Guía definitiva para la gestión de certificados

Prácticas recomendadas para administradores de SSL/TLS que gestionen cientos o miles de certificados

digicert®

Índice

Introducción

Una correcta gestión de los certificados pasa por garantizar que ningún certificado se quede en el limbo. Los certificados caducados u olvidados provocan problemas de seguridad y pérdidas económicas. Para las grandes empresas, el costo medio de cada fallo provocado por problemas con los certificados es de 15 millones de dólares[1]. Su seguridad y reputación también pueden verse afectadas, con la consiguiente pérdida de ventas y confianza de los clientes.

Es posible que usted se encargue de las tareas necesarias para mantener una infraestructura de clave pública (PKI): gestionar los certificados, aplicar las prácticas recomendadas de SSL y garantizar que se aprueben con rapidez, entre otras.

Uno de los principales problemas de este rol es la continua preocupación de que en algún lugar de su red pueda haber un certificado que haya pasado inadvertido en una exploración; algún día se producirá un fallo en un servidor y no será nada fácil hacer limpieza.

¿Qué le parecería disponer de una macrolista de comprobación para gestionar los certificados? Un sistema que le permitiera centrarse solo en las partes más importantes del ciclo de vida de los certificados, es decir, las que son imprescindibles para la seguridad de la red.

No todas las empresas necesitan la misma lista de comprobación, porque cada red tiene sus propias complejidades. Sin embargo, todo administrador de certificados debe encargarse de determinadas tareas para garantizar que los datos, los empleados y la empresa estén protegidos.

En esta guía descubrirá todo lo que se debe tener en cuenta para gestionar los certificados con la máxima eficiencia. Aprenderá a controlar todos los aspectos del ciclo de vida de los certificados, sacar el máximo provecho de las API y optimizar su equipo de colaboradores.

Prácticas recomendadas para controlar la gestión de PKI

Gestionar los diferentes componentes de una PKI, como la autoridad de certificación, la autoridad de registro, las políticas de certificados y el sistema de gestión de certificados, puede ser estresante. Implementar los certificados no tiene por qué ser difícil, pero para garantizar la seguridad es fundamental hacerlo bien y gestionarlos correctamente.

Los administradores de SSL que trabajan en grandes empresas gestionan miles (o incluso millones) de certificados. ¿Cómo garantizar que se implementan y gestionan de forma correcta en todo momento?

El reto es mantener el control, y la solución pasa por aplicar las prácticas recomendadas, con las que podrá aumentar la vigilancia y ahorrar tiempo y trabajo.

Siguiendo estas prácticas, dejará de pensar en los certificados las 24 horas del día y tendrá la tranquilidad de saber que su red está protegida.

Práctica recomendada: Usar una plataforma de gestión de PKI

Con las soluciones de Managed PKI (MPKI), las empresas pueden solicitar y gestionar certificados sin el costo de tener que mantener una autoridad de certificación (CA) propia. Muchas CA públicas ofrecen una solución Managed PKI y la mayoría de las grandes empresas la eligen porque es económica, entre otros motivos.

Con una solución MPKI, la mayor parte del trabajo de mantenimiento de una PKI se traslada a la CA, pero sin renunciar a las ventajas de utilizar los certificados para garantizar la seguridad.

[1] «2015 Cost of Failed Trust Report: When Trust Online Breaks, Businesses Lose Customers». Fecha de acceso: 26 de junio de 2017. https://www.venafi.com/assets/pdf/wp/Ponemon-When-Trust-Online-Breaks-Businesses-Lose-Customers-white-paper.pdf

Mejor aún, con una plataforma de MPKI se simplifican todos los aspectos de la gestión del ciclo de vida de los certificados, como la emisión, inspección, recuperación y renovación.

En general, una MPKI ahorra tiempo y facilita el control de datos importantes de los certificados, como:

- fechas de caducidad,
- errores de puntos externos SSL,
- solicitudes de certificados de miembros del equipo,
- estado en caso de revocación,
- CA emisora.

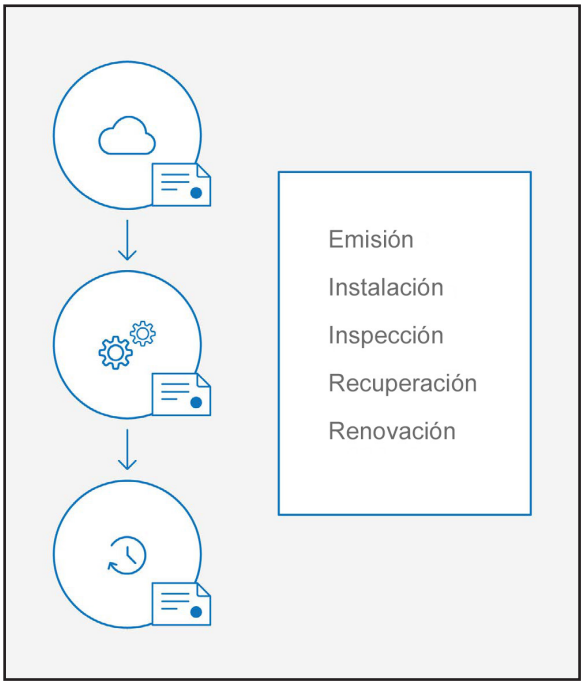
Hasta hace unos años, la mayoría de las empresas gestionaban los certificados manualmente con hojas de cálculo. TechTarget afirma —y más de uno le dará la razón por experiencia propia— que «esto puede provocar errores y dar lugar a certificados perdidos, incompatibles o mal etiquetados»[2].

Con una plataforma de MPKI se evita la necesidad de consignar los datos de los certificados en una hoja de cálculo y rebuscar las solicitudes en el correo electrónico, porque al automatizar estos factores se reduce la posibilidad de cometer errores. La gestión de los certificados se simplifica y se ahorra tiempo.

Práctica recomendada: Empezar a automatizar con las API

Las API eliminan obstáculos entre empresas y permiten a los desarrolladores utilizar diferentes tecnologías para crear aplicaciones. Concretamente, aligeran la carga de los departamentos informáticos que necesitan automatizar y personalizar las funciones de gestión de certificados.

LAS PLATAFORMAS DE MPKI SIMPLIFICAN LA GESTIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS



Es posible que las empresas de menor tamaño utilicen sin problemas la GUI de la herramienta de gestión de SSL, pero las empresas más grandes necesitan personalizarla. Algunas herramientas de gestión de PKI le darán acceso a una API con la que podrá personalizar funciones y flujos de trabajo y automatizar procesos para implementar una gestión de certificados más autónoma. Por medio de una API se puede personalizar totalmente la gestión de SSL.

[2] Shapland, R. «SSL certificate management: Avoiding costly mistakes». Fecha de acceso: 26 de junio de 2017. http://searchsecurity.techtarget.com/tip/SSL-certificate-management-Common-mistakes-and-how-to-avoid-them

Esto permite supervisar miles, o incluso millones, de dispositivos, en función del sector. La automatización simplifica el trabajo y garantiza la seguridad porque reduce los errores manuales y los fallos provocados por los certificados.

Con una API puede ahorrar tiempo y automatizar muchos procesos en el ciclo de vida de los certificados SSL, como los siguientes:

- solicitar certificados,
- aprobar solicitudes,
- rechazar solicitudes,
- descargar certificados,
- renovar certificados,
- revocar certificados,
- volver a emitir certificados.

Debido a los cambios en las normativas y a periodos de validez cada vez más reducidos, en el futuro la automatización de los certificados SSL no será optativa, sino una necesidad.

Utilizando una API se reducen las dificultades que conlleva gestionar los certificados emitidos por diferentes autoridades de certificación. Si el solicitante no forma parte del proceso, se puede tener un mayor control sobre las renovaciones. Si los certificados se renuevan automáticamente 90, 60 o 30 días antes de la fecha de caducidad, ya no es necesario preocuparse de si un miembro del equipo realizará la solicitud desde su proveedor favorito, porque esta decisión ya estará tomada.

Las API son el mejor sistema para ahorrar tiempo automatizando y personalizando la gestión de los certificados.

Práctica recomendada: Recuperar los certificados olvidados

Todos los administradores de certificados temen encontrar certificados desconocidos y problemáticos. Esto ocurre debido al aumento de la demanda de certificados, a que hay más de un responsable de solicitarlos e instalarlos y a la rotación de personal habitual en las grandes empresas. El problema es que es imposible gestionar un certificado cuya existencia se desconoce.

Mediante una herramienta de exploración, tendrá una visión general de la situación de los certificados y podrá profundizar en los detalles específicos de cada certificado en caso necesario. Muchas autoridades de certificación ofrecen una herramienta o agente de inspección que detecta certificados y recopila la información de cada exploración. El objetivo de esta herramienta es encontrar todos los certificados usados en su red, sea cual sea la autoridad de certificación, para que sepa qué certificados tiene implementados. Las herramientas de detección evitan los errores de la supervisión manual y reducen el tiempo necesario para inventariarlos.

Programando exploraciones periódicas (recomendamos al menos una a la semana) podrá tener una visión completa de todos los certificados utilizados y conocerá mejor los posibles puntos débiles, incluidos los certificados problemáticos que puedan poner en peligro la empresa. Una vez detectados los certificados olvidados o ignorados, podrá solucionar estos puntos débiles.

Práctica recomendada: Organizar el departamento

La organización del departamento encargado de la PKI es clave en la gestión de los certificados.

Es fundamental contar con los profesionales adecuados, segmentarlos en equipos, darles el nivel de acceso adecuado, asegurarse de que sepan cuál es su responsabilidad e informarles puntualmente de los procesos implantados.

DIVIDA SU NEGOCIO

Gestionar las solicitudes de certificados desde diferentes lugares del país o del mundo es mucho más factible si los encargados de la tarea se organizan en departamentos, divisiones o unidades. Independientemente de la opción que elija, podrá segmentar las solicitudes en función de la ubicación, la dirección IP, el equipo interno o cualquier otro tipo de clasificación.

Estos pequeños detalles pueden ser de ayuda cuando se reciben solicitudes con información incompleta, porque le permitirán saber dónde obtener el resto de los datos. También le permitirán ponerse en contacto con la persona adecuada cuando caduque un certificado.

ASIGNE ROLES DE USUARIO

Asignar roles de usuario a cada miembro del equipo es fundamental para mantener el control de la PKI. Si cada persona tiene el nivel de acceso adecuado a la plataforma de gestión, el proceso de renovación será menos estresante y facilitará el seguimiento.

Evalúe la función de cada persona y de qué fase del proceso se encarga. Asignar un rol a cada persona que forma parte de la plataforma de gestión de certificados le otorga la función adecuada, tanto si las solicitudes las debe aprobar un usuario normal como si se encarga un administrador. Si dota a los usuarios de la capacidad de realizar solicitudes, podrá delegar tareas y ganará tiempo.

En ocasiones, es posible que un usuario necesite realizar una única solicitud. En este caso, puede otorgarle la condición de usuario invitado para que tenga acceso de forma temporal y limitada. Esto aporta un nivel de seguridad adicional a los certificados porque solo se da la información estrictamente necesaria.

PROPORCIONE FORMACIÓN E INFORMACIÓN A SUS EMPLEADOS

Proporcionar información sobre los procedimientos a los miembros del departamento y formarlos sobre nuevas tecnologías o implementaciones es un proceso continuo.

Los administradores del sistema y desarrolladores deben tener conocimientos técnicos sobre cómo mantener e implementar los certificados. Son sus colaboradores y, en caso necesario, tendrá que pedirles información sobre todos estos componentes.

También se los debe mantener informados si se modifican los requisitos o las políticas. Para conocer las tendencias del sector y la evolución de las normativas siga el CA/Browser Forum y el blog de su proveedor de SSL favorito.

Práctica recomendada: Agilizar las aprobaciones

Aprobar los certificados de forma rápida y optimizada es fundamental para poder emitir grandes volúmenes y es un factor importante para mantener el control de la PKI. Si trabaja con una autoridad de certificación que utiliza un proceso de validación rápido, el único que puede demorar el proceso de emisión es el administrador de certificados, que es el encargado de aprobar la solicitud.

Una vez organizados los usuarios y departamentos, los correos electrónicos de verificación se deberían enviar a los administradores correspondientes para su aprobación a fin de acelerar la emisión. Al haber segmentado el equipo, el proceso de aprobación será más rápido porque el administrador solo tendrá que verificar que la información sea exacta antes de dar su aprobación. Esto le ahorrará tiempo al no tener que perseguir a nadie para obtener respuestas y acortará la implementación.

Práctica recomendada: Sacar provecho a las notificaciones

La falta de notificaciones es un problema habitual para los administradores de SSL y suele afectar a la seguridad durante la renovación de los certificados. Como mínimo es necesario recibir una notificación sobre su caducidad. Pero las notificaciones también pueden ser útiles en otras fases del ciclo de vida de los certificados, como, por ejemplo, cuando existen solicitudes pendientes, si se ha producido alguna revocación reciente o si es necesario volver a emitir un certificado.

Cuando se gestionan los certificados en una hoja de cálculo, no es posible recurrir a otras instancias si surgen problemas ni utilizar un proceso de notificación. Algunos responsables configuran recordatorios de Outlook para avisarles del momento de la renovación, pero esto tiene algunos inconvenientes (olvidarse de configurarlos, cambiar de trabajo sin comunicarlo o cualquier otro problema técnico). Las hojas de cálculo tampoco tienen una confiabilidad total.

Cuando toca renovar un certificado y el propietario no lo hace en el plazo correspondiente, es necesario conocer su identidad de inmediato, y saber si el certificado se está utilizando y en qué servidor está instalado. Cuanto antes reciba la notificación, antes podrá tener la situación bajo control.

Establezca un proceso de comunicación directa para solucionar problemas concretos de los certificados. Por ejemplo, si un certificado va a caducar en los próximos siete días, debe recibir una notificación directamente. Este proceso permite tener información de primera mano antes de que sea demasiado tarde. Si establece este tipo de comprobaciones evitará que se produzcan fallos debido a certificados caducados.

Práctica recomendada: Monitorear la red y generar informes

No tener visibilidad sobre la red es un foco de preocupaciones. Las plataformas de MPKI pueden tener la capacidad de extraer la información de los certificados obtenida a partir de las exploraciones de la red y mostrarla en un panel de control exhaustivo. Para realizar una inspección más completa, utilice este panel de control,que le permitirá supervisar la red de certificados y evaluar su estado de un vistazo.

En el panel de control podrá ver los certificados a punto de caducar, los problemas de vulnerabilidad de los certificados y las solicitudes pendientes de otros miembros del equipo. Estos son solo algunos de los ejemplos de la información que puede obtener con un panel de control.

Monitorear la red mediante la detección permanente y analizar los informes de resultados ayuda a conseguir la visibilidad necesaria.

La detección y los informes son dos componentes que se combinan para proporcionar la máxima cantidad de información y el máximo control sobre todos los certificados.

Estos son algunos consejos para lograr un excelente nivel de monitoreo:

- Instale un agente que realice exploraciones de la red y genere un informe al menos cada 30 días.
- Siempre que sea posible, cree un script para automatizar las exploraciones.
- Solucione los problemas de vulnerabilidad tras cada exploración.
- Apruebe las solicitudes de certificados a la máxima brevedad.
- Utilice la renovación automática para evitar fallos.

Tener una visión general de los certificados y de los detalles específicos de cada uno de ellos forma parte del proceso de inspección continua del ciclo de vida de los certificados.

Práctica recomendada: Usar una herramienta de detección de vulnerabilidades

En cualquier momento pueden aparecer nuevas vulnerabilidades, y solucionarlas con rapidez es un aspecto de la gestión del ciclo de vida de los certificados.

Según un informe de 2017 realizado por Bay Dynamics, el 74 % de los equipos de seguridad que trabajan en grandes empresas se ven desbordados por las tareas de mantenimiento. De hecho, pueden llegar a gestionar más de un millón de vulnerabilidades en sus sistemas.

«El trabajo de gestionar y mitigar todas las vulnerabilidades puede provocar una gran presión»[3].

Justo ahora es posible que algunas de estas vulnerabilidades estén acechando su red. Un certificado no es suficiente para proteger un servicio SSL si los cifrados son obsoletos o las versiones de SSL/TLS son vulnerables.

[3] Monahan, D. «A Day in the Life of a Cyber Security Pro». Fecha de acceso: 26 de junio de 2017. https:// baydynamics.com/content/uploads/2017/05/4-19-17-FINAL-EMA-A-Day-in-the-Life-of-a-Security-Pro.pdf

Puede reducir la presión que genera gestionar las vulnerabilidades de los puntos externos SSL con una herramienta que explore la red, busque vulnerabilidades y proporcione información al respecto.

Estas herramientas son muy útiles cuando identifican vulnerabilidades concretas y los puntos externos afectados para poder solucionarlas con rapidez y sin provocar confusión.

Práctica recomendada: Elegir una plataforma multifuncional

Con la plataforma de gestión de certificados adecuada vivirá más tranquilo porque podrá:

- utilizar una solución MPKI,
- disponer de un panel de control exhaustivo,
- automatizar la gestión utilizando una API,
- detectar certificados,
- segmentar y asignar roles de usuario,
- configurar notificaciones y procesos de comunicación directa,
- buscar vulnerabilidades.

La plataforma es fundamental para mantener el control de la PKI y gestionar el ciclo de vida de los certificados, que incluye la emisión, instalación, recuperación y renovación.

La plataforma CertCentral® de DigiCert es un paquete de software de gestión de certificados para empresas diseñado para simplificar la gestión, personalizar los flujos de trabajo y automatizar la emisión.

SE DEBEN MONITOREAR TODAS LAS PARTES DE LA RED. ES NECESARIO GENERAR INFORMES DE:

A través de la API de DigiCert Services, los responsables de SSL pueden automatizar prácticamente cualquier proceso. La API se integra con aplicaciones de terceros y se puede adaptar para incluirse en otras herramientas.

Con una plataforma multifuncional para monitorear, gestionar, detectar y explorar las vulnerabilidades eliminará la preocupación de no saber lo que ocurre en su sitio web porque aumentará la visibilidad. Organizar los miembros del departamento, asignarles roles y usar la segmentación en caso necesario incrementa el control.

CertCentral se convertirá en su aliado más valioso y hará que no se pase por alto ningún certificado.

¿Le gustaría obtener más información sobre CertCentral® o nuestra API?
Póngase en contacto con el departamento de ventas llamando al 1.855.800.3444 o enviando un correo electrónico a la dirección sales@digicert.com.

digicert®