Sectigo
Azure Key Vault

Many enterprise cloud applications are tightly integrated with Microsoft Azure Key Vault to store and manage passwords, credentials, and certificates. But Azure Key Vault cannot issue certain certificates, such as those for public-facing websites, Adobe Document Signing, Code Signing, and those from the enterprise private Certificate Authority (CA).

Business benefits of a certificate lifecycle management solution

Integrate with Azure Key Vault to seamlessly provide asymmetric cryptography to applications in Azure

Provide the wide variety of certificate types required by Azure applications

Automatically renew certificates due to expiry, changes in certificate subject name, or cryptographic strength, in a manner that the applications never cease to operate

Improve visibility using a single pane of glass, alleviating the headache of multiple key management portals, across multiple cloud vendors

Sectigo can help

Sectigo Certificate Manager, a complete management platform that automates the end-to-end lifecycle of certificates at scale, you can manage the large inventories of certificates which enable Azure applications to authenticate, encrypt, or digitally sign. Sectigo Certificate Manager supports all certificate types and is interoperable with all leading devices, operating systems, and enrollment protocols.

SECTIGO®

WWW.SECTIGO.COM

Leveraging Sectigo Certificate Manager for Azure Key Vault enables your security team to store and manage certificates in Azure Key Vault while also benefitting from:

- **Scalable certificate issuance**
  Whether your applications require hundreds, thousands, or millions of certificates, Sectigo Certificate Manager lets you issue them in an automated manner directly through Azure Key Vault.

- **Automated certificate lifecycle management**
  With Sectigo Certificate Manager for Azure Key Vault, cloud applications can consume certificates automatically so that you don't have to manually issue, revoke/replace, or renew certificates. The Azure applications request authentication, digital signature, or encryption by the key stored in the Key Vault HSM, eliminating the need to manage multiple certificate management portals.

- **Issuance of enterprise private certificates**
  Your enterprise Microsoft CA cannot automate the issuance of certificates to Azure Key Vault. Sectigo Certificate Manager for Azure Key Vault can augment or replace MSCA by automatically issuing private certificates to Azure Key Vault.

- **Future-proof certificate management**
  If keys are compromised due to an Azure Key Vault deficiency or advancements in quantum computing, the administrator can use Sectigo Certificate Manager for Azure Key Vault to force the early renewal to a cryptographically stronger certificates and keys.

- **Issuance of certificates for Adobe Document Signing and Code Signing**
  Policy requires that keys are stored in a Hardware Security Module (HSM). Sectigo is the first CA to meet that requirement through a native integration with Azure Key Vault.

- **Issuance of SSL certificates**
  Sectigo Certificate Manager for Azure Key Vault can issue all types of SSL certificates, including DV, OV, and EV for web servers, load balancers, and API gateways.
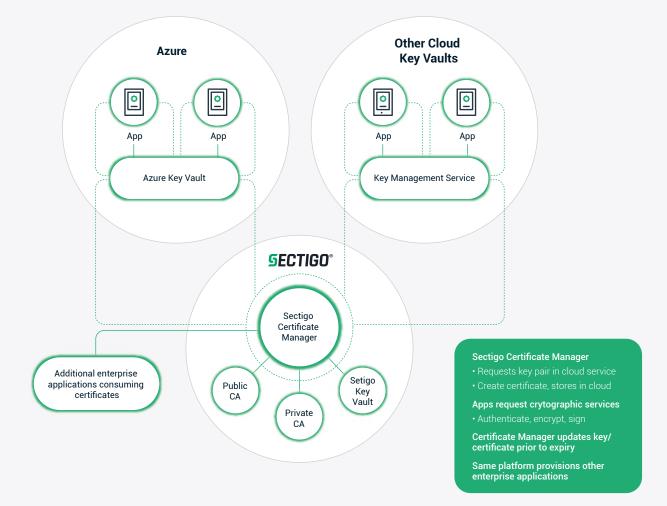
- **Enhanced visibility and reporting**
  Sectigo's native integration with Azure Key Vault lets you view the status of the certificates in use through a single pane of glass, enabling you to see expiration dates and cryptographic strength while eliminating service disruptions for both public and private certificates.

SECTIGO®

WWW.SECTIGO.COM

With Sectigo, you can enforce cryptographic strength, maintain compliance, and future-proof 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 that require digital signing, authentication, and encryption.

Sectigo Certificate Manager

Azure

App   App

Azure Key Vault

Other Cloud Key Vaults

App   App

Key Management Service

SECTIGO®

Sectigo Certificate Manager

Additional enterprise applications consuming certificates

Public CA

Private CA

Setigo Key Vault

Sectigo Certificate Manager
• Requests key pair in cloud service
• Create certificate, stores in cloud

Apps request crytographic services
• Authenticate, encrypt, sign

Certificate Manager updates key/certificate prior to expiry

Same platform provisions other enterprise applications

SECTIGO®

WWW.SECTIGO.COM

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.

LEARN MORE

100M+
Certificates issued

625k+
Businesses on the Sectigo platform

#1
Market leader in commercial SSL Certificates

33M+
Active certificates in the market

~1,200
Active partners

15%+
Of the Fortune 500 use Sectigo

SECTIGO®