Automatización de PKI para empresas

INFORME DE SECTIGO

SECTIGO®

Las empresas necesitan una solución de autenticación que responda a requisitos cada vez más complejos

Las necesidades de autenticación de las empresas son cada vez más complejas. Las aplicaciones y los datos que se ejecutan en múltiples entornos en la nube, una fuerza de trabajo distribuida y los innovadores dispositivos conectados se entrecruzan de manera que exigen un enfoque de identidad digital seguro para protegerse de las amenazas en constante evolución.

Las empresas confían en los certificados PKI como el estándar de oro para proteger la identidad y como parte fundamental de una arquitectura de Confianza cero y sin contraseñas para las identidades de usuarios, dispositivos, servidores y aplicaciones.

Aunque no existe una solución de autenticación y cifrado más segura y fácil de usar que la identidad digital que proporciona la PKI, el reto para los ocupados equipos de TI es que implementar y gestionar manualmente los certificados lleva mucho tiempo y puede provocar interrupciones innecesarias del servicio. Tanto si una empresa implementa un único certificado SSL para un servidor web como si gestiona millones de certificados en todas sus identidades de usuario y dispositivos de red, el proceso completo de emisión, configuración e implementación de los certificados puede llevar horas por certificado. La gestión manual de los certificados también expone a las empresas a un riesgo significativo de que los certificados se olviden hasta su caducidad y de que se expongan a lagunas en la titularidad, lo que provocaría interrupciones repentinas de los sistemas empresariales críticos.

El coste financiero de la gestión manual de certificados

A medida que los entornos, ya de por sí complejos, se amplían para incluir dispositivos móviles, infraestructura en la nube, DevOps, Internet de las cosas, etc., el coste financiero de la gestión eficaz de los certificados PKI ha aumentado de forma espectacular.

La inversión en seguridad más eficaz es aquella que es fácil de implementar y de utilizar por parte de los empleados. Pero las soluciones de seguridad, como las contraseñas, a menudo suponen una carga para los usuarios individuales a la hora de recordar, actualizar y gestionar su propia seguridad. Y los equipos de TI se ven inundados por solicitudes de restablecimiento de contraseñas que consumen mucho tiempo y por la formación de los empleados para que no entreguen sus contraseñas a sofisticados esquemas de phishing. Por ejemplo, si los empleados no pueden cifrar/descifrar en su dispositivo móvil, simplemente omitirán el uso del cifrado del correo electrónico.

Además, tanto los clientes como los usuarios internos confían en que los sistemas críticos de la empresa estén siempre encendidos. Los certificados caducados ya han provocado numerosas caídas de sitios web y servicios de gran repercusión, lo que ha supuesto una pérdida de ingresos de miles de millones de dólares, sanciones contractuales y demandas judiciales, así como una importante pérdida de reputación de la marca.

Una gestión insuficiente de los certificados también puede poner a las empresas en peligro de incumplimiento de los mandatos normativos. Para protegerse contra el robo de información, normativas como HIPAA/HITECH, RGPD y las reglas de adquisición del gobierno federal de Estados Unidos (DFARS) exigen el cifrado de datos para mitigar o minimizar las consecuencias de un incumplimiento o divulgación accidental. No cumplir con los requisitos de cumplimiento puede dar lugar a multas considerables. Además, el RGPD establece que las multas no solo se basan en la magnitud de una infracción individual, sino también en el nivel de negligencia, por lo que la implementación de una protección sólida en sus sistemas y dispositivos no solo ayuda a reducir el riesgo de un incumplimiento en sí mismo, sino que ayuda a reducir el importe de la multa en caso de que se produzca un incumplimiento.

Los costes administrativos se acumulan rápidamente

La gestión de certificados puede parecer una tarea sencilla y cotidiana para un administrador de TI o de la web, pero garantizar que los certificados sean válidos de uno en uno es costoso. El uso de procesos manuales para detectar, instalar, supervisar y renovar todos los certificados PKI de una organización requiere mucho trabajo y es técnicamente exigente.

Por ejemplo, incluso una instalación manual mínima de un certificado SSL con un único dominio web implica múltiples pasos y puede suponer fácilmente más de 50 dólares por servidor web. En la figura 1 se desglosa cada paso que debe realizar un administrador web para instalar correctamente un único certificado SSL. Para una organización con 2.000 servidores web, se necesitaría una persona trabajando a tiempo completo solo para sustituir los certificados antes de que caduquen.

Figura 1 – Pasos necesarios para instalar manualmente certificados SSL

Pasos	Tiempo
Selección/compra de certificados SSL	De minutos a horas
Inicio de sesión SSH en el servidor web	< 2 minutos - Búsqueda de la dirección del servidor y las credenciales.
Introducir un conjunto de comandos para lograr la validación del control de dominio (para nuevos dominios)	De minutos a horas - Leer la documentación, escribir los comandos adecuados. Los foros de administradores web están llenos de preguntas y respuestas y de resolución de problemas, lo que sugiere que muchos tienen problemas con este paso.
Solicitar la emisión del certificado y descargarlo	Hasta 5 o 10 minutos - Leer la documentación, escribir los comandos apropiados.
Copiar los archivos del certificado en la ubicación apropiada del archivo del servidor (varía según el servidor web)	<2 minutos - Buscar la ubicación del archivo del servidor, escribir los comandos apropiados.
Modificar el archivo de configuración del servidor web para permitir que este utilice el certificado SSL y publique https	De minutos a horas - Leer la documentación, escribir los comandos adecuados, guardar el archivo. Los foros de administradores web están llenos de preguntas y respuestas y de resolución de problemas, lo que sugiere que muchos tienen problemas con este paso.
Refrescar/reiniciar el servidor web para que reconozca la configuración	<1 minuto
Prueba Todos los pasos anteriores deben realizarse con precisión. De lo contrario, se desperdicia tiempo y esfuerzo humano, y los sistemas críticos de la empresa quedarán fuera de servicio.	De minutos a horas - Si no hay mensajes de error, la prueba será rápida. Para responder a los mensajes de error será necesario volver a modificar el archivo de configuración del servidor web.

La evolución criptográfica crea nuevos retos de seguridad en las empresas

A medida que evoluciona la criptografía, ahora las empresas se enfrentan a otra nueva amenaza de seguridad. En unos pocos años, la computación cuántica dejará sin valor los actuales algoritmos de cifrado RSA y ECC de los que dependen nuestros sistemas digitales. Mientras que el NIST y entidades de certificación, como los Quantum Labs de Sectigo, están desarrollando certificados X.509 seguros desde el punto de vista cuántico que utilizan algoritmos de cifrado para resistir a la computación cuántica, está claro que las empresas tendrán que adoptar familias de criptografía totalmente nuevas con una velocidad sin precedentes.

Para una empresa que tenga 10.000 certificados instalados manualmente en usuarios, servidores, dispositivos y aplicaciones, se necesitarían hasta cinco personas durante un año para encontrar y reemplazar todos los certificados. Antes de que lo hagan, el delincuente aprovechará la débil criptografía para hacerse pasar por el propietario legítimo o descifrar información sensible.

La empresa moderna necesita soluciones automatizadas

Con los escollos y las ramificaciones financieras inherentes a la gestión manual de los certificados PKI, el rendimiento de la inversión en la gestión automatizada del ciclo de vida de los certificados es evidente. Los profesionales de TI deben replantearse su estrategia de gestión del ciclo de vida de los certificados. Especialmente a medida que las empresas salen al mercado más rápidamente con nuevos servicios habilitados por DevOps, las organizaciones necesitan una solución automatizada que garantice que los certificados se configuran e implementan correctamente sin intervención humana. Esta automatización no solo elimina las interrupciones del servicio, sino que permite a los departamentos de TI controlar los costes operativos y lanzar los servicios al mercado más rápidamente.

Recientemente, la PKI ha evolucionado para ser aún más versátil. La interoperabilidad, el alto tiempo de actividad y la gobernanza siguen siendo beneficios clave. Pero las soluciones actuales de PKI también son funcionalmente capaces de mejorar la administración y la gestión del ciclo de vida de los certificados a través de:

Automatización

Acelerar la implementación de certificados eliminando costes y errores

Escalabilidad

Gestión de certificados que se cuentan por cientos, miles o incluso millones

Criptoagilidad

Actualización de la fortaleza criptográfica y revocación y sustitución de los certificados en riesgo por certificados seguros de quantum muy rápidamente en respuesta a amenazas nuevas o cambiantes

Visibilidad

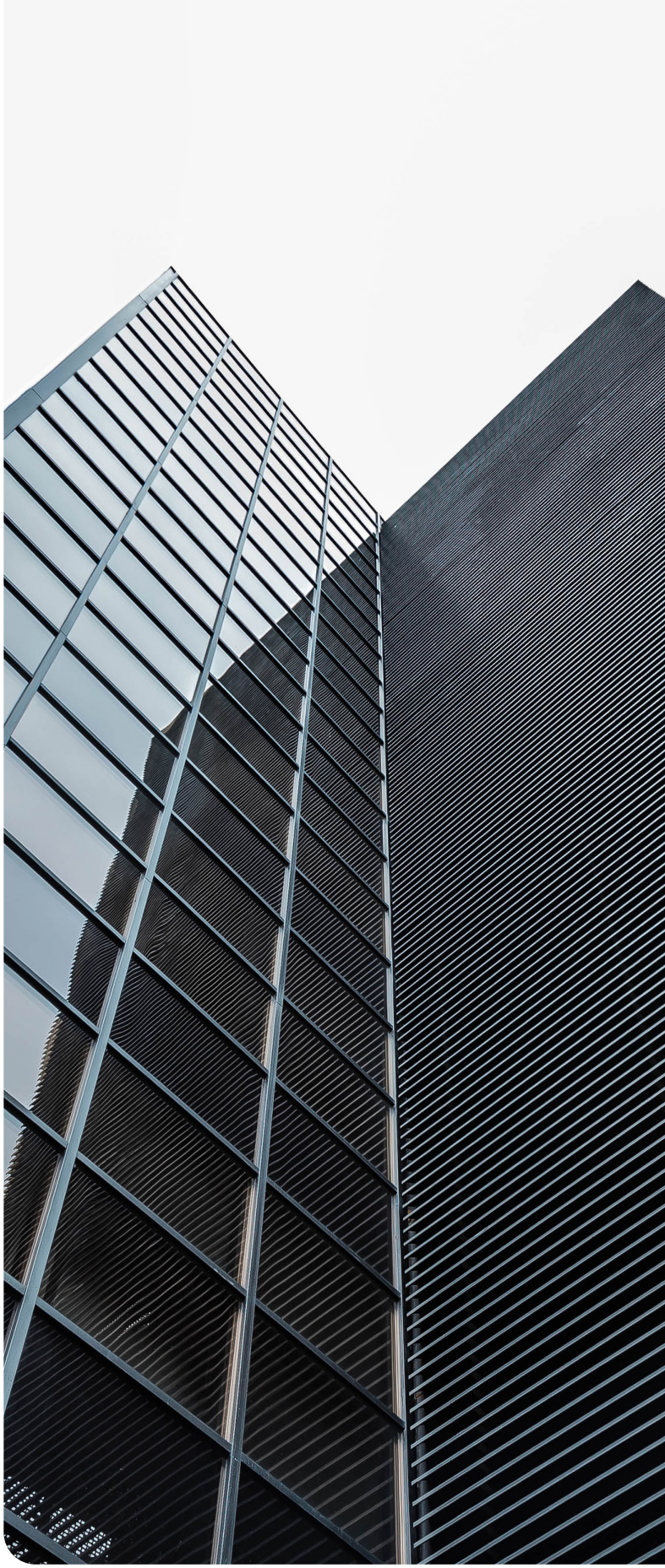
Ver el estado de los certificados de todos los usuarios, dispositivos, servidores y aplicaciones en un solo panel

Ahorre tiempo y mantenga el control con la Automatización de PKI de Sectigo

Dada la disparidad de sistemas, aplicaciones y dispositivos que utilizan certificados digitales, los equipos de TI a menudo gestionan distintos servicios de automatización de muchos proveedores diferentes, con diferentes interfaces de usuario y calidad de soporte. Un único panel de gestión de certificados que automatice la detección, la implementación y la gestión del ciclo de vida en todos los casos de uso y plataformas de proveedores crea la eficiencia que promete la automatización. Y los equipos de TI siguen manteniendo el control de las definiciones y reglas de configuración para que los pasos de la automatización se realicen correctamente.

Sectigo proporciona soluciones de automatización de certificados que permiten a las empresas ser ágiles y eficientes, y mantener el control de todos los certificados en su entorno. Sectigo soporta la instalación, revocación y renovación automatizadas de certificados SSL/TLS y no de SSL a través de protocolos estándar de la industria, API e integraciones de terceros.

Además, con Sectigo, nunca se encontrará con un límite de volumen de certificados, como podría ocurrir con las alternativas de código abierto. Las soluciones de automatización de Sectigo permiten que su equipo de seguridad aplique fácilmente la política de seguridad criptográfica, proteja las comunicaciones, evite la pérdida de datos a través de accesos no autorizados y proteja los sistemas, aplicaciones y dispositivos de toda la empresa.



Automatización de la gestión de certificados SSL/TLS

Para los certificados SSL/TLS, Sectigo proporciona una gestión automatizada de certificados a través de:

- **Soporte para el protocolo de entorno de gestión automática de certificados (Automated Certificate Management Environment, ACME):** El Gestor de certificados de Sectigo soporta el protocolo ACME, permitiéndole automatizar la emisión, instalación y revocación de certificados para una amplia gama de servidores web y equilibradores de carga. El protocolo ACME requiere muy poco tiempo para que los equipos de TI configuren y ejecuten su automatización de gestión de certificados, convirtiéndolo en un componente cada vez más adoptado en la seguridad empresarial.

Sectigo admite los tipos de certificados SSL DV, OV, EV y privados a través de ACME y proporciona un control total a los administradores de TI. Sectigo proporciona el servidor ACME y trabaja con clientes conformes al ACME, incluido Certbot de la Electronic Frontier Foundation (de la que Sectigo es patrocinador). Consulte la Figura 2 para ver cómo funciona la autenticación de certificados mediante ACME.

Cómo funciona el protocolo ACME para la gestión automatizada de certificados PKI

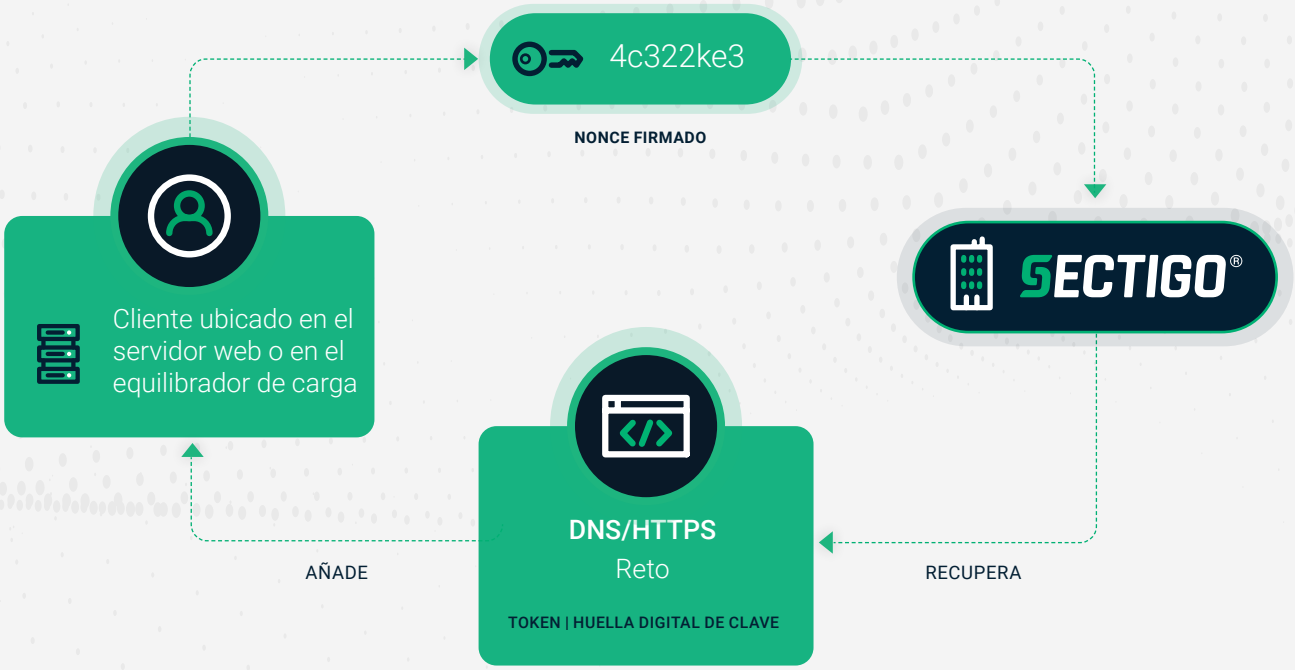


Figura 2 – Proceso de autenticación mediante el protocolo ACME

Automatización de la gestión de certificados SSL/TLS

- **API REST:** En algunos casos, las empresas prefieren integrar las aplicaciones con Sectigo utilizando la API REST de Sectigo. Si bien esto requiere un desarrollo adicional en el lado de la aplicación, le permite aprovechar la gestión de certificados y personalizar su flujo de trabajo.

  Además, a través de la API REST, Sectigo tiene integraciones directas con todos los entornos de herramientas de automatización y creación de contenedores líderes, como Docker, Chef, Ansible, Salt Stack, Terraform, Puppet y Jenkins. También incluimos mecanismos para incorporar PKI en el proceso de integración e implementación continuos (CI/CD), marcos de orquestación como Kubernetes y almacenes de claves de terceros, como Vault de HashiCorp.

- **Un agente de instalación automatizada en las instalaciones del cliente:** Utilizando el Agente de red de Sectigo, puede automatizar la gestión de certificados para una variedad de sistemas, incluidos los servidores web Apache, Tomcat, IIS y F5. El Agente de red en las instalaciones del cliente está integrado con el Gestor de certificados de Sectigo para programar la emisión, instalación y renovación de certificados.
- **Integración con proveedores externos:** Sectigo se integra directamente con proveedores externos líderes para ayudar a los clientes a lograr una automatización completa de los certificados utilizando tecnologías populares ya existentes en los entornos de TI, como el equilibrador de carga Big-IP de F5, el controlador de entrega de aplicaciones ADC de Citrix y la plataforma de flujo de trabajo de TI de ServiceNow.

  Consulte la Figura 3 para ver una lista de las plataformas y tecnologías admitidas actualmente.

Figura 3 – Soluciones de automatización admitidas actualmente para certificados SSL/TLS

Herramientas de servidor web/equipo de red/DevOps		Elección del cliente			
Tipo	**Plataforma**	**Agente de instalación de Sectigo**	**ACME**	**API REST de Sectigo**	**Integración personalizada**
Servidor web	Servidor HTTP Apache	Sí	Sí	Disponible	
	Apache Tomcat	Sí	Sí	Disponible	
	IIS	Sí	Sí	Disponible	
	NGINX		Sí	Disponible	
	Otros servidores web compatibles con Certbot		Sí	Disponible	
Equilibrador de carga	F5	Sí	Sí	Disponible	Sí
	Citrix ADC (antes NetScaler)		Sí	Disponible	Sí
Gestión de servicio de TI	ServiceNow			Disponible	Sí
Herramientas de DevOps	Ansible			Disponible	
	AWS ELB		Sí	Disponible	
	Chef			Disponible	
	Docker			Disponible	
	HashiCorp Vault			Disponible	
	Jenkins			Disponible	
	Kubernetes		Sí	Disponible	
	Puppet			Disponible	
	SaltStack			Disponible	
	Terraform			Disponible	

Automatización de la instalación de certificados no SSL

Muchos sistemas, aplicaciones y dispositivos utilizan certificados no SSL como, por ejemplo, los certificados de identidad para dispositivos móviles. Para la instalación de certificados no SSL, Sectigo proporciona:

- **Protocolo Enrollment over Secure Transport (EST):** Sectigo soporta el protocolo EST, que se utiliza para gestionar equipos de red de muchos proveedores. De hecho, varios proveedores tienen soporte EST ya incorporado. EST también es popular en entornos de Internet de las Cosas (IoT) dada la eficiencia del protocolo y el soporte de claves de criptografía de curva elíptica (ECC). Sectigo ofrece un cliente EST comercial y también soporta varios clientes EST de código abierto disponibles.
- **Protocolo Simple Certificate Enrollment (SCEP):** El protocolo SCEP existe desde hace casi dos décadas y ha ganado una gran popularidad entre las empresas. Como el protocolo SCEP no tiene cuotas de licencia y requiere muy poco tiempo para que los equipos de TI lo configuren y ejecuten, se ha convertido en un componente casi omnipresente de la seguridad empresarial. Los sistemas de gestión de dispositivos móviles (MDM), como Microsoft Intune y AirWatch, utilizan SCEP para la inscripción de certificados PKI. Esto permite a los dispositivos móviles sustituir la contraseña de Wi-Fi y autenticarse para VPN. La mayoría de los equipos de red, incluidos los routers, los equilibradores de carga, los concentradores Wi-Fi, los dispositivos VPN y los cortafuegos, también admiten el protocolo SCEP para la inscripción de certificados.

Figura 4 – SCM utiliza SCEP para transferir los certificados al MDM que los instala en el dispositivo móvil

En el entorno de Sectigo, se puede utilizar SCEP para inscribir certificados en Linux, MacOS y otros sistemas operativos.

- **Agente de Microsoft:** Un servidor proxy de Sectigo puede situarse entre el escritorio de Microsoft y el servicio de certificados de Active Directory. Intercepta las solicitudes de certificados realizadas a través del protocolo de inscripción de certificados de clientes de Windows (WCCE) y proporciona automáticamente el certificado al escritorio sin la intervención de ningún empleado.
- **Gestor de certificados móviles de Sectigo (MCM):** El MCM de Sectigo emite y gestiona certificados y claves en dispositivos móviles iOS, Chrome OS y Android con poca o ninguna intervención del usuario. Admite todos los tipos de certificados y es interoperable con todos los dispositivos, sistemas operativos y protocolos de inscripción principales. Sectigo utiliza un MDM integrado en nuestro Gestor de certificados o un enfoque de portal web de autoservicio, dependiendo de los requisitos del cliente.

Automatización de la instalación de certificados emitidos por ADCS

Mediante el servicio de certificados de Active Directory (ADCS) de Microsoft, los administradores de TI pueden ordenar a todos los equipos de escritorio y servidores que inscriban y renueven automáticamente los certificados emitidos por los servicios de certificados de Active Directory. Pero esta automatización solo se aplica a las aplicaciones que utilizan un sistema operativo Windows. Las empresas actuales tienen dispositivos que no utilizan sistemas operativos de Microsoft, lo que significa que el administrador y el empleado comparten la carga de renovar e instalar manualmente los certificados para cualquier aplicación o dispositivo que no sea de Microsoft. Para estos certificados, los administradores suelen emplear un método propenso a errores que utiliza hojas de cálculo para realizar un seguimiento manual de cuándo se emitieron los certificados, dónde se instalaron, su intensidad criptográfica, cuándo caducan y quién es responsable de ellos.

Sectigo ofrece estas opciones:

- Seguir utilizando ADCS como su CA raíz, establecer Sectigo como la CA que emite los certificados y los instala automáticamente en el dispositivo o aplicación. La empresa no necesita volver a incrustar la CA raíz.
- Seguir utilizando ADCS como la CA que emite los certificados. El gestor de certificados de Sectigo detectará los certificados emitidos por ADCS, informará sobre los atributos/propiedad de los certificados y enviará notificaciones antes de su vencimiento.
- Sustituir tanto la CA raíz como la CA emisora de ADCS por la CA de Sectigo. Esto elimina el costo de utilizar ADCS, a la vez que se automatiza completamente la emisión e instalación de certificados.

ADCS no puede instalar automáticamente los certificados para muchos casos de uso común en la empresa, incluidos:

- Servidores web
- Dispositivos móviles Apple, Android, Chromebook, sin un sistema de gestión móvil
- Almacén de claves de Azure
- Identidades de personas o dispositivos que no están en Microsoft Active Directory
- Equilibradores de carga
- Equipos de red
- Firma de código
- Contenedores de DevOps
- Autenticación de administradores de servidores mediante SSH
- Extensiones seguras multipropósito al correo de Internet (S/MIME) de confianza pública
- Firma de documentos de confianza mediante Adobe Reader, Adobe Sign
- Dispositivos del Internet de las cosas
- Posibilidad de suministrar el mismo historial de claves de cifrado a todos los dispositivos del mismo usuario

El Gestor de certificados de Sectigo aumenta el ADCS automatizando la instalación de certificados, eliminando la necesidad de una gestión manual costosa y propensa a errores. El Gestor de certificados garantiza que los certificados de la empresa se gestionen adecuadamente y no caduquen de forma inesperada.

Conclusión: Gane tranquilidad automatizando la PKI con Sectigo

PKI es la mejor tecnología para eliminar las contraseñas y garantizar que solo los dispositivos y usuarios autorizados accedan a los sistemas de la empresa.

Sectigo fue pionero en SSL y tecnologías relacionadas y ahora es un líder mundial en PKI. Sectigo continúa invirtiendo en nuevas tecnologías, estándares y soluciones para permanecer a la vanguardia de la seguridad, y proteger su negocio de las amenazas digitales.

Con Sectigo, obtiene más:

Elección

Con la filosofía central de Sectigo en torno a la interoperabilidad y el uso de estándares abiertos como ACME, SCEP y EST como nuestra base, puede estar seguro de que tendrá un amplio grado de elección y control sobre su solución de PKI. Y si algo va mal, tiene un único punto de contacto 24/7.

Facilidad de uso

A diferencia de otras empresas, Sectigo se centra en la identidad digital, como CA pública y como proveedor líder de PKI privada. Al aprovechar nuestra automatización de la implementación de certificados y las tecnologías de gestión/informes de panel único para centralizar y simplificar las tediosas tareas asociadas a la gestión del ciclo de vida de los certificados, podrá liberar a su equipo para que se centre en tareas de mayor valor.

Valor

Bajo el modelo de licencias de Sectigo, no cobramos por emisión, sino por uso. Los certificados que ya no están en uso (por ejemplo, cuando alguien deja su compañía) se pueden transferir.

A prueba de futuro

Sectigo es la CA comercial líder en el mundo y estamos invirtiendo constantemente en nuevas tecnologías y soluciones. Cuando se asocia con nosotros, puede estar seguro de que su empresa permanecerá a la vanguardia de la criptografía a medida que sus necesidades cambien y aumenten. Nuestras tecnologías automatizadas garantizarán la agilidad criptográfica para ajustarse a los avances en las técnicas informáticas y criptográficas que requieren actualizaciones de sus algoritmos de hashing y cifrado.

Tranquilidad

Todo esto lleva a una mayor tranquilidad. Sectigo cumple con WebTrust y SOC 3, y nuestras conexiones con el CA/Browser Forum y entidades gubernamentales selectas ayudan a asegurar que recibimos alertas tempranas sobre problemas de seguridad de PKI. Además, nuestro enfoque de código abierto ayuda a reducir las vulnerabilidades de seguridad. Con el tamaño, la escala, el liderazgo y la inversión continua en PKI de Sectigo, no hay mejor socio para proteger la base de su infraestructura digital.

Sectigo es un líder en tecnología de ciberseguridad que proporciona soluciones de identidad digital, incluidos certificados TLS/SSL, seguridad web, DevOps, IoT y gestión de PKI de nivel empresarial. Como la mayor entidad de certificación comercial del mundo, con más de 700.000 clientes en todo el mundo y 20 años de experiencia en la entrega de soluciones de confianza en línea, Sectigo proporciona soluciones de confianza públicas y privadas probadas para proteger servidores web, identidades digitales, dispositivos conectados y aplicaciones. Reconocida por sus galardonadas innovaciones y por el mejor soporte al cliente a nivel mundial, Sectigo ofrece las tecnologías necesarias para proteger los panoramas digitales de hoy y del futuro.

Para obtener más información, visite www.sectigo.com y síganos en @SectigoHQ

SECTIGO®