Secure Key Management with Fully Managed HSM Protection

Managing cryptographic keys manually is risky, complex, and expensive. Software-based key storage, scattered access controls, and inconsistent policies expose organizations to breaches and compliance failures. Qcecuring HSMaaS delivers secure, centralized, and policy-driven key protection—without the cost or complexity of owning physical HSMs.

Introduction

Cryptographic keys are the foundation of digital trust. But storing keys in software, filesystems, or developer machines exposes organizations to theft, misuse, and operational disruptions. Traditional on-prem HSMs solve part of the problem, but they require significant investment, maintenance, and specialized expertise.

Qcecuring HSM as a Service modernizes enterprise key protection by providing fully managed, FIPS-certified HSM-backed key storage accessible through secure APIs and granular policies. Keys never leave the hardware boundary, access is governed by centralized controls, and all cryptographic operations are logged for compliance and auditing. Organizations can generate, store, rotate, and use keys securely—whether for code signing, encryption, authentication, PKI operations, or application workloads—without handling underlying hardware infrastructure.

The Problems

Keys stored insecurely

Expensive, complex HSM management

No central key control

Manual key rotation & No audit visibility

Poor scalability under load

The Solutions

FIPS-grade key protection

Secure API-based crypto operations

Automated key lifecycle

RBAC + policy enforcement

Full audit visibility & Scalable crypto performance

Key Features

FIPS-Certified Key Storage

Keys are generated, stored, and used exclusively inside certified HSMs, ensuring zero exposure.

API-Based Cryptographic Operations

Applications can sign, encrypt, decrypt, and validate operations securely via REST APIs.

Role-Based Access Control (RBAC)

Define exactly who or what can use each key, with full approval workflows.

Automated Key Rotation

Reduce operational risk with scheduled or policy-triggered key rotation.

Full Audit Logging

Track every cryptographic request for compliance and forensic investigations.

Elastic Scaling

HSM clusters automatically scale to handle demanding workloads.

How It Works

Application requests crythappicc operation

QCECuring validates policy, policy, identity & & permissions

HSM performs signing / encryption inside secure boundary

Operation result is returned safely

Audit logs recorded for compliance

Business Benefits

Eliminates key theft & unauthorized usage

Ensures regulatory compliance

Reduces cost & complexity of physical HSMs

Supports high-speed signing & encryption workloads

Use Cases

Code signing key protection

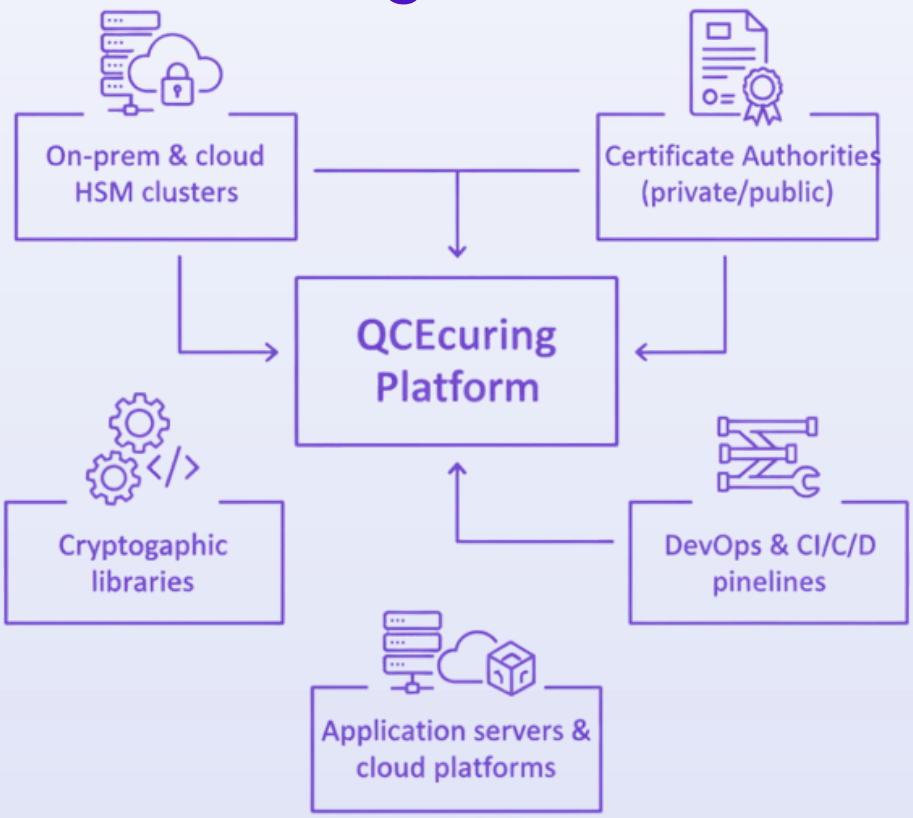
TLS/SSL CA private keys

Database encryption keys

Document signing & e-seals

IoT, device & firmware identity keys

Integrations



Deployment Options

On-Prem (FIPS HSM)

Deploy HSM nodes within your datacenter for complete control, strict compliance, and isolated network environments.

Cloud (HSM-backed)

Fully managed HSM clusters with API-based cryptographic services, ideal for distributed applications and DevOps teams.

SaaS

Instant HSM access with no hardware to manage—secure key operations delivered through highly available cloud services.

Hybrid

Use cloud automation layers while keeping sensitive keys inside on-prem HSMs for maximum assurance.

The Value We Deliver

- Zero key exposure
- Strong access controls
- Developer & DevOps friendly
- Scales with cryptographic demand
- Enterprise-grade security
- Enterprise-grade automation

Ready to secure your cryptographic keys without managing hardware?
Our HSMaaS platform provides strong, compliant, and automated key protection for all your critical workloads.
Speak with **info@qcecuring.com** security experts to explore how HSMaaS can enhance your encryption, signing, and compliance posture.