sectigo

LÖSUNGSÜBERSICHT

Sectigo Orchestration Gateway für Sectigo Certificate Manage (SCM)

Wenn Komplexität, Skalierung & Sicherheit aufeinandertreffen

Unternehmen betreiben heute hybride und Multi-Cloud-Umgebungen, in denen verkürzte Zertifikatslaufzeiten, steigende Integrationskomplexität und fragmentierte Automatisierungswerkzeuge zu zentralen betrieblichen Risiken geworden sind. Oft verlassen sich Teams auf mehrere Konnektoren, fehleranfällige Skripte und uneinheitliche Dokumentationen – was zu Fehlkonfigurationen, blinden Flecken und Hürden bei der Skalierung der Automatisierung führt.

Gleichzeitig explodieren die Zertifikatsvolumina, da Unternehmen ihre Zero-Trust-Architekturen ausbauen und die Authentifizierung zwischen Maschinen erweitern. Laut dem Sectigo **State of Crypto Agility Report 2025** hängen 95 % der Unternehmen immer noch von manuellen Prozessen ab. Dies unterstreicht die wachsenden Hürden, da sich digitale Identitäten über Clouds, Geräte und Workloads hinweg ausbreiten.

Steigender regulatorischer Druck, Anforderungen an die Krypto-Agilität und der Trend zur kontinuierlichen Überprüfung verstärken diese Dringlichkeit. Da sich die Erneuerungszyklen beschleunigen und die Umgebungen immer vielfältiger werden, benötigen Unternehmen eine einheitliche Orchestrierungsebene, die Vertrauen, Compliance und Skalierbarkeit über verschiedene Anbieter und Bereitstellungsmodelle hinweg gewährleistet.

Das Sectigo Orchestration Gateway (SOG) für SCM

Das SOG ist eine schlanke Orchestrierungsebene, die speziell für das Zusammenspiel mit dem **Sectigo Certificate Manager (SCM)** entwickelt wurde. Sie führt Aufgaben im Rahmen des Zertifikats-Lebenszyklus und der Bereitstellung in komplexen Multi-Vendor-Umgebungen aus.

Verwaltet durch den SCM, dient das SOG als sicheres Gateway zwischen dem SCM und den verteilten Unternehmenssystemen. Es ersetzt fehleranfällige Skripte und veraltete Konnektoren durch eine skalierbare, richtliniengesteuerte Automatisierungslösung. Derzeit automatisiert es TLS-Zertifikatsabläufe über eine breite und wachsende Infrastruktur hinweg, wobei die modulare Architektur darauf ausgelegt ist, im Laufe der Zeit weitere Anwendungsfälle zu unterstützen.

Warum Unternehmen SCM mit SOG wählen:

- Automatisiert den gesamten Zertifikats-Lebenszyklus über Server, CDNs, WAFs und Zugangssysteme hinweg.
- Konsolidiert Konnektoren, Skripte und VMs in einer einzigen Gateway-Installation.
- Erkennt jedes Zertifikat durch kombinierte Cloud- und lokale Netzwerk-Scans.
- Setzt strikte Schlüsselhygiene und Just-in-Time-Zugriffe auf Anmeldedaten über PAM- und Vault-Integrationen um.
- Skaliert richtliniengesteuerte Prozesse für kürzere Laufzeiten und Kryptografische Agilität.
- Beschleunigt die Bereitstellung auf modernen Multi-Vendor-Plattformen.

Als integrierte Orchestrierungskomponente innerhalb des Sectigo Certificate Managers (SCM) zentralisiert und vereinfacht das Sectigo Orchestration Gateway die Automatisierung, indem es Skripte und Punkt-zu-Punkt-Integrationen durch eine einzige, schlanke Lösung ersetzt. Gesteuert über SCM-Richtlinien automatisiert das SOG die TLS-Zertifikatsabläufe auf unterstützten Servern, Load Balancern, CDNs, WAFs und Privileged-Access-Systemen und ermöglicht gleichzeitig den sicheren Just-in-Time-Abruf von privilegierten Zugangsdaten. Indem das SOG die Automatisierung von SCM auf Server, Infrastruktur und Zugangsdatenspeicher ausweitet, können Teams ihre Sicherheitsabläufe skalieren, ohne die betriebliche Komplexität zu erhöhen.

Schlanke und sichere Zertifikatsabläufe

Das SOG zentralisiert die Automatisierung über mehrere Server, Load Balancer und Cloud-Plattformen hinweg und ersetzt fragmentierte Skripte sowie manuelle Workflows. Es ruft privilegierte Zugangsdaten dynamisch im Just-in-Time-Verfahren aus entfernten Speichern ab, anstatt sensible Daten lokal zu speichern.

Unterstützte Server:

IIS, BIG-IP, Apache Tomcat, Cloudflare WAF, Apache HTTP Server Project, NGINX, Imperva WAF, NetScaler

... und weitere

Unterstützte Speichersysteme für Zugangsdaten:

Delinea, CyberArk, HashiCorp Vault, BeyondTrust Pathfinder, Local Vaults

... und weitere

Die aktuellste Liste der unterstützten Integrationen finden Sie auf unserer technischen Dokumentationsseite.

Geringer Ressourcenbedarf. Schnelle, vorhersagbare

Schlank und modular lässt sich das Gateway schnell in Linux-, Windows- und Docker-Umgebungen bereitstellen. Die anpassungsfähige Architektur bindet neue Plattformen und Dienste ohne Umgestaltung ein, während die Unterstützung von REST-APIs eine nahtlose Workflow-Integration und eine schnelle Bereitstellung in verteilten Strukturen ermöglicht.

Durchgängige Automatisierung im großen Maßstab

Erkennung, Ausstellung, Erneuerung, Bereitstellung und Widerruf von TLS-Zertifikaten werden über alle vom SOG unterstützten Server, Cloud-Dienste und Unternehmensplattformen hinweg vollständig automatisiert. Parallele Updates stellen sicher, dass die Abläufe mit den verkürzten Zertifikatslaufzeiten und volumenstarken Umgebungen Schritt halten.

Höhere Sicherheit bei jedem Schritt

Jedes Zertifikat wird mit einem eindeutigen Schlüssel gekoppelt. Dadurch werden gemeinsam genutzte oder zentral gespeicherte Schlüssel vermieden, die das Risiko erhöhen. Schlüssel werden lokal oder über PAM- und Key-Vault-Integrationen verwaltet, und die automatisierte Rotation auf den Servern setzt eine konsequente kryptografische Hygiene durch. Kontinuierliche Erkennung identifiziert unverwaltete Zertifikate in Cloud-Umgebungen, verkleinert die Angriffsfläche und stellt Compliance sicher.

Vollständige Transparenz über jede Umgebung hinweg

Cloud- und lokale Erkennung arbeiten zusammen, um Zertifikate in internen und externen Systemen zu identifizieren. Das 24/7 On-Demand-Tracking beseitigt blinde Flecken und führt ein zuverlässiges Inventar über Server, Plattformen und Cloud-Dienste hinweg. Dies unterstützt die Durchsetzung von Richtlinien und ein proaktives Risikomanagement.

Zukunftssicher und anpassungsfähig

Das SOG ist auf Kryptografische Agilität ausgelegt und unterstützt Algorithmen-Wechsel, Vorbereitung auf Post-Quanten-Kryptografie sowie neue Standards über alle unterstützten Server, Plattformen und Protokolle hinweg. Egal ob bei der Modernisierung veralteter Webserver oder der Skalierung von Container-Workloads – Orchestrierungsrichtlinien werden durchgängig angewendet, ohne dass Integrationen neu entworfen werden müssen.

Betriebliche Effizienz mit messbarem Ertrag

Mit dem SOG vereinfachen integrierte Schnittstellen und Automatisierung die Bereitstellung und das Tagesgeschäft. Die Konsolidierung integrationsspezifischer VMs in einem einzigen Gateway reduziert den Infrastrukturbedarf, den Wartungsaufwand und potenzielle Fehlerquellen, was den ROI beschleunigt. Teams eliminieren repetitive Aufgaben, reduzieren Eskalationen und skalieren Zertifikatsabläufe ohne zusätzlichen Aufwand.

Typische SOG-Anwendungsfälle im SCM

TLS in hybriden Umgebungen automatisieren

SSL/TLS-Zertifikate auf Servern, Load Balancern und Cloud-Plattformen ohne manuellen Aufwand entdecken, ausstellen, installieren, erneuern und widerrufen.

Beschleunigte Zertifikatslaufzeiten unterstützen

Verkürzte Gültigkeitsdauern und Kryptografie-Upgrades durch richtliniengesteuerte Automatisierung steuern, um die Abläufe an moderne Sicherheitsanforderungen anzupassen.

Vereinfachter Workflow für 1-zu-n-Abläufe

Richtliniengesteuerte TLS-Zertifikationsaktionen auf mehreren Servern über ein zentrales Gateway ausführen und redundante Aufgaben eliminieren.

Betriebliche Effizienz steigern

Umfangreiche Bereitstellungen vereinfachen, repetitive Aufgaben reduzieren und fragmentierte Skripte durch zentrale Automatisierung ersetzen.

Vollständige Zertifikatstransparenz über den SCM erlangen

Den SCM dabei unterstützen, interne und externe Zertifikate zu scannen und ein vollständiges Inventar über Server, Geräte und Cloud-Endpunkte hinweg zu führen.

Zertifikate systemübergreifend entdecken

Cloud- und lokale Erkennung kombinieren, um blinde Flecken zu beseitigen und kontinuierliche Compliance zu unterstützen.

Angriffsfläche für privilegierte Zugangsdaten reduzieren

Zugangsdaten Just-in-Time über PAM-Integrationen abrufen, lokale Speicherung vermeiden und Risiken begrenzen.

Compliance und Audit-Bereitschaft

Richtlinien zentralisieren, Zertifikatsmanagement automatisieren und einheitliche Audit-Kontrollen aufrechterhalten.

Infrastruktur-Wildwuchs minimieren

Integrationsspezifische VMs und HA-Setups durch ein einziges Gateway ersetzen, um Aufwand und Fehlerquellen zu reduzieren.

Multi-Server- und Multi-Plattform-Unterstützung

Bereitstellung auf IIS, Apache, Tomcat, F5, NGINX, Netscaler, Cloudflare und Imperva über lokale oder entfernte Gateways.

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.

Die umfassende Zertifikatsmanagement-Lösung von Sectigo ermöglicht es Unternehmen, ihre digitale Infrastruktur nahtlos zu automatisieren, abzusichern und zu optimieren. Durch die Vereinfachung komplexer Zertifikatsabläufe, die Stärkung von Sicherheitsprotokollen und die Unterstützung von Compliance-Anforderungen können Unternehmen ihre hybriden Umgebungen zuverlässig schützen und IT-Workflows optimieren.

Fordern Sie noch heute eine persönliche Demo an oder kontaktieren Sie uns unter sales@sectigo.com, um zu erfahren, wie Sectigo Ihre Zertifikatsmanagement-Strategie transformieren kann.