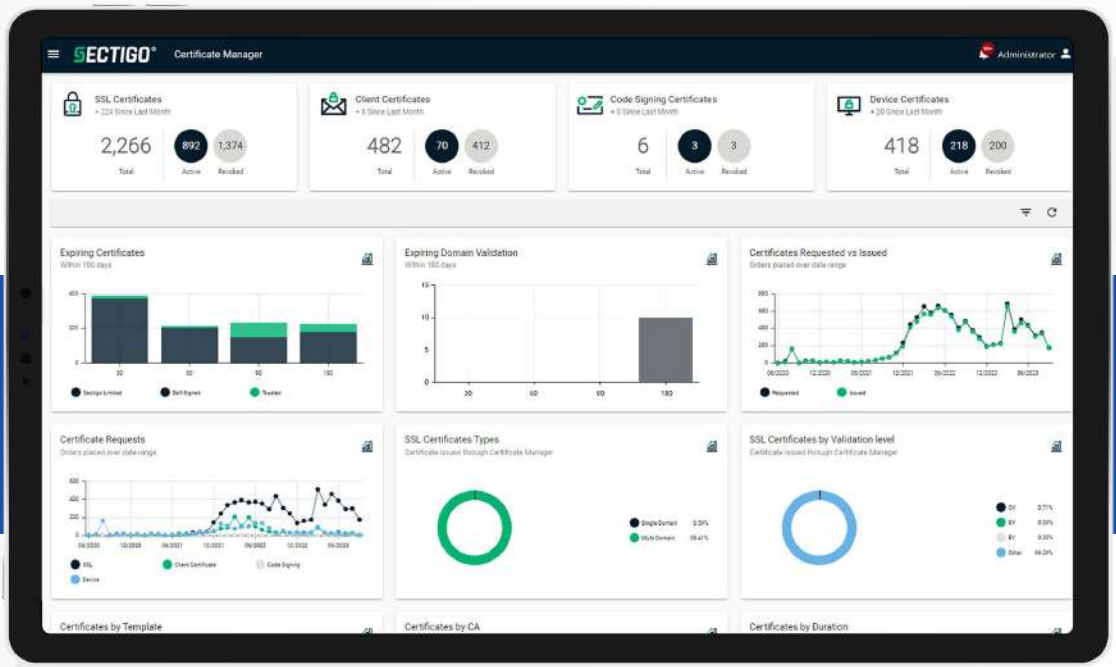
# SECTIGO® | CERTIFICATE MANAGER

Automatisieren Sie die Zertifikatsverwaltung,
um Ausfälle zu vermeiden, die Sicherheit zu erhöhen
und die Produktivität zu maximieren.

## Produktbroschüre






SECTIGO®

# Die Herausforderungen im Umgang mit digitalen Zertifikaten

Unternehmen stehen vor der Herausforderung, zahlreiche digitale Zertifikate über verschiedene Systeme, Anwendungen und Geräte hinweg effizient zu verwalten:

- SSL- (Secure Sockets Layer) / TLS- (Transport Layer Security) Zertifikate für Websites und Load Balancer auf beiden Seiten der Firewall
- Benutzerzertifikate zur Authentifizierung von Mitarbeitern
- Gerätezertifikate zur Authentifizierung von Laptops oder Mobilgeräten

Da Zertifikate häufig von verschiedenen Teams und Zertifizierungsstellen (CAs) stammen, ist ihre Verfolgung und Verwaltung komplex und zeitaufwändig.
Mangelnde Transparenz erhöht das Risiko von Sicherheitslücken, Compliance-Problemen und Ausfällen. Mit der Zunahme digitaler Identitäten und der Verkürzung der Lebensdauer von Zertifikaten stehen IT-Teams unter zunehmendem Druck, Zertifikate auf dem neuesten Stand zu halten und ordnungsgemäß zu konfigurieren. Manuelle Nachverfolgung und dezentrale Verwaltung sind fehleranfällig und nicht nachhaltig. Moderne Unternehmen erkennen die Notwendigkeit einer automatisierten, CA-unabhängigen Lösung, um die Transparenz zu zentralisieren, Zertifikatsaufgaben zu konsolidieren und zertifikatsbezogene Risiken und Ausfälle zu reduzieren.

## Warum Unternehmen sich für Sectigo Certificate Manager (SCM)

**Bereitstellung und Erneuerung in Sekundenschnelle**
Durch Automatisierung vermeiden Sie Ausfälle und sparen wertvolle Zeit

**Behalten Sie den Überblick über jedes Zertifikat**
Erhalten Sie vollständige Transparenz und Kontrolle über alle jemals ausgestellten Zertifikate

**Arbeiten Sie mit mehreren Zertifizierungsstellen**
Verwalten Sie Zertifikate von beliebigen Zertifizierungsstellen mit der CA-unabhängigen Lösung von SCM

**Zentrale Ansicht, vollständige Kontrolle**
Eine einzige Oberfläche für alle Ihre Anforderungen an öffentliche und private Zertifikate

**Profitieren Sie von der Leistungsfähigkeit einer Lösung**
Eliminieren Sie Komplexität mit der All-in-One-Lösung von Sectigo für CA und Zertifikatslebenszyklusmanagement

**Heute geeignet, morgen skalierbar**
Offene, interoperable Plattform mit über 50 geschäftskritischen Integrationen und einfacher Bereitstellung

**Zukunftssichere Sicherheit**
Krypto-Agilität mit kompetenter Unterstützung bereit für Wandel und Compliance

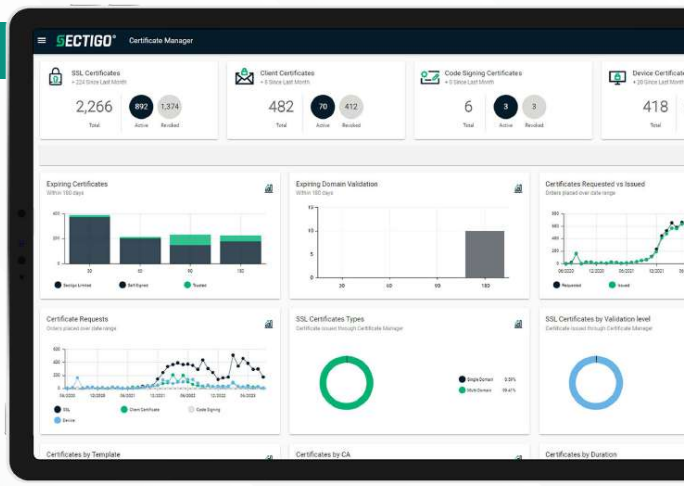
 

SECTIGO®

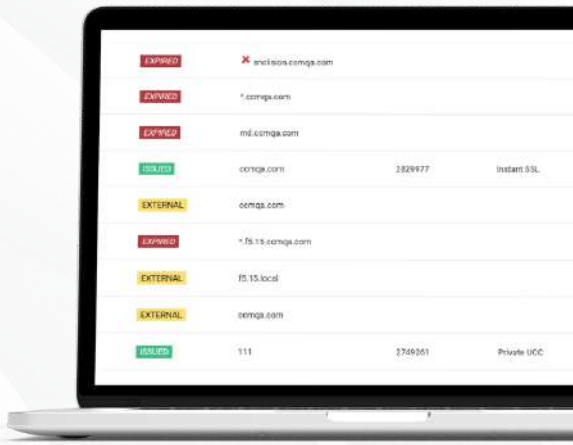
# SCM-Funktionen

SCM automatisiert und zentralisiert Zertifikatsmanagement über alle Ökosysteme hinweg:

- Ausstellung
- Installation
- Überwachung
- Korrektur
- Erneuerung
- Governance
- Compliance




## Kontinuierliche Erkennung von Zertifikaten



Erkennen Sie ganz einfach alle digitalen Zertifikate in Ihrem Unternehmen und erhalten Sie vollständige Transparenz über jedes in Ihrem Netzwerk bereitgestellte Zertifikat. Sectigo erkennt SSL/TLS-Zertifikate, die von einer beliebigen Zertifizierungsstelle stammen, mithilfe eines Port-Scans des Unternehmensnetzwerks. Die Erkennung digitaler Zertifikate kann auch durch direkte Abfrage anderer CA-Verwaltungsplattformen wie Microsoft Active Directory Certificate Services (ADCS), Certificate Transparency (CT) Log Monitoring, Amazon Web Services (AWS) Certificate Manager und Google Cloud Provider (GCP) Certificate Manager erfolgen.

Das Dashboard zeigt eine Liste aller erkannten digitalen Zertifikate mit wichtigen Details zu ihrem Status und ihrer Zugehörigkeit an, sodass Sie Ihren Zertifikatsbestand effizient verfolgen und verwalten können.

Die digitalen Zertifikate werden auf Einhaltung der Unternehmensrichtlinien überprüft. Bei Ablauf eines Zertifikats werden Benachrichtigungen ausgelöst und die automatische Verlängerung aktiviert. Außerdem werden alle Personen oder Maschinen erkannt, die über ein digitales Zertifikat verfügen, das sie nicht haben sollten. Beispielsweise kann ein mit dem Internet verbundener Webserver markiert werden, der ein Zertifikat ohne ordnungsgemäße Autorisierung verwendet.

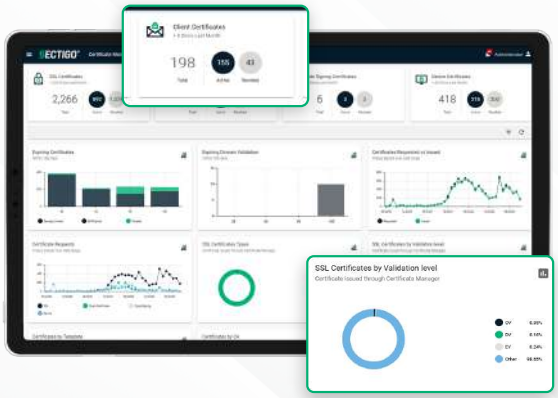
 

# Zertifikatsverwaltung

Stellen Sie eine Vielzahl öffentlicher und privater digitaler Zertifikate bereit, um unterschiedliche Sicherheits- und Identitätsanforderungen zu erfüllen, die alle nahtlos über SCM verwaltet werden:

**Öffentliche Zertifikate**

- SSL/TLS-Zertifikate:
  Optionen für Domänenvalidierung (DV), Organisationsvalidierung (OV) und erweiterte Validierung (EV) für einzelne Domänen, mehrere Domänen und Platzhalter
- S/MIME-Zertifikate
- Code Signing-Zertifikate



**Private Zertifikate**

- SSL/TLS-Zertifikate
- Benutzer- und Gerätezertifikate
- Code Signing-Zertifikate

Digitale Zertifikate können manuell über die SCM-Plattform verwaltet oder mithilfe von Protokollen, Agenten und Konnektoren automatisiert werden.

SCM bietet ein einziges Dashboard, in dem alle Metriken und der Status aller digitalen Zertifikate im gesamten Unternehmen angezeigt werden. Unternehmen können die Erstellung, das Auslaufen und die Erneuerung digitaler Zertifikate verfolgen und kontrollieren, wodurch Krypto-Agilität gewährleistet und eine starke Grundlage für digitales Vertrauen geschaffen wird.

> Die Funktionen von SCM für das Lebenszyklusmanagement von Zertifikaten reduzieren den manuellen Aufwand erheblich, verhindern menschliche Fehler, vermeiden Dienstausfälle und senken die Gesamtbetriebskosten.

**Der Trend zu kürzeren Lebensdauern von Zertifikaten hat einen großen Schritt nach vorne gemacht. Das CA/B Forum hat den Vorschlag von Apple genehmigt, die Gültigkeit öffentlicher SSL/TLS-Zertifikate bis 2029 auf 47 Tage zu reduzieren.**

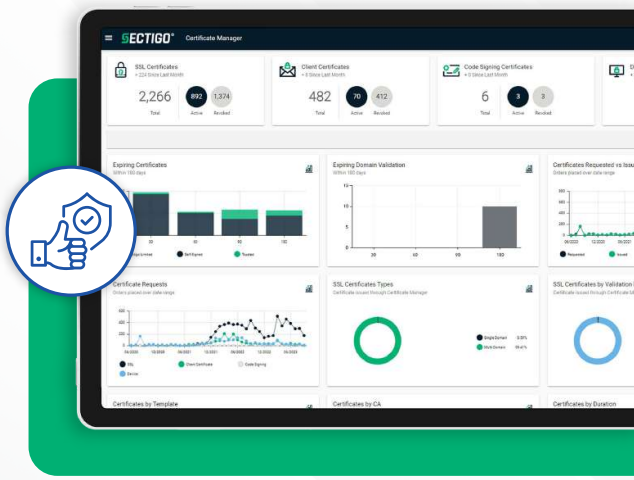
Um die Gefahr von Kompromittierungen zu verringern, sollten Benutzer ähnliche Gültigkeitszeiträume für E-Mail- und Dokumentensignaturzertifikate in Betracht ziehen. Um die Kontinuität der Dienste zu gewährleisten, muss ein digitales Zertifikat vor seinem Ablauf erneuert werden.

Daher kann die Verwendung einer Tabellenkalkulation zur Verfolgung von Ablauf- und Erneuerungsdaten für eine kleine Anzahl von Zertifikaten sinnvoll sein. Mit zunehmender Größe des Unternehmens und immer kürzeren Zertifikatslebenszyklen birgt die ausschließliche Verwendung manueller Verfahren jedoch erhebliche Risiken für Unternehmen jeder Größe.

# Zertifikatautomatisierung

Mit SCM automatisieren Sie die Bereitstellung und Installation digitaler Zertifikate aus öffentlichen und privaten Zertifizierungsstellen. Dadurch wird die Zertifikatsverwaltung zentralisiert und vereinfacht, während digitale Identitäten von Menschen und Maschinen zuverlässig authentifiziert und geschützt werden – für sichere Kommunikation, Benutzerzugriffe und Verschlüsselung.




SCM unterstützt Zertifikate von Sectigo, ADCS, AWS, GCP und weiteren Anbietern. Es erfüllt alle Anforderungen an Ausstellung, Flexibilität, Redundanz und Compliance.

Benutzer können Zertifikate effizient für zugelassene Benutzer und Geräte bereitstellen, manuelle Prozesse ersetzen und gleichzeitig die automatische Zertifikatserneuerung aktivieren.

Technologiestandards, die Zertifikate wie X.509 definieren, bieten eine Reihe von Feldern und Werten, die zur Unterstützung neuer Anwendungen wie Identifizierung, Richtlinienverwaltung und Autorisierung genutzt werden können. Die meisten Plattformen für die Verwaltung des Zertifikatslebenszyklus verfügen nur über begrenzte Möglichkeiten, diese Felder auszufüllen, wodurch sie auf die grundlegendsten Zertifikatsrollen beschränkt sind. Nur Sectigo bietet die Möglichkeit, diese Felder auszufüllen und zu verwalten, wobei komplexe Regelsätze zur Steuerung der Formatierung und zur Vermeidung von Duplikaten angewendet werden. Dank dieser Funktionen kann SCM Unternehmen dabei unterstützen, komplexe Lösungen für moderne IT-Abläufe zu entwickeln. IT-Abteilungen müssen in der Lage sein, die Zertifikatsverwaltung zu konsolidieren und zu automatisieren und dabei in Echtzeit Einblick in ablaufende Zertifikate zu erhalten, damit sie schnell Maßnahmen zur Vermeidung von Ausfällen ergreifen können.

Die automatisierte Domain Control Validation (DCV) von SCM, die Teil unserer umfassenden CLM-Automatisierungssuite ist, hilft Unternehmen dabei, die Domain-Validierung und -Erneuerung zu optimieren. Dieser Ansatz spart nicht nur Zeit pro verwalteter Domain, sondern minimiert auch menschliche Fehler und verbessert so die betriebliche Effizienz und Zuverlässigkeit.

## Von SCM unterstützte Domain Name System (DNS)-Anbieter:

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

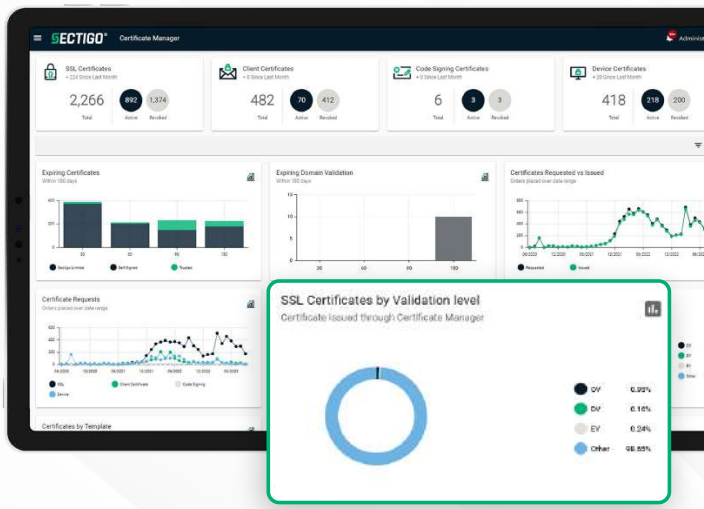
SECTIGO®

# Zertifikat-Governance

Mit SCM können Unternehmen einheitliche Richtlinien für alle digitalen Zertifikate durchsetzen – unabhängig von der CA. Durch die Definition kryptografischer Standards und Inhalte wird die Compliance bereits vor der Ausstellung sichergestellt.

Diese Richtlinien gelten auch für Zertifikate anderer CAs, die von SCM erkannt werden. So lassen sich nicht konforme Zertifikate schnell identifizieren und beheben.

Das zentrale Dashboard von SCM bietet vollständige Transparenz über Status und Eigenschaften aller Zertifikate im Bestand – für eine effiziente Kontrolle von Konformität und Integrität.




Benutzer können die leistungsstarken Berichtsfunktionen von SCM nutzen, um Audits zu vereinfachen und die Compliance sicherzustellen. Eine einzige Plattform mit vollständiger Transparenz aller Aktivitäten im Zusammenhang mit digitalen Zertifikaten im gesamten Unternehmen ist die einzige effektive Möglichkeit, um die Einhaltung von Richtlinien sicherzustellen. Es können Berichte erstellt werden, die den Status und die Aktivitäten digitaler Zertifikate anzeigen und nach Zeitachse, Organisation usw. gefiltert werden können. Dies wird für Ereignisse wie Angriffe durch Quantencomputer von entscheidender Bedeutung sein, bei denen Sie alle kompromittierten digitalen Zertifikate finden und schnell und automatisch ersetzen müssen.

Verwalten Sie alle Aspekte des Zertifikatslebenszyklus, einschließlich Konfiguration, Ausstellung, Widerruf, Erneuerung und Verteilung – alles auf einer einzigen Plattform. Dadurch werden Zertifikatssilos beseitigt, Abläufe optimiert und die Effizienz gesteigert. Mit der modernen Cloud-basierten Architektur von SCM profitieren Unternehmen von Skalierbarkeit, Ausfallsicherheit und sofortigem Zugriff auf die neuesten Funktionen für das Lebenszyklusmanagement.

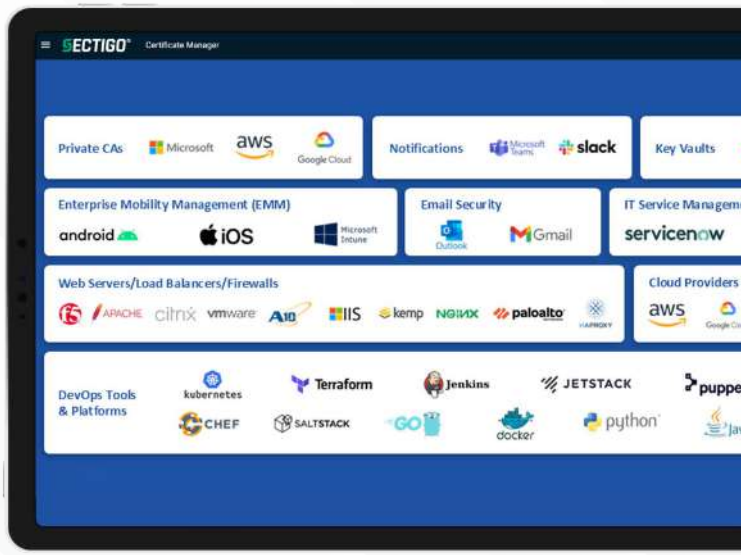
SECTIGO®

# Integration

Sectigo setzt sich für offene Interoperabilität ein und entwickelt seine Integrationsroadmap ständig weiter, um sie an die sich wandelnden Anforderungen von Unternehmen anzupassen. SCM lässt sich nahtlos in alle gängigen Unternehmensanwendungen integrieren und gewährleistet so Flexibilität und reibungslose Konnektivität.

Einige Beispiele:

- DevOps-Orchestrierungstools und Containerisierung
- Automatisierungsstandards für die Integration mit Anwendungen, die denselben Standard verwenden, wie z. B. Simple Certificate Enrollment Protocol (SCEP), IoT-Geräte (Internet of Things) mit Enrollment over Secure Transport (EST) und Automatic Certificate Management Environment (ACME)
- Anwendungen von Cloud-Anbietern wie AWS Certificate Manager, CloudFront, Elastic Load Balancer, Azure Key Vault
- Integrationen für Sicherheitsinformations- und Ereignismanagement (SIEM): Splunk, Microsoft




# Schnelle Amortisierung

Unternehmen können die Flexibilität der offenen, cloudbasierten und CA-unabhängigen Plattform von SCM nutzen, um sie nahtlos und ohne Unterbrechungen in ihre bestehende Infrastruktur zu integrieren. Dies gewährleistet eine schnelle Amortisierung, da Ausfälle im Zusammenhang mit Zertifikaten vermieden, manuelle Prozesse reduziert und die Sicherheit sofort erhöht werden.

> Die Implementierung der Zertifikatsmanagement-Lösungen von Sectigo hat nicht nur unsere Prozesse optimiert, sondern auch unsere Gesamtbetriebskosten erheblich gesenkt.
>
> *~Senior Manager für Cybersicherheit, Rundfunk- und Kabelindustrie*

## Laut einer aktuellen Forrester-Studie[1]:

**2.4M $** Dank automatisierter Verlängerungen und proaktiver Nachverfolgung spart die SCM-Lösung von Sectigo Unternehmen bis zu 2,4 Mio. USD an Ausfallkosten.

**<6monate** Unternehmen, die SCM einsetzen, erzielen eine Amortisation und einen Mehrwert in weniger als sechs Monaten.

**243%ROI** Unternehmen, die SCM einsetzen, erzielen einen ROI von 243 % und senken deutlich Kosten in Betrieb, Personal und durch vermiedene Unterbrechungen.

SECTIGO®

# Unsere Kunden sprechen für uns

Gartner Peer Insights™ 4.7 ★★★★★

5.0 ★★★★★ Bewertet am 21. März 2024

## Vereinfachen Sie die Zertifikatsverwaltung und erhöhen Sie die Sicherheit

Die Lösung ist ein benutzerfreundliches Produkt, das Unternehmen bei der Verwaltung und Kontrolle von Zertifikaten unterstützt und so die Sicherheit und Transparenz erhöht.

5.0 ★★★★★ Bewertet am 21. März 2024

## Reduziert den Aufwand und die Risiken bei der Verwaltung von SSL-Zertifikaten

Leistungsstarke Lösung, die mittelständischen und großen Unternehmen bei der Verwaltung ihrer SSL-Zertifikate hilft.

G2 4.8 ★★★★½

5.0 ★★★★★ Bewertet am 21. März 2024

## "Zertifikatsverwaltung"

**Was gefällt Ihnen am besten an Sectigo Certificate Manager?**

Il vantaggio di Sectigo Certificate Manager è quello di consolidare facilmente le richieste di certificati e di stabilire una governance chiara per il rilascio di quelli nuovi. È anche possibile automatizzare gran parte della rotazione dei certificati.

5.0 ★★★★★ Bewertet am 21. März 2024

## "Zeit und Kosten bei der Verwaltung von SSL-Zertifikaten reduzieren"

**Was gefällt Ihnen am besten an Sectigo Certificate Manager?**

Sectigo ist das führende Tool zur Automatisierung der SSL-Zertifikatsverwaltung – von der Erneuerung bis zur Löschung. Durch Massenaktualisierung statt manueller Einzelverlängerung sparen Unternehmen wertvolle Zeit.

**Zuletzt aktualisiert: Februar 2025**

> Der Sectigo Certificate Manager ist zu einem wichtigen Bestandteil unserer IT-Management-Infrastruktur geworden und ermöglicht es uns, Tausende von digitalen Zertifikaten über ein optimiertes Dashboard und ein E-Mail-Benachrichtigungssystem zu aktualisieren, hinzuzufügen und zu
>
> *~Craig Hurter*
> *IT-Sicherheitsmanager, University of Colorado in Boulder*

SECTIGO®

## Entscheiden Sie sich für Vertrauen

Für robuste und zuverlässige Zertifizierungsdienste zur Sicherung Ihrer Websites und Netzwerke sowie zur Authentifizierung von Benutzern, Geräten und Anwendungen ist Sectigo eine hervorragende Wahl.

Als eine der weltweit größten kommerziellen Zertifizierungsstellen und führender Anbieter von innovativem Zertifikatslebenszyklusmanagement (CLM) bietet Sectigo eine Vielzahl von Lösungen, die auf Ihre spezifischen Anforderungen zugeschnitten sind und durch unseren preisgekrönten Kundensupport unterstützt werden.

## Über Sectigo

Sectigo ist der innovativste Anbieter von Zertifikat-Lebenszyklusmanagement (CLM) und liefert umfassende Lösungen, die die Identitäten von Menschen und Maschinen für die weltweit größten Marken schützen. Die automatisierte, cloudnative CLM-Plattform von Sectigo stellt digitale Zertifikate für alle Zertifizierungsstellen (CAs) aus und verwaltet diese, um die Sicherheitsprotokolle innerhalb des Unternehmens zu vereinfachen und zu verbessern. Sectigo ist eine der größten, ältesten und renommiertesten CAs mit mehr als 700.000 Kunden und zwei Jahrzehnten Erfahrung in der Bereitstellung von beispiellosem digitalem Vertrauen.

**+700,000**
Kunden weltweit

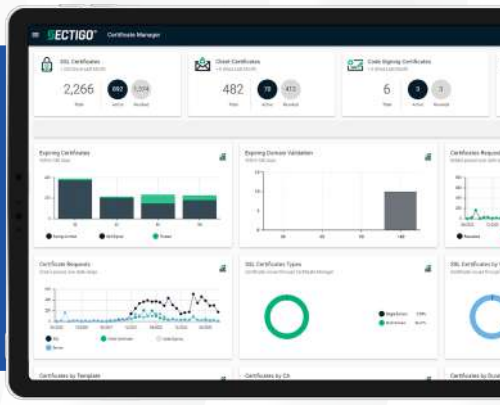
**+1000M**
ausgestellte Zertifikate

**2,700**
aktive Partner

**57M**
aktive Zertifikate

**98%**
Kundenbindungsrate

**1998**
gegründet



## Vermeiden Sie Ausfälle und übernehmen Sie noch heute die Kontrolle über Ihre Zertifikate!

Vereinbaren Sie eine Demo oder kontaktieren Sie uns unter sales@sectigo.com, um loszulegen.