4QUAYS CRYPTO AGILITY FOR MACHINE-TO-MACHINE

One decision. Every connection.

Your services, APIs, devices and partner feeds each carry cryptography chosen by different teams at different times. 4Quays brings those decisions into one place, with expertly implemented cryptography. So **policy reaches every connection,** in hours instead of quarters, with the evidence to prove it.

Lower operating cost | Respond in hours | No vendor lock-in

CHANGING CRYPTOGRAPHY	TODAY	WITH 4QUAYS
Who decides	Each team	One policy
Deprecation	A program	A policy edit
Rotate keys	Per system	Fleet-wide
Switch provider	Rewrite code	Behind the policy
Audit answer	Per codebase	One record

WHAT'S AT STAKE

More machines, faster change. Same manual process.

Every connection between systems depends on keys and algorithms that now have to change more often, across far more identities than people can track by hand.

82:1[1]

Machine identities per human

Across enterprises in 2025, and expected to keep growing with AI and cloud.

47 days[2]

Maximum certificate life by 2029

Down from 398 days. The industry is mandating faster cryptographic change.

86%[3]

Suffered a certificate outage

From expired or mismanaged certificates in a single year. Nearly a third, every quarter.

PQC is one transition, not the last. Deprecations, vulnerabilities and vendor changes will keep coming. Agility means absorbing each one as an operation, not starting a new program, leaving testing cryptographic algorithms to us.

WHAT THE BUSINESS GETS

Centralize the decision. Keep everything else.

Systems keep their code, teams and release cycles. Only the cryptographic decisions move to one place.

01

Lower operating cost

One team runs cryptography for the fleet. App teams stop hiring for it.

02

Respond in hours

A broken algorithm or leaked key becomes a policy action, not a hunt.

03

No lock-in

Swap cryptographic providers behind the policy. Applications never notice.

04

Prove it on demand

One record of what protects every connection, ready for auditors.

1

Place to decide, with n-of-m

Every algorithm, key and provider choice, for every connection.

0

App changes per update

Teams keep shipping even though the cryptography evolves.

Hours

Not quarters, to respond

Retire an algorithm or rotate keys across the fleet.

HOW IT WORKS

Register once. Govern by policy.

Every system is registered once, and every connection between systems is governed by a central policy.

Observe

Map services, APIs, devices and partner links with the crypto behind each.

Execute

One `protect` / `unprotect` call at each end. The policy does the cryptography.

Govern

Algorithm, cipher and key ownership per connection, staged with rollback.

Prove

Every operation audited, with alerts on drift and evidence in your SIEM.

One map of every connection

Services, APIs, devices and partner links, with the algorithm and key behind each, in one view.

Policy, not code

Each connection's algorithm, cipher and key ownership live in a central policy, not in a codebase.

Fleet-wide change

Apply a new algorithm to one connection, a group or all of them, staged and with rollback.

Centralized key lifecycle

Generate, rotate and retire keys from one place, platform- or destination-managed, without redeploys.

Provider independence

Change cryptographic providers and key stores behind the policy. Applications never notice.

Contained credentials

Every connection has its own credential, revoked on its own, so a compromise stays one connection.

Common platform

INCLUDED IN EVERY 4QUAYS DEPLOYMENT

Discovery
Cloud KMS, code, network, endpoints and AI agents.

Prioritization
Risk scoring against NIST guidance and vendor readiness.

Monitoring
Latency, error rate, throughput and volume per policy.

Alerting
Threshold, drift and missing-activity rules.

Auditing
Every operation, with policy, algorithm and key.

SIEM & logging
Monitoring, audit and alert data to your SIEM.

TECHNICAL SPECIFICATIONS

Model	Services (source / destination) · policies per connection · per-policy credentials
Algorithms	ML-KEM-512 / 768 / 1024 (FIPS 203) · ML-DSA-44 / 65 / 87 (FIPS 204) · RSA · ECDSA · AES-GCM
Key ownership	Platform-managed or destination-managed · scheduled and on-demand rotation
Integration	REST API (`protect`, `unprotect`) · `@4quays/sdk` · passthrough dev mode · gateways
SIEM & logging	Splunk · Sentinel · Datadog · Elastic · QRadar · Sumo Logic · Falcon LogScale · webhook

1. CyberArk, *2025 Identity Security Landscape*, Apr 2025.
2. CA/Browser Forum Ballot SC-081v3, Apr 2025.
3. Keyfactor, *2025 Digital Trust Digest.*

SEE IT LIVE

See 4Quays change cryptography in a live environment.

Book a demo

contact@4quays.com
4quays.com