

Sectigo Automation

Die Public-Key-Verschlüsselung (PKI) ist der Goldstandard für digitale Privatsphäre, Identität und Sicherheit und sollte unstrittig das Sicherheitsfundament für jedes Gerät, jeden Server, jeden Benutzer und jede Anwendung im Unternehmen bilden. Die Nutzung manueller Prozesse zur Installation, Überwachung und Verlängerung aller mittlerweile erforderlichen PKI-Zertifikate ist jedoch arbeitsintensiv, technisch anspruchsvoll und risikobehaftet. Zudem können sich die Kosten schnell aufsummieren. Eine minimale manuelle TLS/SSL-Zertifikatsinstallation (einzelner Webserver und eine Domain-Instanz) umfasst mehrere Schritte und kann sich leicht auf 50 bis 100 US-Dollar pro Webserver belaufen.

Darüber hinaus bewegt sich die Branche hin zu kürzeren Zertifikatslaufzeiten – zuerst von drei Jahren auf zwei und dann von zwei Jahren auf ein Jahr. Mit der bevorstehenden Verkürzung der Lebensdauer von TLS/SSL-Zertifikaten ist mit steigenden Installations- und Verwaltungskosten zu rechnen. Und der Zeitpunkt könnte kaum schlechter sein. Da immer mehr Unternehmen die Nutzung mobiler Geräte, des Internets der Dinge (IoT), von DevOps und anderen digitalen Umgebungen ausweiten, steigt der Bedarf an PKI ebenso wie die Dringlichkeit, Zertifikate schnell, zuverlässig und im Unternehmensmaßstab ausstellen, widerrufen und ersetzen zu können.

Automatisierung der TLS/SSL-Zertifikatsinstallation

Automatisierung ist heute eindeutig entscheidend für jedes Zertifikatsverwaltungssystem. Sie senkt nicht nur die Gesamtbetriebskosten, sondern setzt auch die kryptografische Compliance durch und verhindert potenzielle Dienstunterbrechungen durch menschliche Fehler.

Angesichts der unterschiedlichen Systeme, Anwendungen und Geräte, die digitale Zertifikate nutzen und einbinden, ist ein universeller Ansatz jedoch kaum geeignet, die Automatisierungsanforderungen verschiedener Anwendungsfälle abzudecken. Aus diesem Grund bietet Sectigo mehrere verschiedene Automatisierungsoptionen an.

Für die Installation von TLS/SSL-Zertifikaten bietet Sectigo:

- **Unterstützung für das ACME-Protokoll (Automated Certificate Management Environment):**
Sectigo Certificate Manager unterstützt ACME, sodass Sie die Ausstellung und Installation von Zertifikaten für eine Vielzahl von Webservern, Load Balancern, Routern, Firewalls und anderen Netzwerkgeräten automatisieren können. Sectigo unterstützt DV-, OV- und EV-Zertifikatstypen über ACME und bietet IT-Administratoren vollständige Kontrolle. Viele DevOps-Tools unterstützen ACME zur Registrierung und Verwaltung von Zertifikaten, und für diesen Zweck steht eine Vielzahl von Open-Source-Tools zur Verfügung. Diese Tools sind bei IT-Administratoren beliebt und werden regelmäßig um neue Funktionen erweitert.

Wenn Sectigo die Server- oder Zertifizierungsstellenseite des ACME-Protokollstandards implementiert, funktioniert dies mit ACME-konformen Clients, und wir unterstützen jedes Kundenprojekt, das diese Integration erfordert (was voraussetzt, dass der Client ACME-konform ist). Die folgende Tabelle enthält eine Liste der derzeit unterstützten Plattformen.

- **Ein Sectigo Automation Agent:**

Mit dem Network Agent von Sectigo können Sie die Verwaltung von Zertifikaten für eine Vielzahl von Systemen automatisieren, darunter Apache, Apache Tomcat, Windows IIS und F5 BIG-IP Load Balancer. Der Network Agent, der beim Kunden vor Ort installiert ist, ist mit der Cloud-Lösung Sectigo Certificate Manager integriert, um die Ausstellung, Installation und Verlängerung von Zertifikaten zu planen.

- **REST API:**

In einigen Fällen bevorzugen Unternehmen eine engere Integration von Anwendungen mit Sectigo, was über die REST API von Sectigo möglich ist. Dies erfordert zwar zusätzlichen Entwicklungsaufwand auf Anwendungsseite, ermöglicht es Ihnen jedoch, das Zertifikatsmanagement optimal zu nutzen und Ihren Workflow anzupassen.

- **Integration mit Drittanbietern:**

Sectigo sucht kontinuierlich nach Möglichkeiten zur Integration mit Drittanbietern, um Kunden bei der vollständigen Automatisierung zu unterstützen. Der BIG-IP Load Balancer von F5 bietet beispielsweise eine Integration über sein Verwaltungssystem, um die Zertifikatsverwaltung von Sectigo zu automatisieren.

Automatisierung der Domain Control Validation (DCV)

Mit der Verkürzung der Zertifikatslaufzeiten ist die Aufrechterhaltung validierter Domains zu einer dauerhaften Anforderung geworden. Manuelle Validierungsprozesse sind zeitaufwendig, fehleranfällig und auf Unternehmensebene nicht tragbar. Sectigo Certificate Manager rationalisiert diesen Prozess mit integrierter, automatisierter Domain Control Validation (DCV) als Teil seiner umfassenderen Funktionen zur Automatisierung des Zertifikatslebenszyklus. Durch die Nutzung von DNS-Konnektoren integriert sich SCM direkt mit unterstützten DNS-Anbietern, um CNAME-Record-Challenges automatisch zu erstellen und zu validieren. Dies eliminiert manuelle Eingriffe, reduziert das Risiko fehlgeschlagener Verlängerungen und stellt sicher, dass Domains kontinuierlich validiert bleiben.

SCM erweitert seine Liste unterstützter DNS-Anbieter kontinuierlich, darunter aktuell:

Cloudflare

Amazon Route 53

Azure DNS

GoDaddy DNS

Akamai Edge DNS

DNSimple

OVHcloud

Die vollständige Liste der von SCM unterstützten DNS-Anbieter finden Sie [hier](#).

Automatisierung der Client- und Gerätezertifikatsinstallation

Viele Systeme, Anwendungen und Geräte nutzen Nicht-SSL-Zertifikate. Für die Installation von Nicht-SSL-Zertifikaten bietet Sectigo:

- **EST-Protokoll (Enrollment over Secure Transport):**

Sectigo unterstützt das EST-Protokoll, das zur Verwaltung von Netzwerkgeräten vieler Hersteller verwendet wird. Tatsächlich haben mehrere Anbieter die EST-Unterstützung bereits integriert. EST ist auch in Internet-of-Things-Umgebungen (IoT) aufgrund der Effizienz des Protokolls und der Unterstützung von ECC-Schlüsseln (Elliptic Curve Cryptography) beliebt. Es stehen auch mehrere Open-Source-EST-Clients zur Verfügung. Sectigo Certificate Manager zeigt die ausgetellten Zertifikate an und verwaltet sie.

- **Simple Certificate Enrollment Protocol (SCEP):**

In der Sectigo-Umgebung kann SCEP verwendet werden, um Zertifikate in Linux, macOS und anderen Betriebssystemen zu registrieren. Mobile Geräte, der NDES-Server von Microsoft und MDM-Lösungen nutzen typischerweise SCEP.

- **Sectigo MS Automation Agent:**

Ein Sectigo MS Agent, der zwischen dem Microsoft Active Directory Certificate Service und Sectigo Certificate Manager sitzt. Er hört auf Zertifikatsanforderungen über das Windows Client Certificate Enrollment Protocol (WCCE) und stellt das Zertifikat dem Desktop automatisch ohne Eingreifen des Mitarbeiters zur Verfügung.

Wie Sie sehen, bietet Sectigo eine Vielzahl von Optionen für die Zertifikatsinstallation sowie den Komfort und die Sicherheit einer nahtlosen Lösung mit einer zentralen Benutzeroberfläche sowohl für die Ausstellung als auch für die Verwaltung öffentlicher und privater Zertifikate. Darüber hinaus werden Sie bei Sectigo nie an eine Obergrenze für das Zertifikatsvolumen stoßen, wie dies bei Open-Source-Alternativen der Fall sein kann. Sectigo ermöglicht es Ihrem Sicherheitsteam, kryptografische Sicherheitsrichtlinien einfach durchzusetzen, die Kommunikation zu schützen, Datenverlust durch unbefugten Zugriff zu verhindern und Systeme, Anwendungen sowie Geräte im gesamten Unternehmen zukunftssicher zu machen.



TLS/SSL-Automatisierung mit SCM:

ACME-Clients und native Integrationen

Content Delivery Network (CDN)

Anbieter	Anwendung	Native ACME-Unterstützung	Verwendeter ACME-Client	Von Sectigo entwickelte Integration (out-of-the-box)	Sectigo-Integrationstechnologie
Akamai	Terraform			Sectigo Connector für Akamai Terraform	REST API
Akamai	CLI			Sectigo Connector für Akamai Terraform	REST API

Containerisierung

Anbieter	Anwendung	Native ACME-Unterstützung	Verwendeter ACME-Client	Von Sectigo entwickelte Integration (out-of-the-box)	Sectigo-Integrationstechnologie
Amazon	Elastic Kubernetes Service	✓	jetstack (cert-manager)		
Google	Google Kubernetes Engine	✓	jetstack (cert-manager)		
Kubernetes	Kubernetes	✓	jetstack (cert-manager)		
Microsoft	Azure Kubernetes Services	✓	jetstack (cert-manager)		
Redhat	Openshift Container Platform	✓	jetstack (cert-manager)		
Docker	Docker	✓	ACME.sh		

DevOps-Tools

Anbieter	Anwendung	Native ACME-Unterstützung	Verwendeter ACME-Client	Von Sectigo entwickelte Integration (out-of-the-box)	Sectigo-Integrationstechnologie
Ansible	Ansible	✓	Ansible ACME	Sectigo Ansible Integration	REST API
Chef	Chef			Sectigo Chef Integration	REST API
HashiCorp	Terraform	✓	Vancluever	Sectigo Terraform Integration	REST API
Jenkins	Jenkins			Sectigo Jenkins Integration	REST API
Jetstack	Jetstack	✓	jetstack (cert-manager)		
Puppet				Sectigo Puppet Integration	REST API
SaltStack				Sectigo SaltStack Integration	REST API

Webserver / Load Balancer / Firewalls

Anbieter	Anwendung	Native ACME-Unterstützung	Verwendeter ACME-Client	Integrazione realizzata da Sectigo (pronta all'uso)	Sectigo-Integrationstechnologie
A10	Thunder ADC	✓	In A10 integriert	Sectigo Connector für A10	REST API
Amazon	AWS Certificate Manager			Sectigo Connector für AWS	ACME
Apache	Apache	✓	Certbot mod_md	Network Agent	Network Agent / REST API
Cisco	Cisco FTD			Sectigo Connector für Cisco FTD	REST API
Citrix	ADC			Citrix Connector für Citrix	REST API
Citrix	Gateway			Citrix Connector für Citrix	REST API
Citrix	FAS			MS Agent	APIs
F5	BIG-IP	✓	Kojot ACME	Sectigo Connector für F5 BIG-IP Network Agent	ACME Network Agent / REST API
F5	NGINX	✓	Certbot ACME.sh		
Google	Google Load Balancer			Sectigo Connector für GCP	ACME
HAProxy	HAProxy	✓	Certbot ACME.sh	Sectigo HAProxy Connector	ACME
Kemp	LoadMaster	✓	ACME.sh	Sectigo Kemp Connector	REST API
Microsoft	IIS	✓	Win-ACME posh ACME Certify the Web	Sectigo Kemp Connector	REST API
PaloAlto	PAN OS	✓	ACME.sh		
VMWare	Avi Vantage			Sectigo Connector für Avi Vantage	REST API

Almacén de claves (Key Vault)

Anbieter	Anwendung	Native ACME-Unterstützung	Verwendeter ACME-Client	Integrazione realizzata da Sectigo (pronta all'uso)	Sectigo-Integrationstechnologie
Hashicorp	HashiCorp Vault			Sectigo HashiCorp Vault Integration	REST API
Microsoft	Azure Key Vault	✓	az-acme	SCM PK Agent	APIs

Lenguaje de programación

Anbieter	Anwendung	Native ACME-Unterstützung	Verwendeter ACME-Client	Integrazione realizzata da Sectigo (pronta all'uso)	Sectigo-Integrationstechnologie
Golang	Golang	✓	Lets Encrypt Go		
Java	Java	✓	ACME4j	Sectigo Connector für Java	REST API
Python	Python	✓	certbot		
Ruby	Ruby	✓	acme-client		



Altro

Anbieter	Anwendung	Native ACME-Unterstützung	Verwendeter ACME-Client	Integrazione realizzata da Sectigo (pronta all'uso)	Sectigo-Integrationstechnologie
BeyondTrust	BeyondTrust	✓	Native Beyond Trust		
Kong HQ	Kong Gateway	✓	Nativ in Kong ACME.sh		
NodeJS	Python	✓	certbot		

Diese Liste ist nicht vollzählig. Wir fügen kontinuierlich Unterstützung für neue Anwendungen hinzu.
Kontaktieren Sie uns für die neuesten Informationen.

Über Sectigo

Sectigo ist ein führender Anbieter im Bereich des Zertifikatslebenszyklusmanagements (CLM) und bietet innovative und umfassende Lösungen zur Sicherung von Identitäten von Menschen und Maschinen für einige der weltweit bekanntesten Marken. Die cloudnative, automatisierte und universelle CLM-Plattform vereinfacht und verbessert die Unternehmenssicherheit durch die Ausstellung und Verwaltung digitaler Zertifikate aller vertrauenswürdigen Zertifizierungsstellen (CAs). Mit über zwei Jahrzehnten Erfahrung zählt Sectigo zu den größten und etabliertesten Zertifizierungsstellen und betreut weltweit mehr als 700.000 Kunden.

Durch die Schaffung von beispiellosem digitalem Vertrauen ermöglicht Sectigo Unternehmen weiterhin, robuste Sicherheitsprotokolle effizient und sicher umzusetzen.

