ENCRYPTION CONSULTING

CASE STUDY

PKI SERVICES

A PKI rebuilt from the root for a global retailer

A prominent global retailer, running thousands of stores and a major online presence, had let its PKI grow without a plan: an expiring Root CA on end-of-support infrastructure, nine uncoordinated Issuing CAs, and keys outside secure hardware. Encryption Consulting assessed and rebuilt it.

SECTOR	PLATFORM	ENGAGEMENT
Retail (global)	Microsoft ADCS	Assess + deploy

Offline
Root CA established

HSM
FIPS 140-2 L3 keys

4
Domain forests covered

Global scale, an aging PKI

This retail organization is a prominent global player, operating a vast network of stores selling everything from clothing and electronics to groceries and home essentials. With a major online presence, it's known for convenience, service, and competitive pricing, and employs thousands worldwide.

Its PKI, central to securing daily digital transactions and signing sensitive data, had fallen behind. Outdated technology couldn't support the scale, and a shortage of staff skilled in modern PKI made it hard to upgrade or manage, putting data integrity and customer trust at risk.

A PKI is only as trustworthy as its Root CA. On end-of-support infrastructure and nearing expiry, this one needed rebuilding.

A PKI grown without a plan

No planning, no skilled team, an exposed Root CA, weak lifecycle management, and unprotected keys all undermined trust.

1

No planning or tracking

Built without structured planning, the PKI made it easy to lose track of which certificates existed, when they expired, and where, risking failed audits and key misuse.

2

No skilled PKI team

Running an in-house PKI takes a dedicated, skilled team, and without one the organization couldn't respond effectively to an outage or security incident.

3

Root CA security

All trust flows from the Root CA. If it can't be trusted, nothing below it can, yet this Root CA sat exposed on end-of-support infrastructure.

4

Poor lifecycle management

Without forward planning for the full certificate lifecycle, expired certificates went unmanaged, inviting outages and significant unplanned costs.

5

Keys outside secure hardware

Keys can be analyzed and stolen in use or in transit, and these were not held in FIPS 140-2 Level 3 hardware, leaving the foundation of trust exposed.

> The PKI had grown with the business but without a plan. An expiring Root CA on end-of-support infrastructure, 9 uncoordinated Issuing CAs, and keys outside secure hardware needed a full rebuild.

ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · PKI SERVICES

A modern PKI, from the root up

Encryption Consulting assessed the old PKI and rebuilt it on Microsoft ADCS 2016 R2, with an offline Root CA, HSM-protected keys, consolidated Issuing CAs, and full CP/CPS documentation.

PKI Assessment

The engagement began with a PKI Assessment of the existing infrastructure, surfacing the gaps that a new design would need to close.

New PKI on ADCS 2016 R2

A new PKI service was designed on Microsoft ADCS 2016 R2, retiring a Root CA that ran on end-of-support ADCS 2008.

CP/CPS and consolidation

CP and CPS documents were created and the Issuing CAs consolidated from nine to four, closing the gaps in policy and procedure.

HSM-protected keys

An HSM was installed to hold CA and ICA keys, with formal Key Ceremony procedures and clear roles for key management.

Offline Root CA hierarchy

The new hierarchy pairs an offline Root CA with four Issuing CAs connected to four domain forests across the business.

Templates and CDP

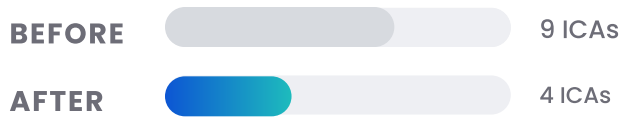
Existing certificate templates were validated and new ones created, with the existing HTTP server and LDAP used for the CRL distribution point.

Leaner, modern, audit-ready

The new PKI gave the retailer a well-defined, lower-cost foundation of trust, audit-ready and able to support modern certificate needs across the business.

9 → 4

Issuing CAs consolidated



A well-defined PKI

A redesigned, modern PKI now defines the people, processes, and technology needed to run it day to day.

Lower infra costs

Consolidating and removing redundant Issuing CAs cut infrastructure and maintenance costs across the estate.

Audit-ready

The assessment and deployment produced exactly the information auditors needed, simplifying compliance.

Ready for MDM, VPN, IoT

The new PKI supports modern certificate demands like MDM, VPN, and IoT, plus valid chains for internal web apps.

IN SUMMARY

Trust, rebuilt from the root

Encryption Consulting's PKI Assessment and Deployment proved transformative for this global retailer. After assessing the aging environment, the team rebuilt the PKI on Microsoft ADCS 2016 R2, with an offline Root CA, an HSM protecting CA and ICA keys under formal Key Ceremony procedures, and Issuing CAs consolidated from nine to four across four domain forests. New CP and CPS documentation, validated certificate templates, and clearly defined roles brought structure to certificate and key management. The result is a well-defined, lower-cost PKI that satisfies auditors and supports modern certificate demands like MDM, VPN, and IoT, restoring a dependable foundation of trust.

GET STARTED

Rebuild your PKI on solid ground.

Talk to our PKI team →