SECTIGO®

Solution Brief

Sectigo Orchestration Gateway

for Sectigo Certificate Manager (SCM)

When complexity, scale & security collide

Enterprises today are running hybrid and multi-cloud environments where shortened certificate lifecycles, rising integration complexity, and fragmented automation tooling have become core operational risks. Often teams rely on multiple connectors, brittle scripts, and inconsistent documentation, creating misconfigurations, blind spots, and barriers to scaling automation.

At the same time, certificate volumes are exploding as organizations mature zero trust architectures and expand machine to machine authentication. According to the Sectigo State of Crypto Agility Report 2025, 95% of organizations still depend on manual processes, underscoring the growing friction as digital identity surfaces expand across clouds, devices, and workloads.

Evolving regulatory pressure, crypto agility requirements, and the push toward continuous verification amplify this urgency. As renewal cycles accelerate and environments diversify, enterprises need a unified orchestration layer that ensures trust, compliance, and scalability across vendors and deployment models.

Introducing the Sectigo Orchestration Gateway (SOG) for SCM

SOG is a lightweight orchestration layer purpose-built to work with Sectigo Certificate Manager (SCM), executing certificate lifecycle and deployment tasks across complex, multi-vendor environments. Managed by SCM, SOG serves as a secure gateway between SCM and distributed enterprise systems, replacing brittle scripts and legacy connectors with a scalable, policy-driven automation capability. It is designed for TLS certificate automation today, with a roadmap that expands into additional certificate use cases over time.

Why enterprises choose Sectigo Orchestration Gateway (SOG)

- Automate certificate lifecycle end-to-end
- Consolidate multi-vendor connectors and scripts into one gateway
- Strengthen compliance through just-in-time credential retrieval
- Accelerate deployment across modern platforms
- Scale policy-driven certificate operations for shorter lifecycles and crypto-agility
- Enforce key hygiene via PAM and vault integrations

As an integrated orchestration component within Sectigo Certificate Manager (SCM), the Sectigo Orchestration Gateway centralizes and streamlines automation by replacing scripts and point integrations with a single, lightweight capability. Managed through SCM policies, SOG automates TLS certificate lifecycle operations across supported servers and platforms while also enabling secure, just-in-time retrieval of privileged credentials. By extending SCM's automation across servers, infrastructure, and credential stores, SOG allows teams to scale trust operations without adding operational complexity.

Streamlined and secured certificate operations

SOG centralizes automation spans multiple servers, load balancers, and cloud platforms, replacing fragmented scripts and manual workflows. It dynamically retrieves privileged credentials from remote credential stores just-in-time, rather than storing sensitive credentials locally.

Supported servers

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

Supported credential stores

Delinea · CyberArk · Personal Vaults · HashiCorp Vault

SECTIGO®

Light footprint. Fast, predictable deployment

Lightweight and modular, the gateway deploys quickly on Linux, Windows, and Docker environments. Its adaptable framework integrates new platforms and services without requiring redesign, while REST API support enables seamless workflow integration and rapid rollout across distributed estates.

End-to-end automation at scale

TLS certificate discovery, issuance, renewal, deployment, and revocation are fully automated across supported servers, cloud services, and enterprise platforms with SOG. Parallel updates ensure operations keep pace with shortened certificate lifecycles and high-volume environments.

Stronger security at every step

Each certificate is paired with a unique key, eliminating shared or centrally stored keys that increase risk. Keys are managed locally or through PAM and key vault integrations, and automated rotation across servers enforces consistent cryptographic hygiene. Continuous discovery identifies unmanaged certificates across cloud environments, reducing attack surface and ensuring compliance.

Future-ready and adaptable

SOG is built for crypto agility, supporting algorithm transitions, post-quantum readiness, and emerging standards across all supported servers, platforms, and protocols. Whether modernizing legacy web servers or scaling containerized workloads, orchestration policies apply consistently without requiring integration redesign.

Operational efficiency with measurable return

With SOG, built-in integrations and automation streamline deployment and day-to-day operations. Teams can eliminate repetitive manual work, cut support escalations, and scale certificate tasks efficiently without expanding administrative overhead.

SECTIGO®

Common SOG use cases within SCM

Automate TLS across hybrid environments

Discover, issue, install, renew, and revoke SSL/TLS certificates across servers, load balancers, and cloud platforms without manual efforts.

Reduce the privileged credential attack surface

Integrate with PAM providers to dynamically retrieve elevated credentials when needed, avoiding local credential storage and reducing operational security risk.

Gain full certificate visibility via SCM

Support SCM to scan internal and external certificates and maintain a complete inventory across servers, devices, and cloud-facing endpoints.

Support accelerated certificate lifecycles

Manage shortened certificate lifecycles and crypto upgrades with policy-driven automation, keeping operations aligned with modern security requirements.

Simplified workflow for one-to-many automation

Execute policy-driven TLS certificate actions across multiple servers through a single centralized gateway, eliminating redundant tasks.

Boost operational efficiency

Streamline high-volume deployments, reduce repetitive tasks, and replace fragmented scripts with centralized automation.

Multi-server and platform support

Deploy certificates across supported servers, including IIS , Apache HTTP server, Apache Tomcat, F5 BIG-IP and NGINX, using local or remote gateways for discovery and installation.

Compliance and audit readiness

Centralize certificate management, dynamically retrieve on-demand credentials, and maintain consistent policies to support regulatory and internal audit requirements.

SECTIGO®

About Sectigo

Sectigo's comprehensive certificate management solution empowers organizations to seamlessly automate, secure, and optimize their digital infrastructure. By simplifying complex certificate operations, strengthening security protocols, and supporting compliance requirements, organizations can confidently protect their hybrid environments and streamline IT workflows.

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 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.