ENCRYPTION CONSULTING

CASE STUDY

PKI ASSESSMENT

Strengthening retail security at national scale with a full PKI assessment

How one of the largest farm and ranch retailers in the U.S. uncovered hidden gaps in its public key infrastructure and built a clear roadmap to a stronger, more resilient security foundation.

STORES	REGION	ENGAGEMENT
1,800+	United States	PKI Assessment

End-to-end
Remediation roadmap

2048 bit+
Hardened key baseline

FIPS 140-2/3
Level 3 HSM key protection

A retail leader serving rural America, scaling with security in mind

Encryption Consulting partnered with one of the largest farm and ranch store chains in the United States, a retailer that serves recreational farmers, ranchers, and rural homeowners. With more than 1,800 stores across 40-plus states, the chain sells everything from livestock feed and pet supplies to tools, hardware, clothing, and outdoor living goods, and it has built its reputation on knowledgeable staff and genuine support for rural communities.

As the business kept growing, its leaders wanted to be sure their security could grow with it. They asked us to assess their Public Key Infrastructure (PKI), the system of certificates and keys that protects sensitive data across the company. The goal was clear: understand the current state of the environment, find the gaps, and define what the PKI needed to look like to support the next phase of growth.

In retail, trust is everything. When the certificates and keys behind your systems go unmanaged, customer data, store operations, and brand reputation are all on the line.

The gaps hiding inside a growing PKI

The building blocks of a PKI were in place, but our assessment found that much of it was undocumented, ungoverned, and unmonitored. Five themes stood out.

1

Aging platform and architecture

The managed PKI ran on a legacy Windows Server with private keys outside HSMs, an overly long Root CA validity, and no upgrade path, backups, or SIEM logging.

2

Missing governance and documentation

No Certificate Policy, Practice Statement, or subscriber agreement, and core architecture, operations, and recovery documentation was missing or incomplete.

3

Loose access control and accountability

Least privilege wasn't enforced, leaving weak access control, room for rogue CAs and unauthorized key access, and cross-border data-sovereignty exposure.

4

Outdated cryptography and risky templates

More than 60% of keystores still used 1024-bit keys, certificates were issued with no key-length or usage checks, and many private keys had no HSM protection or backups.

5

No lifecycle automation or visibility

With no certificate discovery and no central inventory, the team tracked everything by email. The full lifecycle was manual, monitoring was absent, and only a few staff had the PKI skills to keep up.

> The chain's PKI had drifted into a state where governance, cryptography, and lifecycle management were all running on assumption rather than control.

ENCRYPTION CONSULTING ASSESSMENT TEAM
ENTERPRISE CHALLENGES SUMMARY: ENCRYPTION CONSULTING · PKI ASSESSMENT

A prioritized roadmap, from quick wins to long-term change

We turned the findings into a prioritized strategy and a clear remediation roadmap, with immediate fixes and longer-term programs across the platform, lifecycle, governance, and people.

Template and CSR governance

A defined process to create, approve, and track certificate templates, backed by a central inventory, standardized CSR approval workflow, CA database cleanup, and templates meeting Microsoft's Strong Certificate Mapping (SID) requirements.

A modernized, future-proof platform

A migration to Windows Server 2022, FIPS 140-2/3 Level 3 HSMs for key protection, a dedicated test environment, and full architecture documentation.

A structured PKI assessment

We reviewed policies and configurations, ran stakeholder workshops, and used a PKI assessment tool and a CMMI maturity model to measure how mature their practices really were.

Automated certificate lifecycle

Automated renewal for managed and public CAs, a Certificate Lifecycle Management tool for discovery and automation, and CA auditing for accountability.

Policy, risk, and resilience

CP, CPS, and subscriber agreement. Least-privilege access with Two-Person Integrity. Formal key destruction and recovery procedures. Disaster recovery with CA backups every three to six months and Root CA keys stored offline. A risk and compliance program and PKI/HSM training for the team.

Health monitoring and alerting

Scheduled PKI health monitoring with alerts, regular vulnerability scanning of issued certificates, and quarterly configuration reviews against an operations checklist.

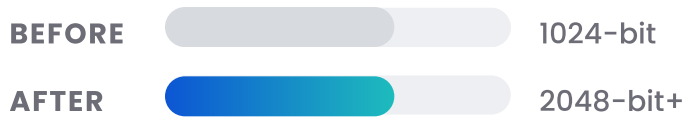
04 THE IMPACT

From hidden risk to a resilient foundation

Put into action, the roadmap moved the client from scattered, manual practices to a secure, well-governed PKI built to scale with the business.

60%+

Keystores hardened off 1024-bit keys



Visibility restored

Discovery, active monitoring, and a central inventory replaced email threads and guesswork, giving the team real insight into the keys and certificates across their environment.

Ownership and accountability

Clear policies, roles, and audit trails defined responsibilities; least-privilege access shrank the attack surface and unauthorized-issuance risk. On-demand PKI/HSM training and knowledge transfer built in-house expertise, cutting reliance on individuals.

Hardened and modernized

A move to Windows Server 2022, HSM-backed keys, and a 2048-bit or higher baseline closed long-standing cryptographic and platform risks.

Resilient by design

Automated lifecycle management, a disaster recovery plan, and regular backups keep renewals on time and the business running through incidents and system failures.

IN SUMMARY

A stronger PKI, ready for what comes next

With more than 60% of keystores still running on 1024-bit keys, no CP or CPS in place, and the entire certificate lifecycle managed by email, the assessment revealed a PKI environment that had scaled in footprint but not in governance. Encryption Consulting delivered a prioritized remediation roadmap covering infrastructure modernization to Windows Server 2022, FIPS 140-2/3 Level 3 HSM key protection, a 2048-bit minimum key baseline, automated lifecycle management, and a formal governance framework with least-privilege access and Two-Person Integrity controls.

For a retailer operating 1,800+ stores across 40+ states, every unmanaged certificate is a risk to store operations, customer data, and brand trust. With clear policies, disaster recovery procedures, and PKI and HSM training now in place, the organization has a security foundation built to grow with the business rather than silently fall behind it. Cross-border data sovereignty and compliance obligations were also formally assessed with stakeholders, positioning the organization to meet regional regulatory requirements as it continues to expand.

GET STARTED

See where your PKI stands. Then make it stronger.

Book a PKI assessment →