ENCRYPTION CONSULTING

CASE STUDY

CERTIFICATE LIFECYCLE MANAGEMENT

Certificate management for a nationwide retailer without the renewal fire drills

A US retail giant was juggling certificates across more than twenty domains and five certificate authorities, with manual renewals and missed alerts threatening outages. CertSecure Manager brought it all into one automated, policy-driven platform.

SECTOR	FOOTPRINT	SOLUTION
Retail (US)	Nationwide stores	CertSecure Manager

5+
Certificate authorities, one portal

50+
Domains under policy control

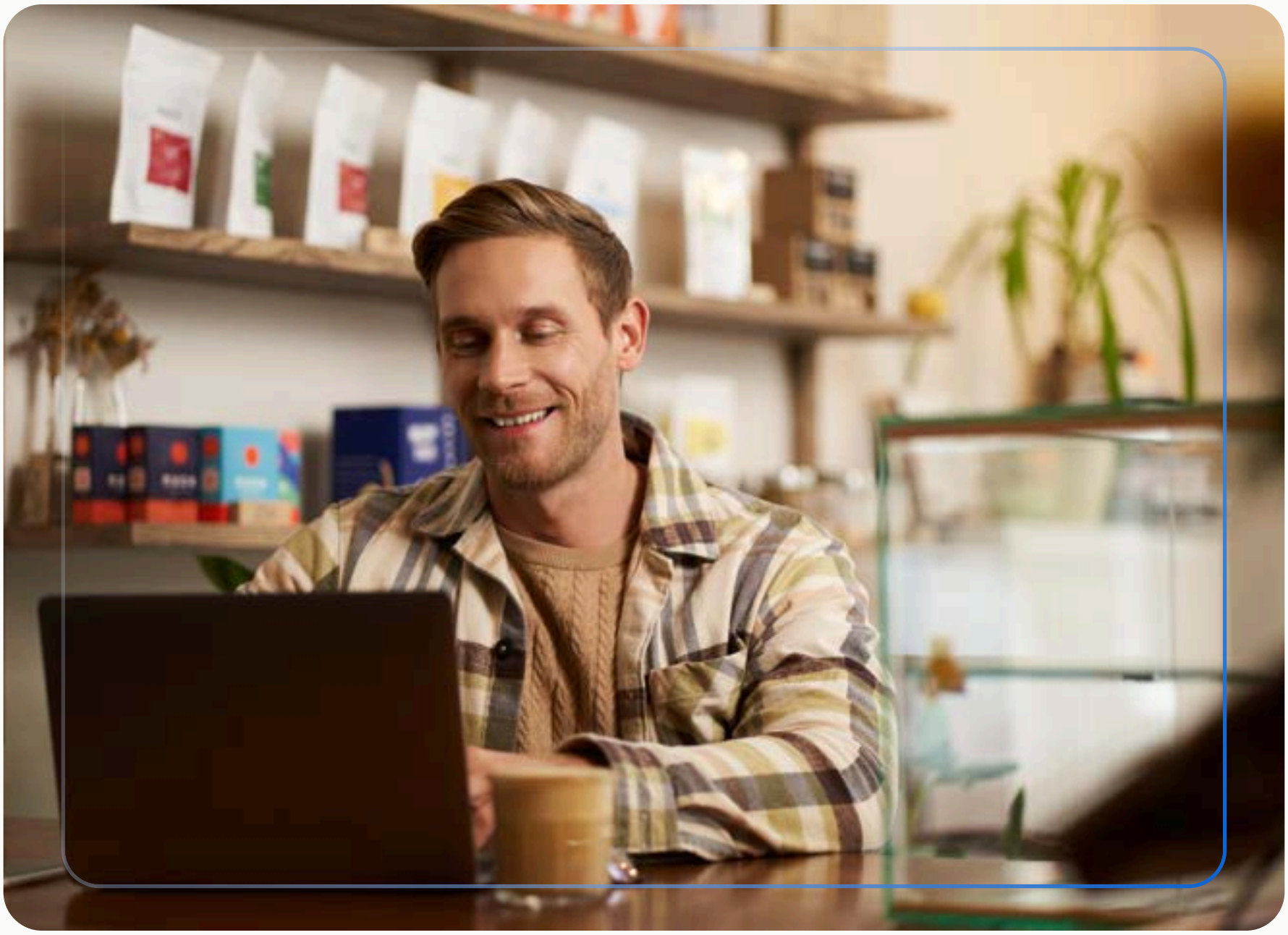
0
Outages from missed renewals

A national retailer, outgrowing manual certificate work

Our customer is a major US retail player, an industry disruptor with stores across the country. As digital certificates shifted from a nice-to-have to a hard requirement for nearly every user, device, and service, the sheer volume became one of the organization's biggest operational headaches.

Small teams can track a few hundred certificates by hand. At this scale, with strict internal policies, compliance requirements, and a mandate for zero outages, manual management simply breaks down. The bigger the company grew, the less manageable its certificates became.

When every store, server, and service needs a certificate, certificate management stops being paperwork and becomes core infrastructure.



Certificate sprawl, and no easy way to tame it

The retailer hit every common certificate headache at once, plus a set of demands unique to its scale and structure.

1

Too many CAs to manage

Across 20+ forests the retailer ran five or more certificate authorities, on-prem, cloud, and public, each with its own procedures, handbooks, and training.

2

Outdated Microsoft PKI

Web enrollment forced users to lean on other staff to get certificates, and with no REST API, the DevOps team struggled to get them on time.

3

Missed renewals, real outages

Without reliable alerting, admins had to track expirations by hand, and a single missed renewal could take a critical application offline.

4

No guardrails on requests

The team needed to whitelist domains, auto-reject wildcard and off-list requests, and lock down costly public CAs to a trusted few.

5

No structure for teams or DevOps

They wanted users segregated by department with their own CA access so dev and production never co-mingled, plus REST API access so DevOps could request certificates programmatically.

> “Before CertSecure, every renewal cycle was a fire drill across five CAs and twenty domains. Now the policies enforce themselves and the team sleeps through the weekend.
>
> **ENCRYPTION CONSULTING — CERTSECURE MANAGER TEAM**

One platform for every certificate

After mapping the retailer's processes, we deployed CertSecure Manager in the cloud and tailored it to their policies, pulling every CA, team, and workflow into a single system.

One portal for every CA

CA Connectors link every authority into a single pane of glass to issue, revoke, and renew, with cloud deployment for nationwide and remote access.

Modern enrollment for DevOps

REST APIs, ACME, and EST replace clunky web enrollment, so DevOps and IoT teams can request and obtain certificates programmatically.

Policy-driven guardrails

The policy module auto-rejects reused CSRs, wildcard requests, and any domain that isn't on the approved whitelist, cutting human error.

Approval workflows and RBAC

Least-privilege roles and approval workflows restrict sensitive and public CAs, so only authorized users can issue from them.

Departments and clean tagging

Users are split into departments with their own PKI admins, and standardized tagging for city, state, and team prevents mislabeled certificates.

Automated renewals and alerts

Renewal Agents on IIS, Apache, Tomcat, F5, and custom apps auto-renew before expiry, with alerts through Teams, ServiceNow, and email.

From fire drills to autopilot

With CertSecure Manager in place, certificate management went from a constant scramble to a controlled, automated routine.

0

Outages, once renewals run themselves

BEFORE — manual renewals

AFTER — auto-renewals

One pane of glass

Every CA, from on-prem to cloud, is now managed from a single portal, cutting training time and collapsing scattered processes.

Policies that enforce themselves

Wildcard, reused-CSR, and off-list domain requests are rejected automatically, reducing human error and impersonation risk.

Renewals on autopilot

Renewal Agents keep certificates active and renew them before expiry, so outages caused by missed renewals simply stop happening.

Built to scale

Departmental structure, RBAC, and modern API access give the retailer a certificate platform that grows alongside the business.

IN SUMMARY

Certificate management that runs itself

By bringing every certificate authority, policy, and team into one cloud platform, CertSecure Manager turned a sprawling, manual process into a scalable system the retailer can trust. Renewal agents keep certificates alive without human effort, the policy module rejects risky requests automatically, RBAC and departmental structure keep access clean, and modern protocols give DevOps the speed it needs. The result is a certificate program that is efficient, secure, and built to grow with the business.

SEE IT IN ACTION

Put your certificates on autopilot.

Book a CertSecure Manager demo →