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.

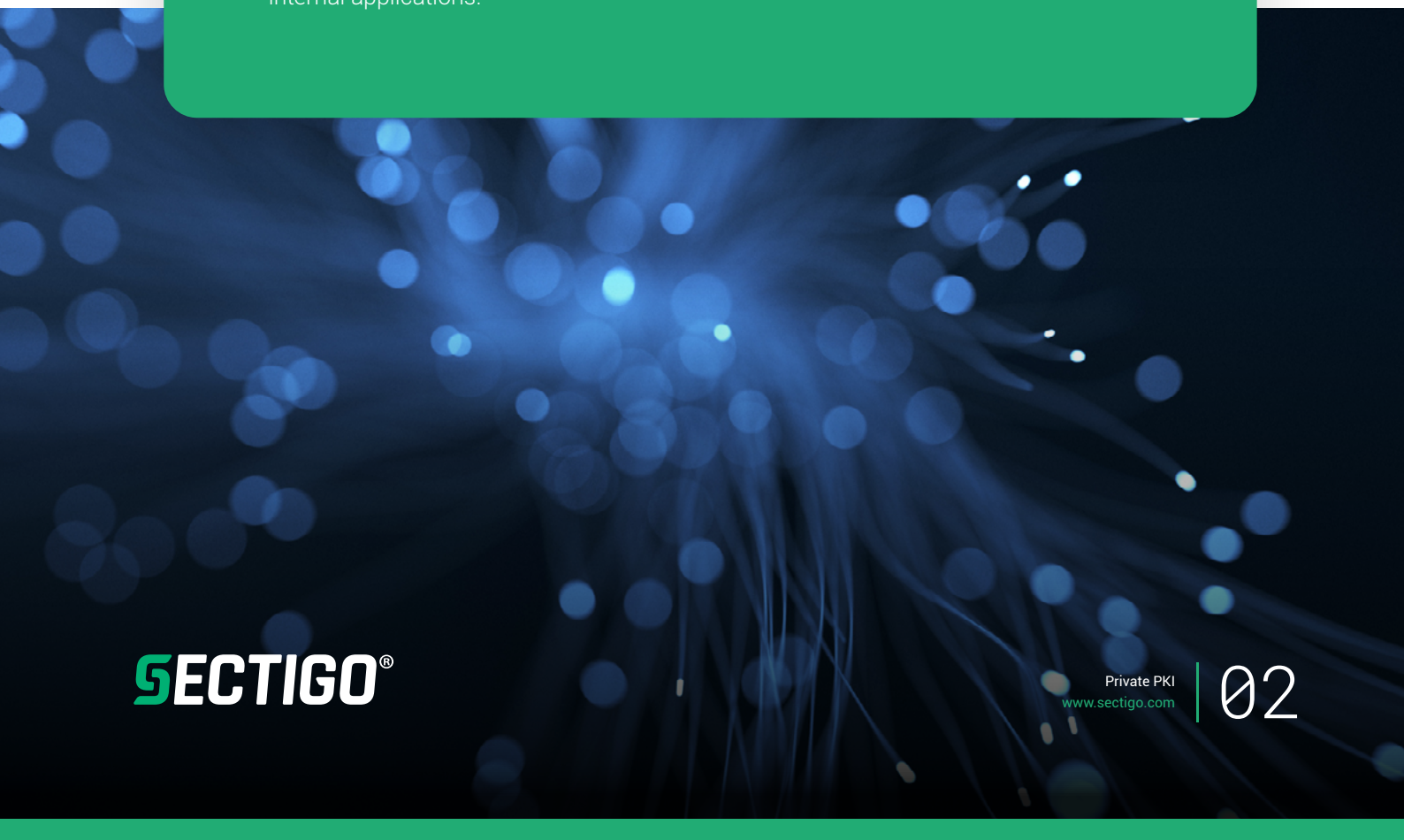
SECTIGO®

WWW.SECTIGO.COM

Types of Certificates

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:

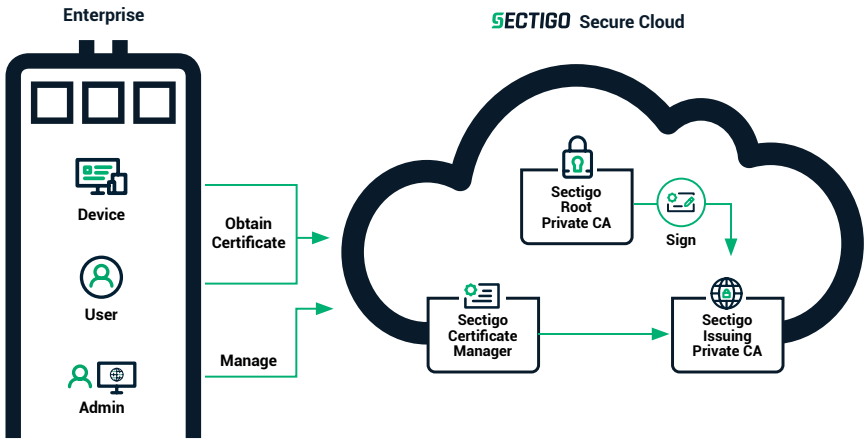
- **User Seats:** Certificates issued to human subscribers that authenticate access to the network, including VPN, WiFi, and S/MIME certificates.
- **Device Seats:** Certificates issued to computing and mobile devices, such as laptops, computers, and smartphones.
- **Container Seats:** Certificates issued 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.



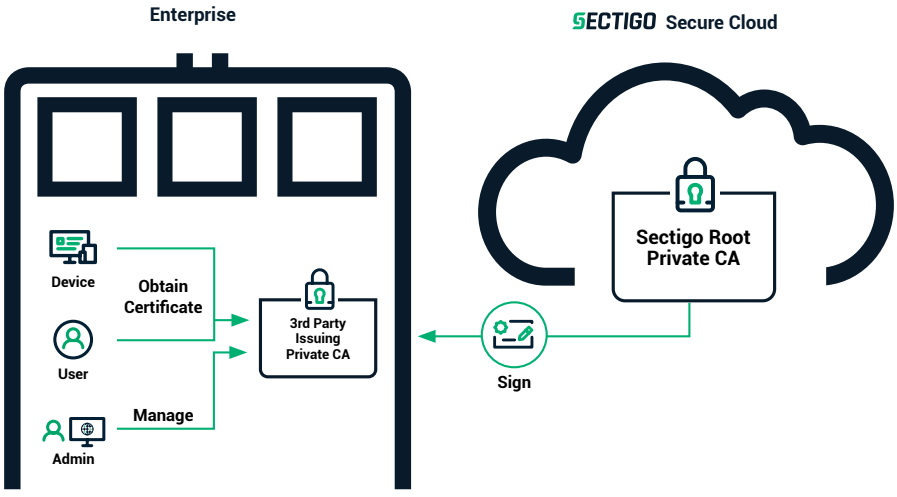
Private CA Infrastructure

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)

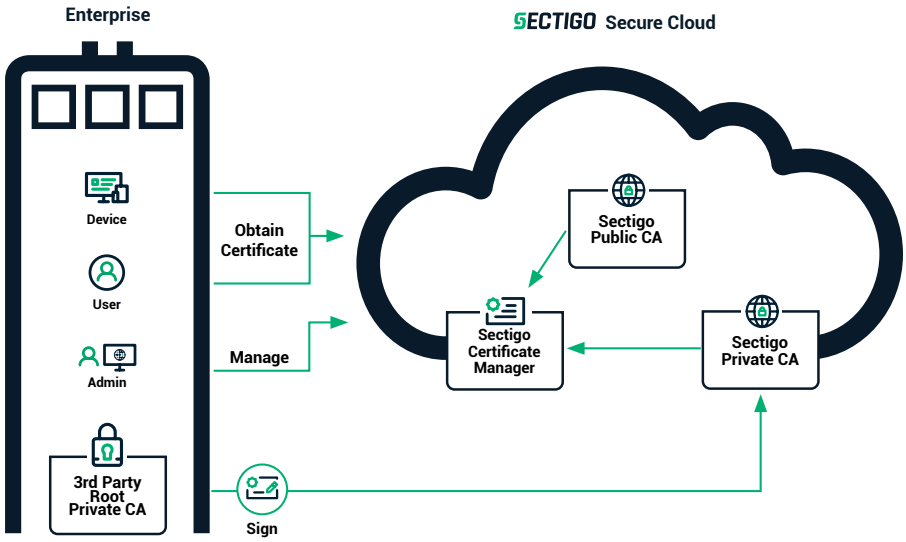


2. Sectigo hosts the Private Root CA and the organization hosts issuing CA(s) on its own



Private CA Infrastructure (cont'd)

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



Many organizations prefer to have all operational aspects of their Private CA including hosting, maintenance, security, and compliance taken care of by a 3rd party like Sectigo. For enterprises that already have their own Private Root CA or use Microsoft CA (MSCA) for Windows-based servers and devices, Sectigo Private PKI works alongside the existing Private CA or MSCA so that organizations can secure all devices and applications from a single platform.

Automated Certificate Management

Enterprises need a reliable and scalable certificate management solution to ensure critical business systems are protected without time-consuming administrative tasks or the risk of unexpected certificate expirations or outages. With Sectigo Certificate Manager, enterprises get a complete management platform that automates the end-to-end lifecycle of public and Private PKI certificates at scale.

Leveraging Sectigo Certificate Manager enables IT teams to trust the identity of all users, devices, and applications across the enterprise while also benefitting from:

Easy provisioning: Sectigo enables IT administrators to program configurations and policies just once and then push to all users, devices, and applications using automation standards, including ACME, EST (Enrollment over Secure Transport), SCEP (Simple Certificate Enrollment Protocol), and Sectigo's Microsoft CA proxy agent.

Certificate discovery: Sectigo Certificate Manager provides in-depth scanning to uncover and monitor all certificates installed across an entire environment, regardless of the Certificate Authority. For each certificate, Sectigo certificate Manager shows your issuing CA, expiration date, signature algorithm, and ciphers.

Full certificate lifecycle management: Sectigo Certificate Manager provides automatic certificate renewal and replacement to avoid downtime to critical business systems. In addition, you can also easily revoke certificates, for example, when a server is replaced or an employee leaves your organization and access needs to be terminated.

Secure key storage: Sectigo ensures only authorized devices can join the network by storing the private key and certificate into end points' trusted key storage, including Windows 10 Trusted Platform Modules (TPM), Apple's Secure Enclave, or Sectigo's software-based secure certificate storage.

Enhanced visibility and reporting: Use a single pane of glass to view the status of certificates on all devices in use, enabling you to see expiration dates and minimize or eliminate service disruptions.

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 leading cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As the world's largest commercial Certificate Authority with more than 700,000 customers and over 20 years of experience in online trust, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions for securing webservers, user access, connected devices, and applications. Recognized for its award-winning innovation and best-in-class global customer support, Sectigo has the proven performance needed to secure the digital landscape of today and tomorrow. For more information, visit www.sectigo.com and follow @SectigoHQ.

SECTIGO®