

Sectigo Orchestration Gateway für Sectigo Certificate Manager (SCM)

SCM-Automatisierung im großen Maßstab orchestrieren

Da Unternehmen in hybriden und Multi-Cloud-Umgebungen agieren, hat sich das Zertifikatsmanagement zu einer zentralen Infrastrukturdizziplin entwickelt. Kürzere Zertifikatslaufzeiten, eine wachsende Anzahl digitaler Identitäten und zunehmend verteilte Systeme haben die Art und Weise verändert, wie Zertifikate ausgestellt, bereitgestellt und gewartet werden müssen. Dies stellt neue Anforderungen an die Automatisierung und die betriebliche Konsistenz.

Betriebliche Belastungspunkte:

- **Fragmentierter Betrieb:** Zertifikatsaufgaben sind häufig über veraltete Konnektoren, benutzerdefinierte Skripte und manuelle Schritte verteilt, was eine Standardisierung erschwert.
- **Manuelle Prozesse bestehen weiter:** Trotz zunehmender Skalierung und Komplexität verlassen sich 95 % der Unternehmen immer noch auf manuelle Zertifikatsabläufe.
- **Wachsende Zertifikatsvolumina:** Zero-Trust-Initiativen, die Ausweitung der Maschinen-zu-Maschinen-Authentifizierung und kürzere Laufzeiten führen zu einer höheren Anzahl von Zertifikatsausstellungen über Server, Anwendungen und Plattformen hinweg.
- **Sich verändernde Anforderungen:** Regulatorische Vorgaben, die Planung von Krypto-Agilität und die kontinuierliche Überprüfung erhöhen die Anforderungen an Kontrolle und Konsistenz.

[\[State of Crypto Agility Report 2025\]](#)

Wenn der Zertifikatsbetrieb fragmentiert bleibt, zahlen Unternehmen den Preis mit mangelnder Zuverlässigkeit und fehlender Kontrolle. Versäumte Verlängerungen und uneinheitliche Workflows erhöhen das Risiko von Systemausfällen. Wenn die Automatisierung auf separaten VMs, Skripten und Konnektoren für jede Plattform basiert, wird die Skalierung zu einem Risikomultiplikator. Mit steigenden Zertifikatsvolumina und sich beschleunigenden Erneuerungszyklen stoßen traditionelle Automatisierungsansätze nicht nur an ihre Grenzen, sondern werden zu einem Sicherheitsrisiko, das IT- und Sicherheitsteams daran hindert, die vom Unternehmen benötigte Resilienz zu liefern.

Was IT-Teams von einer modernen Zertifikatsautomatisierung erwarten sollten

- ✓ **Eine optimierte Automatisierungsebene**
Ein konsolidierter Ansatz, der integrationsspezifische VMs, Konnektoren und Skripte durch eine einzige Automatisierungsebene ersetzt, die die wichtigsten Umgebungen abdeckt.
- ✓ **Entwickelt für kürzere Laufzeiten**
Automatisierung, die mit wachsenden Zertifikatsvolumina und beschleunigten Erneuerungszyklen ohne zusätzlichen betrieblichen Aufwand Schritt hält.
- ✓ **Sichere Schlüsselhandhabung als Standard**
Der Just-in-Time-Abruf von privilegierten Zugangsdaten stellt sicher, dass der Zugriff nur bei Bedarf gewährt wird, was die Schlüsselexposition reduziert.
- ✓ **Zukunftssicher**
Flexibilität zur Anpassung an neue Plattformen, sich entwickelnde Kryptografiestandards und regulatorische Änderungen ohne Neugestaltung der Automatisierung.
- ✓ **Konsistenz im großen Maßstab**
Standardisierte Workflows, die sich in hybriden und Multi-Cloud-Infrastrukturen auch bei steigendem Volumen und höherer Erneuerungsfrequenz vorhersehbar verhalten.
- ✓ **Klare betriebliche Transparenz**
Praktische Echtzeit-Einblicke darüber, wo Zertifikate vorhanden sind, wann sie ablaufen und wie Lebenszyklus-Ereignisse ablaufen.
- ✓ **Geringer Aufwand bei Bereitstellung und Wartung**
Schlanke Einrichtung, minimaler Wartungsaufwand und eine Architektur, die den Betrieb vereinfacht, anstatt neue Komplexität zu schaffen.

Was ist das Sectigo Orchestration Gateway (SOG)?

Das SOG ist eine schlanke, modulare Orchestrierungsebene, die speziell für das nahtlose Zusammenspiel mit dem [Sectigo Certificate Manager \(SCM\)](#) entwickelt wurde. Es führt Aufgaben im Rahmen des Zertifikats-Lebenszyklus und der Bereitstellung in komplexen, verteilten Multi-Vendor-Umgebungen aus und nimmt IT-Teams die Last fehleranfälliger Skripte, manueller Eingriffe und veralteter Konnektoren ab.

In Kombination mit dem SCM bietet das SOG eine sichere, skalierbare und richtliniengesteuerte Automatisierungsbasis, die für die Realität moderner hybrider und Multi-Cloud-Infrastrukturen entwickelt wurde. Als erweiterbares Gateway konzipiert, automatisiert seine modulare Architektur heute TLS-Zertifikatsabläufe und lässt sich bei sich ändernden Anforderungen problemlos auf neue Anwendungsfälle ausweiten.

Kontinuierlich wachsende Ökosystem-Kompatibilität

Unterstützte TLS-Endpunkte:



Unterstützte Speichersysteme für Zugangsdaten:



Die aktuellste Liste der unterstützten Integrationen finden Sie auf [unserer technischen Dokumentationsseite](#).



Beim Einsatz mit dem Sectigo Certificate Manager hilft das SOG IT-Teams folgendes zu erreichen:



Vereinfachte, vorhersehbare Zertifikatsabläufe

Unternehmen erhalten eine einheitliche Automatisierungsebene, die Zertifikats-Workflows über Cloud-Umgebungen hinweg standardisiert.

- **Vereinheitlichte Orchestrierung des Zertifikats-Lebenszyklus**

Automatisiert Erkennung, Ausstellung, Erneuerung, Bereitstellung und Widerruf, ohne mit Skripten oder spezialisierten Konnektoren jonglieren zu müssen.

- **Standardisierte, richtliniengesteuerte Workflows**

Wenden Sie einheitliche Richtlinien für Zertifikate und Schlüssel in hybriden und Multi-Cloud-Umgebungen an, um Abweichungen, manuelle Ausnahmen und Konfigurationslücken zu reduzieren.

- **Schnelle und schlanke Bereitstellung**

Ein modularer Ressourcenbedarf ermöglicht eine schnelle Einführung mit minimalen Voraussetzungen, was sowohl den Einrichtungsaufwand als auch die laufende Wartung minimiert.



Durchgängige Automatisierung im großen Maßstab

Halten Sie Schritt mit sich beschleunigenden Zertifikatslaufzeiten und explodierenden Zertifikatsvolumina und eliminieren Sie die Hektik, die oft mit manueller Nachverfolgung oder Verlängerungen in letzter Minute verbunden ist.

- **Mühelose hochfrequente Erneuerungen**

Kürzere Zyklen und volumenstarke Erneuerungen werden vollständig automatisiert, was die betriebliche Belastung reduziert und gleichzeitig die Kontinuität in verteilten Systemen sicherstellt.

- **Parallele Zertifikatsoperationen**

Zertifikate können gleichzeitig auf mehreren Plattformen ausgestellt, rotiert und bereitgestellt werden, wodurch Engpässe durch sequenzielle Updates vermieden werden.

- **Vollständige Abdeckung des Zertifikats-Lebenszyklus**

Von der Cloud- und lokalen Erkennung bis hin zur Endpunkt-Bereitstellung werden alle Zertifikatsabläufe automatisch zentral über den SCM orchestriert.

- **Vollständige Transparenz über die gesamte Umgebung**

Cloud- und lokale Erkennung scannen interne Netzwerke und externe Systeme gemeinsam, führen ein aktuelles Inventar und beseitigen blinde Flecken.



Sichere Schlüsselhandhabung als Standard

Die Schlüsselsicherheit wird bei jedem Schritt gestärkt, was die Exposition verringert und eine nachhaltige kryptografische Hygiene im großen Maßstab gewährleistet.

- **Verhindert Schlüssel-Wildwuchs**

Private Schlüssel werden bei Bedarf direkt auf dem jeweiligen Endpunkt Just-in-Time erzeugt. Dies verhindert Wildwuchs und sorgt für eine kontrollierte, vorhersehbare Schlüsselverwaltung.

- **Schlüsselerzeugung pro Zertifikat**

Jedes Zertifikat erhält seinen eigenen, auf dem Endpunkt generierten privaten Schlüssel, was eine Wiederverwendung ausschließt und die Angriffsfläche verkleinert.

- **Kein zentraler Schlüsselspeicher**

Vermeiden Sie zentrale Repositories und gemeinsam genutzte Vault-Strukturen, die mit steigendem Zertifikatsvolumen Sicherheitsrisiken bergen.



Automatisierung, die sich mit Ihrer Umgebung weiterentwickelt

Eine modulare und zukunftsorientierte Architektur stellt sicher, dass die Automatisierung stets einsatzbereit bleibt.

- **Erweiterbare, modulare Architektur**

Unterstützung für neue Server, Plattformen, Vaults und PAM-Systeme kann hinzugefügt werden, ohne bestehende Workflows neu gestalten zu müssen.

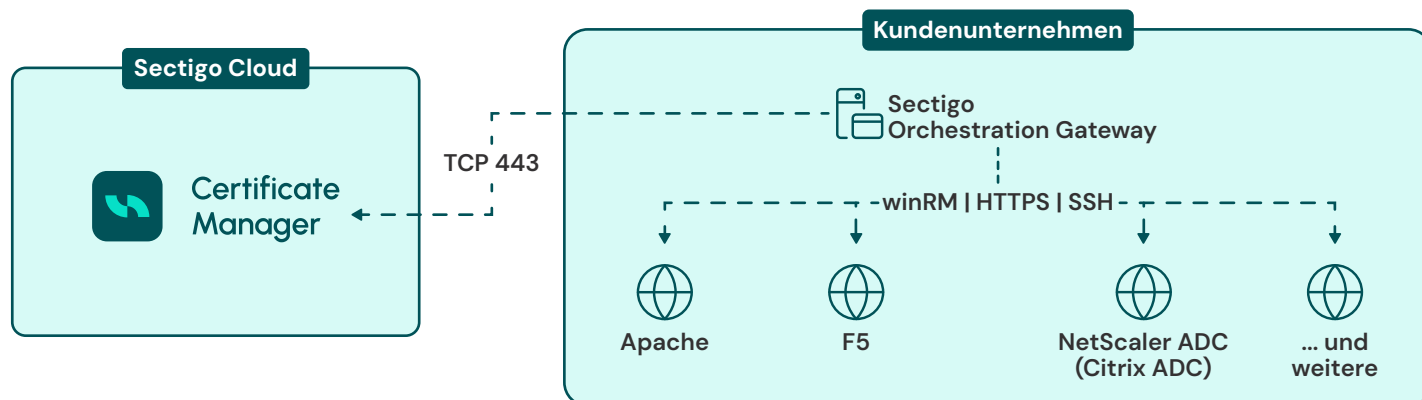
- **1-zu-n-Automatisierung**

Eine einzige Gateway-Instanz verbindet sich mit mehreren Endpunkten im Netzwerk und ersetzt integrationsspezifische VMs, HA-Setups und Patch-Zyklen durch eine einzige Installation.

- **Vorbereitung auf Krypto-Agilität**

Bereitet Unternehmen auf neue Kryptografiestandards und Algorithmen-Wechsel vor – einschließlich Post-Quanten-Anforderungen – ohne dass eine betriebliche Neugestaltung erforderlich ist.

Wie es funktioniert



Besuchen Sie die [technische Dokumentationsseite](#) für die vollständige Liste der vom Orchestration Gateway unterstützten Integrationen.

Der Sectigo-Vorteil

Sectigo kombiniert tiefgreifendes PKI-Know-how mit maßgeschneiderter Orchestrierung, um Unternehmen bei der Modernisierung ihrer Zertifikatsabläufe zu unterstützen, ohne zusätzliche Komplexität einzuführen. Der SCM bietet zentrale Transparenz, Governance und Richtliniensteuerung. Das SOG weitet diese Kontrolle über eine sichere Orchestrierung auf reale Umgebungen aus – einschließlich richtliniengesteuerter Ausführung, Just-in-Time-Zugriff auf Zugangsdaten und einheitlichem Lebenszyklus-Management über Plattformen hinweg. Gemeinsam ersetzen sie fragmentierte Skripte und Punkt-Lösungen durch eine vorhersehbare, durchgängige CLM-Ausführung in hybriden und Multi-Cloud-Infrastrukturen.

Dieser integrierte Ansatz reduziert den betrieblichen Aufwand, minimiert Konfigurationsabweichungen und eliminiert verlängerungsbedingte Risiken. Gleichzeitig bietet er eine modulare Grundlage, die sich mit veränderten Umgebungen und kryptografischen Anforderungen weiterentwickelt. Mit Sectigo erhalten IT-Teams eine automatisierte Vertrauensinfrastruktur, die für die heutigen Skalierungsanforderungen gebaut ist und sich flexibel an zukünftige Herausforderungen anpassen lässt.

Über Sectigo

Sectigo ist ein führender Anbieter von Certificate Lifecycle Management (CLM) und unterstützt Unternehmen dabei, menschliche und maschinelle Identitäten abzusichern sowie verdeckte Risiken im Bereich der digitalen Identitäten zu reduzieren. Da Zertifikatsvolumina steigen und Laufzeiten sinken, werden unverwaltete Zertifikate zunehmend zu einer Ursache für Ausfälle, Compliance-Lücken und Störungen im Betriebsablauf. Sectigo nutzt orchestrierte Automatisierung, um einfache Steuerung in großen Umgebungen über seine cloudnative CLM-Plattform zu ermöglichen. Die Lösung führt Transparenz, Kontrolle und Lebenszyklus-Management in komplexen Infrastrukturen zusammen. Mit mehr als 700.000 Kunden, darunter 65 % der Fortune 500, ist Sectigo eine der größten und etabliertesten Zertifizierungsstellen mit über 20 Jahren Erfahrung im Bereich der digitalen Sicherheit.

Für weitere Informationen zum Sectigo Orchestration Gateway oder zu Zertifikatsmanagement-Lösungen wenden Sie sich bitte an den Sectigo-Vertrieb unter sales@sectigo.com.

