First Commercial Certificate Authority To Augment Microsoft CA, Sectigo Manages Private and Public Certificates in a Single Platform

Submitted by: Sectigo
Thursday, 20 June 2019

Enterprise Private PKI Service Enables Issuance and Management of Digital Identities for DevOps, Mobile/BYOD, Email, Multi-Cloud, IoT, and Other Uses

ROSELAND, N.J. – June 20, 2019 – Sectigo (https://sectigo.com/) (formerly Comodo CA), the world's largest commercial Certificate Authority and a provider of purpose-built and automated PKI management solutions, today announced its Private PKI service for issuance and management of SSL certificates, private PKI, and identity certificates for users, servers, devices, and applications. Sectigo Private PKI (https://sectigo.com/enterprise/sectigo-certificate-manager/enterprise-private-pki) enables enterprises to augment or replace their Microsoft Active Directory Services (Microsoft CA) by managing non-Microsoft devices and applications, including mobile, Internet of Things (IoT), email, cloud, and DevOps, all in a single platform—making it the most flexible solution offered by a commercial Certificate Authority.

Private PKI (Public Key Infrastructure) is an enterprise-branded Certificate Authority (CA) that functions like a publicly trusted CA but runs exclusively for a single enterprise. Sectigo provides private roots and subordinates capable of issuing end-entity certificates to internal applications. Certificates issued from a private CA are trusted only within the controlled environments of the enterprise's infrastructure, partners, and customers. The Private PKI solution utilizes an existing Microsoft CA as a root to Sectigo, eliminating the need to provision a new root certificate.

"With the explosion of applications managed outside the Microsoft stack, Microsoft Active Directory Certificate Service no longer addresses all critical use cases. Sectigo Private PKI delivers a managed PKI solution to alleviate problems associated with establishing and managing internal PKI," explained Lindsay Kent, VP of Product Management, Sectigo.

Augmenting Microsoft CA for Today's Complex Environments

Sectigo Private PKI is a capability of Sectigo Certificate Manager (https://sectigo.com/products/management-solutions/sectigo-certificate-manager), a platform that enables enterprises to productively manage private certificates and adhere to corporate and industry compliance standards. This control center automatically delivers certificates across the enterprise through industry-standard enrollment protocols. Administrators can discover previously issued certificates and then issue, view, and manage all certificates from a single platform—avoiding the risks, errors, or hidden costs associated with manual installation and renewal.

Microsoft's automatic certificate management allows IT administrators to instruct desktops and servers to enroll and renew certificates without employee involvement. However, today's enterprise has myriad applications that reside outside any Microsoft operating system, leaving administrators and employees to manually track, enroll, and renew certificates and keys. Through enrollment protocols such as SCEP, EST, ACME (https://datatracker.ietf.org/wg/acme/about/), and REST API, Sectigo Certificate Manager can provision certificates for all enterprise environments.

“With Sectigo Private PKI, you can connect to the network or the Microsoft agent and the software automatically discovers all certificates, so that you can manage all of your certificates from a single dashboard,” said Bryan Seely, Senior Systems Engineer, IT Security, Lighthouse Global (https://sectigo.com/resources/lighthouse-global-case-study).

Private PKI Scales for DevOps

DevOps environments require high certificate volumes for the just-in-time needs of many computing processes that may live for just hours or minutes. Whether using self-signed CAs on Kubernetes clusters, issuing SSL/TLS certificates into Docker containers, or automating installation of public SSL certificates, today’s enterprises benefit from Sectigo’s ability to host secure offline roots for customer-premise subordinates embedded into DevOps tools.

Because of the difficulty of setting up a private CA, many enterprises turn to free public certificates, only to run up against unworkably low certificate volume caps. In response, companies are increasingly using Sectigo Certificate Manager in conjunction with ACME to scale DevOps without such interference.

Digital Identity Management for All Enterprise Applications

Private PKI use cases extend well beyond DevOps. The service supports all necessary certificate types in a single SaaS application, providing strong digital identity across the enterprise with the assurance of best-of-breed PKI practices and security. Common use cases include:

Mobile/BYOD – Works with MDM vendors and on-device MDM capabilities to issue certificates across non-Windows devices running iOS and Android.
S/MIME for email – Industry-first Zero-Touch Deployment (https://sectigo.com/resources/sectigo-zero-touch-deployment-s-mime-solution) provisions the same S/MIME email certificate across multiple mobile and desktop devices without requiring user installation.
Multi-cloud computing – Trusted roots enable distribution among and repatriation between multiple cloud environments with full interoperability between workstreams.
IoT – High volume delivery and automated issuance, including supply chain provisioning and lifecycle operations, for deployed devices.
Windows login – Secure logins using Windows Virtual Smart Card or Windows Hello for Business.
Other – Sectigo Private PKI services can be used for networking gear, VPN access, WiFi access, client-side SSL authentication, and other use cases. For more information visit Sectigo’s Private PKI page (https://sectigo.com/enterprise/sectigo-certificate-manager/enterprise-private-pki).

About Sectigo
Sectigo (formerly Comodo CA) provides award-winning (https://sectigo.com/awards), purpose-built and automated PKI management solutions to secure websites, connected devices, applications, and digital identities. 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. For

more information, visit www.sectigo.com (http://www.sectigo.com/).
###

Elliot Harrison
Positive
+44 (0)20 3637 0649
eharrison@positivemarketing.com