

# Sectigo as your private Certificate Authority (CA)

---

**SECTIGO®**

# Role of private Certificate Authority (CA)

Private CAs enable organizations to issue internal certificates, providing them with the ability to have complete control over encryption, authentication, and signing within their networks. They ensure device and workload security, provide flexible certificate management, and maintain confidentiality by not exposing internal information to external sources. In addition, Private CAs provide more control over the lifecycles and revocation processes of certificates compared to public CAs.

## Private CA Use Cases

Enterprises often use private CAs for internal websites and communications, implementing certificate-based authentication to prevent unauthorized access and enhance security. Common use cases include:

- **Secure Tunneling:** Private CAs provide certificates for robust authentication and encryption for routers and switches, protecting network infrastructure.

Organizations across various sectors use private CAs to secure communication between locations, data centers, and cloud environments, protecting sensitive information and ensuring compliance.

*Applicable industries include but are not limited to:*

**Finance:** Secures communication across trader stations, branch offices, and data centers.

**Healthcare:** Protects electronic health records (EHRs) and patient data between facilities.

**Tech:** Secures data transfer between cloud environments and global data centers.

**Manufacturing:** Safeguards communication between factory systems and monitoring stations.

**Retail:** Ensures secure data transfer for e-commerce and point-of-sale systems.

**Energy and utilities:** Secures communication between SCADA systems and smart grids.

**Government:** Protects sensitive communication between agencies and data centers.

- **Device Authentication:** Certificates from private CAs ensure only authorized IoT devices can connect to the network, maintaining consistent identity security standards.

Laptops, tablets, and mobile phones receive certificates from private CAs, ensuring that only trusted devices can access critical network resources and sensitive information.

*Applicable industries include but are not limited to:*

**Finance:** Enhances data protection and compliance for trader workstations and financial devices.

**Healthcare:** Protects patient data with certificates for medical equipment and staff tablets.

**Tech:** Certificates for laptops and smart office devices to access protected resources and systems.

**Manufacturing:** Prevents unauthorized access for production equipment and control systems.

**Retail:** Ensures transaction integrity for point-of-sale terminals and inventory systems.

**Energy and utilities:** Maintains operational reliability for SCADA systems and monitoring stations.

**Government:** Safeguards sensitive information for official workstations and devices.

- **VPN:** Private CAs issue certificates supporting VPNs, replacing traditional tokens or mobile apps to streamline employee access while securing connections between remote sites.

Employees across various industries receive certificates from private CAs to ensure secure VPN access, protect data integrity, and maintain compliance across remote locations.

*Applicable industries include but are not limited to:*

**Finance:** Protects sensitive financial data and ensures PCI DSS compliance.

**Healthcare:** Secures patient data among EHR systems and ensures HIPAA compliance.

**Tech:** Enhances secure application communications and access control to internal systems.

**Manufacturing:** Safeguards communication between factory systems and monitoring stations.

**Retail:** Ensures secure data transfer for e-commerce and point-of-sale systems.

**Energy and utilities:** Secures communication between SCADA systems and smart grids.

**Government:** Protects sensitive communication between agencies and data centers.

- **DevOps:** Certificates from private CAs secure DevOps containers and CI/CD pipelines, orchestration frameworks, and key vaults, integrating PKI into development workflows.

Employees across various industries receive certificates from private CAs to ensure secure VPN access, protect data integrity, and maintain compliance across remote locations.

*Applicable industries include but are not limited to:*

**Finance:** Protects sensitive financial data across digital banking platforms and CI/CD pipelines.

**Healthcare:** Secures patient information and authenticates DevOps tools throughout development.

**Tech:** Enhances security for containerized microservices, DevOps tools, and CI/CD code commits.

**Manufacturing:** Ensures data integrity in automated production systems.

**Retail:** Shields customer data and maintains the integrity of CI/CD pipelines for retail platforms.

**Energy and utilities:** Secures data from smart grids and validates code for management systems.

**Government:** Safeguards classified information for critical public sector applications.

- **API Authentication:** Private CAs generate code-signing certificates for APIs, ensuring code integrity in communications with third parties and enabling secure interoperability.

Employees across various industries receive certificates from private CAs to ensure secure VPN access, protect data integrity, and maintain compliance across remote locations.

*Applicable industries include but are not limited to:*

**Finance:** Secures open banking APIs, ensuring safe communication with fintech partners.

**Healthcare:** Protects medical data exchange with partner institutions, ensuring HIPAA compliance.

**Tech:** Facilitates communication between microservices and controls access to sensitive data.

**Manufacturing:** Safeguards industrial IoT APIs, ensuring reliable supply chain integration.

**Retail:** Authenticates e-commerce APIs, protecting customer data and securing transactions.

**Energy and utilities:** Secures smart grid APIs, ensuring secure data exchange and management.

**Government:** Protects APIs for public sector applications, safeguarding sensitive information.

Using private CAs for non-public endpoints is crucial to safeguard internal systems against threats like man-in-the-middle exploits, which can result in data loss or security breaches. Historically, enterprises heavily utilized Microsoft CA, integrated with Active Directory, primarily in Windows-centric environments. However, the rising adoption of mobile devices including bring your own device (BYOD), IoT, cloud, and DevOps has driven the need for alternative private CAs from IT security vendors to support diverse operating systems and evolving architectures.

## Choose a Private CA that works for you

Choosing a Private CA that fits your needs is crucial as the landscape of certificate management evolves. Every connection needs strong authentication and encryption to ensure network integrity, protect against attacks, and prevent downtime. Modern cloud-native solutions have streamlined what was once complex and costly, offering faster deployment and affordability. Private CAs offer robust control over cryptographic assets, ensuring confidentiality and meeting rigorous security standards, making them indispensable in modern cybersecurity.

To safeguard the entire network environment effectively, IT teams should look for a Private CA solution that:

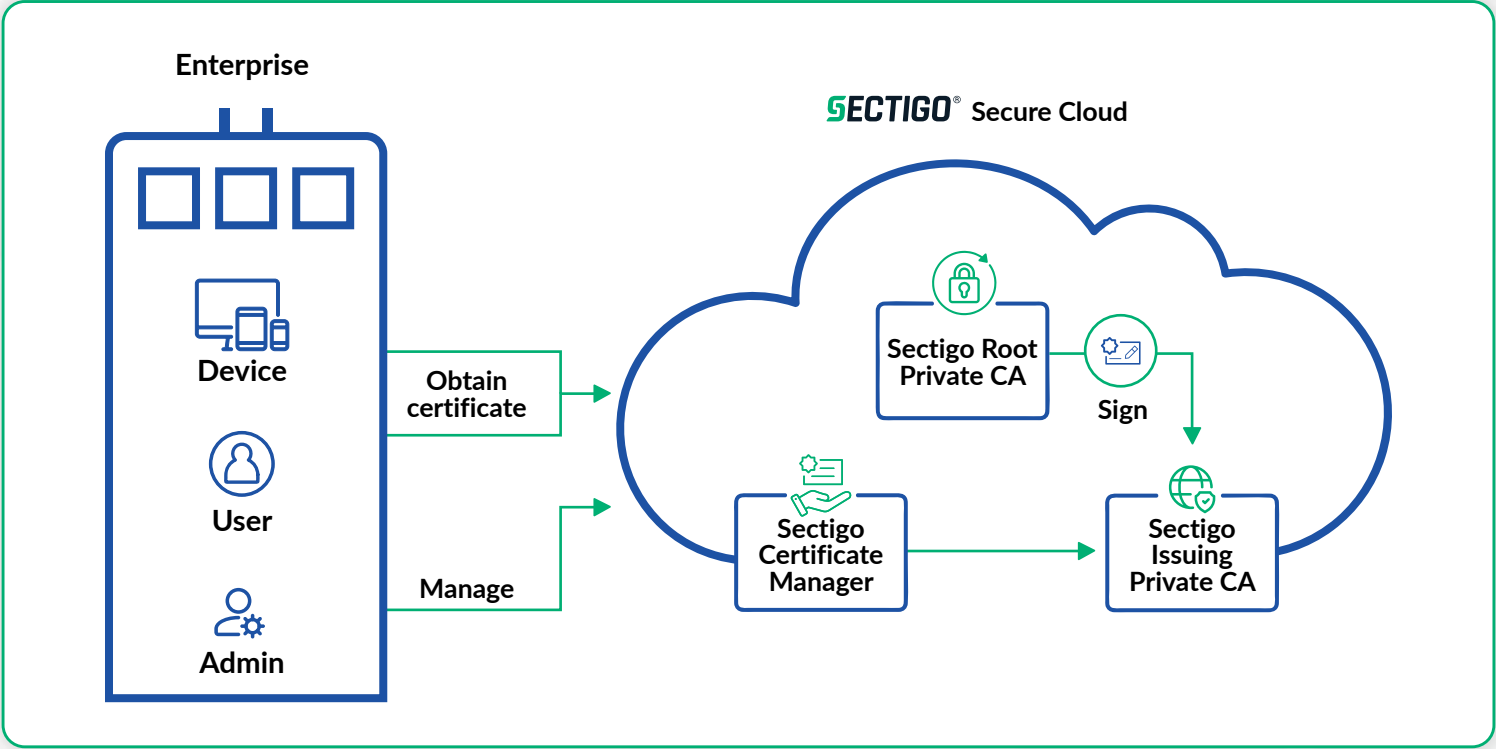
- Covers all types of certificates used across the enterprise.
- Seamlessly integrates with your existing IT systems and security protocols.
- Supports an architecture with any combination of root CA and issuing CA from private and 3rd party authorities.
- Enables automated workflow of rapid, reliable, and scalable issuance, deployment, renewal, and replacement of certificates.
- Meets all relevant regulatory requirements and can adapt to changes in compliance standards.
- Offers robust support and expertise to assist with implementation and ongoing management.



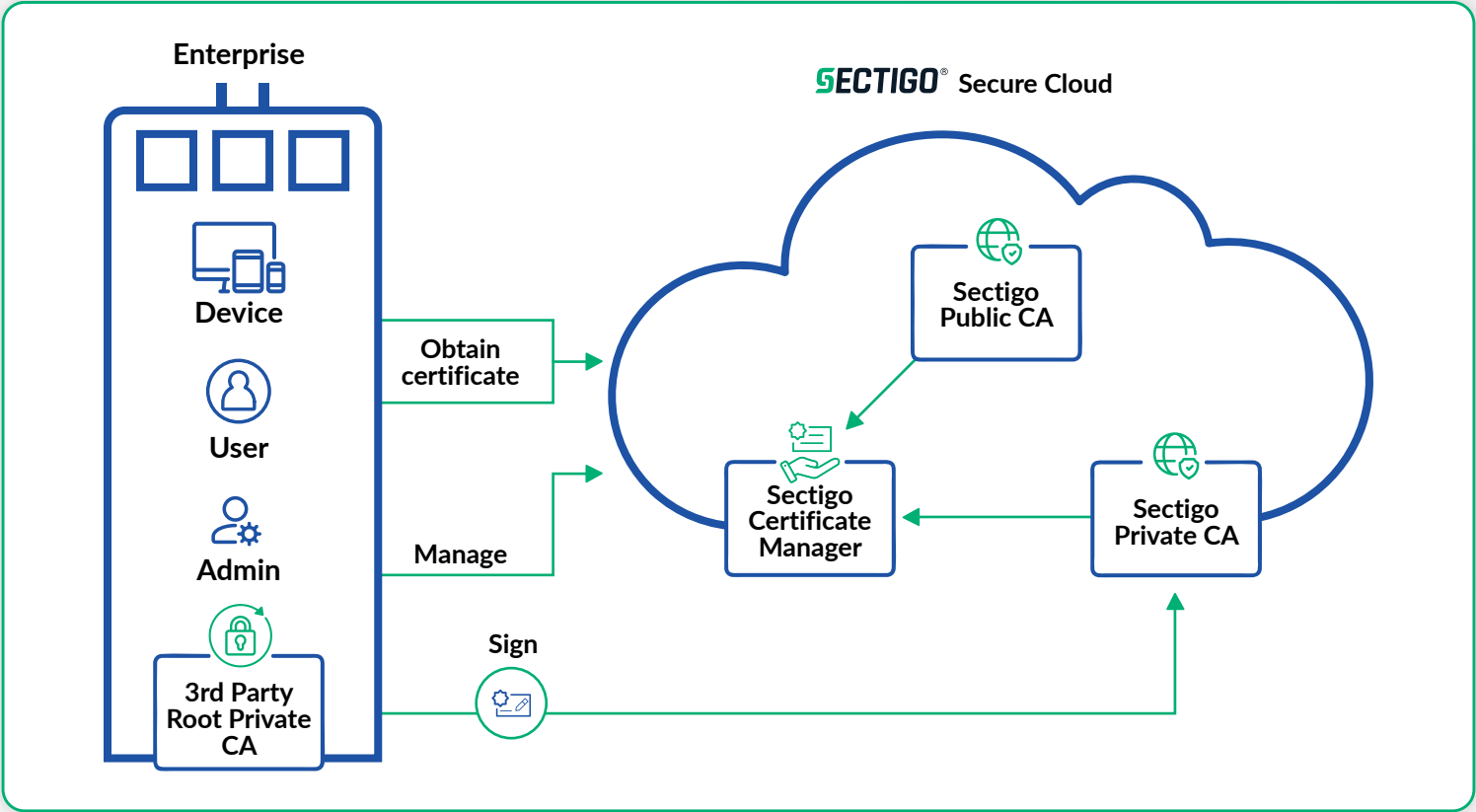
# Sectigo as a Private CA

Sectigo provides a highly scalable infrastructure with near-instant certificate issuance, supporting a flexible Private PKI architecture. This allows for any combination of hosted private PKI or hosted issuing CAs signed by on-premises third-party root CAs:

Sectigo hosts both the Private Root CA and issuing CA(s)



The organization hosts their own Private Root CA 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's Private CA integrates seamlessly with existing setups, allowing organizations to secure all devices and applications through a unified platform.

## Types of certificates issued by Sectigo

Sectigo offers a flexible licensing configuration known as seats to maximize digital identity management across enterprises. Each seat provides issuance of Private CA certificates for various use cases:

- **User Seats/Certificates:**  
Certificates for human subscribers authenticating network access (e.g., VPN, WiFi, S/MIME).
- **Device Seats/Certificates:**  
Certificates for computing and mobile devices (e.g., laptops, computers, smartphones).
- **Server Seats/Certificates:**  
Certificates for internal physical and virtualized servers (e.g., intranet websites, load balancers).
- **SSL Seats/Certificates:**  
Certificates for external servers hosting public websites and applications.
- **Private Code Signing Certificates:**  
Certificates to sign software code for internal applications.





## Choose trust

With Sectigo Private PKI, you ensure robust cryptographic strength, compliance maintenance, and futureproofing for your business while minimizing costs. Our automated solution manages the lifecycle of private SSL certificates securing internal web servers, user access, connected devices, and applications across your organization. As the industry's leading CA for over two decades, Sectigo safeguards not just the certificates we issue, but also all the transactions and exchanges protected by those certificates. Sectigo's Private CA 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

## Sectigo Certificate Manager: One-stop shop for all your certificate needs



### Lead by automation:

Sectigo Certificate Manager (SCM) enhances workflow automation and efficiency as a first-class ACME citizen and supports all major certificate automation standards.



### CA-agnostic single pane of glass:

Experience streamlined certificate management by consolidating all public and private certificates in one place for effortless administration, regardless of their origins.



### Proven Reliability:

Benefit from a robust and award-winning certificate management solution known for its proven reliability and performance.



## Let our customers speak for us



“Sectigo Certificate Manager has become a major part of our IT management infrastructure, allowing us to update, add and delete thousands of digital certificates with a streamlined dashboard and email alert system.”

- Craig Hurter  
IT security Manager, University of Colorado at Boulder

For more information on Sectigo's Private CA practices, SSL/TLS certificates or certificate management in general please contact Sectigo Sales at [sales@sectigo.com](mailto:sales@sectigo.com).

## Explore related resources:

**Website:** [Managed PKI Solutions for Enterprises | Sectigo® Official](#)

**Webinar:** [An introduction to managed private CAs](#)

**E-book:** [How to Move beyond Microsoft AD CS](#)

**Datasheet:** [Sectigo Private PKI | Sectigo® Official](#)

**Sectigo Blog:** [Enterprise Use Cases For A Private Certificate Authority | Sectigo® Official](#)

**Sectigo Blog:** [What is a Private CA? How to Manage Internal Certificates | Sectigo® Official](#)

**Sectigo Blog:** [What Is A Self-Signed Certificate & How to Create One | Sectigo® Official](#)