

HSM-AS-A-SERVICE

Hardware-backed key security for a banking institution

An established bank, trusted for rigorous data protection, had no hardware security modules in its infrastructure, capping how far it could secure cryptographic operations and key management. HSM-as-a-Service gave it hardware-backed control, performance, and auditability.

SECTOR

Banking

MODEL

HSM-as-a-Service

FOCUS

Key protection

HSM

Hardware root of trust

RBAC

Delegated admin control

SIEM

Continuous monitoring

A trusted bank, missing one layer

This established banking institution is a cornerstone of financial stability and trust, serving a broad clientele with a wide range of banking services. It's known for rigorous data protection, advanced encryption, and compliance with global banking security standards.

One layer was missing. Without hardware security modules in its infrastructure, the bank couldn't reach the highest level of cryptographic-operations security, leaving gaps in key management and data integrity. It set out to integrate HSMs and close them.

Strong encryption still needs a hardware root of trust. Without HSMs, the bank's keys and crypto operations could only go so far.



No hardware, no headroom

No administrative control, weak performance, hard management, insecure execution, and no monitoring all held the bank back.

1

No administrative control

The bank had no autonomy over its cryptographic operations, with keys, access, and configuration mismanaged and no granular control over user permissions.

2

Low performance

There was no infrastructure built for high-volume cryptographic operations, no scalable architecture, load balancing, or caching to keep latency low.

3

Difficult HSM management

Without intuitive consoles, expert support, automated provisioning, or centralized multi-HSM control, day-to-day operation was hard.

4

Insecure code execution

There was no code isolation in the HSM environment, no tamper resistance, and no real-time monitoring of execution for anomalies.

5

No continuous monitoring

Cryptographic operations ran without real-time monitoring, automated alerts, SIEM integration, or regular audits, so anomalies and security gaps could go unnoticed.

“

Without HSMs in its cryptographic infrastructure, the institution could not deliver the key protection, performance, and auditability that modern banking security requires.

ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · HSM-AS-A-SERVICE

Hardware-backed, fully managed

HSM-as-a-Service gave the bank a hardware root of trust: secure key storage, signing and encryption, layered access control, and the administrative grip it had been missing.



Sign, timestamp, encrypt

HSMs sign, timestamp, and encrypt content, preserving the legitimacy and privacy of documents even beyond the bank's boundaries.



Secure key storage

An HSM gives primary and private keys a secure home, solving the problem of safely storing keys across a large organization.



Client-data protection

HSMs give the highest level of security to the keys that encrypt client data, enabling an effective cloud solution for financial services.



HSM as Root of Trust

HSMs anchor a PKI built on top-tier hardware, giving robust performance, availability, and scalability as the root of trust.



Administrative control

The bank regained autonomy over keys, access, and configuration, with the granular control and audit trails it had lacked.



Layered access control

Multiple layers of access control and hardened HSM security let the bank process new e-identity documents in less time.

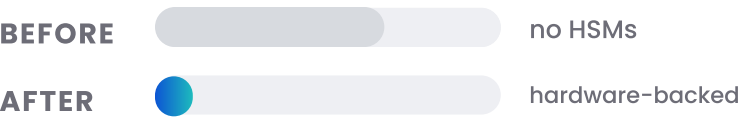
More control, higher assurance

With HSMs in place, the bank gained hardware-backed key protection, audited compliance, and high-performance cryptographic operations, delivered on time and under budget.

HSM-backed



Cryptographic operations



Fast, low-effort rollout

Signing, timestamping, and encryption came online quickly, raising security with no development work required.



Safe, cost-effective keys

Private keys gained a secure home, with flexible, cost-effective storage and fast implementation.



Audited and compliant

The cloud HSM solution was audited and found compliant with all applicable regulatory obligations.



High performance and uptime

Built on top-tier hardware as a root of trust, the bank gained high performance, availability, and data throughput.

— IN SUMMARY

A hardware root of trust

By adopting HSM-as-a-Service, the bank closed the one gap in an otherwise strong security posture. Hardware security modules now anchor its cryptographic operations, giving it a true root of trust with secure key storage, signing and encryption, layered access control, and the administrative oversight it previously lacked. The cloud HSM solution was audited and found compliant with regulatory obligations, delivered on time and under budget, and built for high performance, availability, and throughput. The result is stronger data integrity, tighter control, and a renewed ability to protect client assets to the standards modern banking demands.

GET STARTED

Build on a hardware root of trust.

[Talk to our HSM team →](#)