ManageEngine
Key Manager Plus

Gestión de certificados 101

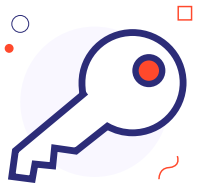
La gestión de certificados es el proceso de monitoreo y gestión de los ciclos de vida de todos los certificados SSL/TLS implementados dentro de una red, desde la adquisición y la implementación hasta la supervisión de la renovación, el uso y el vencimiento. Este proceso da a los administradores de TI una visibilidad y control completos sobre sus entornos de SSL/TLS y los ayuda a evitar brechas de seguridad, interrupciones y problemas de cumplimiento.

Antes de entender por qué la gestión de los certificados de SSL/TLS debe ser un componente integral de la estrategia de seguridad de TI de su organización y cómo generar un programa para la gestión de certificados empresarial. Demos un vistazo a cómo los certificados mantienen seguras las comunicaciones en línea.

Certificados de SSL y su rol en la protección de las comunicaciones en línea.

Un certificado SSL, también conocido como un certificado de clave pública, es un documento electrónico que verifica si una clave pública efectivamente pertenece a una persona. Cuando los propietarios del sitio instalan certificados de SSL en sus servidores web, todo el tráfico entre sus servidores y los navegadores de los usuarios se codifica, lo que garantiza la confidencialidad de la información intercambiada. El protocolo de aplicación HTTP cambia automáticamente a HTTPS en la omnibox del navegador y aparece un ícono de un candado que indica que todas las conexiones al sitio web permanecen como privadas.

Usted puede ver el certificado SSL de cualquier sitio web que se ejecuta en HTTPS y encontrará la siguiente información:



Clave pública: muestra detalles de qué clave pública y algoritmo criptográfico se usan para firmar el certificado.

Identidad del propietario del sitio: identifica el propietario del sitio que ha instalado el certificado en su sitio web.

Firma digital: muestra la firma de un tercero de confianza que autoriza la legitimidad de la identidad del propietario del sitio y de su sitio web.

Generalmente, las entidades llamadas Autoridades de Certificación (CA) firman y emiten los certificados SSL. Estas son organizaciones externas que desempeñan un rol fundamental en la seguridad de internet al actuar como el epítome de la confianza para ambas partes: los propietarios de los sitios compran certificados SSL para ganar la confianza de sus clientes y los visitantes de los sitios confían en SSL para garantizar la privacidad de sus datos. Las compañías de navegadores confían solo en aquellos certificados SSL emitidos por CA reconocidas internacionalmente y mostrarán mensajes de error cuando se conecten a sitios web que usen certificados SSL generados localmente.

¿Cómo funcionan los certificados SSL?

Cuando los navegadores intentan establecer una sesión codificada con un sitio web protegido con SSL, se da la siguiente secuencia de operaciones en segundo plano:

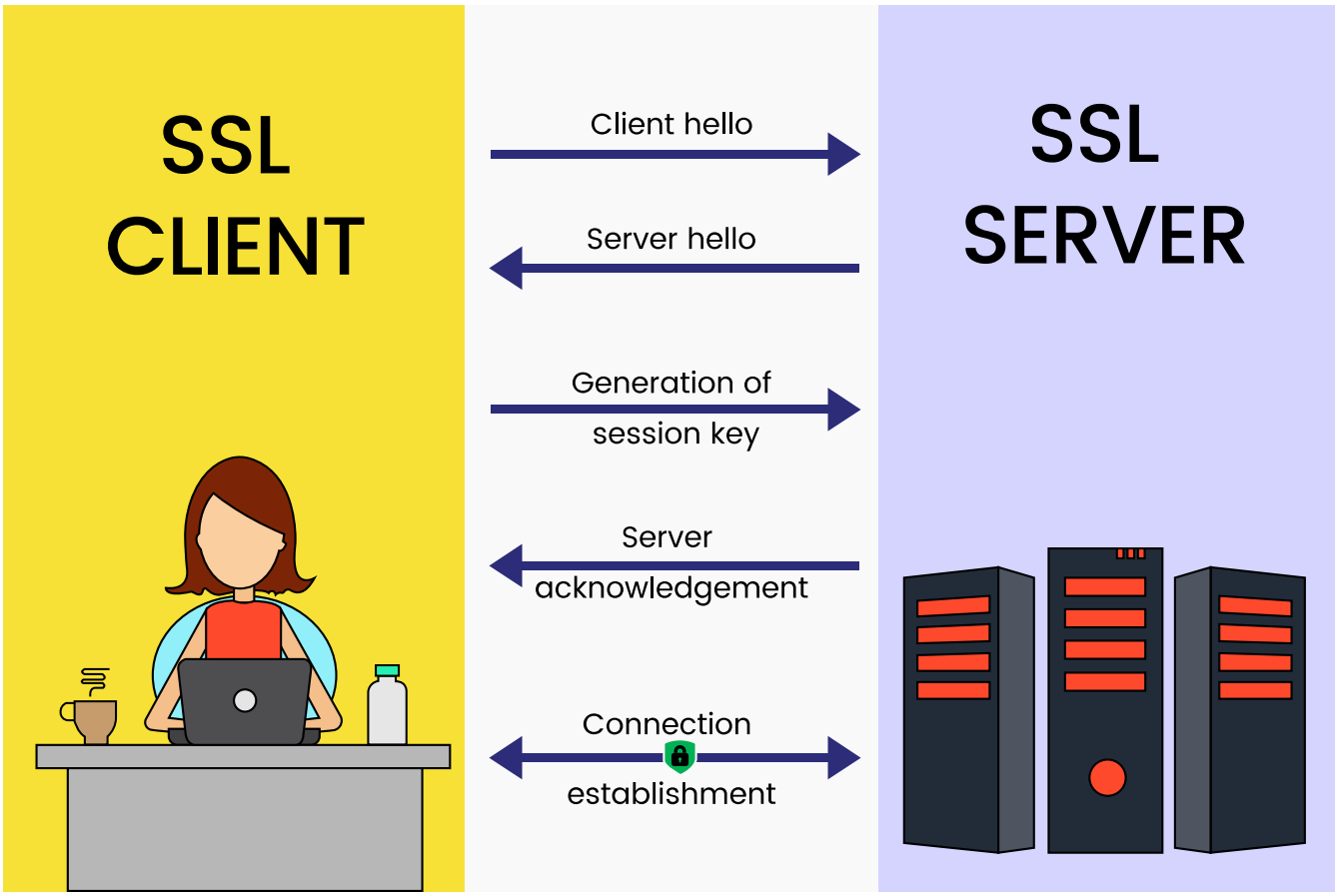
1. El navegador se conecta con un servidor web protegido con SSL y solicita al servidor comprobar su identidad.

2. El servidor web recibe la solicitud y envía de vuelta una copia de su certificado SSL junto con su clave pública.

3. El navegador recibe el certificado y verifica su legitimidad al compararla con una lista predefinida de CA de confianza. Si el navegador confía en el certificado, crea una clave simétrica llamada clave de sesión, codifica la clave usando la clave pública del servidor y la envía de vuelta al servidor.

4. El servidor web decodifica el mensaje con su clave privada, envía un reconocimiento, que se codifica con la clave de sesión, de vuelta al navegador para iniciar la sesión.

5. El navegador y el servidor empiezan entonces la sesión, en la cual toda la información intercambiada se codifica con la clave de la sesión.

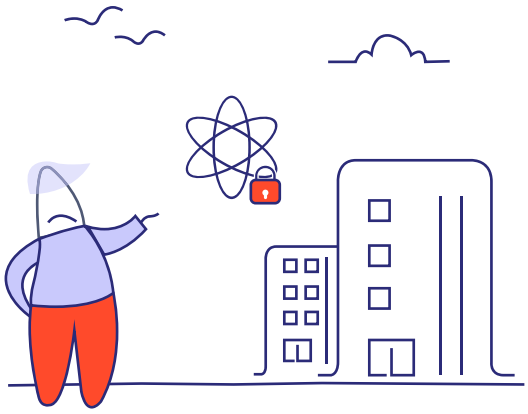


No obstante, implementar la codificación SSL para sitios web no es un proceso de una única vez. Los certificados SSL vencen después de un periodo definido y deben renovarse constantemente. No renovarlos hará que los navegadores pierdan confianza en la legitimidad de dicho sitio web, lo que se evidencia en mensajes de error. El peor caso es que los certificados vencidos también abran paso a brechas de seguridad. Por tanto, las organizaciones necesitan vigilar los ciclos de vida de todos los certificados implementados dentro de la red y monitorear constantemente su uso para evitar cualquier oportunidad de que se produzcan violaciones de datos o interrupciones de los sitios web.

Estado actual de la gestión de certificados en la TI empresarial*

61% de las empresas están implementando más claves y certificados debido al tiempo de vida reducido

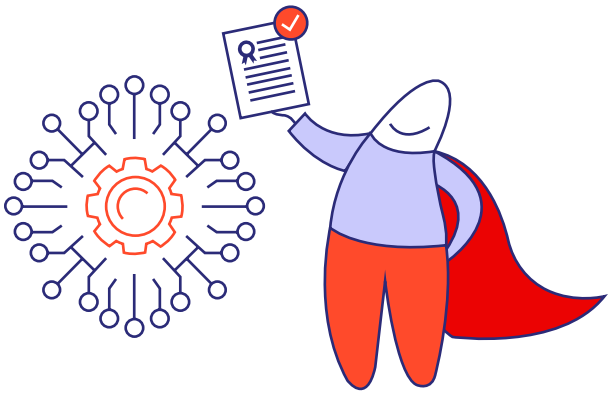
60% de las empresas no tienen una estrategia criptográfica empresarial para implementar claves y certificados

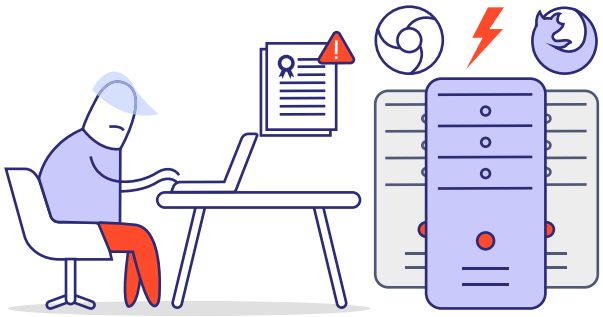


51% de las empresas consideran la agilidad criptográfica como una prioridad estratégica principal para la seguridad

* Estado de la gestión de la identidad de equipos, Ponemon Institute, 2021

82% de las organizaciones sienten que los certificados SSL/TLS son la identidad de equipos más crucial





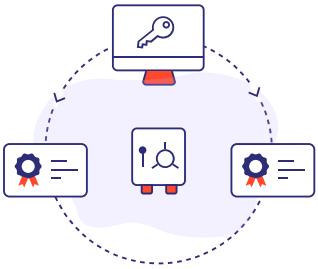
41% de las compañías experimentan 4 o más interrupciones de servicios debido a certificados vencidos en los últimos 24 meses.

Evite dudas en la gestión de certificados SSL/TLS

Con la transformación digital y la adopción de la nube para casi todas las industrias, las organizaciones son testigos de un despilfarro de certificados en sus redes. Además, las comunidades de navegadores se mueven cada vez más hacia certificados de corta duración en un intento de mejorar la seguridad base de los servicios en línea. Estos factores han dejado a los administradores de TI con la enorme responsabilidad de supervisar el ciclo de vida de todo certificado de seguridad implementado dentro de su red, monitoreando estos certificados en busca de cualquier actividad inusual y renovándolos antes de su vencimiento. Esto es muy abrumador, especialmente para las organizaciones grandes que deben manejar una gran cantidad de certificados. Lo que necesitan los administradores de TI es una plataforma centralizada que pueda automatizar las operaciones de la gestión de certificados y dar información sobre el entorno SSL de una organización. He aquí algunas de las muchas ventajas de implementar una solución para la gestión centralizada de certificados:

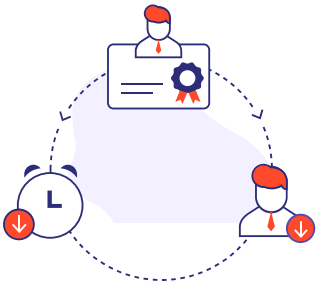
1. Alertas oportunas para evitar interrupciones y proteger la reputación de la marca.

En ocasiones, las organizaciones permiten que por accidente se venzan un par de certificados. Pero un certificado SSL vencido es todo lo que se necesita para que los visitantes pierdan la confianza en la credibilidad de la marca. Al implementar una solución para la gestión centralizada de certificados se alerta a los administradores cuando un certificado está por vencer y se reduce la posibilidad de interrupciones en el sitio web debido al vencimiento inesperado de certificados.



2. Inventario centralizado y aumento de la transparencia.

Con frecuencia los equipos solicitan e implementan certificados SSL localmente, según se necesiten, pero luego se olvidan de su existencia. La gestión centralizada consolida todos los certificados de una organización en un solo repositorio y optimiza los procesos de adquisición, implementación y renovación. Esto da a los administradores transparencia y control completos sobre sus entornos de SSL.

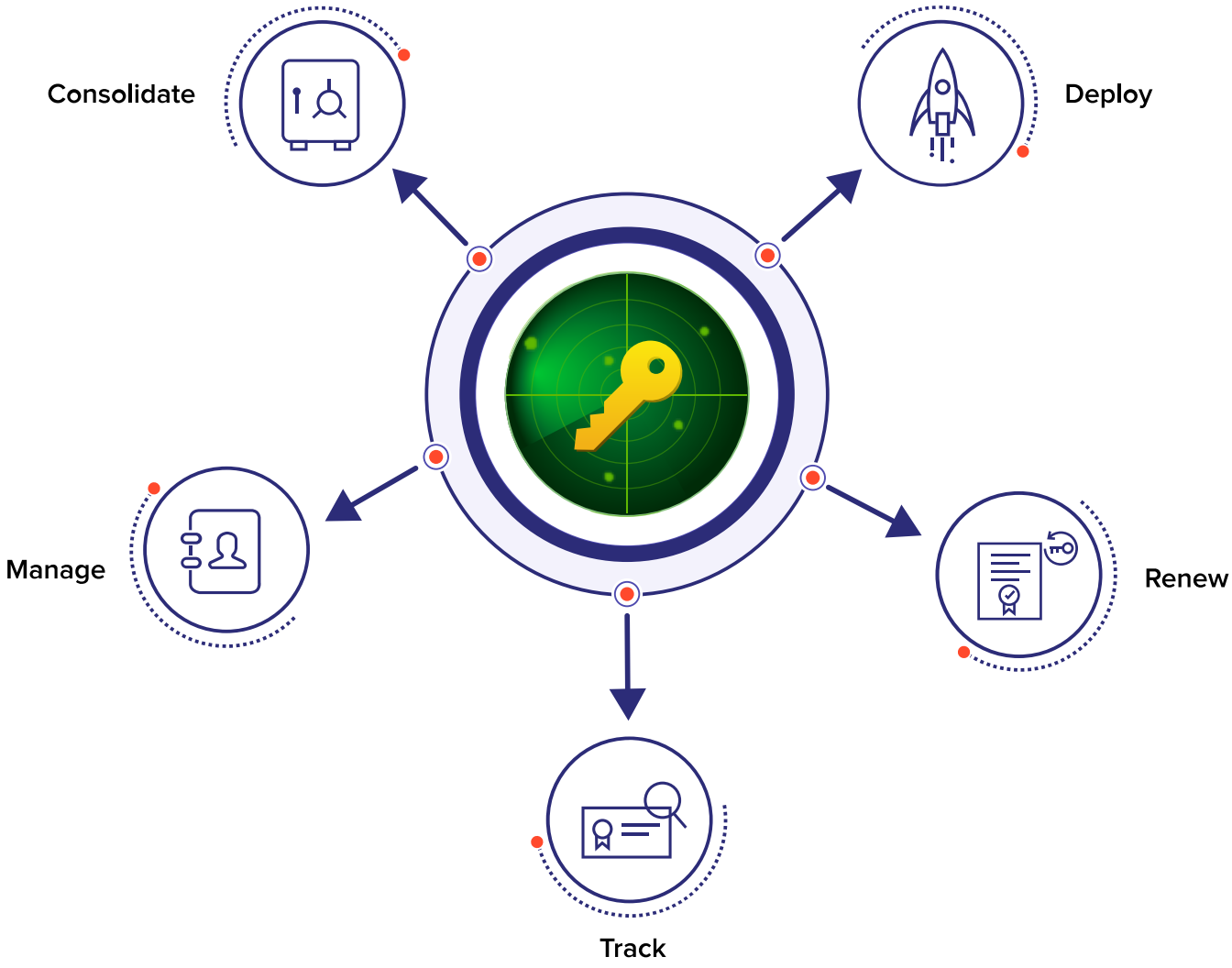


3. Reducción del tiempo y el esfuerzo.

Sobre todo, centralizar y automatizar la gestión de certificados reduce significativamente los costos operativos y el tiempo que el personal dedica a la gestión de certificados individuales.

Elimine el agotamiento relacionado con los certificados al centralizar la gestión de los ciclos de vida con Key Manager Plus.

Key Manager Plus, nuestra solución web para la gestión de claves y certificados, da a los administradores la visibilidad y control tan necesarios sobre su entorno SSL. Centraliza y automatiza las operaciones relacionadas con la gestión de los ciclos de vida de los certificados y ayuda a evitar ataques de seguridad, problemas de cumplimiento e interrupciones en el sitio debido a vencimientos inesperados de los certificados. He aquí un resumen rápido de las funciones de Key Manager Plus:



- Descubrimiento e inventario centralizados de certificados SSL
- Herramienta integrada para la generación de CSR
- Optimización del flujo de trabajo para solicitudes de certificados
- Gestión del ciclo de vida de extremo a extremo mediante integraciones de CA externas
- Integraciones de Active Directory y MS Store
- Informes instantáneos e integrales sobre todas las operaciones de gestión de certificados
- Vista de dashboard intuitivo

Obtenga visibilidad y control completos sobre su entorno SSL/TLS

Programe una demo personalizada

www.keymanagerplus.com

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.keymanagerplus.com

ManageEngine
Key Manager Plus