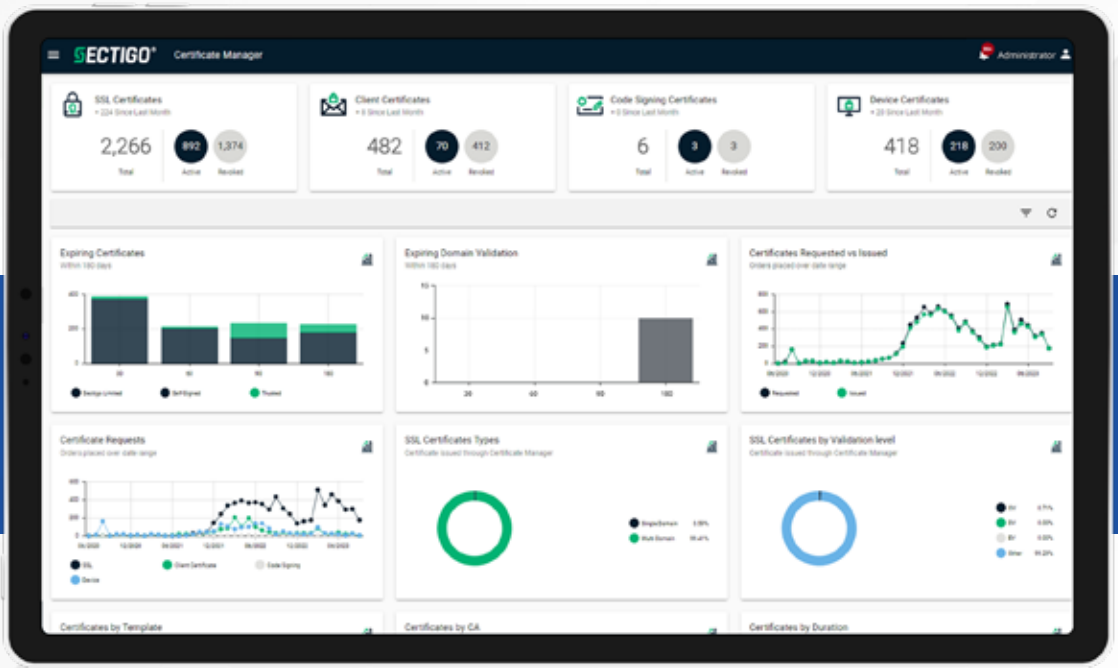
SECTIGO® | CERTIFICATE MANAGER

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

Product Brochure



SECTIGO®

The digital certificates struggle is real

Enterprises today face significant challenges in managing the diverse set of digital certificates spread across various systems, applications, and devices. These may include:

- Secure Sockets Layer (SSL) / Transport Layer Security (TLS) certificates for websites and load balancers on both sides of the firewall
- User certificates to authenticate employees
- Device certificates to authenticate laptops or mobile devices

With certificates often sourced from different teams and certificate authorities (CAs), tracking and managing them becomes complex and time-consuming.
Lack of visibility increases the risk of security gaps, compliance issues, and disruptions. As digital identities grow and certificate lifespans shorten, IT teams face mounting pressure to keep certificates up to date and properly configured.
Manual tracking and decentralized management are error-prone and unsustainable. Modern enterprises recognize the need for an automated, CA-agnostic solution to centralize visibility, consolidate certificate tasks, and reduce certificate-related risks and outages.

Why enterprises choose Sectigo Certificate Manager (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 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

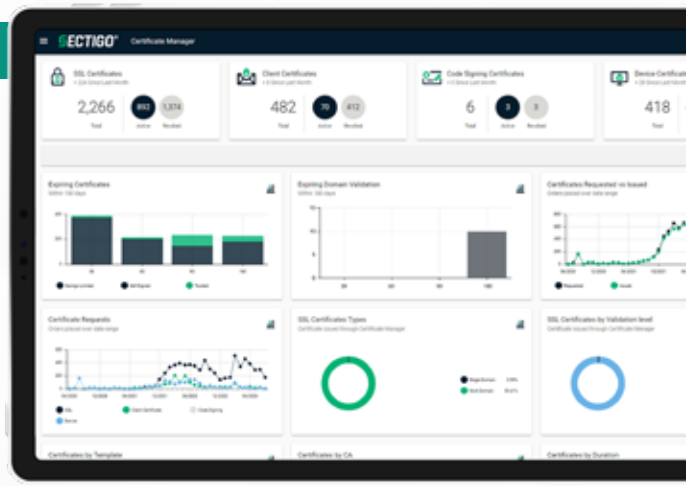
Future-proof security
Achieve crypto agility with expert support to adapt to industry changes and compliance

SECTIGO®

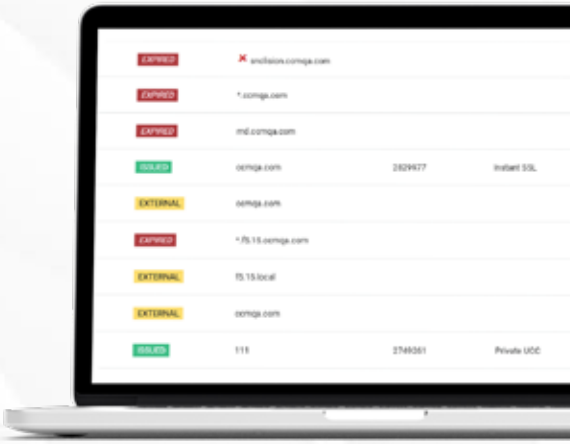
SCM capabilities

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

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



Continuous certificate discovery



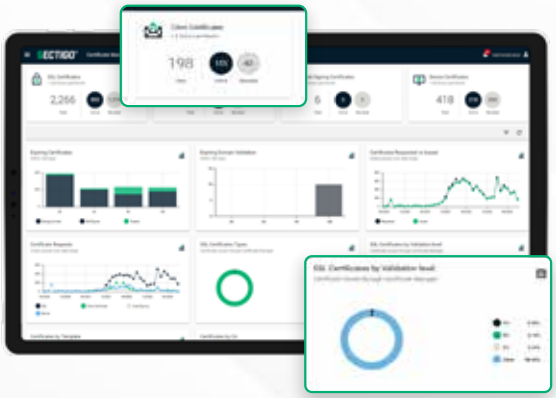
Easily discover all digital certificates across your enterprise, gaining full visibility into every certificate deployed throughout your network. Sectigo discovers SSL/TLS certificates originating from any CA using a port scan of the enterprise network. The discovery of digital certificates can also be achieved by directly querying other CA management platforms such as Microsoft Active Directory Certificate Services (ADCS), Certificate Transparency (CT) Log Monitoring, Amazon Web Services (AWS) Certificate Manager, and Google Cloud Provider (GCP) Certificate Manager.

The dashboard displays a list of all discovered digital certificates, offering key details about their status and ownership, allowing you to efficiently track and manage your certificate inventory.

The digital certificates will be verified for compliance to the corporate policy, triggering notifications in the event a certificate is about to expire, and enabling its automatic renewal. It will also detect any humans or machines that have a digital certificate that should not. For example, it may flag a web server connected to the internet that is using a certificate without proper authorization.

Certificate management

Deploy a wide range of public and private digital certificates to meet diverse security and identity needs, all seamlessly managed through SCM:



Public certificates

- SSL/TLS certificates:
  Domain Validation (DV), Organization Validation (OV), and Extended Validation (EV) options for single domains, multi-domains, and wildcards
- S/MIME certificates
- Code Signing certificates

Private certificates

- SSL/TLS certificates
- User and device certificates
- Code signing certificates

Digital certificates can be managed manually, using the SCM platform or can be automated using protocols, agents and connectors.

SCM offers a single dashboard to view all digital certificate metrics and status across the entire enterprise. An enterprise can track and control digital certificate creation, expiration and renewal ensuring crypto-agility and creating a strong foundation of digital trust.

> SCM's certificate lifecycle management capabilities significantly reduce manual effort, prevent human error, avoid service outages and reduce overall cost of operations.

The trend toward shorter certificate lifespans has taken a major step forward. The CA/B Forum has approved Apple's proposal to reduce public SSL/TLS certificate validity to 47 days by 2029.

Similarly in order to lower the danger of compromise users should consider similar validity periods for email and document signing certificates. Subsequently to guarantee service continuity, a digital certificate must be renewed prior to its expiration.

Therefore using a spreadsheet to track expirations and renewals could be feasible for a small number of certificates, but as businesses grow and certificate lifecycles get shorter, depending solely on manual procedures poses serious risks to any sized organization.

Certificate Automation

Automate the delivery and installation of digital certificates from both public and private CAs with SCM, streamlining certificate management. This authenticates and secures the digital identities for humans and machines, driving secure communication, user authentication and encryption capabilities.

Issue and manage digital certificates from Sectigo's own CA, as well as public and private CAs like Microsoft Active Directory Certificate Services (ADCS), AWS Cloud Services, and Google Cloud Platform (GCP) with SCM. It addresses all certificate issuance needs, supporting flexibility, redundancy, and compliance.

Users can efficiently deploy certificates to approved users and devices, replacing manual processes, while also enabling automatic certificate renewal.

Technology standards that define certificates such as X.509 provide for a range of fields and values that can be leveraged to support new applications such as identification, policy management and authorization. Most certificate lifecycle management platforms have limited ability to populate these fields, restricting their only the most basic certificate roles. Only Sectigo provides the ability to populate and manage these fields, applying complex rulesets to control formatting and prevent duplication. It is these capabilities that help SCM enable enterprises to build complex solutions supporting modern IT operations. IT departments need the ability to consolidate and automate certificate management, with real-time visibility into expiring certificates, so they can take swift action to prevent outages.

SCM's automated Domain Control Validation (DCV), as part of our broader CLM automation suite, helps organizations streamline domain validation and renewal. This approach not only saves hours per domain managed but also minimizes human error, enhancing operational efficiency and reliability.

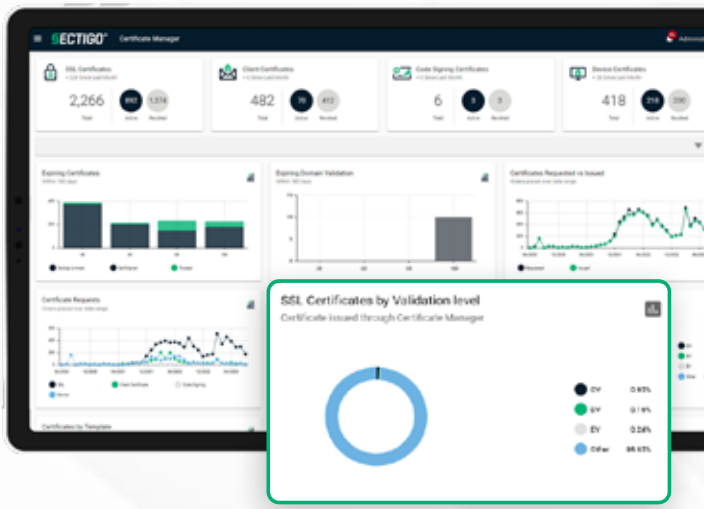
SCM supported Domain Name System (DNS) providers:

- Azure DNS
- AWS Route 53
- DNSimple
- GoDaddy
- Akamai Edge DNS
- Cloudflare
- OVH

SECTIGO®

Certificate governance

Organizations can enforce consistent corporate policies across all digital certificates from any CA with SCM by defining cryptographic strength and contents, effortlessly ensuring compliance before issuing certificates.



These same enforcement rules can be applied to digital certificates issued by other CAs and discovered by SCM. This allows the IT administrator to quickly identify digital certificates that are out of compliance.

The SCM dashboard provides full visibility into the status and other characteristics of all digital certificates across the entire inventory, enabling efficient tracking and control of certificate compliance and health.

Users can leverage SCM's powerful reporting capabilities to facilitate audits and ensure compliance. Having one platform with full visibility of all digital certificate activity throughout the enterprise is the only effective way of ensuring policies are being complied with. Reports can be created showing digital certificate status and activity, filtered by timeline, organization, etc. This will become critical for events like quantum computing attacks, where you need to find all compromised digital certificates and replace them quickly and automatically.

Manage every aspect of the certificate lifecycle including configuration, issuance, revocation, renewal, and distribution - all on a single platform. This eliminates certificate silos, streamlines operations, and enhances efficiency. With SCM's modern cloud-based architecture, organizations gain scalability, resilience, and instant access to the latest lifecycle management capabilities.

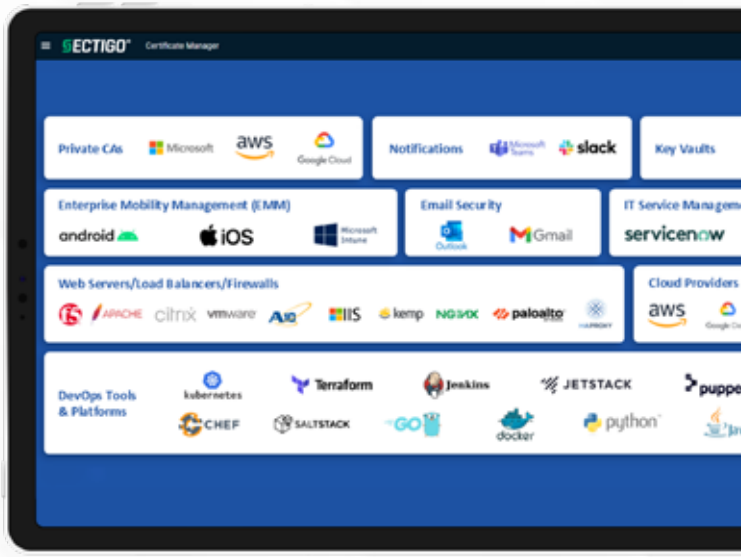
SECTIGO®

Integrations

Sectigo is dedicated to open interoperability, constantly evolving its integration roadmap to align with organizations' evolving needs. SCM integrates seamlessly with all major enterprise applications, ensuring flexibility and smooth connectivity.

Some examples:

- DevOps orchestration tools & containerization
- Automation standards to integrate with applications using that same standard, such as Simple Certificate Enrollment Protocol (SCEP), Internet of Things (IoT) devices using Enrollment over Secure Transport(EST) and Automatic Certificate Management Environment (ACME)
- Cloud vendor applications such as AWS Certificate Manager, CloudFront, Elastic Load Balancer, Azure Key Vault
- Security Information and Event Management (SIEM) Integrations: Splunk, Microsoft Sentinel



Rapid time to value

Organizations can leverage the flexibility of SCM's open, cloud-based, and CA-agnostic platform to seamlessly integrate into their existing infrastructure without disruption. This ensures rapid time to value—eliminating certificate-related outages, reducing manual processes, and enhancing security immediately.

> "The implementation of Sectigo's certificate management solutions not only streamlined our processes but also significantly reduced our overall operational costs."
>
> *~Senior Manager of Cybersecurity, Broadcasting and Cable Industry*

According to a recent Forrester study[1]:

$2.4M With automated renewals and proactive tracking, Sectigo's SCM solution has been proven to save enterprises $2.4 million by preventing outage-related expenses

<6months Organizations deploying SCM are realizing payback and seeing value in less than six months

243%ROI Companies adopting SCM are achieving an estimated 243% ROI, with substantial cost savings in operations, labor, and business disruptions

SECTIGO®

Let our customers speak for us

Gartner Peer Insights 4.7

5.0 Reviewed on Mar 21, 2024

Simplify the Certificate Management, Boost Security

The solution is an easy-to-use products that helps the organization to manage and control certificate, increasing the security and visibility.

5.0 Reviewed on Mar 21, 2024

Reduces operations and risks for SSL certificates management

Powerful solution that helps mid size and big companies to manage this SSL certificates install base.

G2 4.8

5.0 Reviewed on Mar 21, 2024

"Certificate Governance"

What do you like best about Sectigo Certificate Manager?

The advantage of Sectigo Certificate Manager is to easily consolidate your certificate requests and put clear governance for issuing new ones. You can also automate a lot of the rotation of certificates.

5.0 Reviewed on Mar 21, 2024

"Reduce time & cost in managing SSL certificates"

What do you like best about Sectigo Certificate Manager?

Sectigo is the very best in automating the SSL certificate management, whether to renew it or to delete it. It saves time from having to manually renew the certificates one-by-one and use the automation to bulk update them.

Last updated: February 2025

> Sectigo Certificate Manager has become a major part of our IT management infrastructure, allowing us to update, add and delete thousands of digital certificates with a streamlined dashboard and email alert system.
>
> *~Craig Hurter*
> *IT security Manager, University of Colorado at Boulder*

SECTIGO®

Choose trust

For robust and reliable Certificate Authority services to secure your websites, networks, and authenticate users, devices, and applications, Sectigo stands out as an exceptional choice.

As one of the largest commercial CAs globally and a leader in innovative certificate lifecycle management (CLM), Sectigo provides a diverse array of solutions tailored to meet your specific needs, backed by our award-winning customer support.

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

