI IMPLEMENTATION

Meeting a Fortune 100 SPDM mandate with PKI-based device authentication

How we designed and built a custom, on-premises PKI for a Fortune 100 hardware and IoT enterprise, engineered for SPDM, never-expiring device certificates, and the post-quantum era.

SECTOR	PROFILE	ENGAGEMENT
Hardware & IoT	Fortune 100, Global	Custom PKI build

70+/min
Certificates issued at peak

FIPS 140-3
HSM-secured keys

Quantum-safe
Hybrid ML-DSA + RSA

A Fortune 100 hardware maker, trusted to secure every device

We recently completed one of our most technically demanding PKI implementations for a global Fortune 100 hardware and IoT enterprise. With more than 25 years of leadership, they are a pioneer in hardware innovation, manufacturing, and secure device management, with a portfolio spanning on-chip SSDs, high-performance RAM, CoRIM solutions, and SBOM integration for product traceability.

A reputation like that depends on trust at the silicon level. They came to us for a custom, on-premises PKI, not something off the shelf, built to meet the SPDM specifications from the DMTF for secure communication and attestation between hardware and software, and to support both their near-term and long-term goals.

For a hardware maker, trust starts in the silicon. Every device that ships needs an identity strong enough to prove it is genuine, for its entire life.

Five requirements, no off-the-shelf answer

This Fortune 100 hardware maker didn't want anything off the shelf. They came to us with a precise set of requirements that shaped every design decision.

1

Never-expiring certificates

Device certificates are embedded into hardware for life, so they needed a validity running to 12/31/9999 while still meeting OCP, DICE, and IEEE 802.1AR standards.

2

Post-quantum readiness

With the NIST PQC transition expected around 2030, the PKI had to support quantum-safe algorithms from day one and stay vendor-neutral as standards evolve.

3

HSM-backed key security

Every root and subordinate CA and signing key had to live in FIPS 140-3 HSMs, using a shared, high-availability setup rather than a separate HSM per CA.

4

Strict issuance policies

Operator signing limits, path length constraints to block cross-certification, custom SAN formats, variable field data controls, device-specific certificate profiles, and a legally reviewed CP and CPS.

5

Resilience, scale, and a tight clock

The design had to include hot and cold disaster recovery from day one, issue 70+ devices per minute at peak (around 50,000 a year), and be production-ready by the end of Q3, with work starting only in Q2.

> The result was a secure, scalable, future-ready PKI, purpose-built to integrate with hardware manufacturing and enable trusted device identity at every stage of production.

ENGAGEMENT SUMMARY
ENCRYPTION CONSULTING · PKI SERVICES

A custom PKI, engineered to spec

We started with collaborative workshops to learn their manufacturing and security workflows, then designed a PKI to match, running parallel workstreams and constant testing to hit a tight deadline.

Certificates that never expire

We built templates and validation workflows for non-expiring device certificates, valid to 12/31/9999 and compliant with OCP, DICE, and IEEE 802.1AR, ready to embed for a device's entire life.

Hybrid, quantum-safe crypto

We issued certificates using both ML-DSA 87, a quantum-safe signature algorithm, and classic RSA, so legacy hardware keeps working today while newer devices are ready for the post-quantum era.

Hot-and-cold disaster recovery

We deployed a redundant PKI across hot and cold recovery sites, with automated backups, replication, and failover, so device authentication keeps running even if a site goes down.

Granular issuance policies

We enforced operator signing limits, set path length to none to block cross-certification, defined custom SAN formats and device-specific certificate profiles, and delivered a legally reviewed CP and CPS governing all issuance.

HSM with quorum control

We delivered a vendor-neutral, FIPS 140-3 HSM setup in a high-availability configuration, with quorum-based access requiring at least three custodians, ensuring separation of duties.

Speed, scale, and on-time delivery

We tuned the PKI to issue 70+ devices per minute with low latency and tens of thousands a year, and delivered the whole build, tested and documented, by the end of Q3.

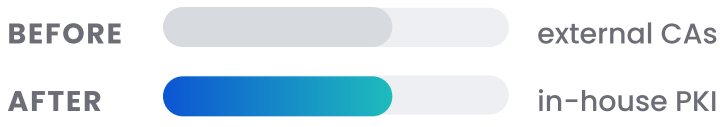
04 THE IMPACT

A foundation for millions of trusted devices

The new PKI became more than an upgrade. It now anchors secure identity and trust across millions of devices, from the factory floor to the field.

In-house

Full ownership of the certificate lifecycle



Scales with production

The PKI handles 70+ devices per minute and tens of thousands a year, so the company can grow manufacturing capacity without re-architecting its security.

Instant, self-served issuance

The team issues certificates instantly, enforces custom policies, and changes configuration without external vendors, reducing operational risk and long-term costs.

Compliant by design

All cryptographic operations and private keys stay inside the organization's own infrastructure, keeping them aligned with FIPS 140-3 and industry best practices.

Trusted device identity

Every device carries a unique, verifiable identity with full traceability from production to deployment, blocking unauthorized devices and strengthening the supply chain.

IN SUMMARY

A secure foundation for every device shipped

We delivered a custom, on-premises PKI built to an exacting brief: never-expiring device certificates valid to 12/31/9999 and compliant with OCP, DICE, and IEEE 802.1AR; hybrid ML-DSA 87 and RSA cryptography for post-quantum readiness; FIPS 140-3 HSMs with quorum-based three-custodian access; granular issuance policies with a legally reviewed CP/CPS; and high-volume scalability at 70+ devices per minute and 50,000 devices per year, all delivered production-ready within a single quarter.

The result is a fully in-house PKI that gives every device a trusted, verifiable identity from manufacturing to deployment. External CA reliance was eliminated, compliance with FIPS 140-3 is maintained within the organization's own infrastructure, and the architecture scales with production capacity without re-architecting security. The organization now has complete control over its certificate lifecycle and a secure foundation for long-term innovation and growth.

GET STARTED

Need a PKI built to your exact spec?

Talk to our PKI team →