Sectigo Adds ACME Protocol Support in Certificate Manager Platform to Automate SSL Lifecycle Management

Submitted by: Sectigo
Thursday, 4 April 2019

Limits Human Error and Website Outages While Enabling Enterprises to Configure Automation Workflow

ROSELAND, N.J – April 4, 2019 – Despite enterprises' increasing use of modern, agile computing environments including virtualization, containerization, Internet of Things (IoT), and cloud, a vast number of IT administrators continue to deploy and manage certificates using old-fashioned techniques better suited to the infrastructure of the 90s than today's DevOps environments. This "management by spreadsheet" introduces inefficiency and risk of outage or non-compliance due to human error. To address the problem, Sectigo (https://sectigo.com/) (formerly Comodo CA), the world's largest commercial Certificate Authority and a leader in web security solutions, today announced support for the ACME protocol in its popular Sectigo Certificate Manager (https://sectigo.com/products/management-solutions/sectigo-certificate-manager) platform. By adding ACME support, Sectigo brings the reliability and efficiency of automation to enterprise certificate management.

"Any organization managing certificates manually across hundreds of web servers is at huge risk of unexpected certificate expiration and the resulting system failures that can cripple a business for a period of time," said Lindsay Kent, VP of Product Management, Sectigo.

Lowering the TCO of Certificate Management

A single-server SSL Certificate installation requires up to nine time-intensive steps including login, download, renewal configuration, and testing, and costs an estimated $50 to $100 per web for each installation or renewal. Plus, complexity and cost only increase for web servers using multiple domains, wildcard certificates, reverse proxies, or load balancers.

Each step requires precise management by a web administrator or employee with technical skills to avoid the risk of human error and unexpected outages, which can be quite costly. For example, mobile operator O2 sought millions in damages (https://www.bbc.com/news/business-46499366) from Ericsson following the loss of service for 32 million of its customers, along with those of other carriers around the globe. The day-long network data collapse in December 2018 owed itself to an expired certificate in the Ericsson technology stack servicing these carriers.

"Manually installing SSL certificates requires specialized skills, without which the enterprise risks misconfiguration, lack of visibility into installed certificates, and the inability to rapidly replace certificates due to unplanned events. A web administrator who is more skilled with HTML coding and web site building, and less experienced in Linux shell, may have significant difficulty performing the necessary steps, or may spend a great deal of time learning," added Kent.

Four Ways to Automate While Maintaining Control

Advancements in the Sectigo Certificate Manager platform address these enterprise-scale challenges by

providing mechanisms to automate installation and renewal of SSL certificates to servers within the traditional data center or in a DevOps environment — fully automating both deployment and ongoing management. This ACME support applies to Extended Validation (EV), Organization Validation (OV), and Domain Validation (DV) SSL certificates.

Industry-standard ACME protocol – Developed by the IETF, Automated Certificate Management Environment (ACME) defines an extensible framework for automating issuance and validation procedures for certificates, enabling servers to obtain DV, OV, and EV SSL certificates without manual user interaction. More than 100 open-source ACME clients are available to automate certificate issuance on Apache, IIS, NGINX, F5 BIG-IP, Citrix Netscaler, and other popular web servers and networking gear. The ACME tools fully automate key generation, domain control validation, certificate creation, and installation on the server. Where public certificates are needed, the client can request them directly from Sectigo.

Proprietary automated method – For Apache, IIS, Tomcat, and F5 BIG-IP environments, Sectigo provides a client for installation in one location at the customer premise that can then communicate with all the enterprise's servers. Sectigo Certificate Manager embeds the web server administrator credentials into this agent for installation of certificates and private key propagation.

Custom workflows with REST API – Customers may use Sectigo's RESTful (https://www.smashingmagazine.com/2018/01/understanding-using-rest-api/) (Representational State Transfer) API to install certificates, allowing for a customized workflow, including approvals and other steps. The administrator can require approval for certificate requests originating from the ACME client and can discover, track, run reports on, and make manual changes to certificates.

Tighter integration with third-party products - Sectigo has integrated with F5 BIG-IP and is working on additional third-party integrations to deliver full automation and workflow management.

To learn more, watch the Sectigo ACME Automation Video (https://sectigo.com/resources/sectigos-acme-automation).

About Sectigo

Sectigo (https://sectigo.com/) (formerly Comodo CA) provides web security products that help customers protect, monitor, recover, and manage their web presence and connected devices. As the largest commercial Certificate Authority trusted by enterprises globally for more than 20 years, and more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape. Follow Sectigo on LinkedIn (https://www.linkedin.com/company/sectigo/) or Twitter @SectigoHQ (https://twitter.com/SectigoHQ).

###

Contact
Elliot Harrison
eharrison@positivemarketing.com
020 3637 0640