DATASHEET

Sectigo Certificate Integration for Apache Using ACME

Sectigo has collaborated with Apache to embed the ACME (Automated Certificate Management Environment) protocol for all Apache web servers. This new integration means that ACME can now be used to automatically deploy certificates to Apache servers and load balancers both inside and outside business firewalls.

Eliminate Labor Costs and Security Risks of Manual Certificate Management

Apache is a free and open-source webserver platform that is used to run almost half of internet websites globally. This powerful new integration between Sectigo and Apache is driven by the need to automate the deployment and renewal of digital certificates at scale.

The mismanagement of digital certificates has become a leading cause of downtime and data breaches. Due to the drastic increase in devices and users accessing business networks remotely in recent years, managing digital certificates manually is now considered a significant security risk.

Additionally, digital certificates that use public key infrastructure (PKI) have come under increased scrutiny. New standards established by the CA/Browser Forum require all public certificates to have a lifespan no longer than 397 days. These requirements apply to websites, public-facing applications and services.

What Is ACME?

ACME is an industry-standard protocol used for the deployment and management of digital certificates to servers and web infrastructure. The use of ACME enables automation of certificate deployment, greatly reducing dependencies on manual processes and eliminating human error.

Certificate management platforms were previously unable to automate the installation of certificates to Apache webservers using ACME because External Account Binding (EAB) was not available between the Certificate Authority and the web server/load balancer without installing additional software. The platform could be notified of a certificate having been installed, enabling it to be monitored, but it was not possible to natively automate the installation process.

Some Certificate Lifecycle Management (CLM) platform vendors offer solutions based on custom agents, but these require embedded credentials, introducing security risks and administration headaches.

Sectigo Provides Full Certificate Lifecycle Management for Apache Web Servers and Load Balancers

In a new approach, Sectigo has partnered with Apache to implement the ACME protocol directly within the Apache platform, so there is no longer a requirement to install a custom software agent at the customer premise. This also removes the need to configure and manage passwords for server access, resulting in reduced risk and significantly reduced costs. ACME is an open standard, so the enterprise is not locked into a proprietary agent implementation.

ACME provides considerable benefits in the automation of certificate deployment. By partnering with Apache to implement ACME, Sectigo leads the industry in implementation and is the preferred CLM vendor for websites built on Apache.

The module supporting the ACME protocol is compatible with Apache version 2.4.48 and later. For more information on Sectigo's Apache support, SSL/TLS certificates or certificate management in general please contact Sectigo Sales at sales@sectigo.com

About Sectigo

Sectigo is a leading provider of digital certificates and automated certificate lifecycle management solutions to leading brands globally. As one of the longest-standing and largest Certificate Authorities (CA), Sectigo has over 20 years of experience delivering innovative security solutions to over 700,000 businesses worldwide. Sectigo is the leading certificate lifecycle management provider supporting multiple CA vendors and integrating with the largest software ecosystems in the world.

SECTIGO®