SECTIGO

Enterprise Certificate Authority Made Easy

Microsoft Windows plays an important role in the Enterprise, serving as the access point to company assets within the firewall, over a virtual private network, or from the browser to cloud services. However, authentication is required to ensure only authorized employees and devices can access the company assets. Passwords are expensive to manage, difficult to use and can be stolen by malware. To eliminate passwords, Microsoft has introduced 2 new features to meet the enterprise authentication need for an easy to use approach, where the employee's identity cannot be impersonated:

- **Microsoft Hello for Business:** The employee will begin the authentication process using a facial or fingerprint biometric. After the biometric match is performed, the digital identity issued by the Certificate Authority will complete the authentication process.

- **Microsoft Virtual Smart Card:** Microsoft has long supported the digital identity issued by a Certificate Authority, but there remained a concern that the private key could be stolen by malware from its location in the hard drive. This led to the use of one-time passwords on an external device or mobile application. Microsoft now protects the private key from theft by using the Trusted Platform Module hardware, and a user PIN, driving the displacement of one-time password devices and mobile apps.

The enterprise has the same authentication requirement for non-Windows platforms such as mobile devices, SSL/TLS on internal web servers, networking equipment, WiFi and Internet of Things. While several authentication technologies exist, Public Key Infrastructure (PKI) is the only approach which can deliver a single strong digital identity for the person or device for all use cases, and all platforms.

While PKI is the most secure and easy to use digital identity, the challenge remains to make it the easiest to deploy and Sectigo makes deployment and management easy for both a customer premises Microsoft CA and Sectigo, giving the customer the choice of what makes sense for their business.

The Microsoft Certificate Authority is well designed to issue and manage the certificates to Microsoft clients. Where MSCA is lacking, is the management and visibility of all the certificates issued, whether they be for a Microsoft client or a non-Microsoft application inside or outside the firewall such as:

- **Web Servers**
- **Load Balancers**
- **Networking Gear**
- **Mobile Devices with and without a mobile management system**
- **People or devices not defined in the enterprise Active Directory**

Automated certificate issuance, installation and renewal to non-Microsoft clients is required to prevent a failure to authenticate, leading to a customer, partner or the employee not being able to do their job. Sectigo provides Certificate Management for certificates issued from a customer premise Microsoft Certificate Authority, protecting your investment while preventing the outage of authentication services. There is no need to displace your Microsoft CA to take advantage of the management capabilities from one console. While the management is centralized, the administration of groups can be delegated to match your organizational structure; Migration to Sectigo is easy, it starts by automatically discovering all the past certificates issued by the Microsoft CA.

Why outsource the Certificate Authority?

The setup of a Microsoft Certificate Authority itself is a relatively simple task, but making effective use of the certificates across the enterprise will require PKI expertise that an enterprise may not possess. The solution design must address:

- Where certificate authentication can be used, and how it should be architected for maximum security with zero impact to employee, partner or customer productivity
- How to protect the private key from theft with evolving threats
- How to exploit digital signature to realize savings, while speeding up manual processes
- How to identity-proof employees and devices prior to enrollment for certificates
- Migration from your current authentication, by using it to enroll for a certificate
- Migration from an out-of-support certificate authority to its replacement
- Integrating with your staffing or inventory system, to ensure digital identities are only for authorized people and devices

The cost of the setup and the maintenance of the Microsoft Certificate Authority varies greatly depending on the security and availability required by the certificate authority. More sophisticated deployments will require advanced PKI knowledge that the enterprise may not possess.

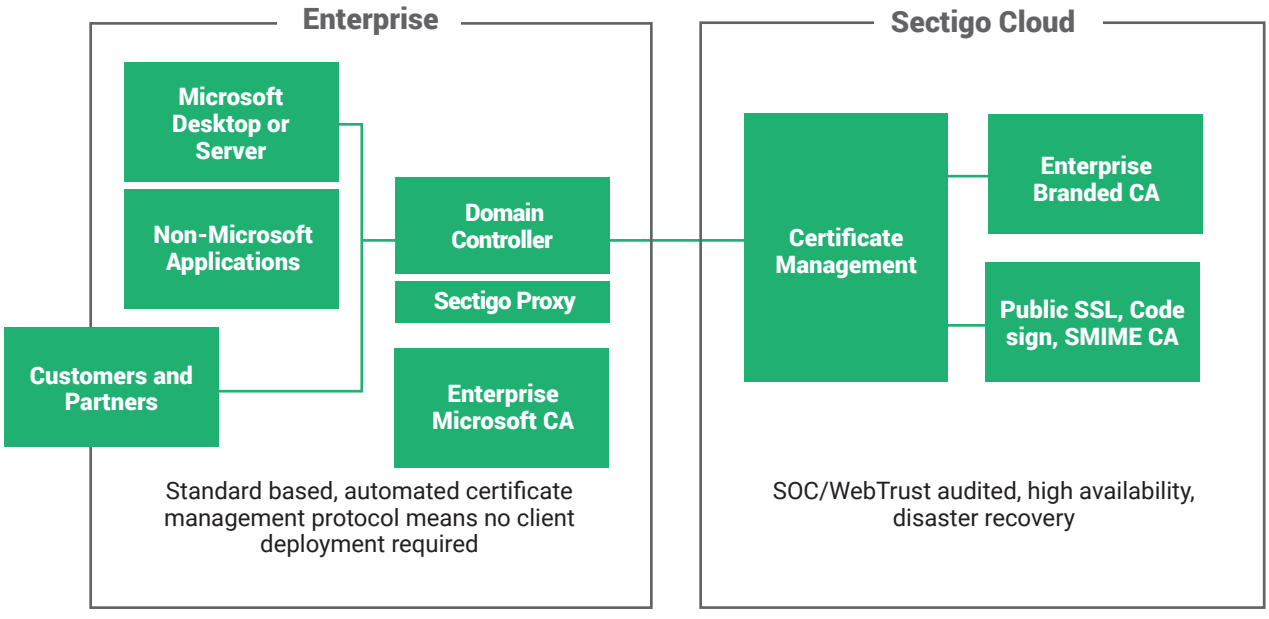
Microsoft CA Features	High End Cost	Low End Cost
Hardware Security Module – A dedicated server which stores and protects the certificate authority private key(s). If you do not use this, there is a chance that malware could steal your private key from the hard drive.	✓	✓
Backups – Periodically back up all the user/device encryption private keys held in escrow + all the certificates and associated data used by the Microsoft Certificate Authority. In the event the hard drive crashes, you can restore from a backup.	✓	✓
Secure Facility – To reduce the risk of a person compromising the Certificate Authority, the Certificate Authority is protected in a locked room, where only authorized people have access to the computer which runs the CA.	✓	
Directory storage of certs – When a sender encrypts an email or file for a recipient, the sender needs a centralized repository to find the recipient's digital certificate (which has the public key). That repository is called a directory.	✓	
High Availability – In the event the certificate authority or revocation system should go out of service, say a hard drive crash, then a 2nd certificate authority or revocation system takes over processing the requests so the business is not impacted. It is more expensive because you need to setup 2 or more redundant systems.	✓	
Disaster Recovery – In the event the building housing the certificate authority or revocation system is damaged/fire/loses internet/power, a remote computing facility takes over automatically. It is expensive because now you need to rent multiple building with hundreds of miles between them.	✓	
Annual Security Audits – To verify the system is not compromised, a 3rd party auditor will look at your processes, people and computer systems to ensure they were run as compliant to Service Organization Control 3.	✓	
Root Key Generation Ceremony – When the CA is first setup, it generates it's private key and certificate (its digital identity). A 3rd party auditor watches and documents every step. To ensure the person setting up the CA did not maliciously or accidentally steal/loose the private key or install malware.	✓	
Setup Costs	**$530,000**	**$115,000**
Annual Costs	**$240,000**	**$65,000**

Why Choose Sectigo for Certificate Management and Certification Authority

Sectigo allows the customer to purchase a turn-key service, paying only for what they need at the time, using an annual subscription fee. There are no large upfront setup costs. As the largest commercial certification authority, the Sectigo support team has the expertise to deploy PKI to your enterprise.

Sectigo is the only CA that allows the enterprise to simultaneously issue and manage certificates issued from:

- Customer premise Microsoft Certificate Authority. Migrate from the customer premise MSCA to the Sectigo Cloud Certificate Authority at your own pace or stay on MSCA indefinitely.
- Sectigo's cloud-based Certificate Authority is branded and dedicated for the customer. The Sectigo solution is designed for the cloud where we will have you issuing certificates in half the time of other providers.
- Publicly trusted SSL, Code Signing and S/MIME can all be managed from the same console, while allowing for delegated administration along enterprise organizational boundaries.



For more information about how to implement Sectigo CCM, contact us today.

