ENCRYPTION CONSULTING

CASE STUDY

PKI ASSESSMENT & SUPPORT

Strengthening the PKI behind a gas network with assessment and 24/7 support

How a North American energy company strengthened a fragile PKI, replacing expired certificates and manual processes with automation, governance, and round-the-clock support that keeps gas service reliable.

CUSTOMERS	REGION	ENGAGEMENT
300,000+ gas	North America	PKI Assessment & Support

24/7
Ongoing PKI support

Automated
Certificate Lifecycle

Real-time
Monitoring & detection

An energy leader serving 300,000 gas customers

This leading North American energy infrastructure company is built around clean, economical energy and long-term sustainability. It serves more than 300,000 industrial, commercial, and domestic gas customers, with safety, reliability, and environmental responsibility at the center of everything it does.

With 1,000 employees and customer satisfaction as a top priority, the company invests heavily in operational excellence. That means strong security protocols, disciplined risk management, and modern cryptographic standards, with access controls, encryption, and continuous monitoring protecting both its infrastructure and its customers' trust.

For a gas provider, reliability is a promise. A weak PKI quietly threatens the certificates and systems that keep that promise running.

A fragile PKI under a growing threat landscape

As cyber threats grew, an assessment of the company's PKI surfaced deep, overlapping weaknesses across security, governance, and operations.

1

Expired certs and weak crypto

Expired certificates were still in use alongside weak cryptographic algorithms and possibly misconfigured CAs, leaving the environment exposed to modern threats.

2

Blind to risk

Insufficient monitoring, inefficient risk detection, inconsistent CRL updates, and missing logging made it hard to catch anomalies or respond in time.

3

No governance baseline

With no CP or CPS and no defined key-security standards for algorithms, key lengths, or hashing, certificate issuance was inconsistent and hard to interoperate.

4

Manual lifecycle, frequent outages

Manual certificate management drove human error, and unmanaged certificates caused frequent outages that pushed operational costs up by around 10%.

5

No operating model or compliance program

Without a Target Operating Model the PKI couldn't centralize or scale, and with no formal risk assessment, self-signed and wildcard guidelines, or key destruction and discovery, the company struggled to meet NIST, FIPS, and PCI DSS.

> “Expired certificates and manual processes weren't just technical debt, they were a direct risk to gas service reliability for hundreds of thousands of customers.

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

From a deep assessment to round-the-clock support

We assessed their full PKI across on-premises, cloud, and hybrid, built a remediation roadmap, then stayed on as their 24/7 support team to put it into practice.

PKI assessment and roadmap

We evaluated their policies, architecture, and use cases across on-premises, cloud, and hybrid, ran stakeholder workshops, and built a prioritized remediation roadmap.

24/7 PKI support

They subscribed to our round-the-clock support for PKI restoration and troubleshooting, with fast response plans that limit the impact of certificate expirations or HSM failures.

CP and CPS governance

We built a Certificate Policy and Certificate Practice Statement to standardize how certificates are issued and managed, closing long-standing governance gaps.

Certificate lifecycle automation

With CertSecure Manager, we automated certificate renewals, CRL updates, and status monitoring, removing the manual steps behind missed renewals and bad CRLs.

HSM upgrade

We planned and executed a move to nShield 5s HSMs while keeping their existing Microsoft AD CS PKI running, with end-to-end support throughout the transition.

NDES enrollment and CRLs

We guided them through Network Device Enrollment Service for seamless certificate distribution, and created and published CRLs to retire compromised certificates.

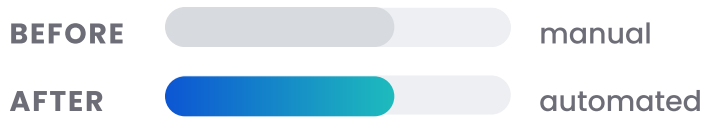
04 THE IMPACT

From reactive and manual to proactive and resilient

With the gaps closed and support in place, the company turned a fragile, reactive PKI into a secure, automated one that scales with demand.

~10%

Outage-driven operating costs, reclaimed



Scalable, compliant PKI

A microservices model and a real governance framework let them scale issuance, revocation, and validation on demand, aligned with NIST, FIPS, and PCI DSS.

Fewer errors, smoother operations

Automated renewals and revocations cut manual errors and service disruptions, keeping critical operations and business continuity on track.

Centralized visibility and control

Centralized management of cryptographic assets gave the team clear visibility and control, reducing disruptions and improving agility.

Proactive, real-time monitoring

Real-time monitoring surfaces risks early, and active CRL management retires outdated or compromised certificates fast, strengthening trust across systems.

IN SUMMARY

A secure, scalable PKI, supported around the clock

With our assessment, remediation roadmap, and ongoing support, the energy company turned a fragile PKI into a secure, scalable, and resilient one. Automated certificate lifecycle management, a clear governance framework, upgraded HSMs, and real-time monitoring cut operational costs and service disruptions, while round-the-clock support keeps the environment current with the latest cryptographic standards. The result is a future-proof foundation that protects critical infrastructure and the trust of hundreds of thousands of customers.

GET STARTED

Assess your PKI, then keep it secure.

Book a PKI Assessment →