Sectigo’s Automation Offering

Proprietary and Confidential
Sectigo is the only vendor to provide the customer all these options:

1. Automated Certificate Management Environment (ACME), an open standard, RFC8555
2. Sectigo customer premise agent
3. Sectigo open source integrations with all the popular DevOps tools
4. REST API for customer authored automation, with custom workflow
5. Azure Key Vault
6. ServiceNow integration

For Public & Private Web Servers & Load Balancers
Automated SSL installation via ACME

Current State
- Excessive cost to purchase multiple tools
- Excessive cost to integrate different tools
- Slow certificate replacement in the event of an immediate threat

Sectigo Value
- A. Single Pane of Glass for all identity management
- B. Automated certificate creation and installation
- C. ACME client collocated with web server or load balancer
  - ACME is an industry standard between Certificate Authorities and applications using SSL (RFC8555)
- D. Web Servers (Apache) are building ACME into their product. It is the future.
Sectigo Value Add to ACME

Made it enterprise-grade by binding to Sectigo Certificate Manager (SCM) Account
  ✓ Provides admin control
  ✓ Protects from unauthorized use

Incorporated customer workflows

Integrated reporting capability via SCM to provide visibility

Able to discover ACME issued certs in the enterprise environment via SCM

Supports DV, OV, EV SSL certificates
  ✓ Some implementations offer DV only; some, OV/EV only

Supports DevOps tools/processes as well
  ✓ Supports Kubernetes cert-manager
Supported ACME Tools

A. Certbot
   ✓ Widely used

B. Lego

C. ACME4j
   ✓ For JAVA environment

D. Cert-manager
   ✓ For DevOps Kubernetes environment

E. Sectigo Citrix ACME Integration
Automatic Issuance via ACME Client Certbot

Precondition:
SCM Admin provides the ACME credentials

1. Install Certbot (once)
2. Register (once)

1. Install Certbot (once)
2. Register (once)
3. Issue cert

Enterprise

Apache Web Server

Certbot (ACME client)

3a. Request cert
3b. Install cert

Administrator

Sectigo Secure Cloud

Sectigo Certificate Manager
EST
ACME
SCEP
REST API

Sectigo Public CA
Citrix ADC (Netscaler) Solution with ACME

2a. Obtain certificate
2b. Install certificate

Precondition: SCM Admin provides the ACME credentials
Appendix: Additional Automation

Proprietary and Confidential
Automated SSL installation - AGENT

Current State
- Excessive cost to purchase multiple tools
- Excessive cost to integrate different tools
- Slow certificate replacement in the event of an immediate threat

Sectigo Value
- A. Single Pane of Glass for all identity management
- B. Automated certificate creation and installation
- C. Agent manages several web servers, load balancers, migrates private keys across multi-domain/wild card certs
- D. Supported: Apache – IIS – Tomcat – F5
Automated SSL Approvals Workflow – ServiceNow

**Current State**

Enterprise policy requires sophisticated approvals process, in common corporate tool, ServiceNow

Lack of management and slow approvals leads to certificate expiry

Slow certificate replacement in the event of a threat

**Sectigo Value**

A. Single Pane of Glass for all identity management

B. Automated certificate creation

C. Employee initiates change, executes workflow, obtains approvals, certificate issued

D. Only vendor that allows for all reporting and management from ServiceNow UI
Automated SSL installation – DEVOPS Automation Tools

Current State
- Excessive cost to purchase multiple tools
- Excessive cost to integrate different tools
- Slow certificate replacement in the event of a threat
- DevSecOps team cannot enforce compliance without slowing the pipeline
- Requirement to setup the webserver or load balancer, including SSL
- Free SSL rate limit impacts enterprise

Sectigo Value
- A. Single Pane of Glass for all identity management
- B. Automated certificate creation and installation
- C. Out of the box DevOps automation tool integrations: Ansible – Chef – Puppet - Jenkins/Saltstack – HashiCorp Vault
Automated SSL installation – DEVOPS Orchestration Tools

Current State
- Excessive cost to purchase multiple tools
- Excessive cost to integrate different tools
- Slow certificate replacement in the event of a threat
- DevSecOps team cannot enforce compliance without slowing the pipeline
- Requirement to provision certificates into containers for SSL and inter-container TLS across cloud platforms
- Free SSL rate limit impacts enterprise

Sectigo Value
- A. Single Pane of Glass for all identity management
- B. Automated certificate creation and installation
- C. Out of the box DevOps Orchestration tool integrations:
  - Docker – Kubernetes - Istio/Citadel – Terraform
Automated SSL installation – Azure Key Vault

**Current State**
- Manual, expensive process to provision keys and certs to Azure Key Vault
- Lack of management leads to certificate expiry
- Slow certificate replacement in the event of a threat
- Requirement to provision certificates into key vaults which span cloud providers

**Sectigo Value**

A. Single Pane of Glass for all identity management
B. Automated certificate creation and installation
C. Web Servers, load balancers or applications do not need to embed certificate renewal logic
D. Amazon and Google are on the roadmap
E. Same platform for other enterprise applications (document signing, encryption)