ENCRYPTION CONSULTING

CASE STUDY

CERTIFICATE LIFECYCLE MANAGEMENT

Transitioning a financial firm to FIPS 140-3 at Level 4, the highest bar

A US financial organization with over 10,000 employees was already FIPS 140-2 compliant, but wanted Level 4 of FIPS 140-3, the standard's highest. We mapped the gaps and built a clear roadmap to get them there.

SECTOR	SIZE	ENGAGEMENT
Financial services	10,000+ employees	FIPS 140-3 transition

140-3
New FIPS standard met

Level 4
Highest assurance level

0
Gaps left open

A financial firm scaling to the highest standard

Our client is a US financial organization with more than 10,000 employees and thousands of customers, from individuals and small businesses to large institutions. Every day it handles sensitive data and financial transactions that demand the strongest possible protection.

The company already relied on encryption and secure key management to safeguard that data and earn customer trust. As it grew, it set out to scale its infrastructure to the latest security standard, FIPS 140-3, as a public signal of its commitment to protecting customer information.

For a financial institution, a compliance attestation isn't a checkbox. It's proof to every customer that their most sensitive data is handled with care.

Compliant already, but not at Level 4

The client was already FIPS 140-2 compliant, but the jump to 140-3 at Level 4 surfaced gaps across modules, keys, and controls.

1

Inconsistent crypto modules

Some cryptographic modules met existing standards while others lacked clear specs for key management, strong algorithms, and testing, opening gaps attackers could exploit.

2

Weak auditing and monitoring

Logging, automated alerts, and access-control reviews weren't detailed enough to detect and respond to security events the way FIPS 140-3 expects.

3

Key management gaps

Key generation lacked approved RNG and entropy, transmission didn't use trusted channels, and keys weren't zeroized before deletion, short of 140-3 rules.

4

No multifactor authentication

Reaching Level 4 demanded strong identity-based MFA across every system touching cryptographic modules, which the client did not yet have.

5

Thin documentation, and efficiency vs compliance

Lifecycle changes weren't tracked well enough for clean audits, and the team struggled to balance automation with strict 140-3 requirements while mapping gaps and a roadmap on their own.

> “FIPS 140-2 compliance wasn't enough. Achieving Level 4 required rebuilding the cryptographic foundation, not just updating it.
>
> **ENCRYPTION CONSULTING · FIPS ADVISORY SERVICES**

From gap analysis to a transition plan

We mapped the client's cryptographic environment end to end, updated their policies, and delivered a tailored roadmap to reach FIPS 140-3 at Level 4.

Scope and discovery

We defined the scope and inventoried data at rest, in transit, and key and certificate policies, then identified every module and app that had to meet FIPS 140-3.

Gap assessment and roadmap

Through workshops we assessed the security framework, pinpointed every gap, and built a prioritized roadmap with remediation for each one.

Updated crypto policies

We rewrote cryptographic controls, certificate and key lifecycle policies, and data classification to align fully with FIPS 140-3 requirements.

Hardened key management

We introduced approved RNG, trusted-channel distribution over TLS 1.3, key zeroization, and a centralized KMS with HSM storage and periodic rotation.

MFA for Level 4

We rolled out multifactor, identity-based authentication across every system touching cryptographic modules, binding tokens to user sessions.

Logging and audit trails

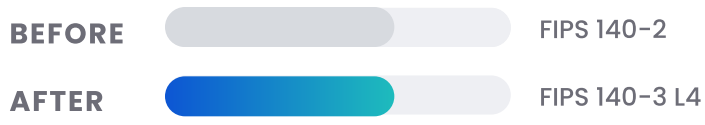
We stood up comprehensive, encrypted logging so every cryptographic-module action is recorded, retrievable, and ready for audit.

Compliant, resilient, and ready for what's next

By closing every gap we found, the client didn't just reach FIPS 140-3, they came out with a stronger, more resilient security posture.

Level 4

FIPS 140-3 compliance, the highest assurance



Stronger key management

Approved RNG, trusted channels, zeroization, and a centralized KMS now protect keys across their full lifecycle.

MFA everywhere

Identity-based multifactor authentication adds a strong layer against phishing and credential theft across sensitive systems.

Faster incident response

Automated backups, recovery, and a streamlined incident response process keep data available and breaches contained.

Audit-ready and future-proof

Detailed lifecycle assurance policies keep the organization compliant with FIPS 140-3 and ready for what comes next.

IN SUMMARY

A cryptographic foundation, rebuilt to last

The transition plan we delivered took the client from FIPS 140-2 to FIPS 140-3 at Level 4, the standard's highest. Updated policies now cover every cryptographic module, key management runs on approved RNG, trusted channels, and a centralized KMS, multifactor authentication guards every sensitive system, and detailed logging keeps everything audit-ready. The result is more than a compliance attestation: it's a resilient cryptographic foundation that protects customer data today and adapts to the threats of tomorrow.

GET STARTED

Plan your move to FIPS 140-3.

Talk to our FIPS Advisory team →