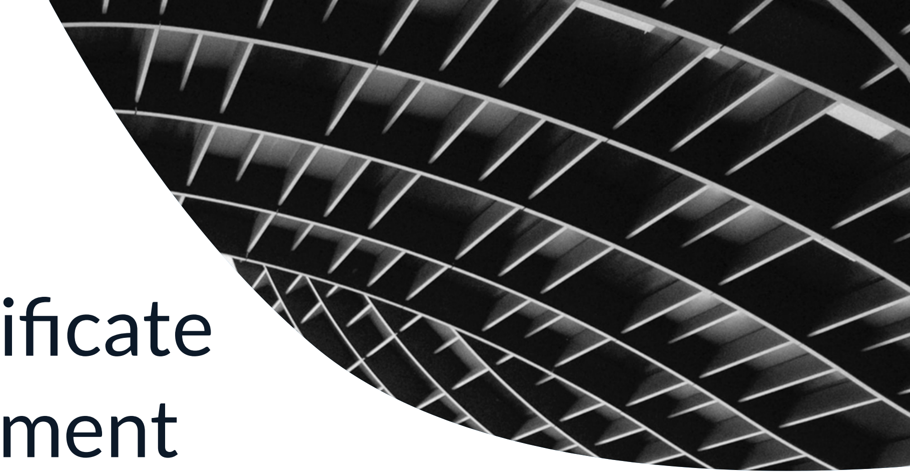


DATASHEET

CA Agnostic Certificate Lifecycle Management

Sectigo Certificate Manager Works With Other Certificate Authorities

A typical enterprise may need to work with multiple certificate authorities. This may be for business reasons, or to ensure resilience, or it may be for historical or organizational reasons. Whatever the case, the flexibility to issue, manage, and renew certificates from a variety of public CAs is a common ask from Sectigo customers.

Sectigo is dedicated to ensuring openness and interoperability to help customers consolidate platforms, reduce costs, and maximise resources.

Sectigo Certificate Manager (SCM) now includes the capability of issuing certificates from third party public CAs, including Entrust and DigiCert. SCM can also issue certifcates from Private CAs such as AWS Cloud Services, Google Cloud Platform (GCP) and Microsoft ADCS. This means that IT departments can have a single full featured platform providing Certificate Lifecycle Management (CLM) across multiple certificate vendors. Enterprises can continue to employ certificates from other vendors, or can transition to Sectigo certificates if and when they choose.

Other CLM vendors support multiple Certificate Authorities, but only Sectigo provides the complete solution of a top tier CA Independent CLM solution combined with a leading Certificate Authority and a rich set of available certificate types.

Sectigo Automates Certificate Deployment

Sectigo Certificate Manager brings all the power of its automated installation and renewals to your existing CA, with no need to change vendor. It automates the installation of certificates into all your web servers, load balancers, cloud (AWS, Google) applications and DevOps tools. SCM performs the automation using the latest open standards lowering your cost of deployment, without locking you into a single vendor.

SECTIGO®

How Does This Work?

PUBLIC CA

For public CAs such as DigiCert and Entrust, customers have access to APIs that facilitate the programmatic issuance and renewal of certificates. These APIs require credentials which the CAs provide to their customers. SCM now includes a configurable module for support of third party CAs where the customer can enter their credentials for Entrust or DigiCert APIs, providing access to on demand certificate issuance.

The process for setting up connectivity to DigiCert or Entrust is very straightforward and takes only a few minutes. The API credentials are never shared with Sectigo, and the customer is not required to disclose them. This ensures that customers are in full compliance with their contracts with the other CAs.

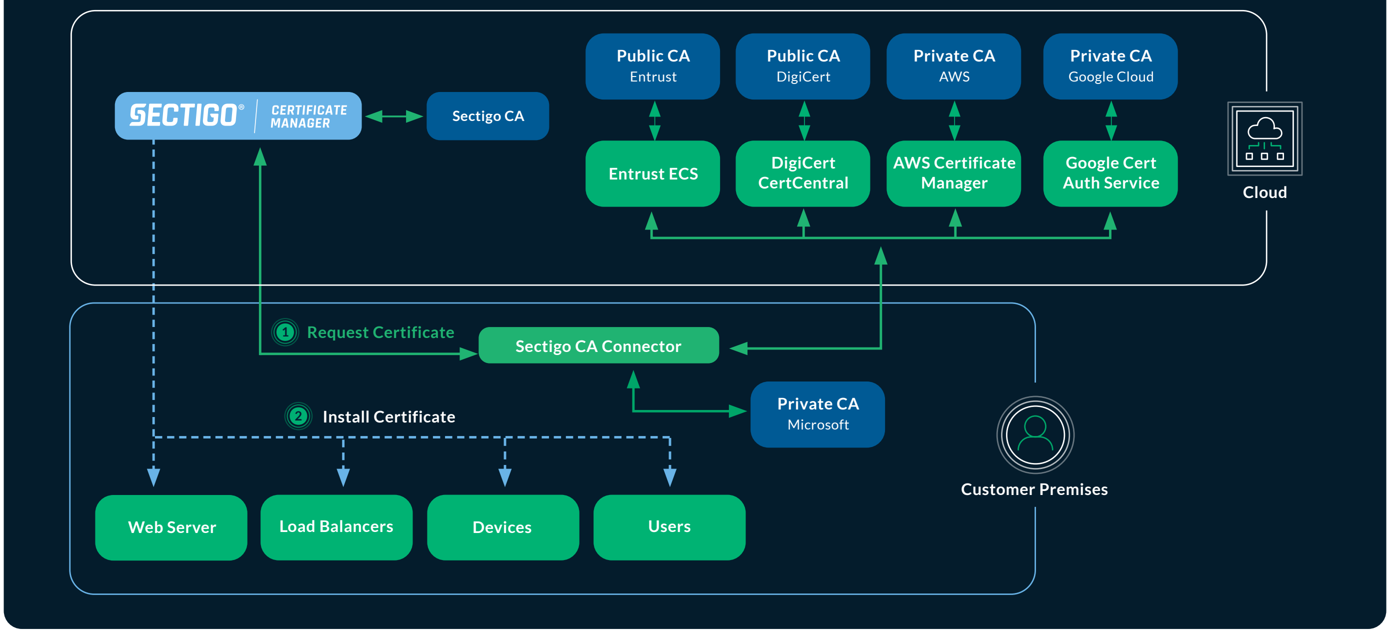
PRIVATE CA

An enterprise CA, or private CA, is commonly used by businesses to support their authentication infrastructure, internal servers, mobile devices or code and document signing activities. Sectigo provides a private CA as an option with Sectigo Certificate Manager. But many enterprises may already have established Private CAs with Microsoft CA (ADCS), Google Cloud and AWS Cloud. SCM can issue and manage certificates from these CAs, interfacing directly with the vendor's platform. The Sectigo Connector can be configured for multiple instances of these Private CAs, providing complete flexibility and coverage of an enterprises certificate needs.

CONSOLIDATED PLATFORM

Once the required CAs have been configured, SCM is then used to define a certificate issuance policy with the public or private CA as the source. Requests are issued to the appropriate CA and the certificates can be managed via SCM for installation, renewal, revocation and automation. This provides the customer with the greatest flexibility to continue issuing and renewing certificates sourced from other CAs while managing them via SCM.

Issuance and Renewal of Certificates From Other CAs



SCM offers the following benefits:

- A single management console for issuance, management, and renewal of certificates, regardless of the certificate vendor
- A more controlled transition from one CA to another
- Support for multiple CAs to ensure resilience in case of a root becoming distrusted
- Greater level of choice for customers enabling them to meet business operational and organizational needs

Sectigo's unique approach to the market for a leading CA is both revolutionary and transformative with better alignment with the customer need. It is an acknowledgement of the critical role certificates play in many aspects of IT infrastructure and facilitates the management of increasingly important digital identities without creating unnecessary complexity.

For further information on Sectigo's certificate solutions contact your Sectigo sales representative or email sales@sectigo.com.

About Sectigo

Sectigo is the leading provider of digital certificates and automated Certificate Lifecycle Management (CLM) solutions trusted by the world's largest brands. Its cloud-based universal CLM platform issues and manages the lifecycles of digital certificates issued by Sectigo and other Certificate Authorities (CAs) to secure every human and machine identity across the enterprise. With over 20 years of experience establishing digital trust, Sectigo is one of the longest-standing and largest CAs with more than 700,000 customers, including 40% of the Fortune 1000. For more information, visit **www.sectigo.com**.