Sectigo Integrates Microsoft Azure Key Vault with Certificate Manager Platform

Submitted by: Sectigo
Thursday, 30 January 2020

First CA to Enable Administrators to Manage Azure Application Keys, and Public SSL Keys from a Single Platform; Fully Automates the Certificate Renewal in Azure Key Vault

ROSELAND, N.J., – January 30, 2020 – Sectigo, the world's largest commercial Certificate Authority (CA) and a leading provider of automated PKI management solutions, has consolidated key storage and management for applications in Azure by integrating Microsoft Azure Key Vault with Sectigo Certificate Manager (https://sectigo.com/enterprise/sectigo-certificate-manager). The integration offers enterprises the industry's first one-stop issuance and management of keys from both publicly trusted and private CAs—and now key management for Microsoft Azure Key Vault—using a single platform.

Public IaaS and PaaS markets, led by Amazon Web Services and Microsoft Azure, doubled in size during the past two years and are forecast to double again by the end of 2023. Microsoft Azure, the fastest-growing platform in the public cloud services market (Synergy Research (https://www.business2community.com/cloud-computing/the-latest-public-cloud-market-share-and-beyond-02258898)), is a set of cloud services that provide organizations with the freedom to build, manage, and deploy applications on a massive, global network, using their preferred tools and frameworks. A critical part of the service, Azure Key Vault (https://azure.microsoft.com/en-us/services/key-vault/) safeguards cryptographic keys and other sensitive information, such as passwords, where the keys are stored in software or hardware security modules (HSMs) for the applications running in Azure Cloud

"As more enterprises use the Azure platform, they need a solution to automate the management of the publicly and privately trusted certificates required to provide authentication, encryption, and digital signature capability to applications," explained Lindsay Kent, VP of Product Management, Sectigo. "Microsoft does not issue publicly trusted certificates, such as those used on public-facing web servers, code signing, and document signing, nor does it issue and renew private CA certificates, leaving security administrators with a multi-step process to manage these important digital identities."

"Sectigo is the first commercial CA to provide key Management to Azure applications for all flavors of public and private certificates. Our Azure Key Vault integration is one-stop in that our customers can now issue and manage public and private digital certificates for these applications, all within the Sectigo Certificate Manager platform," added Mr. Kent.

Automation and Integration Consolidate Four Steps into One

Before Sectigo's Azure Key Vault integration, customers using Microsoft Azure would undertake several manual processes to provision certificates for applications deployed within the Azure environment. This process would then be repeated on the renewal of the certificates:

Generate keys and go through multiple steps to generate the certificate signing request (CSR)
Submit the CSR to the certificate authority
Obtain a certificate via email, or download from certificate authority web portal

Import the certificate to the Azure Key Vault

With the new Azure Key Vault integration, security administrators can use automation in Sectigo Certificate Manager to provision and manage cryptographic keys automatically and transparently in a fraction of the time required using manual processes. Sectigo Certificate Manager (https://sectigo.com/enterprise/sectigo-certificate-manager) enables an enterprise to install/renew a key with the click of a single button, without modification to any apps used in Microsoft Azure, triggering Certificate Manager to create the CSR, issue the certificate, and store keys in Azure Key Vault to be used by applications deployed in Azure Cloud.

The Azure Key Vault integration for Sectigo Certificate Manager is available today. Enterprises may read more at www.sectigo.com (http://www.sectigo.com) or contact sales@sectigo.com for more information. Sectigo will also be releasing integration with Azure Key Vault HSM for issuing document signing and Extended Validation (EV) code signing certificates.

About Sectigo

Sectigo 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/).

###

Contacts:

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

Ines Mitsou
Positive
+44 (0)20 3637 0640
imitsou@positivemarketing.com