ENCRYPTION CONSULTING

CASE STUDY

CERTSECURE MANAGER

Certificate management, centralized for a banking institution

A US bank, trusted for personal banking, wealth management, and corporate finance, struggled to track its SSL/TLS certificates across on-prem and multi-cloud, leading to outages and audit headaches. CertSecure Manager centralized discovery and automated the certificate lifecycle.

SECTOR	FOOTPRINT	SOLUTION
Banking	Multi-cloud + K8s	CertSecure Manger

Discovery
Across cloud and on-prem

K8s
Kubernetes visibility

RBAC
Role-based lifecycle

Strong security, scattered certs

This banking institution is highly recognized in the US for personal banking, wealth management, and corporate finance. It has a reputation for solid data security and uses advanced encryption to protect client information and assets.

Certificate management was the weak spot. The bank struggled to manage the digital certificates behind its secure communications, and that gap had led to service disruptions and data-security vulnerabilities it was determined to fix.

Certificates scattered across servers, domains, and clouds are easy to lose track of, and a single expiry can take a service down.

One gap behind it all: discovery

Scattered certificates, outages, complicated audits, and weak crypto-agility all pointed to one gap: discovery.

1

Inefficient discovery

SSL/TLS certificates were scattered across domains, servers, devices, and clouds, and tracking them by hand left the bank with a weakening security posture.

2

Certificate outages

An expired, revoked, or invalid certificate breaks secure connections, and outages ripple out into downtime, lost trust, and exposure to attack.

3

Complicated audits

Without real-time visibility and reporting across on-prem and multi-cloud, every certificate audit became slow and complicated.

4

Weak crypto-agility

With little cryptographic diversification, the bank couldn't adapt quickly to new requirements, leaving it exposed as standards evolve.

5

Multiple PKIs, little visibility

Several PKIs ran across the environment with no single view, so no one could see every certificate or react before expiries became outages.

> “For a banking institution managing certificates across multi-cloud and Kubernetes, the gap between where certificate management was and where it needed to be was significant. Centralized discovery and automated lifecycle control were the clear priorities.
>
> **ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · CERTSECURE MANAGER**

Discovery, automation, and control

CertSecure Manager unified certificate discovery across multi-cloud and Kubernetes, automated the lifecycle, and gave the bank policy-based control and real-time reporting.

Certificate discovery

CertSecure Manager finds and tracks certificates across multi-cloud environments and Kubernetes clusters, ending manual discovery and revocation.

Policy-based control

Administrators define policies that match the bank's rules, tracking key and certificate usage and monitoring expiration and renewal.

Automated requests

Certificate requests are managed and monitored centrally, removing the manual processing behind IoT, Kubernetes, and distribution.

Granular access control

End-to-end lifecycle management is governed by user and role, with auditing on the key size and signing algorithm of every certificate.

Kubernetes visibility

Full visibility into the Kubernetes environment closed the risk left by multiple PKIs running without a single view.

Reporting and posture

Extensive reporting surfaces certificate usage and overall enterprise security posture in a single, real-time view.

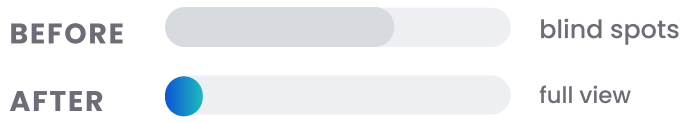
04 THE IMPACT

Full visibility, fewer outages

CertSecure Manager gave the bank a single, real-time view of every certificate across its infrastructure, cutting outages, simplifying audits, and strengthening crypto-agility.

100%

Certificate visibility



Discovery solved

Certificates across multi-cloud and Kubernetes are now found and tracked automatically, ending the manual discovery problem.

Fewer outages

With every certificate monitored and renewals tracked, expiries no longer slip through into service outages.

Audits made simple

Real-time visibility and reporting across on-prem and multi-cloud turned complicated audits into straightforward ones.

Greater crypto-agility

Centralized control and policy enforcement let the bank diversify and adapt its cryptography as standards change.

IN SUMMARY

Every certificate, under control

For a bank running certificates across on-prem, multi-cloud, and Kubernetes, the discovery gap was the real risk. CertSecure Manager centralized SSL/TLS certificate management across that sprawling estate, ending manual discovery and revocation and giving the bank a single, real-time view of every certificate. Policy-based controls and granular, role-based access let it enforce strict standards while staying flexible, Kubernetes visibility closed the gap left by multiple PKIs, and comprehensive reporting surfaced actionable insight into certificate usage and security posture. The result is fewer outages, simpler audits, stronger crypto-agility, and a certificate practice ready for whatever comes next.

GET STARTED

Take control of your certificates.

Talk to our certificate team →