ENCRYPTION CONSULTING

CASE STUDY

CODE SIGNING SECURITY

An end to certificate outages for a financial firm

A leading US financial firm, decades into banking and investment, kept getting hit by certificate-based outages that damaged its reputation and data protection. CertSecure Manager gave it the visibility, automation, and controls to make certificates a strength, not a risk.

SECTOR	ENVIRONMENT	SOLUTION
Financial services (US)	Multi-cloud + on-prem	CertSecure Manager

1
Certificate dashboard

30/60/90
Day expiry alerts

Multi-CA
Public + private, unified

A financial firm, built on trust

This organization is one of the leading financial firms in the United States, offering banking and investment services. For decades, it has been at the forefront of financial innovation and customer experience.

Serving everyone from individuals to small businesses and corporate clients, it keeps a strong focus on protecting the financial information it handles. Yet despite that focus, certificate-based outages had repeatedly hurt its reputation and its data protection strategy.

For a firm built on trust, every certificate outage was more than downtime. It was a crack in its reputation.

When certificates become the risk

Repeated certificate outages, slow response, blind spots, and weak crypto-agility had turned certificates into a liability.

1

Certificate outages

Expired, revoked, or invalid SSL/TLS certificates broke secure connections, disrupting websites and opening the door to intrusions and breaches.

2

Mounting risk

Slow replacement and revocation of weak or non-compliant certificates raised the odds of a breach, and made certificates an easy target for attackers.

3

Complicated audits

With no real-time visibility across multi-cloud and on-prem, every certificate audit became slow, manual, and hard to get right.

4

Weak crypto-agility

Without diversification or the ability to adapt quickly, the firm couldn't keep pace with current or future security needs.

5

Certificates as a liability

Taken together, these gaps turned certificates from a security control into a recurring weak point that the firm could no longer afford to leave unmanaged.

> "Certificate outages had already exposed critical gaps in the firm's security posture. The challenge went beyond preventing the next outage. It meant building the visibility, automation, and controls so certificates never become a vulnerability again.
>
> **ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · CERTSECURE MANAGER**

Visibility, automation, and control

CertSecure Manager automates the certificate lifecycle, surfaces every certificate in one dashboard, and enforces the policies that keep issuance trusted and compliant.

Automated renewal and issuance

CertSecure Manager automates certificate renewal and issuance, removing the manual gaps that let certificates expire.

30/60/90-day alerts

It emails Microsoft PKI admins 30, 60, and 90 days before expiry, so renewals happen well ahead of any outage.

Restricted templates

Templates can be marked restricted, requiring PKI admin approval so only authentic requests are ever issued.

Centralized inventory dashboard

A single dashboard gives full insight into every certificate in the Microsoft CA, with search and filtering for dispersed teams.

Public and private CAs, unified

It brings public CAs like Entrust, DigiCert, and Sectigo together with Microsoft private CAs under one console.

Policy controls for compliance

Policy controls block CSR reuse, govern wildcard issuance, and enforce approvals, keeping the firm continuously compliant.

04 THE IMPACT

Certificates, now a strength

With CertSecure Manager in place, the firm stopped the outages, tightened control over issuance, and made certificate management fast, visible, and audit-ready.

0

Certificate outages

BEFORE frequent

AFTER prevented

Less downtime

Automated renewals and early alerts keep certificates valid, reducing downtime and protecting business continuity.

Fewer rogue certs

Restricted templates and approvals ensure only authentic requests are issued, cutting compliance and security risk.

Audit-ready visibility

A centralized dashboard with search and filtering makes certificate audits fast and far less manual.

Trust and compliance

Fewer outages and stronger controls protect the firm from fines and reputational damage, reinforcing customer trust.

IN SUMMARY

From liability to strength

For a financial firm, every certificate outage chips away at the trust it depends on. CertSecure Manager turned the firm's certificates from a recurring liability into a managed strength. Automated renewal and issuance with 30, 60, and 90-day alerts ended expiry-driven outages, restricted templates and policy controls keep issuance authentic and compliant, and a centralized dashboard unifies public and private CAs with the visibility audits demand. The result is less downtime, lower legal and breach risk, and certificates that reinforce customer trust instead of threatening it.

GET STARTED

Put an end to certificate outages.

Talk to our CLM team →