TECNOLÓGICA DEL ORIENTE
INSTITUCIÓN DE EDUCACIÓN SUPERIOR

SEGURIDAD EN SOFTWARE

CERTIFICADOS DIGITALES

MANEJO DE CERTIFICADOS DIGITALES

en las comunicaciones electrónicas, ya que permite verificar la identidad de usuarios, dispositivos o servicios mediante tecnologías de clave pública. Estos certificados, emitidos por autoridades de certificación confiables, se utilizan para establecer conexiones cifradas, firmar digitalmente documentos y autenticar servidores web, entre otras funciones. Una correcta gestión de certificados implica su generación, instalación, renovación, revocación y almacenamiento seguro, asegurando así la confianza y la integridad en los entornos digitales (Gómez Vieites, 2015).

Introducción a los certificados digitales

Los certificados digitales constituyen uno de los pilares fundamentales en los sistemas de seguridad informática, ya que permiten establecer relaciones de confianza en entornos digitales donde no existe contacto físico entre las partes. Estos certificados son documentos electrónicos que vinculan una identidad con una clave pública, y su validez está garantizada por una entidad de confianza conocida como Autoridad Certificadora (CA, por sus siglas en inglés).

Desde una perspectiva técnica, un certificado digital contiene información crítica como el nombre del titular, la clave pública asociada, la entidad emisora, la fecha de expiración y una firma digital que autentica su legitimidad. Este mecanismo es esencial en la implementación de protocolos como HTTPS, donde se asegura que el servidor web con el que el usuario se comunica es auténtico y no ha sido suplantado (Gómez Vieites, 2015).

El proceso de uso de certificados se basa en la criptografía de clave pública: lo que una parte cifra con su clave privada puede ser verificado por cualquier otra parte que posea su clave pública. Esta verificación es lo que habilita funciones como la autenticación, el cifrado de información y la firma digital de documentos.

Un ejemplo común del uso de certificados digitales se da al acceder a una página web segura. El navegador solicita un certificado al servidor, lo valida con la CA correspondiente, y si todo es correcto, establece una conexión segura que protege los datos del usuario frente a terceros. Este sencillo acto, imperceptible para la mayoría de los usuarios, representa una compleja cadena de confianza construida sobre certificados digitales correctamente administrados.

Infraestructura de Clave Pública (PKI)

1. ¿Qué es la PKI?

La Infraestructura de Clave Pública (PKI, por sus siglas en inglés) es un sistema integral que permite gestionar de manera segura la creación, distribución, validación y revocación de certificados digitales. Su función principal es garantizar la autenticidad, integridad y confidencialidad de la información en entornos digitales, especialmente cuando se manejan datos sensibles o se realizan transacciones electrónicas.

2. Componentes esenciales de la PKI

- **Autoridad Certificadora (CA):** Es la entidad central que emite y firma los certificados digitales. Su firma proporciona confianza a los certificados.
- **Autoridad de Registro (RA):** Actúa como intermediaria entre los usuarios y la CA, verificando la identidad antes de que se emita un certificado.
- **Certificados digitales:** Son documentos electrónicos que vinculan una clave pública con la identidad de una persona, organización o sistema.
- **Listas de revocación de certificados (CRL):** Contienen certificados que han sido anulados antes de su vencimiento.
- **Repositorios seguros:** Almacenan certificados válidos y CRL para su consulta pública.

3. Funcionamiento general

El funcionamiento de la PKI se basa en la criptografía asimétrica, que utiliza un par de claves: una privada y una pública (González Manzano & De Fuentes García-Romero de Tejada, 2023). La clave privada se mantiene en secreto por el titular, mientras que la pública se incluye en el certificado digital. Cuando alguien recibe un mensaje firmado digitalmente, utiliza la clave pública del remitente para verificar la firma. Si coincide, se garantiza que el mensaje proviene del titular legítimo y no ha sido alterado.

4. Aplicaciones prácticas

La PKI es ampliamente utilizada en diversas áreas, como:

- **Autenticación de usuarios:** Por ejemplo, en una organización, los empleados pueden iniciar sesión en sus equipos usando certificados digitales en lugar de contraseñas.
- **Firmas electrónicas:** Un abogado que firma digitalmente un contrato utiliza su clave privada, y el receptor puede verificar la validez con la clave pública del certificado.
- **Cifrado de correos electrónicos y datos:** En sistemas de mensajería como S/MIME, los correos se cifran y autentican usando certificados.
- **Seguridad web:** Sitios web con HTTPS utilizan certificados digitales emitidos por una CA para asegurar la conexión con los usuarios.

5. Ejemplo concreto

Imaginemos una empresa que ofrece servicios financieros en línea. Para garantizar que sus clientes accedan a un portal seguro, implementa HTTPS mediante un certificado digital emitido por una CA reconocida. Así, los datos de acceso y transacciones quedan protegidos, y los usuarios confían en que están navegando en un sitio legítimo.

6. Beneficios clave

- **Confianza digital:** Los usuarios pueden verificar la autenticidad de las entidades con las que se comunican.
- **Seguridad en las comunicaciones:** Protege contra ataques de suplantación e intercepción de datos.
- **Cumplimiento normativo:** Muchas regulaciones exigen el uso de PKI en operaciones digitales (como GDPR, eIDAS, etc.).
- **No repudio:** Garantiza que una acción digital pueda atribuirse legalmente a una persona específica.

Tipos de certificados digitales

Los certificados digitales son piezas clave en la seguridad informática moderna, ya que permiten verificar la identidad de usuarios, servidores o dispositivos y cifrar comunicaciones. Existen distintos tipos, cada uno diseñado para cumplir funciones específicas según el contexto de uso. Conocer estos tipos es fundamental para implementar una infraestructura de seguridad eficaz y ajustada a las necesidades de una organización o sistema (González Manzano & De Fuentes García-Romero de Tejada, 2023).

1. Certificado de servidor SSL/TLS

Este tipo de certificado se utiliza para autenticar servidores web y establecer conexiones seguras a través del protocolo HTTPS. Cuando un usuario accede a un sitio web que utiliza un certificado SSL/TLS, su navegador verifica la validez del certificado antes de iniciar la comunicación cifrada.

- **Ejemplo:** Un banco en línea utiliza un certificado SSL para que los clientes puedan realizar operaciones financieras con confidencialidad y autenticidad.

2. Certificado de firma digital

Permite verificar la autoría e integridad de documentos electrónicos. Está asociado a una clave privada única del firmante y garantiza que el contenido no ha sido modificado desde que fue firmado.

- **Ejemplo:** Un abogado firma un contrato PDF con su certificado digital personal, permitiendo a las partes verificar su identidad y la autenticidad del documento.

3. Certificado de cliente (usuario final)

Este certificado identifica y autentica a un usuario dentro de una red, sistema o aplicación. Se usa frecuentemente para controlar accesos seguros sin necesidad de contraseñas.

- **Ejemplo:** En una empresa, los empleados acceden al sistema interno usando un certificado almacenado en una tarjeta inteligente o token USB, eliminando el uso de credenciales vulnerables.

4. Certificado de código o software

Está destinado a desarrolladores o empresas que necesitan firmar digitalmente el código de sus aplicaciones. Esto permite a los usuarios finales verificar que el software proviene de una fuente confiable y no ha sido alterado.

- **Ejemplo:** Una empresa de software firma su instalador con un certificado de código, evitando advertencias de seguridad al ejecutarlo en los equipos de los clientes.

5. Certificado de entidad emisora (CA)

Estos certificados se utilizan dentro de una jerarquía PKI para autorizar a una entidad como autoridad certificadora. Puede ser una CA raíz (Root CA) o una CA subordinada (Intermediate CA), y su función es emitir y firmar otros certificados (Gómez Vieites, 2015).

- **Ejemplo:** Una institución gubernamental puede actuar como CA raíz para emitir certificados digitales a múltiples organismos públicos que necesitan asegurar sus plataformas.

6. Certificado de dispositivo o máquina

Se utiliza para autenticar dispositivos dentro de una red, como routers, impresoras, cámaras IP o servidores. Permite el establecimiento de conexiones seguras entre máquinas sin intervención humana.

- **Ejemplo:** En una red empresarial, un servidor de correo utiliza un certificado de máquina para garantizar la comunicación cifrada con otros servidores dentro del dominio.

Cada tipo de certificado digital cumple un propósito único en el ecosistema de seguridad informática. Desde proteger sitios web hasta validar la autoría de un documento o autenticar dispositivos, estos certificados conforman la columna vertebral de la confianza digital. Elegir el tipo correcto depende de las necesidades específicas de seguridad, autenticación y cifrado en cada entorno.

Generación, solicitud e instalación de certificados

La implementación de certificados digitales dentro de una infraestructura segura requiere un proceso técnico ordenado, que incluye tres etapas fundamentales: generación, solicitud e instalación. Cada una de estas fases garantiza que el certificado funcione correctamente y cumpla su propósito, ya sea la autenticación de una entidad, el cifrado de datos o la firma digital de documentos o software (Gómez Vieites, 2015).

1. Generación de la clave y del archivo CSR

El primer paso consiste en generar un par de claves criptográficas: una clave privada y una clave pública. La clave privada se mantiene protegida en el servidor o dispositivo, mientras que la clave pública se integra en una solicitud de firma de certificado o CSR (Certificate Signing Request). Esta solicitud contiene datos relevantes como el nombre del dominio, la organización y la ubicación, y será enviada a una autoridad certificadora (CA) para validar la identidad del solicitante.

- **Ejemplo:** Un administrador de un sitio web genera desde su servidor un archivo CSR que incluye el nombre del dominio "www.seguridadavanzada.com" y su clave pública, listo para ser enviado a una CA como DigiCert o Let's Encrypt.

2. Envío de la solicitud a la Autoridad Certificadora (CA)

Con el archivo CSR preparado, el siguiente paso es enviarlo a una autoridad certificadora confiable, que será responsable de verificar la legitimidad de la información contenida en la solicitud. Dependiendo del tipo de certificado (de dominio, de organización o extendido), el nivel de verificación varía. Una vez aprobada la solicitud, la CA emite un certificado digital firmado con su propia clave privada (Gómez Vieites, 2015).

- **Ejemplo:** Una empresa solicita un certificado EV (Extended Validation) para su portal de banca en línea. La CA realiza una validación exhaustiva de la identidad legal de la empresa antes de emitir el certificado correspondiente.

3. Recepción e instalación del certificado

Después de recibir el certificado digital emitido, el administrador del sistema debe instalarlo en el servidor o dispositivo correspondiente. Esta etapa implica configurar correctamente el servidor para utilizar el certificado y habilitar protocolos como HTTPS, permitiendo conexiones cifradas seguras. En algunos entornos, también es necesario instalar certificados intermedios que completan la cadena de confianza entre el certificado del servidor y la CA raíz.

- **Ejemplo:** Tras recibir su certificado SSL, un administrador lo instala en un servidor Apache, configurando los archivos .crt y .key en el archivo de configuración del sitio web. Posteriormente, prueba la conexión usando un navegador para verificar que el sitio muestre el candado de seguridad.

4. Consideraciones de seguridad

Durante todo el proceso, es fundamental mantener protegida la clave privada, ya que su exposición comprometería la autenticidad del certificado. Se recomienda almacenarla en dispositivos seguros, como módulos HSM (Hardware Security Modules) o usar herramientas de gestión de certificados con funciones de control de acceso (González Manzano & De Fuentes García-Romero de Tejada, 2023).

La generación, solicitud e instalación de certificados digitales es un proceso técnico pero esencial para establecer entornos digitales confiables. A través de estos pasos, organizaciones y usuarios aseguran sus comunicaciones, autentican identidades y refuerzan la protección frente a amenazas informáticas. Su correcta implementación fortalece la integridad y la privacidad en aplicaciones web, redes empresariales y sistemas distribuidos.

Revocación y renovación de certificados

Dentro del ciclo de vida de los certificados digitales, las etapas de revocación y renovación son fundamentales para garantizar que la infraestructura de seguridad continúe funcionando de forma fiable y que no se comprometan los canales de

comunicación cifrados. Ambas acciones responden a distintos escenarios y deben gestionarse con precisión para evitar interrupciones o vulnerabilidades en los sistemas (González Manzano & De Fuentes García-Romero de Tejada, 2023).

1. Revocación de certificados: concepto y finalidad

La revocación de un certificado digital implica invalidar antes de su fecha de expiración, debido a razones de seguridad, errores en su emisión o pérdida de confianza en la entidad certificada. Una vez revocado, el certificado ya no es considerado confiable y no debe ser aceptado por clientes, navegadores ni aplicaciones.

- **Ejemplo:** Si un atacante obtiene acceso a la clave privada de un servidor web, el administrador debe solicitar la revocación inmediata del certificado afectado, evitando así que el atacante pueda suplantar la identidad del sitio.

2. Motivos comunes para la revocación

Un certificado puede ser revocado por diversas razones, entre las cuales destacan:

- Compromiso de la clave privada.
- Errores en la información contenida en el certificado.
- Cambio de nombre de dominio o de entidad.
- Cierre de la empresa u organización emisora.
- Violación de las políticas de uso.

Estos motivos deben ser justificados ante la autoridad certificadora (CA), quien procederá con la revocación.

3. Métodos de verificación de revocación

Para verificar si un certificado ha sido revocado, existen dos mecanismos principales:

- **CRL (Certificate Revocation List):** una lista publicada periódicamente por la CA con todos los certificados revocados.
- **OCSP (Online Certificate Status Protocol):** un protocolo que permite verificar en tiempo real el estado de un certificado consultando directamente a la CA.
- **Ejemplo:** Al acceder a un sitio web, el navegador puede consultar un servidor OCSP para confirmar que el certificado del sitio sigue siendo válido.

4. Renovación de certificados: concepto y propósito

La renovación consiste en emitir un nuevo certificado para reemplazar uno que está próximo a expirar. A diferencia de la revocación, la renovación es parte del mantenimiento natural del certificado y garantiza la continuidad del servicio sin afectar la confianza del usuario (Gómez Vieites, 2015).

- **Ejemplo:** Un certificado SSL con validez de un año debe renovarse antes de la fecha de vencimiento. El administrador genera una nueva CSR y solicita un nuevo certificado con la misma clave o una nueva clave privada, según las políticas de seguridad.

5. Consideraciones durante la renovación

Durante la renovación, es recomendable:

- Revisar y actualizar la información del certificado, como el nombre de dominio o los datos de la organización.
- Generar un nuevo par de claves si se considera que las anteriores pueden estar en riesgo.
- Realizar la renovación antes del vencimiento, para evitar advertencias de seguridad en los navegadores.

6. Automatización del proceso

En entornos donde se manejan múltiples certificados, es útil automatizar los procesos de renovación y revocación mediante herramientas como Certbot, Venafi, o soluciones de gestión de certificados empresariales. Estas herramientas pueden programar renovaciones automáticas y monitorear el estado de los certificados (Gómez Vieites, 2015).

La revocación y renovación de certificados son procesos vitales para mantener la confianza en los sistemas digitales. La revocación protege frente a incidentes de seguridad, mientras que la renovación garantiza la continuidad del cifrado sin interrupciones. Una gestión adecuada de ambos procesos refuerza la seguridad de la infraestructura digital y protege a los usuarios frente a suplantaciones y ataques.

Aplicaciones prácticas y seguridad en el uso de certificados

Los certificados digitales desempeñan un papel central en los sistemas de seguridad de la información, al proporcionar autenticación, confidencialidad, integridad y no repudio. Su uso se extiende más allá del ámbito de la navegación web, alcanzando sectores como el correo electrónico, la banca en línea, las redes corporativas y las transacciones comerciales. El aprovechamiento correcto de los certificados, acompañado de buenas prácticas de seguridad, permite construir entornos digitales confiables (Gómez Vieites, 2015).

1. Autenticación de sitios web (HTTPS)

Una de las aplicaciones más visibles de los certificados digitales es su uso en la autenticación de servidores web. Cuando un sitio implementa HTTPS, el certificado digital garantiza al usuario que está conectado con el dominio legítimo y no con un sitio impostor.

- **Ejemplo:** Al ingresar a un banco en línea como https://bancoejemplo.com, el navegador valida que el certificado SSL/TLS fue emitido por una autoridad confiable y corresponde al dominio correcto, activando el candado de seguridad en la barra de direcciones.

2. Firma digital de correos electrónicos

En el ámbito de las comunicaciones, los certificados permiten firmar digitalmente correos electrónicos, asegurando al receptor que el mensaje proviene realmente del remitente y no ha sido modificado en tránsito (Gómez Vieites, 2015).

- **Ejemplo:** En entornos empresariales, un directivo puede enviar un contrato firmado digitalmente desde su cuenta de correo, y el destinatario podrá verificar su validez sin necesidad de papel o presencia física.

3. Autenticación en redes privadas y VPN

Los certificados también se utilizan para autenticar usuarios y dispositivos en redes privadas virtuales (VPN) o sistemas internos corporativos, reduciendo el riesgo de accesos no autorizados (González Manzano & De Fuentes García-Romero de Tejada, 2023).

- **Ejemplo:** Una organización puede exigir que todos sus empleados utilicen un certificado digital para establecer una conexión VPN segura antes de acceder a los servidores internos.

4. Protección de documentos y software

Los certificados permiten firmar documentos electrónicos (como PDFs) y aplicaciones de software, de modo que cualquier modificación posterior al proceso de firma invalida su autenticidad.

- **Ejemplo:** Un proveedor de software firma sus aplicaciones con un certificado digital, lo que permite a los usuarios confirmar que el programa no ha sido alterado por terceros antes de su instalación.

5. Certificados en dispositivos móviles y autenticación multifactor

En entornos modernos, los certificados son empleados como parte de la autenticación multifactor (MFA), especialmente en dispositivos móviles gestionados por empresas.

- **Ejemplo:** Un empleado que accede a una aplicación corporativa desde su celular puede requerir un certificado previamente instalado como segundo factor de autenticación, además de su contraseña.

6. Buenas prácticas para una implementación segura

El uso de certificados digitales debe estar acompañado de medidas que garanticen su seguridad, tales como:

- Almacenar las claves privadas de forma segura, idealmente en módulos de hardware (HSM).
- Evitar compartir certificados entre sistemas o usuarios.
- Renovar los certificados antes de que expiren.
- Revocar certificados comprometidos de forma inmediata.
- Monitorear el estado de los certificados activos en toda la infraestructura.

Las aplicaciones prácticas de los certificados digitales son amplias y fundamentales para la protección de datos y la verificación de identidades en entornos digitales. Ya sea asegurando una página web, firmando un documento, o controlando el acceso a una red corporativa, su correcto uso fortalece la confianza y la seguridad. Sin embargo, solo una gestión adecuada y responsable de estos certificados garantiza su efectividad a largo plazo.

BIBLIOGRAFÍA

- Gunnar Wolf. (2025, 13 de mayo). Aspectos de sistemas operativos en los dispositivos IoT [Vídeo]. YouTube. https://youtu.be/5eu5o1BlQiE
- LACNIC RIR. (2018, 27 de septiembre). Panel: Despliegue de IoT, Conectividad y Soluciones – el caso Argentina [Vídeo]. YouTube. https://youtu.be/vqloa1THqng
- Red Hat. (s.f.). ¿Qué es el middleware? Red Hat. https://www.redhat.com/es/topics/middleware/what-is-middleware