SECTIGO®

Solution Brief

Private PQC in Sectigo Certificate Manager (SCM)

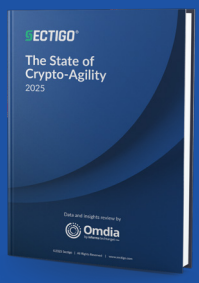
Operationalize post-quantum readiness inside real PKI environments

Quantum risk has moved beyond academic discussion and into practical planning. While a large-scale quantum break is not imminent, the implications for certificate-based trust are already clear. Data encrypted today can be captured and decrypted later ("harvest now, decrypt later" threat), creating long-term exposure for organizations that protect sensitive, regulated, or long-lived information.

What complicates planning is not a lack of algorithms. It is the uncertainty in how they will be deployed. The post-quantum ecosystem is still settling. Certificate profiles, trust models, and implementation guidance continue to evolve, and public trust environments are not positioned for traditional post-quantum X.509 deployment right now.

The challenge, however, is knowing where to begin. Waiting extends future risk. Moving too early risks committing to approaches that may not align with where standards ultimately land.

Preparation at this stage is about understanding impact, trade offs, and dependencies. Not deploying early, not standing still, but building informed readiness while the ecosystem continues to mature.



According to the Sectigo State of Crypto Agility Report 2025, 90% of organizations have budgets allocated to PQC preparedness initiatives within the next 12 months.

Private PQC in SCM

Sectigo Private PQC is a private-only, post-quantum certificate capability built directly into Sectigo Certificate Manager (SCM), available at no additional cost to eligible customers.

It enables organizations to issue and manage private post quantum SSL/TLS certificates using the same governance, approvals, inventory visibility, and lifecycle controls they already use for private PKI in SCM.

Private PQC is not production-ready by design. It exists for one purpose: to help organizations understand the operational impact of post-quantum cryptography before standards are finalized and irreversible decisions are required.

SECTIGO®

What Private PQC Enables

Hands-on operational learning

Private PQC moves post-quantum experimentation into real certificate operations, where certificate approvals, audits, renewals, and visibility expose practical trade-offs early.

PQC Algorithms supported:
ML DSA-44 | ML DSA-65 | ML DSA-87

Certificate types supported:
Private SSL/TLS certificates

A safe environment with deliberate guardrails

Private-only issuance, one-year certificate lifetimes, and a Sectigo-operated Private CA and HSM contain risk by design. These guardrails prevent unintended reliance on evolving cryptography while still enabling meaningful, hands-on evaluation within existing certificate environments.

Why does Sectigo Private PQC support ML-DSA?

Sectigo selected ML-DSA because it is among the first NIST-standardized post-quantum signature algorithms with clear IETF specifications for use in X.509 certificates.

RFC 9881 defines its representation across certificate signatures, public keys, and CRLs, making ML-DSA the most clearly specified and interoperable option available today for certificate-based PQC experimentation.

For more information, see our Private PQC and FAQ landing page.

No cost and no added infrastructure burden

Sectigo operates the PQC CA and cryptographic infrastructure at no additional cost. IT teams gain practical experience without deploying experimental systems, changing architectures, or increasing operational overhead.

Adapt as standards evolve

Private PQC is built with the expectation that post-quantum standards will change. As certificate models, algorithms, and best practices mature, organizations can adapt without abandoning existing workflows or switching platforms.

Backed by deep PKI expertise

Organizations benefit from Sectigo's long-standing operational PKI experience and active leadership in standards development, gaining practical, future-ready guidance shaped by how certificates are managed at scale.

SECTIGO®

Common Private PQC use cases within SCM

Understand operational impact before it becomes urgent

Evaluate how post-quantum certificates affect issuance, installation, renewal, and revocation across servers, load balancers, and cloud environments under real operational conditions.

Extend experimentation beyond PQC labs

Move PQC evaluation into governed environments instead of relying solely on academic testing tools.

Reduce future migration risk

Identify dependencies, bottlenecks, and readiness gaps early, reducing the likelihood of rushed or disruptive transitions as standards and mandates solidify.

Prepare for the inevitable cryptographic change

Build internal readiness and shared understanding across security, PKI, and infrastructure teams ahead of externally driven transitions.

Aligning cross-functional stakeholders

Provide a common, controlled environment for security, infrastructure, and PKI teams to assess post-quantum impact using familiar operational controls.

Partner with Sectigo on evolving PQC needs

Engage directly with Sectigo to shape future post-quantum use cases, capabilities, and roadmap direction, giving your teams early, first-hand insight and practical guidance as standards and deployment models mature.

About Sectigo

Sectigo is the most innovative provider of certificate lifecycle management (CLM), delivering comprehensive solutions that secure human and machine identities for the world's largest brands. Sectigo's automated, cloud-native CLM platform issues and manages digital certificates across all certificate authorities (CAs) to simplify and improve security protocols within the enterprise. Sectigo is one of the largest, longest-standing, and most reputable CAs with more than 700,000 customers and two decades of delivering unparalleled digital trust.

Reach out today for a personalized demo or contact us at sales@sectigo.com to see how Sectigo can transform your certificate management strategy.

SECTIGO®