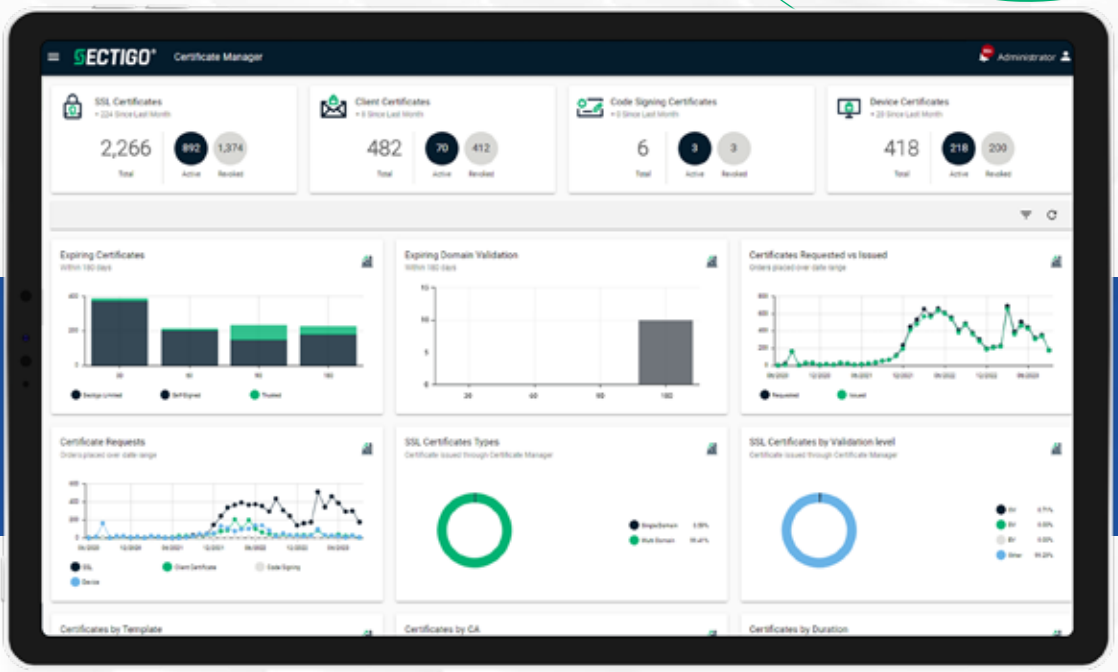

SECTIGO® | CERTIFICATE MANAGER

Automate certificate management to prevent outages, enhance security, and maximize productivity

Solution Brief

SECTIGO®

Sectigo Certificate Manager (SCM) simplifies public and private certificate management across CAs with one centralized platform, offering complete visibility and control tailored for today's enterprise needs at scale.

As digital identities expand across the enterprise, SCM is an integral part to issue certificates to authenticate and secure every human and machine identity. Customers can automate the issuance and management of Sectigo digital certificates, alongside digital certificates originating from other public Certificate Authorities (CAs) and private CAs such as Microsoft Active Directory Certificate Services (ADCS), Amazon Web Services (AWS) Cloud Services, and Google Cloud Platform (GCP).

SCM is an all-in-one solution to consolidate and automate certificate tasks in one place across diverse ecosystems:

- Issuance
- Installation
- Remediation
- Renewal
- Monitoring
- Governance
- Compliance

Why enterprises choose SCM

Provision and renew in seconds
With automation, you avoid outages and save hours of valuable time

Keep tabs on every certificate
Gain full visibility and control over all certificates ever issued

Work with multiple CAs
Manage certificates from any CA(s) with SCM's CA-agnostic solution

Centralized view, total control
A single pane of glass for all your public and private certificate needs

Benefit from the power of one
Eliminate complexity with Sectigo's all-in-one CA and Certificate Lifecycle Management (CLM) solution

Fit for today, ready to scale tomorrow
Open, interoperable platform with 50+ business-critical integrations and easy deployment

Future-proof security
Achieve crypto agility with expert support to adapt to industry changes and compliance

The digital certificates struggle is real

- **Too many certificates, too little visibility**
  Managing SSL/TLS, user, and device certs across multiple platforms and ecosystems is chaotic
- **Shorter lifespans, bigger headaches**
  Frequent renewals and algorithm shifts add pressure
- **Scattered ownership, siloed tracking**
  Different teams, different CAs, endless confusion
- **Manual processes, costly mistakes**
  Errors lead to security gaps, compliance risks, and outages
- **No automation, low efficiency**
  More effort, higher OPEX, slower response times
- **No unification, no visibility**
  Wasted time tracking certificates, blind spots create security risks

SECTIGO®

Optimized with operation

Managing digital certificates across various systems is complex and time-consuming. SCM simplifies this with one-click provisioning and renewals, saving your team hours of manual effort. A key component of this efficiency is the Automatic Certificate Management Environment (ACME), a protocol backed by Google that automates certificate issuance and renewal, particularly for managing shorter certificate lifespans, while reducing manual work and minimizing errors.

Built as an ACME-native open platform, SCM integrates seamlessly with your existing systems and workflows, ensuring full lifecycle automation across your enterprise. With support for the following:

- ✔ ACME
- ✔ Simple Certificate Enrollment Protocol (SCEP)
- ✔ Enrollment over Secure Transport (EST)
- ✔ Representational State Transfer Application Programming Interface (REST APIs)
- ✔ Agents
- ✔ Connectors
- ✔ 3rd party integrations

SCM ensures scalability, lowers compliance risks and frees up valuable time for your IT teams.

Mitigate certificate outages

The real risk isn't the certificates you know about—it's the hidden ones that can cause outages or security breaches when they unexpectedly expire or trigger an audit failure. SCM's discovery function helps mitigate this by finding all your certificates—public and private—across multiple environments, giving you comprehensive visibility. With 24/7 proactive monitoring and automated reports, SCM takes the stress out of manually tracking certificates, helping you stay ahead of risks and avoid costly downtime—all within one simple dashboard.

Manage every certificate

Managing certificates across multiple systems/platforms and CAs can be overwhelming, with the risk of expiring certificates. SCM can scan and inventory both public and private certificates across multiple CAs, network endpoints, and public cloud certificate stores, bringing them all into one centralized view for proactive management. With role-based access controls, every identity is verified as trusted, valid, and compliant, giving you and your team full control and peace of mind.

SECTIGO®

Move fast, stay secure

Coordination delays and dealing with multiple vendors can create inefficiencies, wasting IT resources and slowing down issue resolution. Sectigo simplifies this by offering an all-in-one CA and CLM solution with dedicated expert support, ensuring faster and more efficient issue resolution.

Break down silos

Integrate all your private, public, and cloud-based PKI and CA solutions into one seamless platform. Provide your teams with fast, secure access to certificates through a user-friendly interface, REST API, standard protocols, or out-of-the-box (OOTB) plugins including popular platforms like:

...and more. All while ensuring effortless scalability and streamlined operations.

Stay agile and stay ahead

Keeping up with evolving cryptographic standards, shortening certificate lifespans, and ensuring compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 is no small feat. Sectigo meets these demands by continuously adapting its solutions to industry changes. Audited by WebTrust and with a prominent presence in the Certification Authority Browser Forum (CABF), Sectigo leads the industry in maintaining the highest standards across all its CA and CLM offerings. Its automation capabilities enhance crypto agility, enabling smooth transitions to new cryptographic standards and helping you stay ahead of emerging threats. Trust your infrastructure to the experts and let us help you maintain compliance with ease.

Key cybersecurity trends to watch

- 47-day certificate lifecycles[1]
- NIST Cybersecurity Framework 2.0 compliance
- Passwordless authentication adoption
- Evolving cryptographic standards (e.g. Elliptic Curve Cryptography (ECC) deprecation, quantum readiness)
- Emerging threats (e.g. Harvest now, and decrypt later, man-in-the-middle attacks)

SECTIGO®

Common use cases

Secure Sockets Layer(SSL) / Transport Layer Security (TLS) Management

Automate the deployment, renewal, and management of SSL/TLS certificates across servers and applications

Device Certificate Management

Gain complete control and visibility over issued certificates, ensuring secure device authentication and communication

Certificate-Based Authentication

Authenticate and verify user and device identities using certificates via methods like Virtual Private Network (VPN) and network access, allowing secure access.

DevOps and API Security

Automate certificate management for CI/CD pipelines, containers, and secure API communications

Hybrid and Multi-Cloud Public Key Infrastructure (PKI)

Centralize and simplify certificate management across hybrid and multi-cloud environments

Secure/Multipurpose Internet Mail Extensions (S/MIME) Email Security

Simplify the issuance and management of S/MIME certificates to enable encrypted and digitally signed email communications

Machine-to-Machine Authentication

Automate certificate lifecycle management between virtual machines, servers, and cloud-native environments

Code Signing Security

Protect software integrity with certificates for signing applications, drivers, and updates

Passwordless Authentication

Eliminate passwords with certificate-based authentication for secure user and device verification with hardware-protected keys

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.

700,000+
Global customers

1B+
Certificates issued

2,700
Active partners

57M
Active certificates

98%
Customer retention rate

1998
Founded

Eliminate outages and take control of your certificates today!

Schedule a demo or contact us at *sales@sectigo.com* to get started

