

L'automatisation par Sectigo

Le chiffrement à clé publique (PKI) est la référence absolue en matière de confidentialité, d'identité et de sécurité numériques. Il devrait incontestablement constituer le socle de sécurité de chaque appareil, serveur, utilisateur et application de l'entreprise. Cependant, l'utilisation de processus manuels pour installer, surveiller et renouveler l'ensemble des certificats PKI désormais requis demande une main-d'œuvre importante, s'avère techniquement exigeante et comporte des risques. De plus, les coûts peuvent rapidement s'accumuler. Une installation manuelle minimale de certificat TLS/SSL (un seul serveur web et une seule instance de domaine) implique plusieurs étapes et peut facilement atteindre 50 \$ à 100 \$ par serveur web.

En outre, le secteur évolue vers des durées de vie de certificats plus courtes — d'abord de trois ans à deux ans, puis de deux ans à un an. Avec la réduction à venir de la durée de vie des certificats TLS/SSL, les coûts d'installation et de gestion devraient augmenter. Et le moment ne pourrait pas être pire. Alors que de plus en plus d'entreprises étendent leur utilisation des appareils mobiles, de l'Internet des objets (IoT), du DevOps et d'autres environnements numériques, le besoin de PKI s'accroît, tout comme l'urgence de pouvoir émettre, révoquer et remplacer des certificats rapidement, de manière fiable et à l'échelle de l'entreprise.

Automatiser l'installation des certificats TLS/SSL

Toute évidence montre que l'automatisation est désormais essentielle à tout système de gestion des certificats. Non seulement elle réduit le coût global de possession, mais elle applique également la conformité cryptographique et prévient les interruptions de service potentielles causées par l'erreur humaine.

Cependant, compte tenu de la diversité des systèmes, applications et appareils qui utilisent des certificats numériques et s'y intègrent, une approche unique a peu de chances de répondre aux besoins d'automatisation des différents cas d'usage. C'est pourquoi Sectigo propose plusieurs options d'automatisation distinctes.

Pour l'installation de certificats TLS/SSL, Sectigo fournit :

- **Prise en charge du protocole ACME (Automated Certificate Management Environment) :**

Sectigo Certificate Manager prend en charge ACME, vous permettant d'automatiser l'émission et l'installation de certificats pour une large gamme de serveurs web, répartiteurs de charge, routeurs, pare-feu et autres équipements réseau. Sectigo prend en charge les types de certificats DV, OV et EV via ACME et offre un contrôle total aux administrateurs IT. De nombreux outils DevOps prennent en charge ACME pour inscrire et gérer les certificats, et une myriade d'outils open source sont disponibles à cet effet. Ces outils sont populaires auprès des administrateurs informatiques et bénéficient fréquemment d'améliorations fonctionnelles.

Si Sectigo implémente le côté serveur ou Autorité de Certification de la norme ACME, cela fonctionnera avec les clients compatibles ACME, et nous soutiendrons tout projet client nécessitant cette intégration (ce qui exige que le client soit compatible ACME). Voir le tableau ci-dessous pour la liste des plateformes actuellement prises en charge.

- **Agent d'automatisation Sectigo :**

Grâce à l'agent réseau de Sectigo (Network Agent), vous pouvez automatiser la gestion des certificats pour une variété de systèmes, notamment Apache, Apache Tomcat, Windows IIS et les répartiteurs de charge F5 BIG-IP. L'agent réseau installé sur site chez le client est intégré à la solution cloud Sectigo Certificate Manager pour planifier l'émission, l'installation et le renouvellement des certificats.

- **API REST :**

Dans certains cas, les entreprises préfèrent intégrer leurs applications de manière plus étroite avec Sectigo, ce qui est possible grâce à l'API REST de Sectigo. Bien que cela nécessite un développement supplémentaire du côté de l'application, cela vous permet d'exploiter la gestion des certificats et de personnaliser vos flux de travail.

- **Intégration avec des éditeurs tiers :**

Sectigo cherche continuellement des occasions de s'intégrer avec des éditeurs tiers pour aider ses clients à atteindre une automatisation complète. Par exemple, le répartiteur de charge BIG-IP de F5 propose une intégration depuis son système de gestion pour automatiser la gestion des certificats Sectigo.

Automatiser la validation du contrôle de domaine (DCV)

Avec le raccourcissement de la durée de vie des certificats, le maintien des domaines validés est devenu une exigence continue. Les processus de validation manuels prennent du temps, sont sources d'erreurs et ne sont pas viables à grande échelle. Sectigo Certificate Manager simplifie ce processus grâce à la validation automatisée du contrôle de domaine (DCV) intégrée, qui fait partie de ses capacités plus larges d'automatisation du cycle de vie des certificats. En s'appuyant sur des connecteurs DNS, SCM s'intègre directement aux fournisseurs DNS pris en charge pour créer et valider automatiquement les défis d'enregistrement CNAME. Cela élimine l'intervention manuelle, réduit le risque d'échec des renouvellements et garantit que les domaines restent validés en permanence.

SCM continue d'élargir sa liste de fournisseurs DNS pris en charge, incluant désormais :

Cloudflare

Amazon Route 53

Azure DNS

GoDaddy DNS

Akamai Edge DNS

DNSimple

OVHcloud

Consultez la liste complète des fournisseurs DNS pris en charge par SCM [ici](#).

Automatiser l'installation des certificats clients et appareils

De nombreux systèmes, applications et appareils utilisent des certificats non-SSL. Pour l'installation de certificats non-SSL, Sectigo propose :

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

Sectigo prend en charge le protocole EST, utilisé pour gérer les équipements réseau de nombreux éditeurs. Plusieurs fournisseurs intègrent déjà la prise en charge d'EST de nativement. EST est également populaire dans les environnements d'Internet des objets (IoT) en raison de l'efficacité du protocole et de la prise en charge des clés à cryptographie sur courbes elliptiques (ECC). Plusieurs clients EST open source sont également disponibles. Sectigo Certificate Manager affiche et gère les certificats émis.

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

Dans l'environnement Sectigo, SCEP peut être utilisé pour inscrire des certificats sous Linux, macOS et d'autres systèmes d'exploitation. Les appareils mobiles, le serveur NDES de Microsoft et les solutions MDM utilisent généralement SCEP.

- **Agent d'automatisation Sectigo MS :**

Un agent MS Sectigo positionné entre Active Directory Certificate Services de Microsoft et Sectigo Certificate Manager. Il écoute les demandes de certificats via le protocole WCCE (Windows Client Certificate Enrollment) et fournit automatiquement le certificat au poste de travail sans aucune intervention de l'employé.

Comme vous pouvez le constater, Sectigo propose une variété d'options d'installation de certificats, ainsi que la commodité et la sécurité d'une solution fluide offrant un panneau de contrôle unique pour l'émission et la gestion de certificats publics et privés. De plus, avec Sectigo, vous ne vous heurterez jamais à une limite de volume de certificats, comme cela pourrait être le cas avec des alternatives open source. Sectigo permet à votre équipe de sécurité de faire respecter facilement la politique de sécurité cryptographique, de protéger les communications, de prévenir la perte de données due à des accès non autorisés et d'assurer la pérennité des systèmes, applications et appareils dans toute l'entreprise.



Automatisation TLS/SSL avec SCM :

Clients ACME et intégrations natives

Réseau de diffusion de contenu (CDN)

Fournisseur	Application	Prise en charge native ACME	Client ACME utilisé	Intégration conçue par Sectigo (prête à l'emploi)	Technologie d'intégration Sectigo
Akamai	Terraform			Connecteur Sectigo pour Akamai Terraform	API REST
Akamai	CLI			Connecteur Sectigo pour Akamai CLI	API REST

Containerisation

Fournisseur	Application	Prise en charge native ACME	Client ACME utilisé	Intégration conçue par Sectigo (prête à l'emploi)	Technologie d'intégration Sectigo
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		

Outils DevOps

Fournisseur	Application	Prise en charge native ACME	Client ACME utilisé	Intégration conçue par Sectigo (prête à l'emploi)	Technologie d'intégration Sectigo
Ansible	Ansible	✓	Ansible ACME	Sectigo Ansible Integration	API REST
Chef	Chef			Sectigo Chef Integration	API REST
HashiCorp	Terraform	✓	Vancluever	Sectigo Terraform Integration	API REST
Jenkins	Jenkins			Sectigo Jenkins Integration	API REST
Jetstack	Jetstack	✓	jetstack (cert-manager)		
Puppet				Sectigo Puppet Integration	API REST
SaltStack				Sectigo SaltStack Integration	API REST



Serveurs Web / Répartiteurs de charge / Pare-feu

Fournisseur	Application	Prise en charge native ACME	Client ACME utilisé	Intégration conçue par Sectigo (prête à l'emploi)	Technologie d'intégration Sectigo
A10	Thunder ADC	✓	Intégré à A10	Connecteur Sectigo pour A10	API REST
Amazon	AWS Certificate Manager			Connecteur Sectigo pour AWS	ACME
Apache	Apache	✓	Certbot mod_md	Agent réseau	Agent réseau / API REST
Cisco	Cisco FTD			Connecteur Sectigo pour Cisco FTD	API REST
Citrix	ADC			Connecteur Citrix pour Citrix	API REST
Citrix	Gateway			Connecteur Citrix pour Citrix	API REST
Citrix	FAS			Agent MS	API
F5	BIG-IP	✓	Kojot ACME	Connecteur Sectigo pour F5 BIG-IP	ACME
F5	NGINX	✓	Certbot ACME.sh	Agent réseau	Agent réseau / API REST
Google	Google Load Balancer			Connecteur Sectigo pour GCP	ACME
HAProxy	HAProxy	✓	Certbot ACME.sh	Connecteur Sectigo HAProxy	ACME
Kemp	LoadMaster	✓	ACME.sh	Connecteur Sectigo Kemp	API REST
Microsoft	IIS	✓	Win-ACME posh ACME Certify the Web	Connecteur Sectigo Kemp	API REST
PaloAlto	PAN OS	✓	ACME.sh		
VMWare	Avi Vantage			Connecteur Sectigo pour Avi Vantage	API REST

Coffre-fort de clés (Key Vault)

Fournisseur	Application	Prise en charge native ACME	Client ACME utilisé	Intégration conçue par Sectigo (prête à l'emploi)	Technologie d'intégration Sectigo
Hashicorp	HashiCorp Vault			Intégration Sectigo HashiCorp Vault	API REST
Microsoft	Azure Key Vault	✓	az-acme	SCM PK Agent	API

Langages de programmation

Fournisseur	Application	Prise en charge native ACME	Client ACME utilisé	Intégration conçue par Sectigo (prête à l'emploi)	Technologie d'intégration Sectigo
Golang	Golang	✓	Lets Encrypt Go		
Java	Java	✓	ACME4j	Connecteur Sectigo pour Java	API REST
Python	Python	✓	certbot		
Ruby	Ruby	✓	acme-client		



Autres

Fournisseur	Application	Prise en charge native ACME	Client ACME utilisé	Intégration conçue par Sectigo (prête à l'emploi)	Technologie d'intégration Sectigo
BeyondTrust	BeyondTrust	✓	Native Beyond Trust		
Kong HQ	Kong Gateway	✓	Natif dans Kong ACME.sh		
NodeJS	Python	✓	certbot		

Cette liste n'est pas exhaustive. Nous ajoutons continuellement la prise en charge de nouvelles applications.
Contactez-nous pour obtenir les dernières informations.

À propos de Sectigo

Sectigo est un leader dans la gestion du cycle de vie des certificats (CLM) ; l'entreprise propose des solutions innovantes et complètes pour sécuriser les identités humaines et machines de certaines des marques les plus prestigieuses au monde. Sa plateforme CLM native du cloud, automatisée et universelle simplifie et renforce la sécurité des entreprises en émettant et en gérant des certificats numériques provenant de toutes les autorités de certification (CA) de confiance. Forte de plus de deux décennies d'expérience, Sectigo s'impose comme l'une des autorités de certification les plus importantes et les mieux établies, au service de plus de 700 000 clients à travers le monde.

En offrant une confiance numérique inégalée, Sectigo continue de permettre aux organisations de mettre en œuvre des protocoles de sécurité robustes avec efficacité et confiance.

