

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. With 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.

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.





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.



About Sectigo



Sectigo provides purpose-built, automated PKI solutions that 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