ENCRYPTION CONSULTING

CASE STUDY

PKI SERVICES

From patchwork PKI to a single pane of glass for a US healthcare leader

A Minnesota-based healthcare leader with over 7,000 professionals had grown its PKI ad-hoc, with manual certificate management, local key storage, and no central visibility. Our PKI assessment mapped the gaps and a roadmap to a secure, scalable, compliant environment.

SECTOR	SIZE	ENGAGEMENT
Healthcare (US)	7,000+ professionals	PKI assessment

1
Single pane of glass

HSM
CA keys secured

2048+
Bit key strength

A healthcare leader, 7,000 strong

We completed one of our most extensive PKI assessment projects with a leading Minnesota-based healthcare organization, home to more than 7,000 professionals dedicated to setting new standards for pharmacies, developing treatments, and pursuing cures.

Over decades, the organization became an exemplary name, simplifying complexity and delivering a home-based pharmacy services platform to millions across the country. But the bigger it grew, the more its Public Key Infrastructure struggled to keep pace.

As the organization scaled, its PKI quietly became a patchwork. Functional, but not built to scale, and full of blind spots.

A patchwork PKI, full of blind spots

As the organization scaled, its PKI grew ad-hoc, leaving manual processes, weak key storage, and blind spots.

1

Ad-hoc, patchwork PKI

Their PKI had grown without a structured approach to certificate authorities or revocation, becoming a patchwork that worked but couldn't scale.

2

Manual certificate management

Issuing, renewing, and revoking thousands of certificates by hand slowed operations and risked outages from expired certs left in the system.

3

No policies, weak key storage

There were no CP or CPS documents to guide operations, and root and issuing CA private keys sat in software with weak access controls.

4

Hybrid inconsistency

Across on-prem and cloud, the team struggled to keep cryptographic controls and policy enforcement consistent under differing requirements.

5

No inventory, no discovery

Without a certificate inventory or discovery process, hidden wildcard and self-signed certificates created blind spots, while missing CA backups and a rigid single-CA dependency added data-loss risk and vendor lock-in.

> “
> The organization's PKI environment had evolved to meet immediate security requirements, but without a compliance-focused strategy or centralized oversight, it left critical gaps that could lead to costly penalties.
>
> **ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · PKI SERVICES**

From assessment to a clear roadmap

The organization chose our structured, phased PKI assessment. We reviewed policies, ran a gap analysis against a NIST and FIPS-aligned framework, and delivered a prioritized remediation roadmap.

Phased PKI assessment

A structured, phased assessment reviewed their policies and standards and defined clear use cases for the target PKI environment.

Gap analysis to a framework

Stakeholder workshops compared their as-is PKI to a target state, scored against a custom framework aligned with NIST 2.0 and FIPS 140-2/3.

Multi-CA, no lock-in

We verified the PKI could integrate multiple certificate authorities, freeing the organization from single-vendor dependency across its use cases.

Automated lifecycle and alerts

We recommended automating certificate and key lifecycle management with real-time expiration alerts, cutting manual work and outage risk.

HSM keys and least privilege

Root and issuing CA keys move into HSMs, with 2048-bit-plus key generation and least-privilege access aligned to NIST SP 1800-16.

Single pane of glass

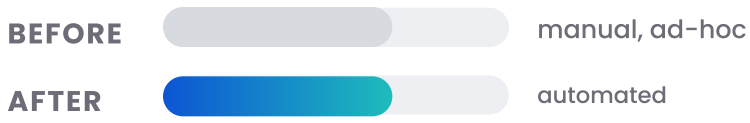
A centralized inventory with automated CA backups tracks status, ownership, and dependencies across on-prem and cloud, ending the blind spots.

One clear view, zero surprises

The assessment turned a fragmented PKI into a centralized, automated one, giving the organization visibility, control, and continuous, outage-free operations.

0

Outages from expired certificates



Automated lifecycle

Automating issuance, renewal, and key management cut manual work and lets the team actively prevent expiry-driven disruptions.

HSM-backed CA keys

Root and issuing CA keys now live in HSMs with strong access controls and clear ownership, building trust in every certificate operation.

Passwordless everywhere

The organization adopted passwordless authentication, deploying certificates across laptops, mobiles, internal web servers, and IoT devices.

Single source of truth

A centralized inventory shows which certificates are active, who owns them, and which need attention, so expirations never come as a surprise.

IN SUMMARY

From fragmented PKI to digital trust

In healthcare, digital trust underpins everything. Our comprehensive PKI assessment took the organization from a fragmented, ad-hoc environment to a secure, scalable one. Automated certificate and key lifecycle management cut manual work and prevents expiry-driven outages, root and issuing CA keys now sit in HSMs with least-privilege access, and a centralized inventory gives a single pane of glass over status, ownership, and dependencies. With standardized policies, passwordless authentication, and a NIST and FIPS-aligned framework, the organization has a future-ready PKI built for years of trust and growth.

GET STARTED

Assess and modernize your PKI.

Talk to our PKI team →