Sectigo PKI Enterprise Use Case: Web Servers

Effectively implementing PKI on web servers requires overcoming significant challenges. To help ensure the highest standard of web server authentication and identity, your security team needs:

- ✓ Volume availability of SSL certificates on an as-needed basis
- ✓ An enterprise SSL certificate management platform

With Sectigo, SSL certificates are available on demand and in whatever volume you need. That means no more struggling to get a certificate when you're on a deadline. Sectigo offers DV, OV, EV, single-domain, wildcard, and multi-domain certificates. You can purchase a pool of SSL certificates to take advantage of Sectigo's volume pricing and then issue certificates from this pool whenever you want, without having to order and go through authentication for each one.

Sectigo Certificate Manager

In addition, Sectigo offers Sectigo Certificate Manager, a complete management platform that automates end-to-end lifecycle management of SSL certificates at scale. It supports all SSL certificate types along with other popular certificates (including S/MIME, code signing, and Private CA) and is interoperable with all leading devices, operating systems, protocols, and chipsets. Sectigo Certificate Manager provides visibility and management through a single pane of glass, enabling security administrators to easily and cost-effectively monitor certificates across the enterprise. And Sectigo can support whatever trust model you use, including public certificates from Sectigo or certificates issued from your own internal PKI.

Leveraging Sectigo Certificate Manager for web servers will enable your security team to benefit from:

- **Automated certificate deployment**
  Sectigo offers a variety of automation options to fit your specific workflow and environment, including automation standards like SCEP (Simple Certificate Enrollment Protocol) and EST (Enrollment over Secure Transport), as well as Sectigo's Microsoft CA proxy agent.

- **Certificate discovery**
  Sectigo's Certificate Discovery Tool allows you to scan for certificates deployed across all your IP addresses so that you can avoid vulnerabilities and outages caused by outlier, misconfigured, or expired certificates. The scan will find public-facing certificates and internal certificates, regardless of the issuing certificate authority.

- **Full certificate lifecycle management**
  This automation speeds and simplifies the renewal, revocation, and replacement of all certificate types, including SSL, TLS, S/MIME, Code Signing, and Private CA.

- **Enhanced visibility and reporting**
  With Sectigo Certificate Manager, you can view the status of all SSL certificates in use through a single pane of glass, including expiration dates to prevent certificate-based service disruptions.

With Sectigo, you can protect your web servers, enforce cryptographic security, maintain regulatory compliance, and futureproof your business while minimizing costs. And Sectigo Certificate Manager can be used to automate issuance and lifecycle management of all other certificates throughout your organization, across a wide variety of use cases, ranging from code signing to device access and email.

About Sectigo

Sectigo is a cybersecurity technology leader providing digital identity solutions, including TLS/SSL certificates, web security, DevOps, IoT, and enterprise-grade PKI management. As the world's largest commercial Certificate Authority, with more than 700,000 customers worldwide and 20 years of experience delivering online trust solutions, Sectigo provides proven public and private trust solutions for securing web servers, digital identities, connected devices, and applications. Recognized for its award-winning innovations and best-in-class global customer support, Sectigo delivers the technologies required to secure the digital landscapes of today, as well as tomorrow. For more information, visit www.sectigo.com and follow @SectigoHQ.

SECTIGO

|