



Machine Identity & Cryptographic Infrastructure Platform

Automate the lifecycle of every certificate, key, and cryptographic asset — from issuance to retirement.

QCeCuring provides a unified platform for machine identity management. We automate certificate lifecycle, SSH key governance, code signing, and cryptographic discovery across hybrid enterprise infrastructure. One platform. Every machine identity. Full control.

4

Product Modules

12+

CA Integrations

11

Certificate Stores

4

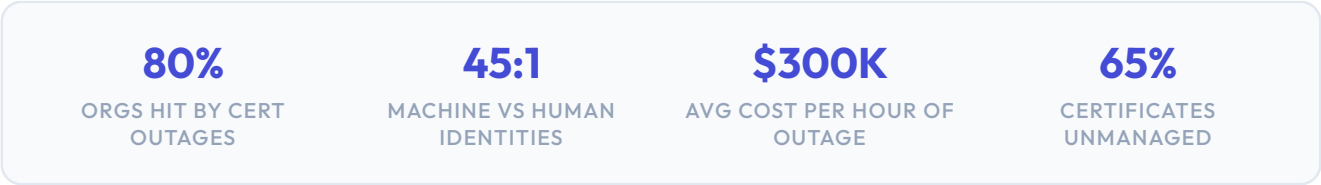
Deployment Models

PQC

Quantum Ready

The Machine Identity Challenge

Machine identities — certificates, keys, and credentials used by servers, devices, workloads, and services — now outnumber human identities 45:1 in the average enterprise. Yet most organizations lack visibility, automation, and governance over these critical assets.



Certificate Sprawl
Thousands of certificates across CAs, servers, and cloud accounts with no single source of truth. Renewals missed, outages inevitable.

Multi-CA Chaos
Internal CA (ADCS), public CAs (DigiCert, Let's Encrypt), cloud CAs (AWS, Azure) — all operating independently with no unified view.

Ownership Fragmentation
DevOps manages some certs, Security manages others, IT manages the rest. Nobody owns the full picture.

SSH Key Sprawl
40%+ of SSH keys are orphaned. Each is a persistent backdoor into production systems.

Manual Processes
Spreadsheets, scripts, and tribal knowledge. Works at 50 certs. Breaks at 500.

Quantum Threat
CNSA 2.0 mandates post-quantum migration by 2033. Without cryptographic inventory, migration is guesswork.

Platform Overview

QCecuring is a unified machine identity management platform with four integrated modules. Each module handles a specific domain of cryptographic infrastructure, while sharing a common discovery engine, policy framework, and audit trail.



SSL Certificate Lifecycle Management

Automated discovery, enrollment, renewal, and deployment of certificates across hybrid infrastructure. Multi-CA support (12+ CAs). Policy-driven automation. Multi-tenant architecture. Built-in ACME server.



Cryptographic Discovery & CBOM

Multi-method discovery of all cryptographic assets — algorithms, keys, certificates, protocols, and libraries. CycloneDX CBOM output. Quantum risk scoring. Compliance assessment (CNSA 2.0, PCI DSS 4.0).



SSH Key Lifecycle Management

Complete SSH key inventory, trust relationship mapping, automated rotation, orphan key detection, and compliance enforcement across all server platforms.



Code Signing

Centralized signing for software artifacts (Authenticode, JAR, Docker, NuGet, macOS, Android). CI/CD integration. Approval workflows. Tamper-proof audit trail.

How the Platform Works

Each module operates independently while sharing a unified discovery engine, policy framework, agent infrastructure, and audit trail. Deploy one module or all four from the same platform.

Shared Discovery Engine	One agent infrastructure discovers certificates, SSH keys, cryptographic assets, and configurations across all environments
Unified Policy Framework	Common rules engine across all modules — algorithm requirements, key sizes, validity, approval workflows
Single Audit Trail	Every operation across all modules logged immutably — who did what, when, where
Agent Architecture	Lightweight agent (Java JAR, ~20MB). mTLS authenticated. Pull model (no inbound ports). One agent serves all modules.
API-First	Every module fully accessible via REST API. Automate anything.

SSL CLM

12+ CA integrations, 11 certificate stores, auto-discovery, auto-renewal, auto-deployment, built-in ACME server, policy engine, RBAC, multi-tenant.

SSH KLM

Agentless + agent discovery, trust relationship mapping, automated rotation, orphan detection, policy enforcement across Linux/Unix/macOS/Windows.

CBOM

6 discovery methods, CycloneDX v1.6 output, quantum risk scoring, CNSA 2.0 / PCI DSS 4.0 compliance profiles, migration roadmap.

Code Signing

HSM-backed signing (15+ formats), CI/CD plugins (Jenkins, GitHub Actions, GitLab CI), approval workflows, tamper-proof audit.

Supported Integrations

QCecuring integrates with enterprise infrastructure across certificate authorities, cloud platforms, web servers, DevOps toolchains, and IT service management.

Certificate Authorities

- Microsoft AD CS
- EJBCA Enterprise
- Smallstep CA
- Let's Encrypt
- DigiCert CertCentral
- AWS Private CA
- Google Cloud CAS
- Custom CA (Gateway SPI)

Certificate Stores & Servers

- Nginx
- Apache HTTP
- Microsoft IIS
- Tomcat / JKS
- F5 BIG-IP
- IBM HTTP Server
- AWS ACM
- Azure Key Vault
- GCP Secret Manager
- PEM / PKCS#12 files
- Windows Certificate Store
- Linux Trust Store

Cloud & DevOps

- AWS (ACM, KMS, EC2, EKS, ALB)
- Azure (Key Vault, AKS, App Gateway)
- GCP (Cloud KMS, CAS, GKE)
- Kubernetes (cert-manager, secrets)
- Docker / Container registries
- Terraform / Pulumi
- Jenkins, GitHub Actions, GitLab CI
- ServiceNow (ITSM)
- Slack / Teams (alerting)
- Splunk / Elastic (SIEM)
- Prometheus / Grafana
- PagerDuty / OpsGenie

Platform Interface

Unified web-based interface for managing all machine identities. Role-based dashboards, real-time alerts, and complete audit trail.

SSL Certificate Lifecycle Management

SSL CLM
v2.0

Dashboard

Certificates

Discovery

Infrastructure

- Certificate Authorities
- Certificate Stores
- DNS Providers
- ACME Server

Governance

- Agents
- Policies
- Audit Trail
- Reports

Jobs

Settings

- License & Quota
- Users

Theme

QCecuring Technologies

Certificates

Search by name, SAN, serial, fingerprint...

14 / 500 managed

Import

+ New Certificate

Columns (13)

All: 30

Managed: 14

Monitored: 16

All

Active

Expiring

Expired

Pending Approval

Pending

Archived

Revoked

	NAME	STATUS	TIER	DAYS LEFT	CA	DEPLOYMENTS	CREATED	KEY PRESENT	SERIAL NUMBER
	onetwo.com	PENDING_APPROVAL	MANAGED	—	stepca-1	0	Aug 1, 2026		—
	demo1.qcecurig.com	ACTIVE	MANAGED	88d	lets-1	0	Jul 31, 2026		38617802176372198826142
	two.com	EXPIRED	MANAGED	0d	stepca-1	0	Jul 31, 2026		439946866474421038081248
	one.com	PENDING_APPROVAL	MANAGED	—	stepca-1	0	Jul 31, 2026		—
	*.mynta.com	ACTIVE	MONITORED	146d	—	1	Jul 30, 2026		162291166540978191261549
	*.cy-peg.a2z.com	ACTIVE	MONITORED	69d	—	1	Jul 30, 2026		148288667604127966180865
	www.flipkart.com	ACTIVE	MONITORED	164d	—	1	Jul 30, 2026		223640962113471599799095
	www.aajtak.in	ACTIVE	MONITORED	130d	—	1	Jul 30, 2026		195606655002388337561097
	something.com	ACTIVE	MONITORED	362d	—	1	Jul 30, 2026		346996864257657447030786
	openai.com	ACTIVE	MONITORED	76d	—	1	Jul 30, 2026		220354057119176599858959

Showing 1–25 of 30

<< < 1 2 > >> 25

CBOM — Cryptographic Inventory Dashboard

CBOM

Dashboard

Custom Analytics

Timeline

Reports

Migration Planner

Inventory

Sensors

Scanner Catalogue

Alerts

Compliance

Source Inspector

Import / Export

Users

Settings

CBOM v1.0

Dashboard

7,295
TOTAL ASSETS

312
CRITICAL

5,974
HIGH RISK

4,394
CERTIFICATES

2,176
KEYS

11%
PQC READY
+1.85mo
View Timeline

6286 assets use quantum-vulnerable algorithms. View critical assets →
463 certificates expired or expiring within 7 days. View expiring →
Cryptographic posture is 11% PQC-ready. Migration recommended.

Quantum Risk & Threats 6286 at risk

Assets using cryptography vulnerable to quantum compu

RISK DISTRIBUTION

HIGH

NONE

CRITICAL

MEDIUM

LOW

VULNERABLE ALGORITHMS

256-bit

2048-bit

3072-bit

4096-bit

384-bit

Unknown-bit

521-bit

1024-bit

EXPIRY TIMELINE

Expired

< 7d

< 30d

< 90d

< 1yr

> 1yr

Certificates 4394

X.509 certificate analysis: algorithms, key sizes, signat...

ALGORITHM FAMILY

RSA

ECDSA

Ed25519

ML-DSA-65

ML-DSA-87

KEY SIZES

1400

1200

1000

800

600

400

SIGNATURE ALGORITHMS

SHA256withRSA

SHA256withECDSA

SHA384withRSA

Ed25519

SHA384withECDSA

SHA512withRSA

ML-DSA-65

ML-DSA-87

SSH Key Lifecycle Management

SSH Key Lifecycle Management

Dashboard

Inventory

All Keys

All Hosts

Logons

Compliance

Logs

Discovery Logs

Audit Logs

Reports

Agent Management

Settings

Inventory > All Keys

All SSH Keys

Manage and monitor all SSH keys in your inventory

SSH Keys Inventory

Total: 6

AllManagedUnmanagedRefresh

Type	Owner	Path	Fingerprint	Created	St
UNKNOWN	Chaitanya	\\Users\\Chaitanya\\ssh\\authorized...	dda3c72e83021c31ac5490ec4dfb413d005233b772a16c879ab275...	11/28/25, 7:44 PM	Unmi
ED25519	Chaitanya	\\Users\\Chaitanya\\ssh\\id_ed25519	08f977ed7a01135e29c182cc0c4cc24fc02764f68da56337d52abf...	11/28/25, 7:44 PM	Unmi
ED25519	Chaitanya	\\Users\\Chaitanya\\ssh\\id_ed2551...	2369636e60f15eeb219a27db7ede7ba215d8b3419193546ac59850...	11/28/25, 7:44 PM	Unmi
UNKNOWN	Chaitanya	\\Users\\Chaitanya\\ssh\\known_hos...	81385b53946cb6287cc3a01a028f35f30040c9d902fa03fd38e805...	11/28/25, 7:44 PM	Unmi
UNKNOWN	Chaitanya	\\Users\\Chaitanya\\ssh\\known_hos...	05d557ba542ca36a2d0c5c8f44fcc9f52de143d03ec063d3b6acd...	11/28/25, 7:44 PM	Unmi
UNKNOWN	Chaitanya	user/home/ssh/authorized_keys	dda3c72e83021c31ac5490ec4dfb413d005233b772a16c879ab275...	11/28/25, 7:44 PM	Unmi

Showing 1 to 6 of 6 keys

SSH Key Lifecycle Management by QCecuring

Code Signing Management

Code Signing

Dashboard

Keys

Certificates

Signing Requests

Agents

Policies

Reports

Audit Events

Users

Roles & Permissions

Email Configuration

Report Schedules

Dashboard

Agents

0 Online 2 Offline

HSM

ACTIVE SoftHSM

Signing Engine

HEALTHY

110

Total Requests (30d)

100

Successful Signatures

0

Failed Operations

22ms

Avg Signing Time

Signing Keys Status

Active Keys

Inactive Keys

Expired Keys

Certificate Expiry Timeline

Expired

< 30 days

30-90 days

90-365 days

> 1 year

Approval Queue Status

Pending Approvals

0

MFA Required

0

Expired (7d)

0

Keys Summary

Active Keys

14

Revoked Keys

0

Rotated Keys

0

Total Keys

0

Certificates Summary

Active Certificates

7

Expiring in 30d

0

Expired

0

Total Certificates

0

Deployment Models

QCecuring supports multiple deployment models to meet enterprise requirements — from self-hosted on-premises to fully managed SaaS.

On-Premises

Deploy within your data center. Full data sovereignty.
Docker-based. Customer-managed with vendor support.

SaaS

Fully managed. Zero infrastructure overhead.
Automatic updates. Multi-region.

Self-Hosted Cloud

Run in your own AWS, Azure, or GCP account. Same software, your infrastructure.

Air-Gapped

Fully disconnected for classified environments. Offline updates. No internet dependency.

Architecture	Microservices, containerized, API-first
Database	MongoDB (primary) / PostgreSQL supported
Scalability	Horizontal scaling, unlimited certificates
High Availability	Clustering, automatic failover
API	REST API (fully documented), Webhooks
Authentication	SAML 2.0, OIDC, LDAP/AD, API tokens, mTLS
Encryption	TLS 1.3 in transit, AES-256 at rest
Agent	Lightweight Java JAR (~20MB), mTLS bootstrap, pull model, auto-upgrade

Professional Services

Our engineering team works directly with your security and infrastructure teams. Scoped engagements with clear deliverables.

PKI Establishment (2-Tier / 3-Tier)	2-4 weeks — Design and deploy enterprise PKI, offline Root CA, templates, key ceremony, CP/CPS, runbooks
PKI Health Assessment	1-2 weeks — Audit existing PKI, misconfigurations, CRL/OCSP health, compliance gaps, remediation roadmap
Certificate Discovery & Inventory	1-2 weeks — Network-wide scan, cloud inventory, Kubernetes enumeration, SSH key discovery, ownership mapping
CLM Platform Deployment	2-4 weeks — Full deployment, CA integrations, agents, automation, dashboards, RBAC, training
Post-Quantum Readiness Assessment	2-3 weeks — Complete CBOM, quantum risk scoring, CNSA 2.0 gap analysis, migration roadmap
Microsoft AD CS Migration	4-8 weeks — Migrate from AD CS to modern PKI, parallel operation, phased migration, decommission plan
SSH Key Audit & Remediation	2-4 weeks — Key inventory, ownership mapping, orphan cleanup, rotation, hardening

Training Programs

Instructor-led workshops for security and infrastructure teams. Available virtual or on-site.

PKI Fundamentals & Enterprise Deployment	3 Days — Build enterprise PKI from scratch. Hierarchy design, CA deployment, templates, key ceremonies, operations, troubleshooting.
Certificate Lifecycle Management	2 Days — Discovery, monitoring, ACME automation, deployment pipelines, incident response, cert-manager.
SSH Key Management & Hardening	1 Day — Inventory, rotation, orphan cleanup, policy enforcement.
Post-Quantum Cryptography Readiness	1 Day — CBOM building, quantum risk assessment, CNSA 2.0, migration planning.

Included with every course

- Live instructor-led sessions (virtual or on-site)
- Dedicated cloud lab per participant
- Step-by-step lab manuals
- Scripts and templates (production-ready)
- Certificate of completion
- 2 weeks post-training support



Automate Machine Identity at Scale

From certificates to keys to quantum readiness — one platform, full lifecycle, complete control.

Start a Pilot

QCecuring Technologies Private Limited

info@qcecuring.com

www.qcecuring.com

© 2026 QCecuring Technologies Private Limited. All Rights Reserved.