Sectigo automation

Public-Key Encryption (PKI) is the gold standard in digital privacy, identity, and security, and should unquestionably be the security foundation for every device, server, user, and application in the enterprise. But using manual processes to install, monitor, and renew all the PKI certificates now required is labor intensive, technically demanding, and risky. Plus, the costs can add up quickly. A minimal manual TLS/SSL certificate installation (single webserver and domain instance) involves multiple steps and can easily add up to $50 to $100 per web server.

On top of that, the industry is moving toward shorter certificate lifetimes—first from three years to two, and then from two years to one. With the upcoming shift to shortening TLS/SSL certificate lifespan, installation and management costs are expected to rise. And the timing couldn't be worse. As more and more companies expand their use of mobile devices, the Internet of Things (IoT), DevOps, and other digital environments, the need for PKI is escalating, as is the urgency around being able to issue, revoke, and replace certificates quickly, reliably, and at enterprise scale.

Automating TLS/SSL certificate installation

Clearly, automation is now critical to any certificate management system. Not only does it reduce the overall cost of ownership; but automation also enforces cryptographic compliance and prevents potential service disruptions caused by human error.

However, given the disparate systems, applications, and devices that use and integrate with digital certificates, a one-size-fits-all approach is unlikely to address the automation needs of various use cases. That's why Sectigo offers several different automation options.

For TLS/SSL Certificate Installation, Sectigo provides:

- **Support for Automated Certificate Management Environment (ACME) protocol:** Sectigo Certificate Manager supports ACME, allowing you to automate certificate issuance and installation for a wide range of web servers, load balancers, routers, firewalls, and other networking gear. Sectigo supports DV, OV, and EV certificate types via ACME and provides full control to IT administrators. Many DevOps tools support ACME to enroll and manage certificates, and a myriad of open source tools are available for this purpose. These tools are popular among IT administrators and are being feature enhanced on a frequent basis.

  If Sectigo implements the server or Certificate Authority side of the ACME protocol standard, it will work with ACME-compliant clients, and we will support any customer project which requires that integration. Of course, that requires the client to be ACME-compliant. See the table below for a list of currently supported platforms.

- **A Sectigo Automation Agent:** Using Sectigo's Network Agent, you can automate management of certificates for a variety of systems, including Apache, Apache Tomcat, Windows IIS, and F5 Big-IP load balancers. The Network Agent that lives in the customer premise is integrated with Sectigo Certificate Manager cloud solution for scheduling issuance, installation, and renewal of certificates.

- **REST API:** In some instances, companies prefer to integrate applications more tightly with Sectigo, which is possible using Sectigo's REST API. While this requires additional development on the application side, it allows you to leverage certificate management and customize your work flow.

- **Integration with third party vendors:** Sectigo is continuously looking for opportunities to integrate with third party vendors to help customers achieve full automation. For instance, F5's Big-IP load balancer provides integration from its management system to automate certificate management from Sectigo.

Automating Domain Control Validation (DCV)

With the shortening of certificate lifespans, maintaining validated domains has become a continuous requirement. Manual validation processes are time-consuming, error-prone, and unsustainable at scale.

Sectigo Certificate Manager streamlines this process with built-in automated Domain Control Validation (DCV) as part of its broader certificate lifecycle automation capabilities. By leveraging DNS connectors, SCM integrates directly with supported DNS providers to automatically create and validate CNAME record challenges. This eliminates manual intervention, reduces the risk of failed renewals, and ensures domains remain continuously validated.

SCM continues to grow its list of supported DNS providers, now including:

Cloudflare | Amazon Route 53 | Azure DNS | GoDaddy DNS

Akamai Edge DNS | DNSimple | OVHcloud

View the full list of SCM supported DNS providers here.

Automating client and device certificate installation

Many sytems, applications, and devices utilize non-SSL certificates. For non-SSL Certificate Installation, Sectigo provides:

- **Enrollment over Secure Transport (EST) protocol:** Sectigo supports the EST protocol which is used for managing networking gear from many vendors. In fact, a number of vendors have EST support already built in. EST is also popular in Internet of Things (IoT) environments given the efficiency of the protocol and support of Elliptic Curve Cryptography (ECC) keys. There are several open source EST clients available as well. Sectigo Certificate Manager displays and manages the certificates issued.

- **Simple Certificate Enrollment Protocol (SCEP):** In the Sectigo environment, SCEP can be used to enroll certificates in Linux, MacOS, and other operation systems. Mobile devices, Microsoft's NDES server, and MDMs typically use SCEP.

- **Sectigo Automation Agent:** A Sectigo MS Agent that sits between the Microsoft Active Directory Certificate Service and Sectigo Certificate Manager. It listens to certificate requests over the Windows Client Certificate Enrollment Protocol (WCCE) and automatically provides the certificate to the desktop without any employee intervention.

As you can see, Sectigo offers a variety of certificate installation options, as well as the convenience and security of a seamless solution with one pane of glass for both public and private certificate issuance and management. Moreover, with Sectigo, you will never run into a certificate volume cap, as you might with open source alternatives. Sectigo enables your security team to easily enforce cryptographic security policy; protect communications; prevent data loss via unauthorized access; and future-proof systems, applications, and devices across the enterprise.

TLS/SSL automation with SCM:
ACME clients and native integrations

Content Delivery Network (CDN)

Vendor	Application	Native ACME Support	ACME Client Used	Sectigo-Built Integration (Out-of-the-box)	Sectigo Integration Technology
Akamai	Terraform			Sectigo Connector for Akamai Terraform	REST API
Akamai	CLI			Sectigo Connector for Akamai CLI	REST API

Containerization

Vendor	Application	Native ACME Support	ACME Client Used	Sectigo-Built Integration (Out-of-the-box)	Sectigo Integration Technology
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

Vendor	Application	Native ACME Support	ACME Client Used	Sectigo-Built Integration (Out-of-the-box)	Sectigo Integration Technology
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

Web Servers / Load Balancers / Firewalls

Vendor	Application	Native ACME Support	ACME Client Used	Sectigo-Built Integration (Out-of-the-box)	Sectigo Integration Technology
A10	Thunder ADC	✓	Built into A10	Sectigo Connector for A10	REST API
Amazon	AWS Certificate Manager			Sectigo Connector for AWS	ACME
Apache	Apache	✓	Certbot mod_md	Network Agent	Network Agent / REST API
Cisco	Cisco FTD			Sectigo Connector for Cisco FTD	REST API
Citrix	ADC			Citrix Connector for Citrix	REST API
Citrix	Gateway			Citrix Connector for Citrix	REST API
Citrix	FAS			MS Agent	APIs
F5	BIG-IP	✓	Kojot ACME	Sectigo Connector for F5 BIG IP Network Agent	ACME Network Agent / REST API
F5	NGINX	✓	Certbot ACME.sh		
Google	Google Load Balancer			Sectigo Connector for GCP	ACME
HAProxy	HAProxy	✓	Certbot ACME.sh	Sectigo HA Proxy 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 for Avi Vantage	REST API

Key Vault

Vendor	Application	Native ACME Support	ACME Client Used	Sectigo-Built Integration (Out-of-the-box)	Sectigo Integration Technology
Hashicorp	HashiCorp Vault			Sectigo HashiCorp Vault Integration	REST API
Microsoft	Azure Key Vault	✓	az-acme	SCM PK Agent	APIs

Programming Language

Vendor	Application	Native ACME Support	ACME Client Used	Sectigo-Built Integration (Out-of-the-box)	Sectigo Integration Technology
Golang	Golang	✓	Lets Encrypt Go	Sectigo Connector for Java	REST API
Java	Java	✓	ACME4j		
Python	Python	✓	certbot		
Ruby	Ruby	✓	acme-client		

Other

Vendor	Application	Native ACME Support	ACME Client Used	Sectigo-Built Integration (Out-of-the-box)	Sectigo Integration Technology
BeyondTrust	BeyondTrust	✓	Native Beyond Trust		
Kong HQ	Kong Gateway	✓	Native in Kong ACME.sh		
NodeJS	Python	✓	certbot		

This list is not exhaustive. We are continuously adding support for new applications.
Contact us for the latest information.

About Sectigo

Sectigo is the industry’s most innovative provider of comprehensive certificate lifecycle management (CLM), with automated solutions and digital certificates that secure every human and machine identity for the world’s largest brands. Its automated, cloud-native, universal CLM platform issues and manages digital certificates provided by all trusted certificate authorities (CAs) to simplify and improve security protocols across the enterprise. Sectigo is one of the longest-standing and largest CAs with more than 700,000 customers and two decades of delivering unparalleled digital trust. For more information, visit www.sectigo.com, follow us on LinkedIn, and subscribe to our Webby award-winning podcast, Root Causes.