ENCRYPTION CONSULTING

CASE STUDY

CODE SIGNING SECURITY

Encryption as a strategic asset for a Fortune 500 bank

A Fortune 500 financial institution, with banks and ATMs across the country, had grown for decades without a structured cryptographic strategy. Our encryption assessment mapped its entire framework and built a scalable, compliant path for its next phase of growth.

SECTOR	FOOTPRINT	ENGAGEMENT
Financial (Fortune 500)	Banks + ATMs, US-wide	Encryption assessment

TLS 1.2+
Data in transit secured

BYOK
Control over cloud keys

PQC-ready
Crypto-agile framework

A Fortune 500 bank, decades in the making

We conducted our encryption assessment for a Fortune 500 organization in the finance sector, with a portfolio of banks and ATMs across the nation and a specialization in credit cards, auto loans, banking, and savings accounts.

Founded decades ago and now operating across many locations, the institution had grown fast, and that growth kept opening new security gaps. To accelerate its next phase, it wanted a complete view of its security architecture, a tailored strategy for expansion, and a clear path to compliance.

For a bank, trust is everything. This assessment set out to turn encryption from a safety net into a strategic asset.

A framework with compounding gaps

A structured encryption assessment exposed unencrypted data, fragmented key management, and inconsistent cloud controls.

1

Unencrypted sensitive data

Sensitive data sat unencrypted across storage, files, databases, and internal communication, exposing it to man-in-the-middle attacks and tampering.

2

No centralized key management

Key management relied on vendor-specific storage and backup appliances, each with limited, inconsistent key rotation and generation.

3

Weak SSH practices

Passwords stood in for key-based SSH authentication, private keys lacked least-privilege controls, and there was no key rotation policy.

4

Inconsistent cloud encryption

Cloud keys were left to AWS KMS and Azure Key Vault defaults, with BYOK unused, reducing control over data in cloud storage.

5

Growth that outpaced security

Decades of rapid expansion added locations and platforms faster than security could keep up, and the cryptographic gaps only multiplied.

> The institution's cryptographic framework had grown alongside the business but without a structured security strategy. Every new location and platform introduced gaps that compounded over time.

ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · ENCRYPTION ADVISORY SERVICES

One framework, built to scale

We assessed the institution's entire cryptographic framework across on-prem and multi-cloud, then standardized encryption, centralized key management, and aligned everything to compliance.

Full framework assessment

A structured assessment evaluated their entire cryptographic framework and key lifecycle across on-prem and multi-cloud environments.

Policy and workshop review

We reviewed existing policies, processes, and standards and ran workshops to map every encryption capability and gap.

Encrypt data everywhere

We standardized encryption across application, database, file, and folder layers, and required TLS 1.2 or higher for all data in transit.

Centralized, automated keys

Certificate and key lifecycle management was centralized and automated, ensuring timely renewals and far fewer outages.

Least-privilege and BYOK

Least-privilege access through RBAC and IAM, with BYOK restoring control over encryption keys across AWS and Azure.

Compliance, by design

We updated cryptographic controls to meet FIPS 140-2/3, NIST 2.0, NIS-2, and DORA across the framework.

Secure, scalable, and future-ready

The assessment turned a fragmented cryptographic framework into a unified one, strengthening access, automating key management, and readying the institution for what's next.

Unified

Cryptographic framework

BEFORE — fragmented

AFTER — standardized

Less unauthorized access

IAM and RBAC tightened access control across the framework, cutting the risk of unauthorized access to keys and data.

Less human error

Centralizing and automating certificate and key management removed manual steps and the mistakes that came with them.

Crypto-agile and quantum-safe

The framework can now adopt quantum-safe algorithms, leaving the institution ready for future cryptographic shifts.

Scalable across clouds

A scalable framework now spans on-prem and multi-cloud, ready to grow with demand while keeping sophisticated threats at bay.

IN SUMMARY

Encryption, now a strategic asset

For a financial institution, trust sits at the core of everything. Our encryption assessment took this Fortune 500 bank from a fragmented cryptographic framework to a unified, scalable one. We standardized encryption across application, database, file, and folder layers with TLS 1.2 and above everywhere, centralized and automated certificate and key management, tightened access with RBAC and IAM, restored key control with BYOK across AWS and Azure, and aligned the framework to FIPS 140-2/3, NIST 2.0, NIS-2, and DORA. The institution is now crypto-agile and quantum-safe ready, with encryption transformed from a safety net into a strategic asset for years of secure growth.

GET STARTED

Make encryption a strategic asset.

Talk to our encryption team →