sectigo

DATASHEET

Sectigo Private PKI

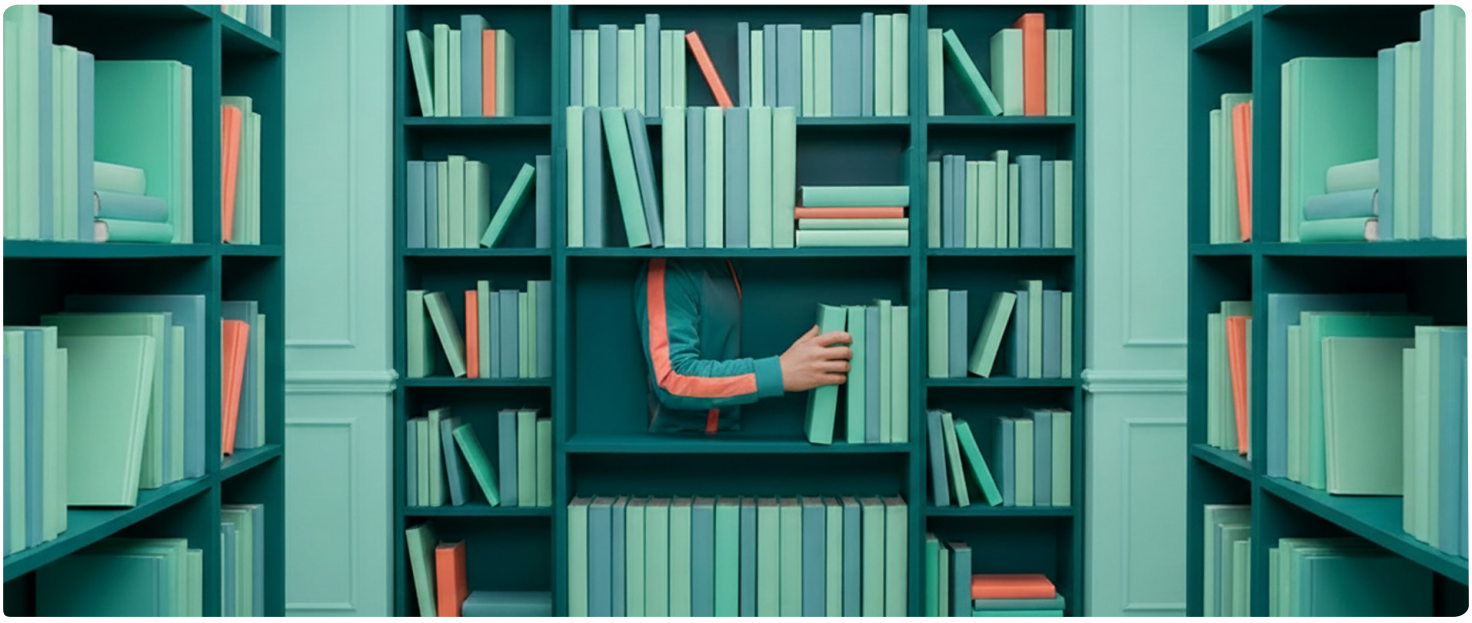
As enterprises connect an increasingly distributed workforce using a complex environment of cloud applications, networked computing and mobile devices, and traditional web servers and network infrastructure, IT teams must secure the identity and access to all internal servers, users, devices, and applications across the enterprise network. Every connection requires both strong authentication and encryption to ensure the integrity of the network, protect against malicious attacks, and guard against unexpected downtime.

Many enterprises now operate their own Private Certificate Authority (CA) to provide tighter control of authentication using Public Key Infrastructure (PKI) certificates that serve that organization only. To ensure the Private CA protects the entire network environment, IT teams need a solution that:

- Covers all types of certificates used across the enterprise
- Supports an architecture with any combination of root CA and issuing CA from private and 3rd party authorities
- Enables issuance, deployment, renewal, and replacement of certificates quickly, reliably, and scalably

Sectigo can help

Sectigo's Private PKI is a complete managed PKI solution for issuing and managing privately trusted TLS/SSL certificates in use across today's enterprise environment. Sectigo's Private PKI provides a fully automated-solution for the lifecycle management of private SSL certificates used to secure internal web servers, user access, connected devices, and applications.



Types of Certificates

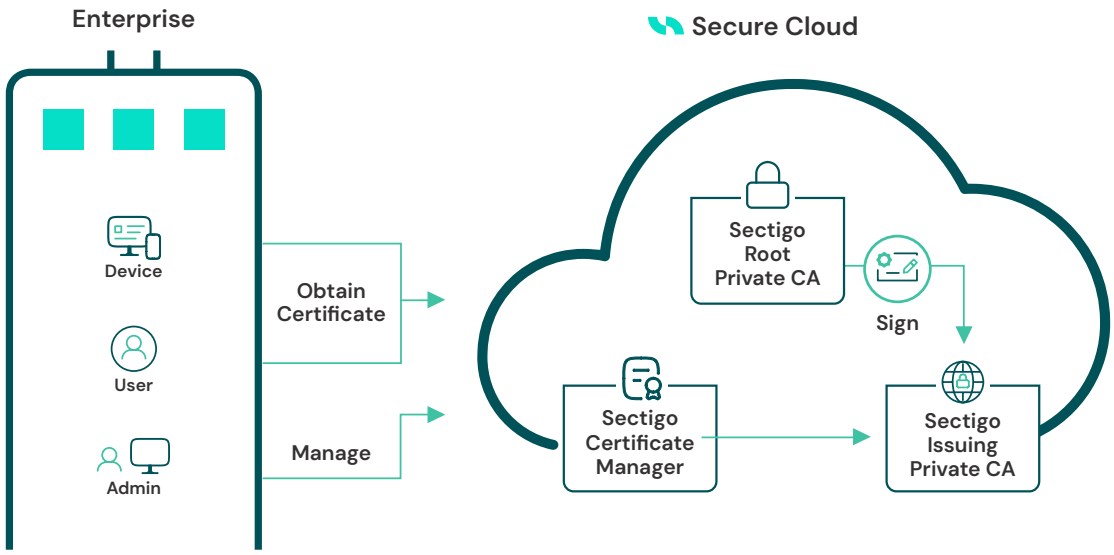
A Common Mark Certificate (CMC) is a specialized digital certificate, designed to confirm organizational identity by Enterprises depend on Private CAs for internal certificates to support a growing number of use cases including mobile devices, IoT, DevOps, secure email, and cloud/multi-cloud. Sectigo empowers IT teams to maximize the power of users' digital identity across the entire enterprise with a flexible licensing configuration known as seats. The Sectigo seat offers issuance of Private CA certificates to all devices and applications used by individual users for all types of use cases:

- **User Seats:** Certificates issued to human subscribers that authenticate access to the network, including VPN, WiFi, and S/MIME certificates.
- **Device Seats:** Certificates issued to computing and mobile devices, such as laptops, computers, and smartphones.
- **Container Seats:** Certificates issued to a container or software entity in development and DevOps environments.
- **Server Seats:** Certificates issued to an organization's internal physical and virtualized servers, including servers used for intranet websites and load balancers.
- **SSL Seats:** Certificates issued to an organization's external servers used for public websites and applications.
- **Private Code Signing Certificates:** Certificates issued to sign software code for internal applications.

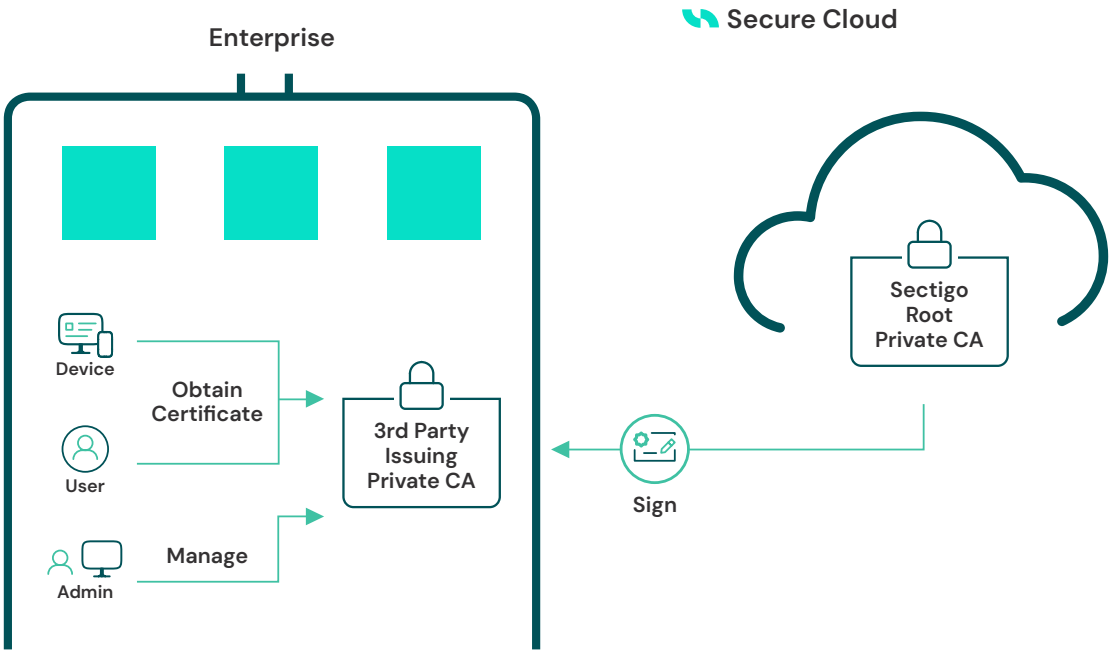
Private CA Infrastructure

Sectigo Private PKI offers a high capacity infrastructure with near instantaneous certificate issuance and supports a Private CA architecture that employs any combination of private and 3rd party root CA and issuing CA. Enterprises have a choice of three primary deployment architectures:

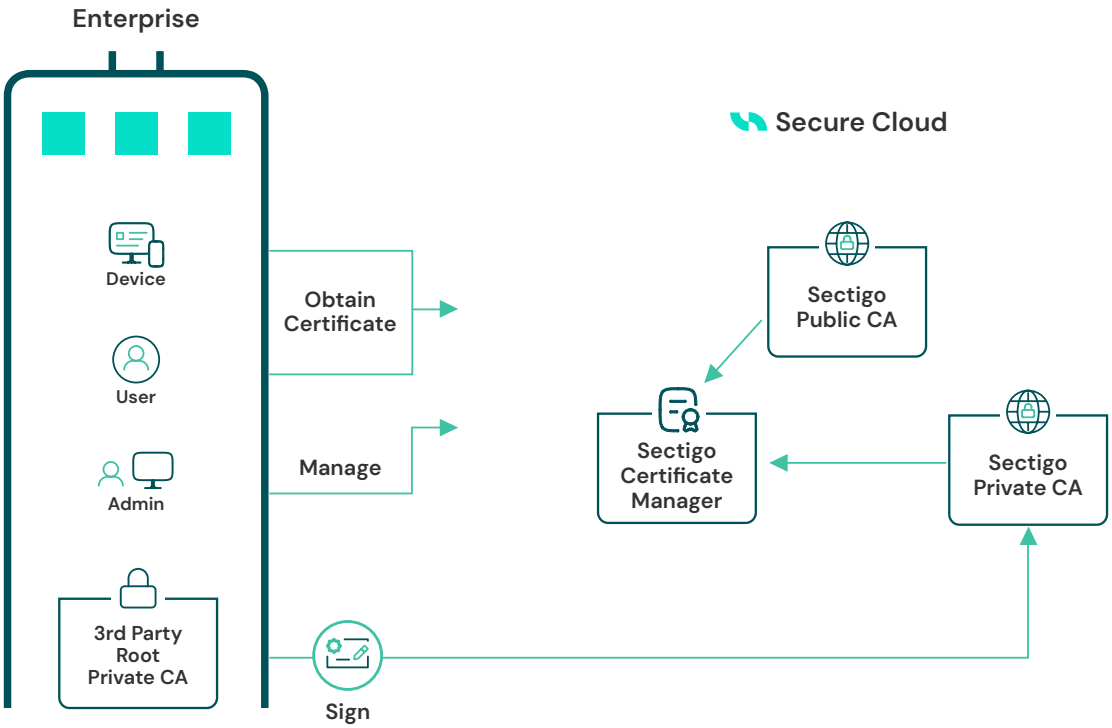
1. Sectigo hosts both the Private Root CA as well as issuing CA(s)



2. Sectigo hosts the Private Root CA and the organization hosts issuing CA(s) on its own



3. The organization hosts the Private Root CA on its own and Sectigo hosts the Issuing CA(s)



Key PKI Certificate Features

As a trusted CA, Sectigo underpins the security of not only the PKI certificates we issue, but all the transactions and exchanges protected by those certificates. Sectigo Private PKI supports key PKI certificate features including:

- Offline and online private CA roots
- Cryptography algorithms by RSA (RSA2048, RSA3072, RSA4096) and Elliptic Curve (ECC P256, P384, P512) for the CA itself and the leaf certificates
- X.509 CRL and OCSP certificate validation
- HSM key protection operating at FIPS140-2 level 3+
- High availability and disaster recovery for the CA keys
- CA key generation witnessed by an external auditor
- High capacity infrastructure with near instantaneous certificate issuance

With Sectigo Private PKI, you can enforce cryptographic strength, maintain compliance, and future-proof your business while minimizing costs. And with Sectigo Certificate Manager's easy provisioning, you can automate issuance and lifecycle management of all of the certificates throughout your entire organization, across a wide variety of use cases that require digital signing, authentication, and encryption.

About Sectigo

Sectigo is a leader in certificate lifecycle management (CLM), providing innovative and comprehensive solutions to secure both human and machine identities for some of the world's most prominent brands. Its cloud-native, automated, and universal CLM platform simplifies and enhances enterprise security by issuing and managing digital certificates from all trusted certificate authorities (CAs). With over two decades of experience, Sectigo stands as one of the largest and most established CAs, serving more than 700,000 customers worldwide.

By delivering unparalleled digital trust, Sectigo continues to empower organizations to implement robust securityprotocols with efficiency and confidence.