SECTIGO

Datasheet

Sectigo Orchestration Gateway (SOG) for Sectigo Certificate Manager (SCM)

Orchestrating SCM atuomation at scale

As enterprises operate across hybrid and multi-cloud environments, certificate management has evolved into a core infrastructure discipline. Shorter certificate lifecycles, growing numbers of digital identities, and increasingly distributed systems have changed how certificates must be issued, deployed, and maintained, placing new demands on automation and operational consistency.

Operational pressure points:

Fragmented operations

Certificate tasks are often spread across legacy connectors, custom scripts, and manual steps, making them difficult to standardize.

Growing certificate volumes

Zero trust initiatives, expanding machine-to-machine authentication, and shorter lifecycles are increasing certificate issuance across servers, applications, and platforms.

Manual processes persist

Despite rising scale and complexity, 95% of organizations still rely on manual certificate operations (Sectigo State of Crypto Agility Report 2025).

Evolving requirements

Regulatory expectations, crypto-agility planning, and continuous verification are raising the bar for consistency and control.

When certificate operations remain fragmented, the cost is paid in reliability and control. Missed renewals and inconsistent workflows increase the risk of outages. As certificate volumes grow and renewal cycles accelerate, legacy automation approaches don't just struggle to keep up, they become a liability, preventing IT and security teams from delivering the resilience and trust the business depends on.

 © 2026 Sectigo. All rights reserved.

SECTIGO

What IT Teams Should Expect from Modern Certificate Automation

One optimized automation layer: A consolidated approach that minimizes connectors, scripts, and tooling while covering the environments that matter most.

Consistency at scale: Standardized workflows that behave predictably across hybrid and multi cloud infrastructure as volume and renewal frequency increase.

Built for shorter lifecycles: Automation that keeps pace with growing certificate volumes and accelerated renewal cycles without added operational load.

Clear operational visibility: Practical, real-time insight into where certificates live, when they expire, and how lifecycle events unfold.

Secure key handling by default: Approaches that reduce key exposure, avoid reuse, and eliminate reliance on shared or centrally stored secrets.

Low friction to deploy and maintain: Lightweight setup, minimal maintenance, and an architecture that simplifies operations rather than adding complexity.

Ready for what's next: Flexibility to adapt to new platforms, evolving crypto standards, and regulatory change without re architecting automation.

What is Sectigo Orchestration Gateway (SOG)?

SOG is a lightweight, modular orchestration layer purpose built to work seamlessly with Sectigo Certificate Manager (SCM). It executes certificate lifecycle and deployment tasks across complex, distributed, multi vendor environments, removing the burden of brittle scripts, manual touchpoints, and legacy connectors.

Working alongside SCM, SOG provides a secure, scalable, and policy-driven automation foundation designed for the realities of modern hybrid and multi-cloud infrastructure. Built as an extensible gateway, SOG handles TLS certificate automation today and is positioned to support broader certificate use cases as the roadmap evolves.

Continuously growing ecosystem compatibility

Servers:

IIS, BIG-IP, Apache Tomcat, Apache HTTP Server Project, NGINX

Supported credential stores:

Delinea, CyberArk, HashiCorp Vault, Personal Vaults

When deployed with Sectigo Certificate Manager, SOG helps IT teams achieve:

Simplified, predictable certificate operations

Organizations gain a single, consistent automation layer that standardizes certificate workflows across cloud environments.

- **Unified certificate lifecycle orchestration:** Automate discovery, issuance, renewal, deployment, and revocation without juggling scripts or specialized connectors.
- **Standardized, policy-driven workflows:** Apply consistent certificate and key handling policies across hybrid and multi cloud environments, reducing drift, manual exceptions, and configuration gaps.
- **Fast and lightweight deployment:** A modular footprint allows rapid rollout with minimal prerequisites, minimizing both setup effort and ongoing maintenance.

End-to-end automation at scale

Keep pace with accelerating certificate lifecycles and exploding certificate volumes, eliminating the firefighting that often accompanies manual tracking or last-minute renewals.

- **Effortless high-frequency renewals:** Shorter cycles and high-volume renewals are fully automated, reducing operational load while ensuring continuity across distributed systems.
- **Parallel certificate operations:** Certificates can be issued, rotated, and deployed across multiple platforms at once, eliminating bottlenecks from sequential updates.
- **Full certificate lifecycle coverage:** From cloud discovery to endpoint deployment, all certificate operations are centrally orchestrated through SCM, automatically.

 © 2026 Sectigo. All rights reserved.

Secure key handling by default

Key security is strengthened at every step, reducing exposure and ensuring hygiene at scale.

- **Eliminates key sprawl:** Private keys are generated fresh on each endpoint rather than retrieved from vaults or PAM tools, eliminating sprawl and ensuring controlled, predictable key management.
- **Per-certificate key generation:** Every certificate receives its own private key generated at the endpoint, eliminating reuse and shrinking the attack surface.
- **No shared key storage:** Avoid centralized repositories and shared vault structures that create risk as certificate volumes grow.

Automation built to evolve with their environment

A modular and forward-looking architecture ensures automation remains future-ready.

- **Extensible, modular architecture:** Support for new servers, platforms, vaults, and PAM systems can be added without redesigning existing workflows.
- **One-to-many automation:** Scale automation across multiple systems from a single deployment, avoiding additional agents, duplicated tooling, or operational overhead.
- **Crypto-agility readiness:** Prepares organizations for new cryptographic standards and algorithm transitions, including post-quantum requirements, without requiring operational re-architecture.

The Sectigo Advantage

Sectigo combines deep PKI expertise with purpose built orchestration to help enterprises modernize certificate operations without introducing additional complexity. SCM provides centralized visibility, governance, and policy control. SOG extends that control into real environments through secure, purpose built orchestration, including policy driven execution, just in time credential access, and consistent lifecycle handling across platforms. Together, they replace fragmented scripts and point tools with predictable, end to end CLM execution across hybrid and multi cloud infrastructure.

This integrated approach reduces operational overhead, minimizes configuration drift, and removes renewal driven risk, while providing a modular foundation that evolves alongside changing environments and cryptographic requirements.

With Sectigo, IT teams gain an automated trust infrastructure built for today's scale and designed to adapt for what's next.

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.

For more information, visit www.sectigo.com, follow us on LinkedIn, and subscribe to our Root Causes podcast.

 © 2026 Sectigo. All rights reserved.