ENCRYPTION CONSULTING

CASE STUDY

PKI DESIGN AND IMPLEMENTATION

Building a secure PKI foundation for healthcare with a two-tier deployment

How one of Texas's largest healthcare providers replaced a risky, online PKI with a hardened, two-tier infrastructure, so its teams can focus on delivering faster, better patient care.

MEMBERS	REGION	ENGAGEMENT
~10 million	United States	PKI Implementation

Two-tier
Microsoft PKI architecture

HSM Backed
Root & issuing CA keys

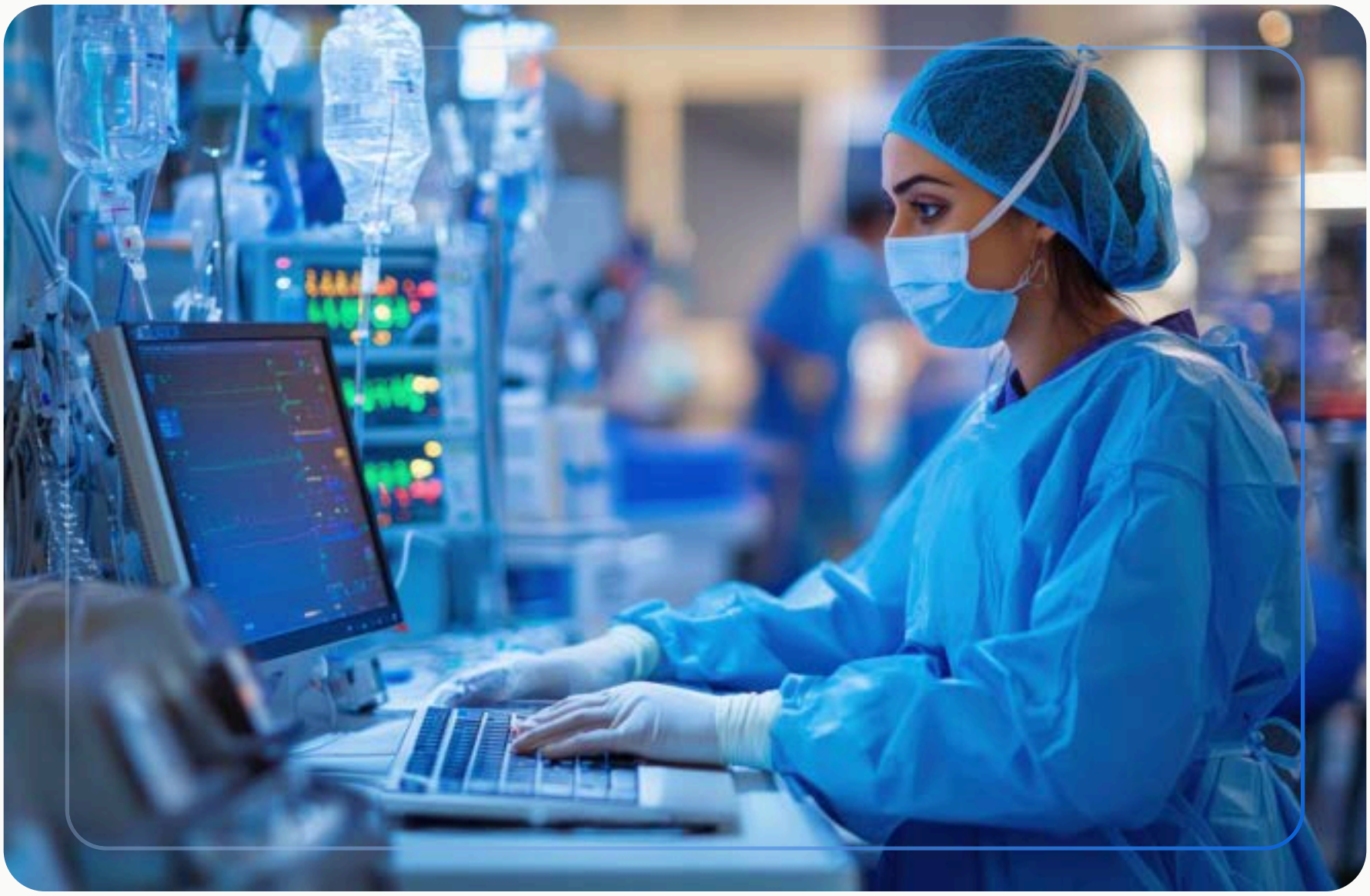
HIPAA + FIPS
Compliant key ceremony

A healthcare leader serving nearly ten million members

Our client is one of the largest healthcare providers in Texas, known for everything from general practice to specialized care in cancer, cardiovascular disease, trauma, and pediatrics. As the state's largest provider of health benefits, they work with more than 150,000 physicians and practitioners and over 500 hospitals to serve close to ten million members across individual, employer, family, Medicaid, Medicare Advantage, dental, and vision plans.

For more than a century, the organization has been a pillar of health and wellness, available around the clock. Public Key Infrastructure sits at the core of that promise, issuing the certificates that authenticate access, encrypt sensitive data, and keep internal communications trustworthy. As their digital services grew more complex, the cracks in that foundation began to show.

In healthcare, digital trust is patient trust. When PKI is the backbone of your security, every weak link in it puts patient data, uptime, and confidence on the line.



A fragile foundation under a growing system

Public Key Infrastructure was the backbone of their security, but as their digital services grew, real weaknesses in that foundation began to surface.

1

Exposed, online Root CA

The Root CA was kept online and domain-joined, widening its attack surface to network and domain threats, against best practices that require an offline, isolated Root CA.

2

Keys outside an HSM

Root and Issuing CA private keys lived in an encrypted file system rather than a dedicated HSM, leaving them exposed if the server was ever breached.

3

Untracked self-signed certificates

With no guidelines or tracking for self-signed certificates, they were issued freely and some expired unnoticed, causing avoidable outages.

4

Misconfigured CA and 25-year validity

CAPolicy.inf was never installed, so a missing PathLength constraint allowed rogue subordinate CAs, and a 25-year validity reused the same keys for decades, raising exposure to quantum and cryptographic weakening.

5

No key custodians or recovery plan

A single administrator could change the CAs with no separation of duties, and with no disaster recovery or business continuity plan, there was no way to restore systems or keep running after an incident.

> “Five gaps, one trust chain. Every weakness traced back to the same Root CA, so the fix had to start there, then rebuild outward.

ENCRYPTION CONSULTING ASSESSMENT TEAM
Pre-Implementation Assessment | Encryption Consulting · PKI Services

A hardened PKI, designed and built end to end

We took the client from a fragile, exposed setup to a secure two-tier PKI, handling design, key ceremony, hardening, enrollment, and recovery from start to finish.

A two-tier Microsoft PKI

We built a scalable two-tier architecture: a secure offline Root CA as the root of trust, with two online subordinate CAs issuing machine and user certificates. Validity periods were reduced to match best practices.

HSM-backed keys and a key ceremony

We integrated tamper-proof HSMs for key storage and ran a HIPAA and FIPS-aligned key ceremony, storing all Root and Issuing CA keys with access limited to authorized custodians.

Discovery and design

We mapped the existing PKI environment, reviewed policies and standards, defined use cases from SSL/TLS to S/MIME, authentication, and code signing, and finalized the new architecture with the client.

Documentation and knowledge transfer

We produced architecture, key ceremony, Certificate Policy, and Practice Statement documentation, then ran knowledge-transfer sessions covering daily operations, disaster recovery, continuity, and redundancy and failover for availability.

Hardened CAs and key custodians

We installed CAPolicy.inf with a PathLength constraint to block rogue subordinate CAs, defined a key custodian matrix requiring multi-person approval, and added tracking, reporting, approval, and revocation controls for self-signed certificates.

Secure enrollment and monitoring

We deployed NDES with a Web Application Proxy for safe certificate enrollment to mobile devices over HTTPS, with firewall rules limiting traffic to port 443, plus an OCSP responder for real-time revocation, all validated through testing.

04 THE IMPACT

From exposed and fragile to secure and resilient

With the new two-tier PKI in place, the organization closed its compliance gaps, shrank its attack surface, and gained a foundation built to scale.

25-year

Long-lived keys, cut to best practice

BEFORE — 25 years

AFTER — short, rotated

A protected root of trust

An offline Root CA and HSM-stored keys put their PKI foundation beyond network attacks, sharply reducing the risk of breaches and exposure of sensitive member health data.

Accountability and control

Key custodians and shorter validity removed single points of control, so changes need multiple approvals and tracked self-signed certificates no longer cause surprise outages.

Clear, scalable operations

Architecture, policy, and procedure documentation made daily management efficient and PKI scaling simple. NDES integration simplified certificate provisioning for mobile devices.

Resilient and compliant

Disaster recovery, business continuity, scheduled backups, and failover keep services running, while the HIPAA and FIPS-aligned build keeps them compliant.

IN SUMMARY

A secure foundation for better patient care

With the Root CA exposed online, private keys stored outside HSMs, a 25-year certificate validity period, and no key custodians or disaster recovery plan, the existing PKI was a liability rather than a foundation. Encryption Consulting designed and deployed a hardened two-tier Microsoft PKI with an offline Root CA, HSM-backed keys secured through a HIPAA and FIPS-aligned key ceremony, CAPolicy.inf with PathLength constraints to block rogue subordinate CAs, a key custodian matrix enforcing multi-person approval, and reduced certificate validity periods aligned to best practices. NDES with OCSP was deployed for secure mobile enrollment and real-time revocation.

For a healthcare provider serving nearly 10 million members through 150,000+ physicians and 500+ hospitals, every PKI weakness is a risk to patient data, system uptime, and regulatory compliance. With comprehensive documentation, disaster recovery with redundancy and failover, formal self-signed certificate controls, and knowledge transfer sessions ensuring the team can operate and recover the infrastructure independently, the organization has a secure, scalable foundation that frees its teams to focus on delivering high-quality, trusted patient care.

GET STARTED

Build a secure PKI you can grow on.

Talk to our PKI team →