

Gestión del ciclo de vida de certificados independiente de la CA

Sectigo Certificate Manager funciona con múltiples orígenes de certificados

Muchas empresas trabajan con múltiples Autoridades de Certificación (CA). Existen diversas razones para ello: garantizar la agilidad criptográfica, consolidar los silos tecnológicos existentes, reducir la complejidad del conjunto de herramientas de seguridad, asegurar el cumplimiento normativo y generar un claro ROI.

Muchas empresas trabajan con múltiples Autoridades de Certificación (CA). Existen diversas razones para ello: garantizar la agilidad criptográfica, consolidar los silos tecnológicos existentes, reducir la complejidad del conjunto de herramientas de seguridad, asegurar el cumplimiento normativo y generar un claro ROI.

Sectigo Certificate Manager (SCM), la plataforma de gestión del ciclo de vida de certificados (CLM) líder del mercado, permite la emisión y gestión fluidas de certificados digitales procedentes de CA privadas (como Google Cloud Platform [GCP], AWS Cloud Services, Microsoft Active Directory Certificate Services [ADCS]) y CA públicas de confianza. Esta cobertura se extiende a las plataformas DevOps populares y a las principales integraciones tecnológicas.

Esto permite a los CISO y a sus equipos descubrir, desplegar, instalar y renovar la totalidad de los certificados digitales en el ecosistema empresarial. La plataforma SCM se ha diseñado con la apertura y la interoperabilidad en su núcleo para resolver la falta de integración en la infraestructura de seguridad.



Sectigo automatiza el despliegue de certificados

Sectigo Certificate Manager es agnóstico con respecto a la CA, lo que significa que puede funcionar con una gran variedad de entornos de TI, tipos de certificados digitales, casos de uso y CA. Automatiza la emisión y renovación de todos los certificados digitales desplegados en una empresa mediante estándares abiertos modernos, sin atar a los clientes a un único proveedor.

¿Cómo funciona?

CA Públicas

Para las CA públicas, los clientes tienen acceso a API que facilitan la emisión y renovación programática de certificados. Estas API requieren credenciales proporcionadas por las propias CA. SCM incluye un módulo configurable para admitir CA de terceros, donde el cliente puede introducir sus credenciales de API para acceder a la emisión bajo demanda.

El proceso dura solo unos minutos y las credenciales nunca se comparten con Sectigo, garantizando el cumplimiento contractual.

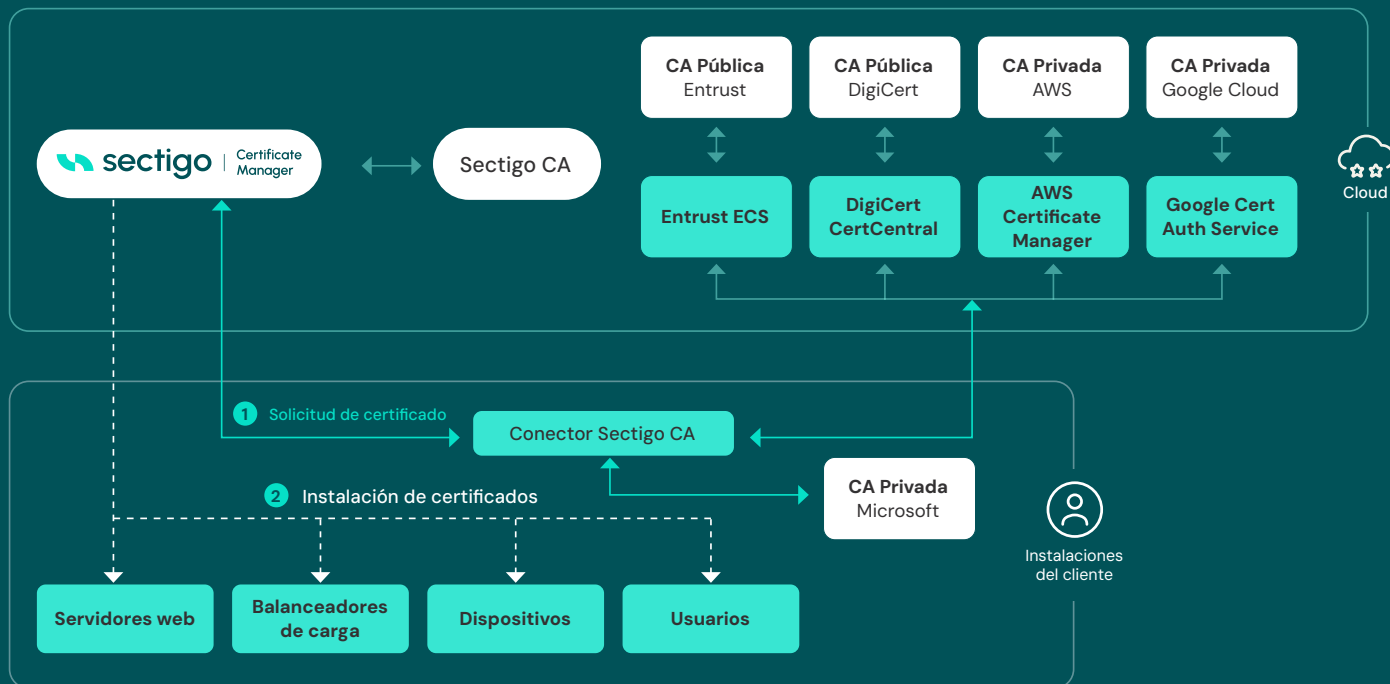
CA Privadas

Una CA privada se utiliza habitualmente para respaldar la infraestructura de autenticación, servidores internos, dispositivos móviles o la firma de código y documentos. Sectigo ofrece una CA privada como opción en SCM. Sin embargo, muchas empresas ya tienen CA privadas establecidas en Microsoft (ADCS), Google Cloud y AWS Cloud. SCM puede emitir y gestionar certificados de estas CA conectándose directamente a su plataforma. El conector de Sectigo se puede configurar para múltiples instancias de estas CA privadas.

Plataforma consolidada

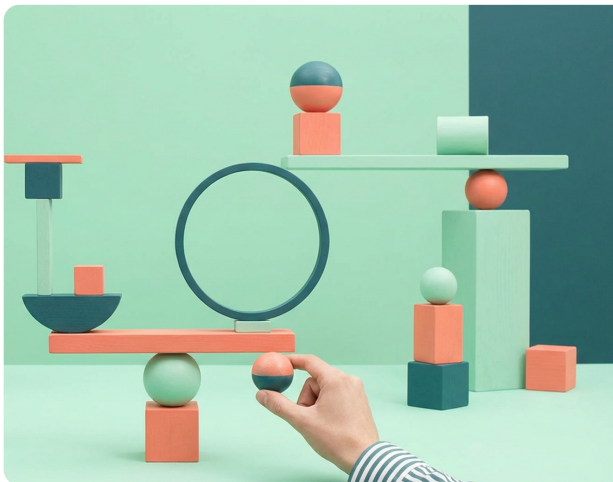
Una vez configuradas las CA, SCM define las directivas de emisión usando la CA pública o privada elegida. Las solicitudes se envían a la CA correspondiente y los certificados se gestionan en SCM para su instalación, renovación, revocación y automatización. Esto ofrece la máxima flexibilidad para seguir emitiendo certificados de otras CA mientras se gestionan desde SCM.

Emisión y renovación de certificados procedentes de otras CA



Principales beneficios de Sectigo Certificate Manager

- ✓ **Control centralizado**
Un panel de control único (single pane of glass) para gestionar certificados públicos y privados de Sectigo o de otras autoridades de certificación.
- ✓ **Fundamentado en la confianza**
Gobernanza de nivel CA, liderazgo en estándares y cumplimiento integrado, respaldados por el papel activo de Sectigo en el CA/Browser Forum, con agilidad criptográfica y preparación poscuántica.
- ✓ **Consolidación de proveedores**
Una plataforma CLM abierta y fácil de desplegar para evitar la dispersión de herramientas y la dependencia de un solo proveedor (vendor lock-in).
- ✓ **Despliegue Zero-Touch**
Funcionalidades avanzadas para instalar automáticamente certificados de usuario y dispositivo con un solo clic.
- ✓ **Gestión de certificados en la nube**
Eficiencia nativa en la nube para reducir costes, acelerar la detección de amenazas y garantizar la seguridad sin perímetro en entornos multicloud.
- ✓ **Integraciones empresariales**
Compatibilidad con los principales proveedores tecnológicos para ofrecer flexibilidad y personalizaciones adaptadas.
- ✓ **Soporte dedicado**
Atención al cliente de primer nivel, desde la incorporación hasta la gestión continua de la cuenta.



El enfoque de Sectigo aporta una visión moderna para asegurar masivamente identidades humanas y de máquinas a gran escala.

Para más información, contacte con su representante comercial o escriba a sales@sectigo.com.

Acerca de Sectigo

Sectigo es un proveedor líder en la gestión del ciclo de vida de certificados (CLM), que ayuda a las organizaciones a asegurar identidades humanas y de máquinas reduciendo los riesgos digitales. Dado que el volumen de certificados aumenta y sus periodos de validez se reducen, los certificados no gestionados generan caídas de servicio e interrupciones operativas. Sectigo utiliza la automatización orquestada para aportar simplicidad a gran escala. Con más de 700.000 clientes y 20 años de experiencia, Sectigo protege al 65 % de las empresas del Fortune 500.

Para obtener más información, visita www.sectigo.com o síguenos en [LinkedIn](#).

