SECTIGO

A WHITEPAPER FROM SECTIGO

Supporting Microsoft CA with Sectigo Certificate Manager Private CA

SECTIGO

Supporting Microsoft CA with Sectigo Certificate Manager Private CA

Sectigo Certificate Manager provides enterprises with a Private Certificate Authority (CA) solution, delivering a complete, managed public key infrastructure (PKI) platform designed to alleviate the problems associated with establishing and managing an internal PKI. Through the Private CA, enterprises can create their own private root certificates, which can issue private end-entity certificates to internal servers and users. These certificates, however, are not publicly trusted and intended only for internal use to support an enterprise's infrastructure and trusted members.

The Certificate Manager Private CA feature gives enterprises a low-cost method of securing and managing their private intranet certificates while adhering to corporate and industry compliance standards. Through the Certificate Manager platform, administrators can issue, view, and manage their internal certificates in addition to public certificates – all from a single platform to avoid the risks, errors, and hidden costs associated with self-signed certificates.

Private Certificate Authority

Public Certificate Authority

Administrators can issue, view, and manage their internal and public certificates.

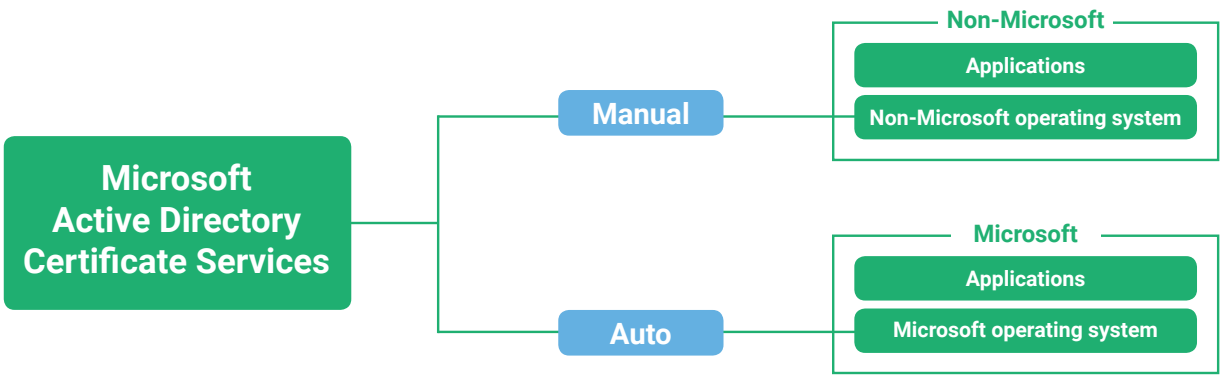
Enterprises Need to Augment Microsoft CA

Through Microsoft's automatic certificate management, IT administrators can easily instruct all desktops and servers to enroll and renew certificates without employee involvement.

But today's enterprises have devices which do not utilize Microsoft operating systems, meaning the administrator and employee share the burden of manually enrolling and renewing certificates. For these certificates, administrators

are stuck using spreadsheets to track when certificates were issued, where they were installed, their cryptographic strength, when they expire, and who is responsible for them.

Sectigo Certificate Manager Private CA works in tandem with an enterprise's Microsoft operating system, augmenting services not provided by the Microsoft CA. By filling in the gaps, the Certificate Manager Private CA helps to ensure an enterprise's private certificates are properly managed and won't unexpectedly expire.



The Rise of Non-Microsoft Applications in the Enterprise

With so many changes in the enterprise landscape over the last several years, there is a growing need to augment the Microsoft Certificate Authority (CA) to enable non-Microsoft applications.

Mobile Devices

Smartphones and tablets are ubiquitous amongst employees, so it's only natural that companies embrace these devices to help enhance worker productivity by granting them access to all enterprise systems, wherever they are. However, certificates need to sync with devices to encrypt and sign emails, authenticate users on the web portal, and validate WiFi networks without passwords. But as most devices are iOS- or Android-based, Microsoft cannot automate the certificate lifecycle.

- To mitigate this issue, enterprises can purchase a commercial mobile device management solution (MDM) to automate certificate management. However, there is still a need for publicly trusted S/MIME certificate management, which the MDM cannot achieve on its own.
- For enterprises without an MDM, Sectigo can utilize the native MDM capability in iOS and Android devices to provision certificates automatically without employee involvement
- Sectigo becomes the enterprise MDM focused strictly on managing registered and accepted certificates.

By integrating with the MDM, Sectigo Certificate Manager enables provisioning of certificates to enterprise mobile devices.

Web Servers

Today, Certificate Authorities can no longer issue public SSL certificates to servers using internal names, as domain control validation is not possible for internal server names. Therefore, many enterprises turn to Microsoft CA for their certificates, only to find they often employ Linux applications that are not managed by Microsoft. The result is that certificates require manual management, leading to increased workload, higher administration costs, and additional execution risk.

Sectigo Certificate Manager makes it easy to manage all of an enterprise's private certificates, cutting the risk of expiration and outages.

Sectigo Certificate Manager makes it easy to manage all of an enterprise's private certificates, cutting the risk of expiration and outages.

IoT Devices

To improve the efficiency of enterprise operations, a growing number of enterprises are turning to IoT devices.

These devices utilize certificates, often provisioned via Enrollment over Secure Transport (RFC7030), to authenticate themselves over Transport Layer Security (TLS) before connecting to other devices or apps. These devices almost never use a Microsoft operating system, which places a burden on the administrator to manually issue and manage certificates from the Microsoft CA. But through Sectigo Certificate Manager Private CA, there's no need to manually manage certificates. This function is executed automatically through Sectigo's single, easy-to-use platform.

DevOps

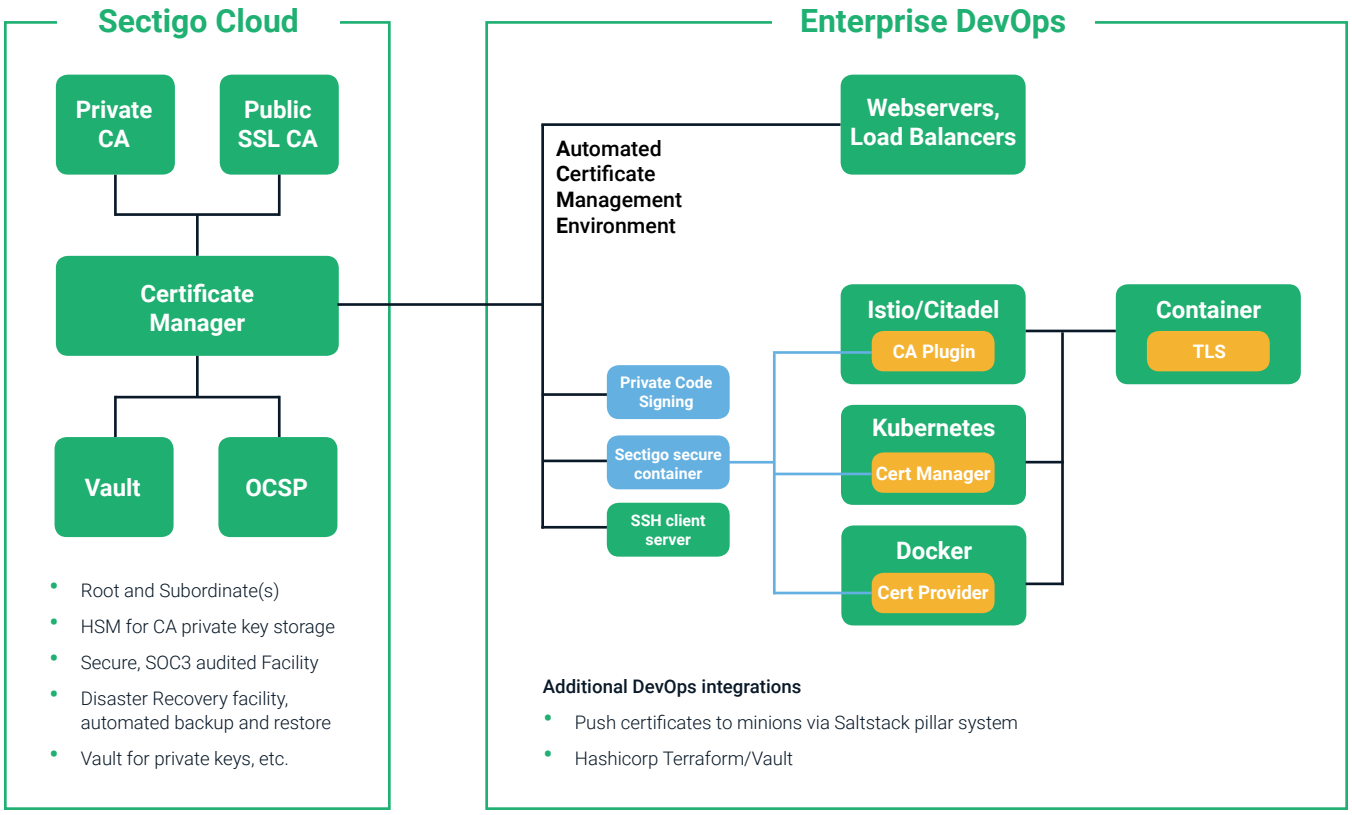
Enterprises are moving *en masse* to DevOps, leveraging its operation automation and efficient solution progression to attain faster time to market for new services, higher quality offerings, and lower development and operational costs. To accomplish this, the development team creates containers, each of which holds a portion of the monolithic application plus a minimized version of the Linux operating system. The development team tests each container before sending it to the operations team, which then executes the container.

Certificate Management plays a key role in these aspects of DevOps:

1. The container encapsulates the application running in the enterprise computing system. To prevent unauthorized applications, the container is digitally signed by a private CA. The time stamp server allows the container management to verify that the code signing certificate was valid when it was signed, even if it subsequently expired. This capability is not available from Microsoft CA.
2. Each container is assigned a certificate, which ensures each container knows what it is communicating with over TLS. The container and its associated tools are not provisioned by the Microsoft CA, as they are not applications running on the domain-joined machine operating the Microsoft operating system. Rather, several DevOps tools have their own embedded certificate authorities.
3. Web servers are often deployed with DevOps, which do not run on the Microsoft OS, but rather use Linux along with the Automated Certificate Management Environment (ACME) provisioning protocol, which cannot be automated through Microsoft CA.

Sectigo Certificate Manager delivers certificates to containers using two possible methods:

1. The customer writes code using the Sectigo REST API, Enrollment over Secure Transport (RFC7030), or ACME.
2. To simplify the deployment of Certificate Manager to DevOps, Sectigo provides integration into five leading DevOps tools, replacing the Certificate Authority built into those tools.



The Sectigo approach offers value to the DevOps project:

- Discovery of Private and Public SSL certificates that may have been issued by uncontrolled CAs
- Automatical installation and renewal of SSL certificates using ACME for OV and EV. The solution is not limited to DV, as is the case for Let's Encrypt
- Sectigo REST API & Enrollment over Secure Transport for customizable certificate provisioning
- A single user interface for reporting and controlling all certificates in the enterprise
- A single root for all applications, with the root and subordinate private keys protected in an HSM, an improvement over the DevOps tools that use roots and subordinate keys in unprotected files
- Policy control by the enterprise security team through a single UI, which can ensure the cryptographic strength of all keys and certificates issued by the DevOps teams without impeding their work. The CAs built into popular DevOps tools have no such controls

- No need for PKI expertise to enable secure communication for the containers, unlike the CAs built into popular DevOps tools, which require the DevOps professionals to fully understand the details of PKI in order to construct certificates
- Sectigo's cloud service to ensure quick setup and delivery of the certificate service
- Availability of code signing, SSH key management (2H19), SSL certificates, and container certificates all from one high availability service
- Highly available OCSP solution

Sectigo's cloud service ensures quick setup and delivery of the certificate service

Public S/MIME

Many enterprises are turning to publicly trusted S/MIME certificates to ensure their email digital signatures are trusted by email clients worldwide. This is key to fighting Business Email Compromise (BEC) fraud, wherein a criminal impersonates an employee to steal from the enterprise, and other spear phishing scams.

While Microsoft CA does an excellent job provisioning certificates for the Windows desktop, it cannot issue publicly trusted S/MIME certificates. The certificates must come from a CA capable of issuing publicly trusted email certificates — like Sectigo S/MIME certificates.

Enterprises Demand the Efficiency of a Cloud Service

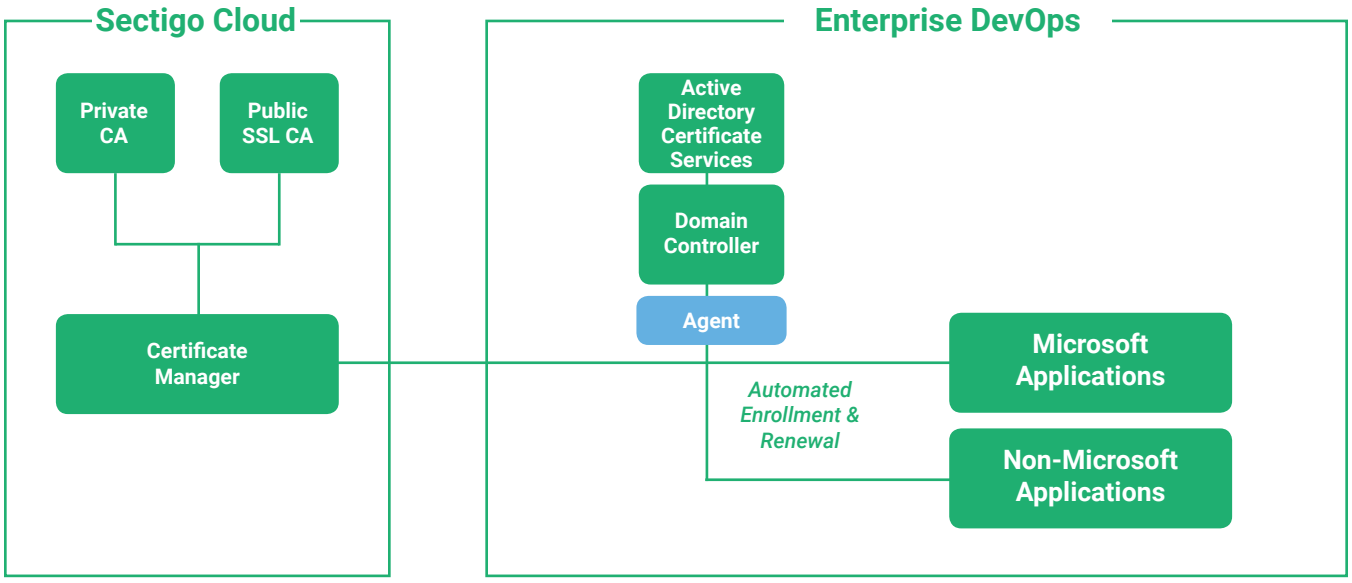
Regulated enterprises require the CA be capable of running a secure facility, complete with a hardware security module to protect mission-critical digital identities. Large enterprises will require high availability and an alternate disaster recovery location. These requirements, coupled with a market-wide shortage of PKI skills, drive enterprises to look for more cost-effective cloud options.

SECTIGO

Empower Your Private CA with Sectigo

Sectigo Certificate Manager augments the Microsoft Private CA, delivering certificates and automated management to applications and removing the need for manual management.

- The enterprise may choose to keep using its Microsoft CA for Microsoft applications and implement the Certificate Manager for the non-Microsoft applications.
- Alternatively, the enterprise can utilize Sectigo Certificate Manager for all applications, eliminating the need for two private CAs.



Sectigo Certificate Manager uses simple steps to augment Microsoft CA:

1. An agent is installed within the enterprise firewall. It allows for the Certificate Manager to participate in the certificate enrollment of Microsoft applications and communicate with the Active Directory.
2. The Certificate Manager sends a request to the agent to discover all Microsoft CA-issued certificates. If the Certificate Manager is assigned to manage only web server certificates, the agent may alternatively scan an IP address range to find installed web server certificates.
3. All certificates are now adopted by the Certificate Manager, allowing for reporting, notifications on expiry and automated certificate enrollment and renewal over industry standard protocols.

Enable the CIO's Success

Sectigo Certificate Manager will manage all the certificate needs within the enterprise from one pane of glass. This allows the administrator to enforce the cryptography policy regardless of which applications use the certificates.

Example:

- Find all certificates using RSA 2048 bit keys, set the policy to the stronger P256 elliptic curve keys, and then automatically push it out to all applications
- Find all certificates issued to former employees and revoke
- Force the use of CA keys in an HSM
- Set the cryptographic key strength for DevOps containers to maximize both security and compatibility with applications that may be limited to certain cryptography

With thousands of employees, servers, devices, and applications using manual management and uncontrolled policy, the risk of a security breach or the loss of services is extremely high — an unacceptable risk for any business. With Sectigo Certificate Manager, enterprises can augment the Microsoft CA offerings, protecting their digital infrastructure from these vulnerabilities while gaining peace of mind knowing they have a reliable partner for maintaining their certificates.

With a full spectrum of certificate management offerings, Sectigo makes it easy and cost effective to oversee lifecycle control of any certificate in an enterprise's digital environment, reducing risks, responding to threats, and controlling operating costs.