Sistemas seguros de acceso y transmisión de datos.

IFCT0109 – Seguridad informática

MF0489_3 (60 horas)

Aplicación de una infraestructura de clave pública (PKI)

- Introducción
- Identificación de los componentes de una PKI y su modelo de relaciones
- Autoridad de certificación y sus elementos
- Política de certificado y declaración de prácticas de certificación (CPS)
- Lista de certificados revocados (CRL)
- Funcionamiento de las solicitudes de firma de certificados (CSR)
- Infraestructura de gestión de privilegios (PMI)
- Campos de certificados de atributos, incluyen la descripción de sus usos habituales y la relación con los certificados digitales
- Aplicaciones que se apoyan en la existencia de una PKI
- Resumen

Introducción

Desde 1976, con la invención de la criptografía de clave pública, el panorama de seguridad en las comunicaciones digitales experimentó una revolución sin precedentes. Este avance tecnológico eliminó la necesidad de una clave secreta compartida entre los interlocutores, instaurando en su lugar el uso de una clave pública conocida por todos y una clave privada en posesión exclusiva de cada usuario. La esencial interrogante que emergió fue cómo validar la autenticidad de la clave pública de un interlocutor, asegurando su correspondencia con la identidad declarada.

Para resolver esta incógnita, se desarrollaron las Infraestructuras de Clave Pública (PKI), sistemas encargados de gestionar, emitir y revocar certificados digitales. Estos certificados son documentos electrónicos que establecen una relación de confianza entre una identidad y su clave pública correspondiente. La función de las PKI es, por tanto, vital para la autenticación electrónica, brindando un marco seguro que garantiza la veracidad de las identidades digitales en el ciberespacio.

Además, en el ámbito de la seguridad electrónica, no solo importa la autenticación de la identidad, sino también la autorización para ejecutar ciertas acciones. Aquí es donde entran en juego las Infraestructuras de Gestión de Privilegios (PMI), diseñadas para administrar los derechos y permisos de los usuarios.

A través de las PMI, se puede controlar eficazmente el acceso y las operaciones permitidas a cada entidad, completando así el espectro de seguridad necesario en entornos digitales complejos.

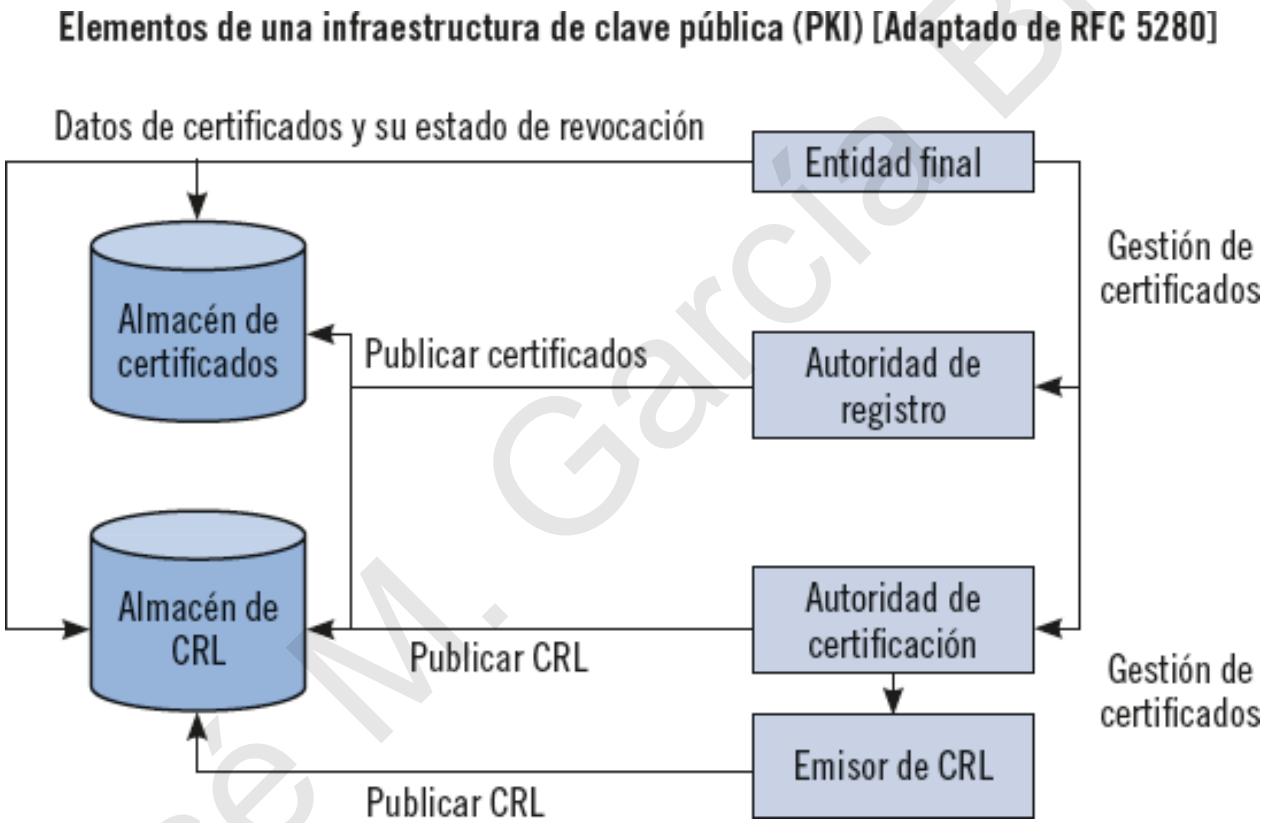
Identificación de los componentes de una PKI y su modelo de relaciones

La Infraestructura de Clave Pública (PKI) es un sistema integral diseñado para la gestión de certificados digitales, esencial en la seguridad de las comunicaciones digitales. Según la normativa ITU-T X.509, una PKI comprende múltiples entidades que intervienen en la emisión, gestión, y revocación de certificados digitales, estableciendo un entorno seguro para la autenticación y el intercambio de información en Internet.

Entidades Clave en una PKI

- Autoridad de Certificación (CA): Emite certificados de clave pública y acredita la identidad de una entidad.
- Certificado de clave pública (PKC): Documento que acredita que la entidad a la que se refiere conoce la clave privada asociada a la pública.
- Autoridad de Registro (AR): Verifica la identidad de la entidad final y los datos que figuran en el certificado.
- Emisor de listas de certificados revocados (CRL issuer): Emite listas de certificados que han sido revocados.
- Repositorio: Almacena certificados de clave pública y listas de certificados revocados.
- Archivo: Almacena información histórica sobre certificados y listas de certificados revocados.

Identificación de los componentes de una PKI y su modelo de relaciones



Identificación de los componentes de una PKI y su modelo de relaciones

Modelo de relaciones:

- La CA emite certificados a entidades finales y otras CA.
- La AR verifica la identidad de la entidad final y los datos del certificado.
- El emisor de CRL emite listas de certificados revocados.
- Los repositorios almacenan certificados y listas de certificados revocados.
- Los archivos almacenan información histórica sobre certificados y listas de certificados revocados.

Consideraciones:

- La seguridad de la PKI depende de la custodia de las claves privadas de la CA y la AR.
- Los repositorios deben ser interoperables para que cualquier persona pueda consultar el estado de los certificados.
- Los archivos garantizan la custodia de la información durante largo tiempo.

Identificación de los componentes de una PKI y su modelo de relaciones

Modelo de relaciones

En el entramado de la Infraestructura de Clave Pública (PKI), la organización y vinculación entre sus autoridades se estructuran predominantemente en un esquema jerárquico, aunque existen otras configuraciones alternativas que se explorarán posteriormente.

Dentro de este esquema jerárquico, se posiciona una Autoridad de Certificación (CA) raíz como el núcleo de máxima confianza. Subordinadas a esta, pueden coexistir una o múltiples CAs, encargadas de la emisión y administración de certificados digitales.

Interesante es saber que el ciberespacio está repleto de Autoridades de Certificación integradas en la PKI. Sin embargo, es viable para cualquier corporación emplear herramientas de código abierto, tal como EJBCA, para instaurar su propia infraestructura de clave pública con fines corporativos.

EJBCA es una solución de software que funciona como una Autoridad Certificadora (CA) en la Infraestructura de Clave Pública (PKI). Se utiliza para emitir, gestionar y validar certificados digitales, que son esenciales para proteger datos sensibles y establecer identidades digitales confiables en entornos en línea.

Es una implementación de referencia de PKI que se puede escalar para satisfacer las necesidades de cualquier infraestructura de PKI y es reconocido por su amplio número de servicios asociados con la firma electrónica. Como una solución de código abierto, EJBCA permite a las empresas configurar y controlar centralmente las políticas de certificados y ejecutar varias jerarquías de PKI en una sola instancia, lo que facilita su despliegue y gestión.

Identificación de los componentes de una PKI y su modelo de relaciones

Modelo de relaciones

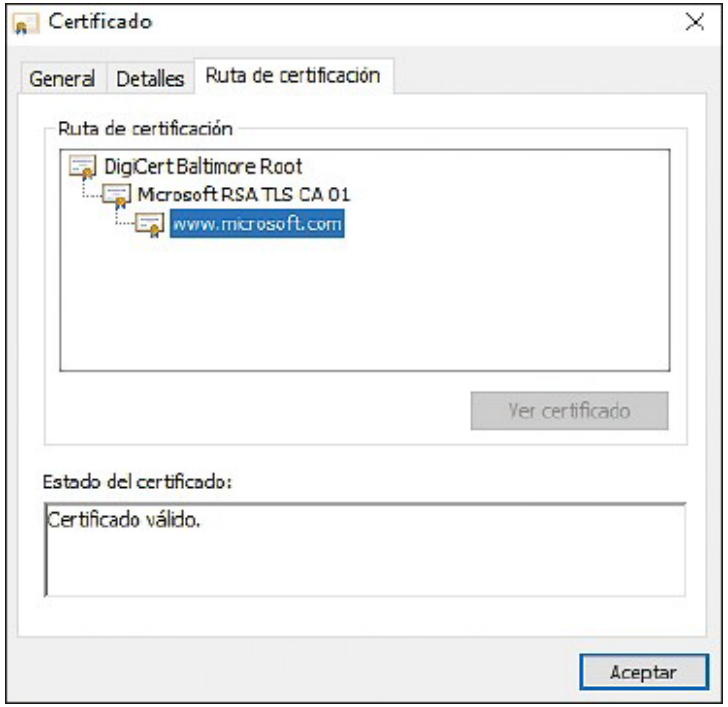
Un punto crucial en la dinámica de la PKI es la emergencia del concepto de cadenas de certificación, facilitado por la presencia de CAs intermedias.

De tal forma, un certificado destinado a un ente terminal (por ejemplo, un usuario) puede ser expedido por una CA intermedia (por ejemplo, CA2), la cual, a su vez, se halla subordinada a otra CA intermedia (por ejemplo, CA1), que finalmente depende de la CA raíz.

Las cadenas de certificación transfiguran las PKI en una realidad palpable, al permitir que la administración de los certificados de un sujeto se disemine entre diversas CAs intermedias o subordinadas.

Esto resulta especialmente útil en contextos geográficamente extensos, como el de un país dividido en varias comunidades autónomas.

En tales casos, resulta más práctico y eficiente disponer de una CA subordinada por cada comunidad, todas supervisadas por una única CA central, en lugar de contar con una sola CA raíz para la gestión de todos los certificados de la población.



Identificación de los componentes de una PKI y su modelo de relaciones

Arquitecturas de una PKI

Las Infraestructuras de Clave Pública (PKI) pueden adoptar distintas arquitecturas para su implementación dentro de una organización, y entre estas se destacan principalmente la arquitectura jerárquica y la arquitectura en red o mesh. Además, existe la arquitectura de puente, que se utiliza para enlazar PKI de diferentes organizaciones.

Arquitectura Jerárquica

Es la arquitectura tradicional de PKI. Se caracteriza por una estructura de árbol, donde una CA raíz (CA1) certifica a otras CA intermedias (CA2, CA3), que a su vez certifican a las entidades finales (usuarios, dispositivos, etc.).

Ventajas:

- Mayor simplicidad y facilidad de gestión.
- Escalabilidad: permite gestionar un gran número de entidades finales.
- Alta seguridad: la CA raíz es la única entidad que puede emitir certificados.

Desventajas:

- Un único punto de fallo: si la CA raíz se ve comprometida, toda la PKI queda vulnerable.
- Menor flexibilidad: puede ser difícil agregar nuevas entidades o modificar la estructura de la PKI.

Identificación de los componentes de una PKI y su modelo de relaciones

Arquitecturas de una PKI

Arquitectura en Red (Mesh)

En esta configuración, las Autoridades de Certificación (CA) se autentican de manera independiente, formando una red de confianza entre sí. Las entidades finales confían y verifican los certificados basándose en las CA que conocen, normalmente la más cercana, siguiendo una cadena de confianza establecida a través de estas conexiones de CA interconectadas. Esta estructura ofrece flexibilidad y puede ser más resistente a puntos únicos de fallo.

Ventajas:

- Mayor seguridad: no existe un único punto de fallo.
- Mayor flexibilidad: es más fácil agregar nuevas entidades o modificar la estructura de la PKI.

Desventajas:

- Mayor complejidad de gestión.
- Menor escalabilidad: puede ser difícil gestionar un gran número de entidades finales.

Identificación de los componentes de una PKI y su modelo de relaciones

Arquitecturas de una PKI

Arquitectura de Puente (Bridge)

La arquitectura de puente está diseñada para facilitar la interconexión de PKI entre diferentes organizaciones. Esto se logra mediante la introducción de una CA de puente, que actúa como un intermediario confiable entre las PKI de las organizaciones involucradas.

Dependiendo de si las arquitecturas originales son jerárquicas o en red, la CA de puente se conectará con la CA raíz en el primer caso, o establecerá una relación con una de las CAs en la red en el segundo. Esto permite a las entidades finales de diferentes organizaciones establecer una confianza recíproca.

Ventajas:

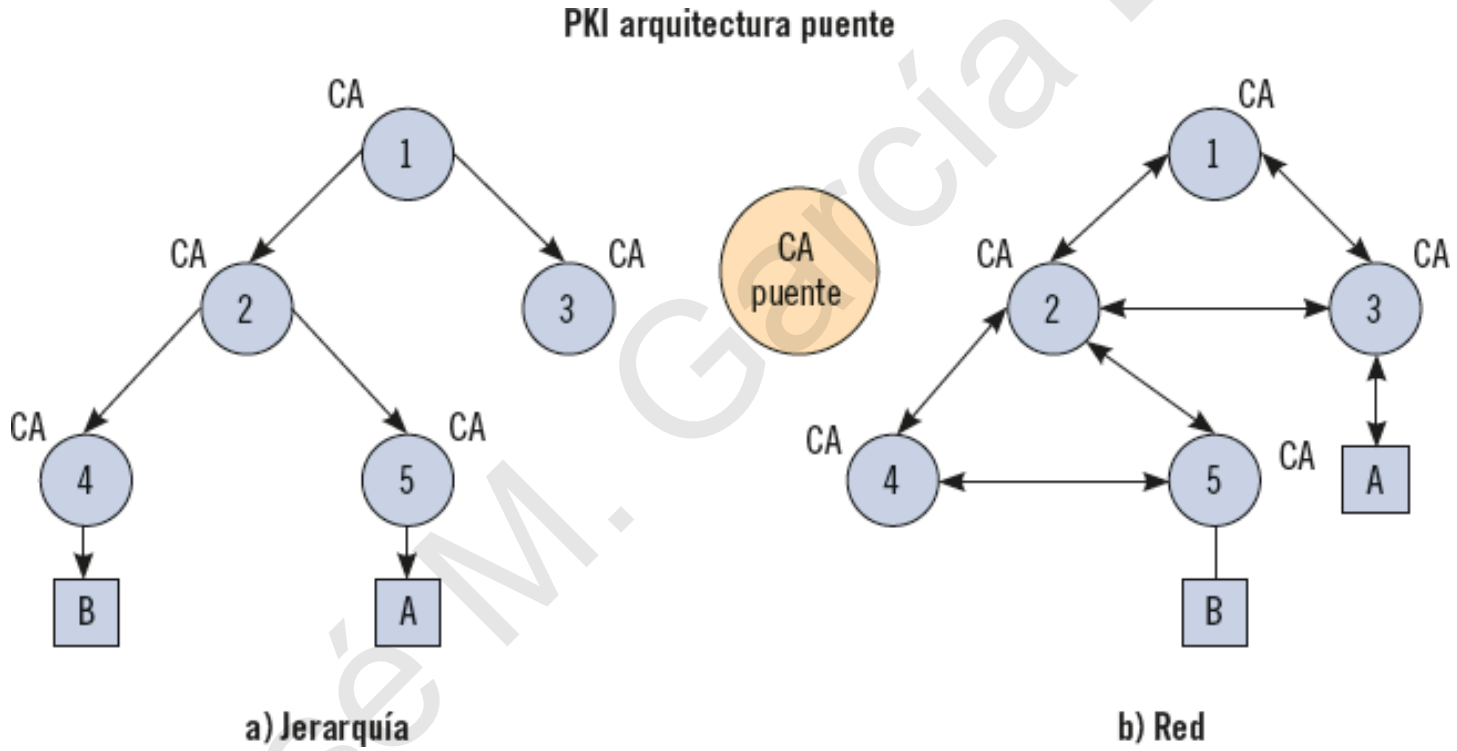
- Permite conectar dos PKI de forma segura.
- No es necesario modificar las PKI existentes.

Desventajas:

- Aumenta la complejidad de la gestión de las PKI.

Identificación de los componentes de una PKI y su modelo de relaciones

Arquitecturas de una PKI



Identificación de los componentes de una PKI y su modelo de relaciones

Arquitecturas de una PKI

Arquitectura física

La arquitectura física de una Infraestructura de Clave Pública (PKI) es fundamental para la seguridad y la eficacia de la gestión de certificados digitales dentro de una organización. La implementación adecuada involucra distribuir los componentes de la PKI en sistemas separados para asegurar la integridad y la disponibilidad del servicio.

Se recomienda que las Autoridades de Certificación (CAs), las Autoridades de Registro (RAs), y los repositorios estén alojados en sistemas distintos y protegidos detrás del cortafuegos de la empresa.

El cortafuegos, o firewall, actúa como un sistema defensivo, ya sea hardware o software, que regula el tráfico de red entrante y saliente, funcionando como una barrera para evitar accesos no autorizados.

Para la gestión de claves públicas, se suele establecer un directorio de borde, situado fuera del cortafuegos, que es accesible para las entidades externas. Este directorio contiene las claves públicas y es actualizado regularmente por un directorio principal, que se encuentra protegido detrás del cortafuegos y es accesible solo para las entidades internas de la empresa.

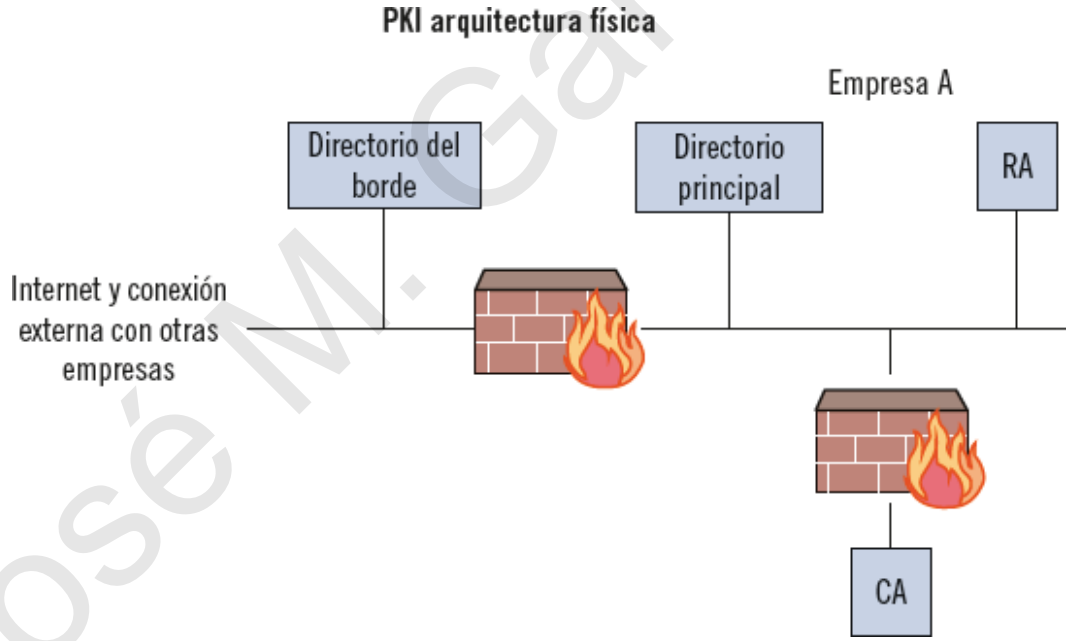
Esta configuración contribuye a que, incluso si la seguridad perimetral se ve comprometida, los datos críticos y los sistemas de gestión de claves permanecen a salvo de ataques externos.

Identificación de los componentes de una PKI y su modelo de relaciones

Arquitecturas de una PKI

Arquitectura física

La arquitectura precisa de la PKI de una organización se puede ilustrar en un diagrama que refleje la ubicación y la relación entre los diferentes componentes, incluyendo los cortafuegos y directorios mencionados. Este diagrama serviría para visualizar la estructura de seguridad y sería un recurso valioso para el diseño e implementación de la PKI.



Autoridad de certificación y sus elementos

Funciones de gestión

La Autoridad de Certificación (CA) es el pilar de la Infraestructura de Clave Pública (PKI), con la responsabilidad de administrar el ciclo de vida de los certificados digitales. La norma X.509 define siete funciones críticas en la gestión de las relaciones entre una entidad final, como un usuario, y la CA:

- Registro: Este es el primer contacto de la entidad con la CA, donde se verifica su identidad, pudiendo ser directamente o mediante una Autoridad de Registro (AR).
- Inicialización: Se suministra a la entidad final todo lo necesario para la verificación de certificados, incluyendo las claves públicas de todas las CAs implicadas en la PKI. Además, se le proporciona su par de claves público-privada, que puede ser más de uno para distintos propósitos, como autenticación y firma.
- Certificación: Es el proceso de emisión del certificado que vincula la clave pública con su propietario. El certificado puede ser entregado directamente o accesible a través de un repositorio.
- Copia de respaldo del par de claves: Se facilita una función para que el usuario pueda realizar y almacenar una copia de seguridad de su par de claves y así recuperarla si fuera necesario.
- Actualización del par de claves: Renovar periódicamente el par de claves ayuda a prevenir ataques y limitar su impacto, ya que las operaciones futuras usarán el nuevo par.
- Revocación de la clave: Se dispone de un procedimiento para invalidar un par de claves en caso de compromiso o pérdida, lo que ayuda a minimizar daños.
- Certificación cruzada: Permite a una CA emitir un certificado a otra CA, facilitando que los certificados emitidos por la segunda sean reconocidos por la primera.

Autoridad de certificación y sus elementos

Funciones de gestión

Estas funciones aseguran la integridad, confidencialidad, autenticación y no repudio en las transacciones digitales, ejemplificado en aplicaciones como el DNI electrónico, que incorpora pares de claves distintos para autenticación y firma electrónica.

La correcta ejecución de estas funciones es crucial, dado que cualquier compromiso en el sistema de la CA puede tener consecuencias graves, obligando a la reemisión de los certificados afectados. Por esta razón, se recomienda encarecidamente que la infraestructura de la CA esté protegida detrás de un cortafuegos robusto.

Autoridad de certificación y sus elementos

Validación de una cadena de certificación

La validación de una cadena de certificación es un procedimiento meticuloso que garantiza la autenticidad y validez de los certificados digitales dentro de una infraestructura de clave pública (PKI). El objetivo es confirmar que cada certificado de la cadena ha sido efectivamente expedido por una autoridad certificadora de confianza y que la cadena es íntegra y fiable. Aquí están los pasos clave de este proceso:

- Verificar la Confianza en la CA Raíz: Comienza por establecer la confianza en la entidad que emitió el primer certificado en la cadena, que suele ser una CA raíz. Este certificado suele ser auto-firmado, identificando a la misma entidad que firma y emite.

- Validar la Cadena de Certificados:
    - Se confirma que la entidad listada como sujeto en un certificado es la que emite el siguiente.
    - Se verifica que todos los certificados estuviesen válidos en el momento de su uso, comprobando que no estén caducados ni revocados.
    - Se asegura que no haya ciclos en la cadena, es decir, que un certificado no aparezca más de una vez.

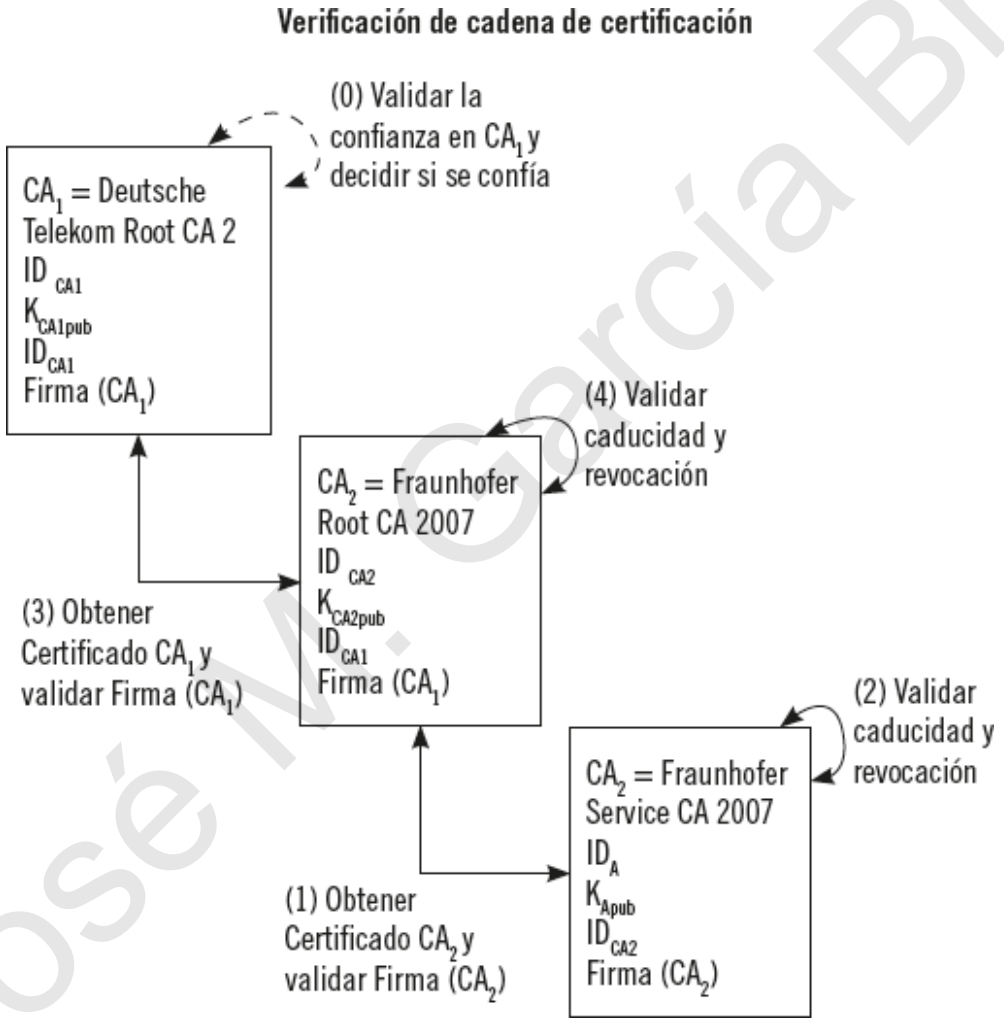
- Comprobar la Firma Electrónica: Se verifica la autenticidad de la firma electrónica de cada certificado utilizando el algoritmo que se especifica en el mismo.

- Coherencia de Políticas: Se revisa que la política de cada certificado concuerde con la de los demás y con el propósito previsto de uso del certificado.

- Ausencia de Ciclos: Se garantiza que dentro de la cadena no se formen bucles, es decir, que un certificado no aparezca listado más de una vez.

Autoridad de certificación y sus elementos

Validación de una cadena de certificación



Autoridad de certificación y sus elementos

Validación de una cadena de certificación en los navegadores

El proceso de validación de certificados en los navegadores es un mecanismo esencial para garantizar la seguridad en la navegación por Internet. Cuando un usuario accede a un sitio web a través de un protocolo seguro como SSL/TLS, el navegador verifica automáticamente el certificado digital del sitio para confirmar su autenticidad.

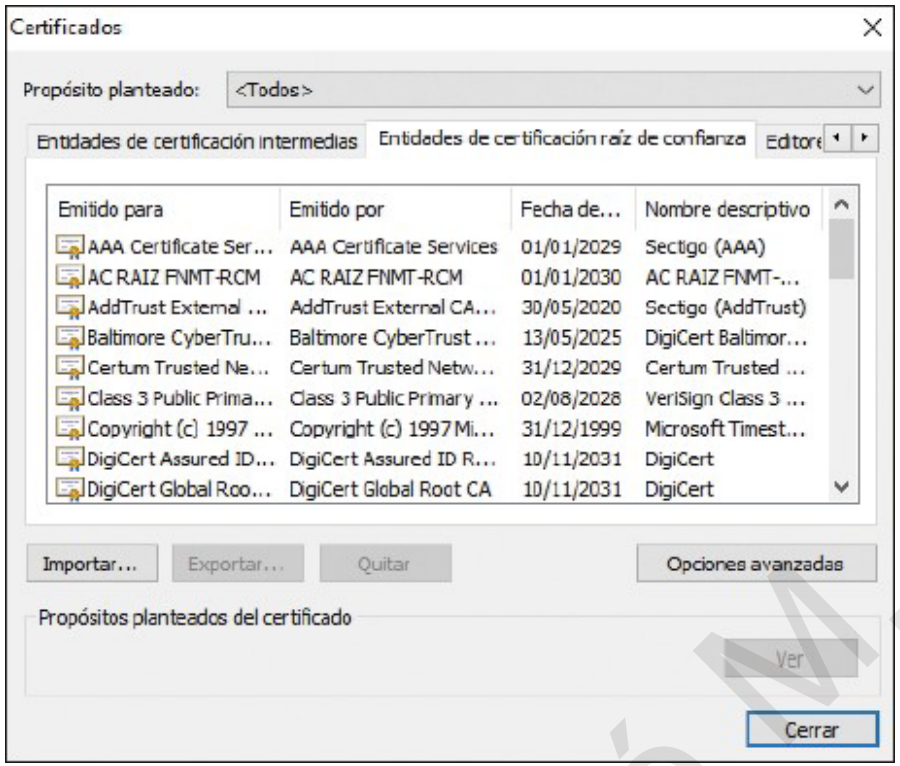
Aspectos clave de la validación de certificados en navegadores:

- Gestión de Certificados Raíz: Los navegadores contienen un conjunto preinstalado de certificados de CA raíz de confianza, que se utilizan para validar certificados de sitios web.
- Validación Automática: Al acceder a un sitio web, el navegador verifica la cadena de certificación para asegurarse de que el certificado del sitio fue emitido por una CA de confianza.
- Avisos de Seguridad: Si se encuentra con un certificado emitido por una CA no reconocida o que tiene problemas de validez (por ejemplo, ha caducado o ha sido revocado), el navegador alertará al usuario con un mensaje de advertencia.
- Prevención de Phishing: Estos avisos de seguridad son cruciales para proteger a los usuarios contra ataques de phishing que intentan imitar sitios web legítimos para obtener información sensible.
- Interfaces de Usuario Intuitivas: Los navegadores modernos han simplificado las alertas para que sean comprensibles para los usuarios, asegurando que sean conscientes de los riesgos potenciales.

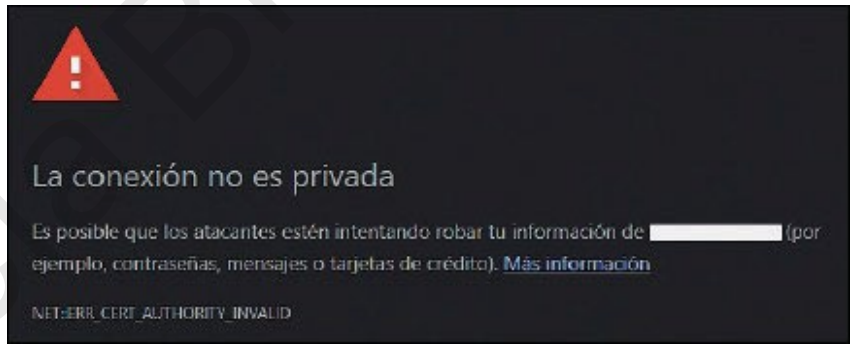
Los usuarios avanzados pueden utilizar esta herramienta para inspeccionar los detalles de los certificados y la confianza depositada en ellos.

Autoridad de certificación y sus elementos

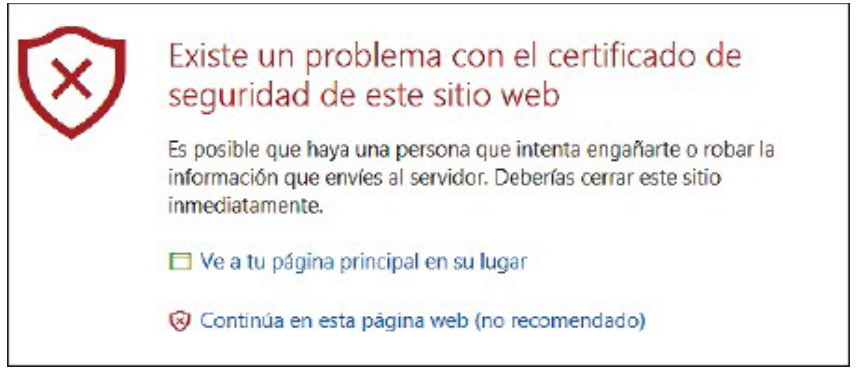
Validación de una cadena de certificación en los navegadores



Certificados gestionados por el navegador, accesibles desde la configuración del navegador



Avisos de seguridad de los navegadores



Política de certificado y declaración de prácticas de certificación (CPS)

La Política de Certificación (CP) y la **Declaración de Prácticas de Certificación (CPS**) son dos documentos fundamentales en la infraestructura de clave pública (PKI), definidos según la RFC 3647. Ambos establecen las reglas y prácticas asociadas al uso y manejo de los certificados digitales emitidos por una Autoridad de Certificación (CA).

Política de Certificación (CP)

La CP es un documento que define el conjunto de reglas que rigen el uso y la confianza depositada en un certificado dentro de una comunidad o tipo de aplicación. Establece los requisitos de seguridad y uso para los certificados y especifica cómo deben ser aplicados.

> Por ejemplo, una CP puede detallar el propósito de los certificados para un tipo de transacción en línea, los niveles de seguridad requeridos y cómo estos deben ser manejados por la comunidad que los utiliza.
>
> Recordatorio: Solo la clave pública se almacena en el certificado digital; la clave privada permanece en secreto con su propietario.

Las CP guían a los usuarios y entidades para comprender y determinar la adecuación del certificado para su uso previsto. Por ende, las CA deben garantizar que los certificados emitidos cumplan con la CP asociada. Estos documentos proporcionan un marco para las auditorías y evaluaciones de las CAs y son referenciados por los certificados a través del campo "Políticas del certificado" en las extensiones X.509.

Cada CP se asocia con un Identificador de Objeto (OI), que puede registrarse para una organización específica, y la entidad registrante es quien publica el texto de la CP. Estos identificadores ayudan a las aplicaciones a automatizar la decisión de confiar o no en un certificado particular.

Política de certificado y declaración de prácticas de certificación (CPS)

Política de Certificación (CP)

En el contexto de una PKI, las CP son cruciales porque definen claramente los propósitos para los que se emiten los certificados, proporcionando a los usuarios y aplicaciones una base para confiar en su validez y autenticidad. Las CP también son esenciales para que una CA emisora evalúe y confíe en una CA receptora durante el proceso de certificación cruzada.

Estos documentos no solo proporcionan una base para la confianza en los certificados digitales, sino que también establecen los cimientos sobre los cuales se construye y mantiene la seguridad de la información en entornos digitales.

Declaración de prácticas de certificación (CPS)

Es un documento detallado que describe los procedimientos y políticas que una Autoridad de Certificación (CA) sigue al emitir y administrar certificados digitales. La CPS es vital porque detalla el funcionamiento práctico y los compromisos de seguridad de la CA, proporcionando a las entidades que confían en la CA la información necesaria para evaluar la fiabilidad de los certificados emitidos.

La CPS cubre aspectos tales como:

- El proceso de emisión de certificados, incluyendo la autenticación de entidades solicitantes.
- Cómo se realizan las revocaciones y las renovaciones de los certificados.
- Los procedimientos para la creación y almacenamiento seguro de las claves.
- La forma en que se protege la infraestructura de la CA contra compromisos de seguridad.

Política de certificado y declaración de prácticas de certificación (CPS)

Declaración de prácticas de certificación (CPS)

A diferencia de la Política de Certificación (CP), que es más una declaración de los propósitos y aplicabilidad de los certificados, la CPS es un manual de cómo la CA implementa esas políticas en la práctica. Aunque una CPS detallada podría revelar información que podría ser explotada por un atacante, a menudo solo se hace público un resumen de la CPS que destaca las cláusulas relevantes para los participantes en la PKI sin revelar detalles de seguridad sensibles.

Las CPS no son en sí mismas contratos, pero establecen expectativas claras y pueden ser referenciadas en acuerdos contractuales entre la CA y los usuarios de los certificados. El contenido de una CPS puede incluir detalles sobre los servicios de confianza ofrecidos, la gestión del ciclo de vida del certificado, y las responsabilidades de las partes involucradas.

La importancia de la CPS radica en su función de asegurar a los usuarios y suscriptores que la CA opera de manera segura y en concordancia con las expectativas de la industria, lo que es crucial para mantener la confianza dentro de un ecosistema digital cada vez más dependiente de la autenticación y el cifrado robustos para transacciones y comunicaciones seguras.

Política de certificado y declaración de prácticas de certificación (CPS)

Diferencias entre política de certificación y declaración de prácticas de certificación

La Política de Certificación (CP) y la Declaración de Prácticas de Certificación (CPS) son documentos relacionados con la emisión de certificados digitales, pero tienen objetivos distintos:

- Objetivo: La CP define qué deben hacer los participantes (ej. autoridades de certificación, usuarios) para garantizar la confianza en los certificados. La CPS detalla cómo una Autoridad Certificadora (CA) implementa esos requisitos para emitir certificados fiables.
- Alcance: Las CP son más generales y sirven como lineamientos para PKI interoperables. Una única CP puede aplicar a varias CA o dominios. Por otro lado, la CPS es específica de una CA y no busca la interoperabilidad
- Nivel de detalle: La CPS suele tener más detalle que la CP, especificando cómo la CA cumple los requisitos de la CP para emitir certificados

En resumen, la CP indica qué se debe hacer, mientras que la CPS describe cómo lo hace una CA específica.

Política de certificado y declaración de prácticas de certificación (CPS)

Diferencias entre política de certificación y declaración de prácticas de certificación

Las Políticas de Certificación (CP) y las Declaraciones de Prácticas de Certificación (CPS) son dos documentos fundamentales en la estructura de una Infraestructura de Clave Pública (PKI), pero tienen propósitos y alcances distintos.

Diferencias entre CP y CPS

- Objetivo y Aplicación:
  - La CP establece las reglas a seguir y es aplicable a múltiples Autoridades de Certificación (CAs), organizaciones o dominios. Está diseñada para ser un conjunto de directrices que las CAs deben seguir para emitir certificados de forma confiable y segura.
  - La CPS, por otro lado, detalla cómo una CA específica, o una organización, cumple con estas directrices en la práctica.
- Implementación:
  - Mientras que la CP es más general y se centra en qué deben hacer las entidades para ser confiables, la CPS describe cómo se implementan estos requisitos en las operaciones diarias de una CA específica.
  - La CPS es, por lo tanto, un documento más técnico y detallado que refleja la aplicación real de las políticas en las prácticas cotidianas de una CA.

Política de certificado y declaración de prácticas de certificación (CPS)

Diferencias entre política de certificación y declaración de prácticas de certificación

Diferencias entre CP y CPS

- Interoperabilidad:
  - La CP se utiliza para guiar las operaciones de PKI que buscan ser interoperables entre sí. Es más, se podría decir que una CP ofrece un estándar que las diferentes CAs pueden seguir para garantizar un nivel básico de interoperabilidad.
  - En contraste, una CPS es única para cada CA y no se utiliza como medio para facilitar la interoperabilidad entre diferentes CAs o infraestructuras.
- Detalles y Especificaciones:
  - Una CPS suele contener más detalles operativos y específicos que una CP. Incluye las medidas y procesos que la CA utiliza para satisfacer los estándares y expectativas establecidos en la CP y puede ser más técnica y específica, adaptándose a las características únicas de la CA que la emite.

Política de certificado y declaración de prácticas de certificación (CPS)

Provisiones: política de certificación y declaración de prácticas de certificación

Tanto las políticas de certificación (CP) como las declaraciones de prácticas de certificación (CPS) se componen de un conjunto de provisiones. Una provisión es una práctica o declaración de política que abarca un tema específico dentro del ámbito de la CP o la CPS.

Diferencias entre CP y CPS en cuanto a provisiones:

- CP: se expresa como un conjunto de provisiones generales.
- CPS: se expresa como un conjunto de provisiones que satisfacen los requisitos establecidos en una o varias CP.

Marco de provisiones. La norma RFC 3647 define un marco compuesto por nueve componentes para organizar las provisiones de CP y CPS:

- Introducción
- Publicación y repositorio
- Identificación y autenticación
- Ciclo de vida de los certificados
- Requisitos de operaciones
- Facilidades, gestión y controles de operación
- Controles técnicos de seguridad
- Perfiles de certificado, CRL y OCSP
- Auditoría de cumplimiento
- Otros asuntos legales y de negocio

Política de certificado y declaración de prácticas de certificación (CPS)

Provisiones: política de certificación y declaración de prácticas de certificación

Utilidad del marco:

- Creación de CP y CPS: el marco proporciona una estructura para organizar las provisiones.
- Acuerdos entre partes involucradas en PKI: el marco facilita la creación de acuerdos de interoperabilidad.

Flexibilidad del marco:

- El marco es extensible y puede ser ampliado para incluir subcomponentes.
- Se recomienda que todos los componentes estén completos, incluso si no incluyen requisitos, para asegurar que se han considerado todos los aspectos relevantes.

Lista de certificados revocados (CRL)

Introducción

Razones para la revocación de un certificado

El propietario de un certificado puede revocarlo si lo considera necesario. Las razones para la revocación, según el estándar X.509, son:

- Inespecífica: No se indica ninguna razón.
- Compromiso de la clave privada: La clave privada asociada al certificado está comprometida.
- Compromiso de la clave privada de la CA: La clave privada de la CA que emitió el certificado está comprometida.
- Ruptura del vínculo: El propietario del certificado ya no tiene derecho a acceder al mismo o no lo necesita.
- Reemplazo del certificado: Un nuevo certificado reemplaza a uno existente.
- Cese de operaciones de la CA: La CA que emitió el certificado deja de ser operable.
- Certificado en espera: El certificado se mantiene en espera de una acción. Se considera revocado hasta que se activa.

Verificación de certificados revocados

Es crucial verificar si un certificado ha sido revocado antes de utilizarlo. Además de verificar la fecha de expiración y la firma de la CA, se debe consultar una lista de certificados revocados (CRL). La CRL contiene los números de serie de todos los certificados revocados.

Lista de certificados revocados (CRL)

Introducción

Listas de certificados revocados (CRL)

Las CA son responsables de indicar el estado de revocación de los certificados. La información de revocación se puede obtener mediante:

- Online Certificate Status Protocol (OCSP). Es un método para verificar el estado de revocación de un certificado digital en tiempo real
- CRL
- Otros mecanismos

En el caso de las CRL, la CA o un emisor delegado las firma y las publica en un repositorio público. Cuando se utiliza un certificado, se verifica que su número de serie no esté en la CRL. Las CRL se actualizan periódicamente (cada hora, día o semana) para garantizar que la información esté actualizada.

Las CRL tienen la ventaja de poder distribuirse de la misma manera que los certificados. Sin embargo, es importante que la frecuencia de actualización sea alta para evitar considerar válidos certificados que deberían ser revocados.

La extensión "CRLDistributionPoint" dentro del certificado permite indicar dónde obtener la CRL correspondiente.

¿Cómo se verifica si un certificado digital ha sido revocado?

Se verifica si el número de serie del certificado está en una lista de certificados revocados (CRL). La CRL se puede obtener de un repositorio público o mediante OCSP.

Lista de certificados revocados (CRL)

Formato de una lista de revocación de certificados

Si bien una CRL puede definirse como una lista con los números de serie de los certificados revocados, la CRL X.509 está compuesta por los siguientes campos:

- Algoritmo de firma: Algoritmo utilizado por la entidad correspondiente para firmar la lista.
- Valor de la firma: Firma de la lista o quién firma.
- Nombre emisor: Nombre de la CA o de la entidad emisora de CRL encargada de emitir la CRL.
- Día de emisión: Día en el que se realiza la emisión de la CRL.
- Día emisión nueva lista: Día en el que se ha de realizar la emisión de la nueva CRL.
- Lista de certificados revocados: Por cada certificado se ha de indicar su número de serie y el momento de la revocación.
- Extensiones: Campos opcionales como el identificador de la clave utilizada para realizar la firma de la CRL, un nombre alternativo de la entidad emisora de la CRL, identificadores de Delta CRL (CRL que contienen actualizaciones sobre otras distribuidas previamente), etc.

Lista de certificados revocados (CRL)

Concepto de Delta CRL

Las listas de revocación de certificados (CRL) se publican periódicamente. Esto significa que existe un lapso entre la publicación de una CRL y la siguiente donde los usuarios no son informados sobre nuevos certificados revocados. Para solucionar este inconveniente se crearon las Delta CRL.

Las Delta CRL son listados parciales de una CRL que contienen únicamente los certificados revocados desde la publicación de la última CRL completa. Gracias a las Delta CRL, la ventana de tiempo donde los usuarios desconocen la revocación de un certificado se reduce. Sin embargo, su uso incrementa la carga de trabajo de la Autoridad Certificadora que debe emitirlas con más frecuencia.

Si bien las Delta CRL son una mejora, no brindan inmediatez absoluta. Es por ello que se desarrolló el protocolo OCS.

Lista de certificados revocados (CRL)

Online Certificate Status Protocol (OCSP)

OCSP, definido en la RFC 2560, es un protocolo alternativo a las CRL para la revocación de certificados X.509. Su objetivo es facilitar la verificación en línea del estado de los certificados, evitando fallos por CRL desactualizadas.

OCSP define el intercambio de datos entre un cliente y un servidor OCSP para conocer el estado de un certificado:

- Solicitud: enviada por el cliente al servidor, contiene la versión del protocolo, el servicio solicitado, el identificador del certificado y, opcionalmente, extensiones.
- Respuesta: enviada por el servidor al cliente, puede ser de varios tipos, no todos soportados por todos los servidores. Todas las respuestas son firmadas por el servidor.

La respuesta básica contiene: la versión de la sintaxis, el nombre del servidor, la respuesta para cada certificado, campos opcionales, el identificador del algoritmo de firma y la firma del hash de la respuesta.

La respuesta para cada certificado contiene: el identificador del certificado, el estado del certificado, el período de validez de la respuesta y extensiones opcionales.

OCSP ofrece ventajas sobre las CRL:

- Información reciente: se requiere conexión con el servidor OCSP que tiene información actualizada.
- Eficiencia: no requiere procesar CRL y consume menos recursos en cliente y servidor.
- Seguridad: no se intercambia información sensible.

Funcionamiento de las solicitudes de firma de certificados (CSR)

Las Solicitudes de Firma de Certificado (Certificate Signing Request, CSR) representan un procedimiento establecido en el estándar PKCS#10/RFC 2986, destinado a la solicitud de certificados digitales. Este proceso permite a las Autoridades Certificadoras (CA) obtener la información necesaria para la emisión de certificados sin requerir la clave privada del solicitante. A continuación, se detallan las fases críticas en el proceso de solicitud de un certificado:

1.- Construcción de la Solicitud:

- La entidad solicitante genera una CSR, la cual incluye:
  - Información de Solicitud de Certificado:
  - Versión actual de la solicitud (actualmente debe ser 0).
  - Nombre del solicitante.
  - Clave pública del solicitante.
  - Otros atributos relevantes para proporcionar información adicional sobre el solicitante.
- Firma de la Solicitud: Indica la firma digital del solicitante, realizada con su clave privada.
- Algoritmo de Firma: Especifica el algoritmo utilizado para firmar la solicitud.

2.- Firma del Solicitante: El solicitante firma la CSR utilizando su clave privada para asegurar la autenticidad e integridad de la solicitud.

3.- Envío y Verificación por la CA: La solicitud completa se envía a la CA o a una Autoridad de Registro (AR) delegada. Esta entidad verifica la identidad del solicitante y la autenticidad de la firma. Además, se asegura de que la solicitud cumpla con las Políticas de Certificación (PC) de la CA. Por ejemplo, si la solicitud demanda una validez del certificado de 10 años, pero la CA solo emite certificados con una duración máxima de 4 años, la duración impuesta será de 4 años.

Funcionamiento de las solicitudes de firma de certificados (CSR)

4.- Emisión del Certificado: Si la solicitud es aceptada y cumple con las políticas de la CA, se emite un certificado X.509. Este certificado contiene:

- Nombre del solicitante.
- Clave pública del solicitante.
- Nombre de la CA emisora.
- Número de serie de la CA.
- Periodo de validez del certificado.
- Algoritmo de firma utilizado.

Este proceso asegura una emisión segura de certificados, manteniendo la privacidad de las claves del solicitante y garantizando la autenticidad de la información proporcionada.

Infraestructura de gestión de privilegios (PMI)

Las Infraestructuras de Gestión de Privilegios (PMI, por sus siglas en inglés de Privilege Management Infrastructure) son sistemas diseñados para administrar de manera efectiva los permisos o acciones autorizadas a entidades específicas dentro de una organización. Estas infraestructuras utilizan certificados de atributos para la asignación de privilegios, proporcionando un mecanismo seguro y controlado para gestionar el acceso y las capacidades dentro de los sistemas informáticos.

Entidades Participantes en una PMI

Dentro de una PMI, que opera conforme a la normativa X.509, las entidades involucradas varían según las fases de emisión, verificación y revocación de los certificados de atributos. Cada fase involucra a diferentes entidades en distintos grados, las cuales se describen a continuación:

- Fuente de Autoridad (SOA): Entidad encargada de emitir los certificados, definiendo los privilegios otorgados a través de uno o más atributos. En la práctica, son pocas las entidades que desempeñan el papel de SOA dentro de una organización.
- Autoridad de Atributos (AA): Entidades que pueden delegar privilegios. A diferencia de los Propietarios del Privilegio (PH), las AA tienen la capacidad de transferir los privilegios otorgados. Debido a su capacidad para delegar, es común encontrar múltiples AA dentro de una organización.
- Propietario del Privilegio (PH): Individuos o entidades que poseen privilegios específicos. Aunque los PH pueden ejercer siempre el privilegio, a diferencia de las AA, no tienen la capacidad de transferirlo.
- Verificador de Privilegios: Se encarga de validar la autenticidad y vigencia de los certificados de atributos cuando un titular desea ejercer su privilegio, como el acceso a un recurso electrónico.

Infraestructura de gestión de privilegios (PMI)

Entidades Participantes en una PMI

La emisión de certificados especifica claramente el privilegio concedido al titular, mientras que la verificación asegura que solo los titulares autorizados puedan ejercer los privilegios especificados en sus certificados. En caso de necesidad, la SOA puede emitir revocaciones de certificados, las cuales se registran en la Lista de Certificados de Atributos Revocados (ACRL, por sus siglas en inglés).

Este sistema de PMI facilita una gestión de privilegios segura y efectiva, diferenciándose de las Infraestructuras de Clave Pública (PKI) en su enfoque específico en la administración de privilegios a través de certificados de atributos, en lugar de la gestión de identidades y cifrado de comunicaciones.

Infraestructura de gestión de privilegios (PMI)

Proceso de verificación de privilegios

El proceso de verificación de privilegios en una Infraestructura de Gestión de Privilegios (PMI) es fundamental para asegurar que solo los usuarios autorizados puedan realizar acciones específicas sobre recursos determinados. Este proceso implica varias etapas clave:

- Solicitud de Acción: El propietario del privilegio inicia el proceso solicitando realizar una acción sobre un recurso específico. Esta solicitud es el primer paso para acceder al recurso deseado.
- Comprobación de Atributos: El verificador evalúa si los atributos de privilegio del solicitante son adecuados para la acción requerida. Este paso implica una revisión detallada de:
  - Los datos contenidos en el certificado del solicitante.
  - La naturaleza del recurso solicitado.
  - Otros factores contextuales, como la fecha y hora de la solicitud.
  - Si los atributos no cumplen con los requisitos, el verificador deniega el permiso.
- Verificación de la Vigencia del Certificado: Esta etapa se divide en dos acciones cruciales:
  - Validación de la Cadena de Certificación: Se verifica que la firma del certificado de atributos sea legítima y emitida por una autoridad autenticada y confiable. Dado que puede haber múltiples Autoridades de Atributos (AA) y una Fuente de Autoridad (SOA) involucradas, es necesario examinar toda la cadena de certificación. La autenticación de estas entidades suele realizarse mediante un certificado de clave pública.
  - Comprobación de Revocación: Se verifica si el certificado ha sido revocado, consultando la lista de certificados de atributos revocados emitida por la SOA.

Infraestructura de gestión de privilegios (PMI)

Aplicación de PMI para el control de acceso

Las Infraestructuras de Gestión de Privilegios (PMI) tienen un papel crucial en los sistemas de control de acceso, facilitando la administración eficiente de quién puede acceder a qué recursos y con qué propósitos. La aplicación de PMI a estos sistemas se manifiesta principalmente en tres modelos de control de acceso:

- Modelo Discrecional (DAC): En este modelo, la asignación de privilegios a usuarios y recursos se realiza de manera individualizada. Es común en entornos donde el administrador controla los permisos de acceso directamente, como en bases de datos o servidores. A través de los certificados de atributos de PMI, se pueden representar los permisos para actuar sobre recursos específicos. Sin embargo, este modelo puede complicar la gestión de privilegios, especialmente cuando se requiere revocar todos los permisos asociados a un usuario, como en el caso de un empleado despedido.

- Sistema de Acceso Multinivel: Este modelo es preferido en entornos con distintos grados de confidencialidad de la información. Los recursos se etiquetan con niveles de seguridad (como "confidencial" o "alto secreto"), y los usuarios tienen permisos que corresponden a estas etiquetas. La implementación de PMI facilita la asignación de certificados de atributos para definir los privilegios sobre recursos etiquetados, mejorando la gestión de acceso según la clasificación de seguridad.

- Control de Acceso Basado en Roles (RBAC): Este enfoque moderno permite asignar conjuntos de privilegios a través de roles, simplificando la administración de permisos. Con RBAC, es posible crear jerarquías de roles para una gestión más eficiente, permitiendo, por ejemplo, que un director tenga todos los privilegios de un subdirector, además de otros exclusivos. La PMI se adapta bien a RBAC, utilizando certificados de atributos específicos para definir los roles y sus privilegios correspondientes.

La PMI mejora la flexibilidad y seguridad de los sistemas de control de acceso, permitiendo una gestión más precisa de los privilegios y facilitando la revocación de accesos cuando es necesario.

Infraestructura de gestión de privilegios (PMI)

Comparación con respecto a una PKI

La Infraestructura de Gestión de Privilegios (PMI) y la Infraestructura de Clave Pública (PKI) comparten varias similitudes fundamentales, derivadas de estar definidas bajo la norma X.509, lo que subraya una base común en términos de estructura y funcionalidad:

- Gestión de Certificados: Tanto la PMI como la PKI gestionan certificados que establecen relaciones de confianza. Los certificados de clave pública en una PKI vinculan a una entidad con su clave pública, facilitando la verificación de la identidad y el cifrado de la comunicación. Por otro lado, en una PMI, los certificados de atributos relacionan al titular con propiedades o privilegios específicos, permitiendo la gestión y control de accesos basada en atributos.

- Jerarquía de Entidades: Ambas infraestructuras implementan una jerarquía de entidades. La PKI se organiza alrededor de una Autoridad Certificadora raíz (CA) y posiblemente múltiples autoridades subordinadas, estableciendo una cadena de confianza. De manera similar, la PMI cuenta con una Fuente de Autoridad (SOA) como entidad raíz y Autoridades de Atributos (AA) que pueden emitir certificados para delegar privilegios.

- Gestión de la Revocación: La revocación de certificados es esencial en ambas estructuras para mantener la seguridad y la confianza. En la PKI, los certificados revocados se listan en una Lista de Certificados Revocados (CRL), mientras que en la PMI se utilizan Listas de Certificados de Atributos Revocados (ACRL). El propósito y el contenido de estas listas son comparables, proporcionando un mecanismo para informar sobre certificados que ya no son válidos o de confianza.

Estas analogías entre la PMI y la PKI destacan cómo ambas infraestructuras aprovechan principios de seguridad similares para diferentes propósitos: la PKI enfocada en la autenticación y el cifrado, y la PMI en la administración detallada de privilegios y control de acceso.

Campos de certificados de atributos, usos habituales y la relación con los certificados digitales

Campos de los certificados de atributos

Los Certificados de Atributos (CA) según el estándar X.509 tienen una estructura definida que incluye varios campos esenciales para su función y gestión. Estos campos permiten la identificación del titular, la autenticación del emisor, y la definición de los privilegios otorgados. Los principales campos son:

- **Versión**: Indica la versión del certificado, siendo "v2" para los CA. Esta versión no es retrocompatible con versiones anteriores.
- **Propietario (Holder)**: Identifica al titular del certificado, pudiendo ser el identificador de un certificado de clave pública asociado (PKC), el nombre del sujeto en el PKC, o un resumen criptográfico.
- **Nombre del Emisor**: Corresponde al nombre de la Source Of Authority (SOA) que emite el certificado.
- **Algoritmo de Firma**: Especifica el algoritmo usado por la SOA para firmar el certificado.
- **Firma**: La firma realizada por la SOA emisora sobre el certificado.
- **Número de Serie**: Un número entero positivo único y largo que identifica el certificado de forma exclusiva.
- **Periodo de Validez**: Fechas que marcan el inicio y fin de la validez del certificado.
- **Atributos**: Contiene una secuencia de atributos que proporcionan información sobre el titular y, si el certificado se usa para autorización, incluirá un conjunto de privilegios. Se permite solo una instancia de cada tipo de atributo por certificado, y debe haber al menos un atributo.
- **Identificador Único del Emisor**: Identifica de manera única a la SOA emisora, usado solo si se aplica en el PKC de la SOA.
- **Extensiones**: Proporcionan información adicional relevante para el uso del certificado, como objetivos de uso, identificador de la clave de la SOA utilizada para verificar la firma del certificado, y los puntos de distribución de la Lista de Certificados Revocados (CRL), entre otros.

Campos de certificados de atributos, usos habituales y la relación con los certificados digitales

Campos de los certificados de atributos

Tipos de Atributos en Certificados de Atributos

Los certificados de atributos son fundamentales en la gestión de privilegios y acceso dentro de las Infraestructuras de Gestión de Privilegios (PMI). Estos certificados pueden contener diversos tipos de atributos, que varían en función de su propósito y la naturaleza de la información que proporcionan. Cada tipo de atributo puede albergar múltiples valores o un único valor, dependiendo de su diseño y utilización. Se pueden distinguir seis tipos principales de atributos:

- **Servicio de Autenticación de la Información**: Facilitan la autenticación de la identidad del titular por aplicaciones distintas a aquella para la que originalmente fue diseñado el certificado. Estos atributos pueden ser cifrados para proteger información sensible, como contraseñas.
- **Identidad de Acceso**: Proporcionan detalles sobre el propietario del certificado, permitiendo que las autoridades de verificación autoricen o denieguen solicitudes de acción por parte de usuarios específicos. Este tipo de atributos es versátil, aceptando múltiples valores para reflejar diversas identidades o capacidades.
- **Identidad de Cobro**: Se utilizan en contextos donde los servicios implican costos, identificando al propietario del certificado para la imputación de gastos. Distinguen al titular en situaciones financieras.
- **Grupo**: Informan sobre la afiliación a grupos del propietario del certificado, permitiendo la clasificación y el manejo colectivo dentro de la organización o sistema.
- **Rol:** Indican los roles específicos asignados al titular del certificado, soportando la asignación de múltiples valores para reflejar diferentes responsabilidades o niveles de acceso.

Campos de certificados de atributos, usos habituales y la relación con los certificados digitales

Campos de los certificados de atributos

Tipos de Atributos en Certificados de Atributos

- **Autorización (Clearance)**: Contienen información detallada sobre las autorizaciones específicas del titular, incluyendo las políticas de seguridad aplicables. Estos atributos son esenciales para el control de acceso basado en políticas, y las organizaciones pueden definir sus propias políticas de seguridad para una gestión detallada.

Estos atributos juegan un papel crucial en la administración efectiva de privilegios y acceso, permitiendo una gestión detallada y flexible de las autorizaciones y capacidades de los usuarios dentro de una infraestructura de seguridad.

Campos de certificados de atributos, usos habituales y la relación con los certificados digitales

Usos habituales de los certificados de atributos

Los certificados de atributos son herramientas poderosas dentro de las infraestructuras de seguridad digital, proporcionando una base sólida para la gestión de identidades y el control de acceso. Estos certificados se utilizan en una amplia gama de servicios, destacando principalmente en:

- **Control de Acceso**: Fundamental en sistemas que implementan control de acceso basado en roles. En estos sistemas, no es necesario utilizar una identidad específica para acceder a un recurso; basta con demostrar la pertenencia a un rol o grupo determinado. Los certificados de atributos permiten una asignación dinámica y flexible de privilegios basada en la afiliación a grupos o roles específicos.

- **Autenticación en el Origen**: La autenticación verifica que una entidad es quien afirma ser. Al incluir una referencia a un Certificado de Clave Pública (PKC) dentro del certificado de atributos, la autenticación se realiza utilizando la clave privada asociada. Esto asegura que la solicitud de acceso proviene del propietario legítimo del certificado.

- **No Repudio**: Los certificados de atributos, al estar ligados a un PKC, permiten el uso de firmas digitales como mecanismo para autenticar la fuente de una acción o documento y prevenir que el emisor niegue haber realizado tal acción. Los atributos contenidos en el certificado brindan información adicional sobre la entidad que realiza la firma, fortaleciendo el principio de no repudio en la transmisión de datos.

La combinación de estos usos proporciona un marco robusto para la seguridad digital, mejorando la gestión de acceso y la autenticidad de las transacciones electrónicas. Los certificados de atributos, por tanto, son esenciales para sistemas que requieren una alta confianza en la identidad de los usuarios y en la integridad de las acciones realizadas, como en el ámbito de la sanidad digital, el comercio electrónico, y la administración electrónica.

Campos de certificados de atributos, usos habituales y la relación con los certificados digitales

Certificados de clave pública digitales frente a certificados de atributos

La distinción entre Certificados de Clave Pública (PKC) y Certificados de Atributos (AC) se centra principalmente en su propósito y estructura:

- PKC: Vinculan a un sujeto con una clave pública. La clave privada correspondiente se mantiene en secreto y no forma parte del certificado. Este enlace entre el sujeto y su clave pública es fundamental para procesos de autenticación y cifrado, garantizando que el sujeto es, efectivamente, el propietario de la clave pública.
- AC: Estos certificados, por otro lado, vinculan un conjunto de atributos con un sujeto o con el identificador de un certificado digital (PKC). Los atributos pueden incluir roles, permisos o cualquier otra información relevante que no esté directamente relacionada con la identidad criptográfica del sujeto.

Ventajas de los AC sobre los PKC en el Proceso de Revocación

- Flexibilidad en la Revocación: Los AC ofrecen ventajas significativas, especialmente en escenarios donde se requiere una revocación más granular. Si los atributos asignados tienen una validez diferente o más extensa que la del PKC asociado, o si se necesita revocar un atributo específico sin afectar a otros, los AC son especialmente útiles.
- Autoridad Certificadora Diferente: También son convenientes cuando la entidad que certifica los atributos es diferente de la que emite el PKC. Esto permite una separación de responsabilidades y una gestión de privilegios más flexible dentro de una organización.
- Inclusión de Atributos en PKC: Si se desea incorporar atributos específicos dentro de los certificados digitales (PKC), se requeriría un proceso adicional para obtener estos atributos de entidades autorizadas que los proporcionen. Esto implica una complejidad adicional en la gestión de los certificados digitales.

Campos de certificados de atributos, usos habituales y la relación con los certificados digitales

Certificados de clave pública digitales frente a certificados de atributos

En resumen, mientras que los PKC se enfocan en establecer una identidad criptográfica segura para autenticación y cifrado, los AC se utilizan para gestionar información adicional sobre el titular del certificado, ofreciendo una mayor flexibilidad en la asignación y gestión de roles y privilegios. Esta diferenciación permite aplicar una seguridad detallada y adaptada a las necesidades específicas de acceso y autorización dentro de sistemas y redes.

Campos de certificados de atributos, usos habituales y la relación con los certificados digitales

Modos de uso de los certificados de atributos

La RFC 3281 establece dos modelos principales para el uso de certificados de atributos (AC) en la autorización de entidades: el modelo push y el modelo pull. Estos modelos definen cómo se transmite y se verifica la información de autorización.

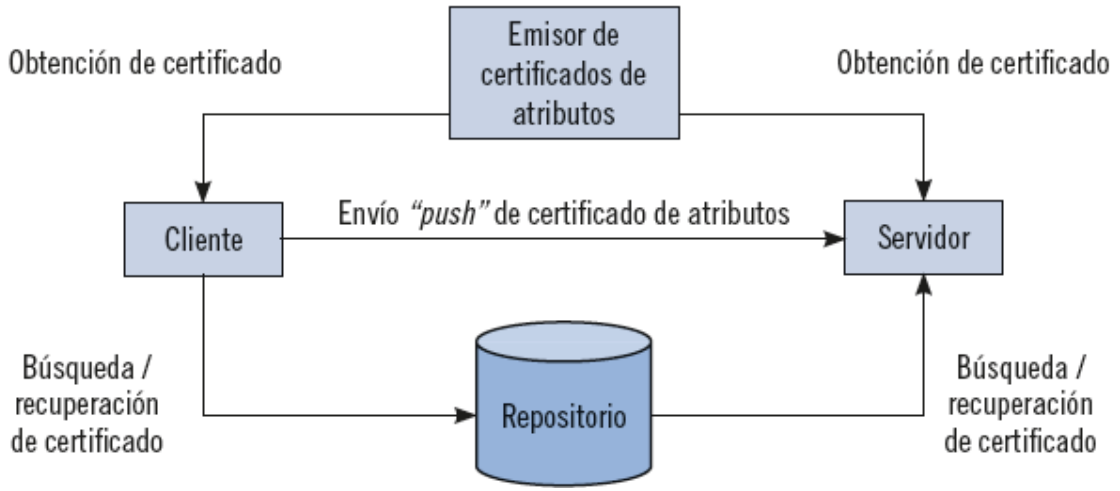
Modelo Push

En este modelo, el cliente envía proactivamente al servidor de autorización toda la información necesaria para autenticarse, así como los certificados de atributos que acreditan sus privilegios. Este enfoque es ideal en escenarios multi-dominio, donde los privilegios del cliente se establecen en un dominio diferente al del servicio que intenta acceder. Por ejemplo, un empleado que quiere acceder a recursos específicos en un dominio externo, donde los privilegios dependen de su rol en el dominio de origen.

Ventajas

- Facilita la autorización en entornos multi-dominio.
- Permite una asignación de privilegios personalizada y específica del contexto.

Intercambios de información relacionados con los certificados de atributos (adaptado de RFC 3281)



Campos de certificados de atributos, usos habituales y la relación con los certificados digitales

Modos de uso de los certificados de atributos

Modelo Pull

En contraste, el modelo pull implica que el cliente primero se autentica ante el servidor, que luego busca activamente cualquier certificado de atributos relevante para el solicitante. Este método es más adecuado cuando los privilegios se gestionan en el mismo dominio que ofrece el servicio, como sería el caso de una suscripción a servicios digitales.

Ventajas

- Reduce la necesidad de que los clientes gestionen activamente y presenten certificados.
- El servidor de autorización puede realizar una gestión centralizada de privilegios.

Inconvenientes

- Puede imponer una carga adicional en el servidor debido a la necesidad de buscar certificados de atributos.

Aplicación Ideal

El modelo pull es preferible en situaciones donde la administración de acceso y privilegios se centraliza en el dominio del servicio, facilitando así una gestión más uniforme y simplificada de las autorizaciones.

Ambos modelos, push y pull, ofrecen mecanismos eficaces para gestionar la autorización de entidades en diversos contextos de seguridad, dependiendo de la estructura y las necesidades específicas de la red o el sistema implicado. La elección entre uno u otro dependerá de factores como la arquitectura de red, los requisitos de seguridad, y la ubicación de la gestión de privilegios.

Aplicaciones que se apoyan en la existencia de una PKI

Las Infraestructuras de Clave Pública (PKI) se han convertido en un pilar fundamental de la seguridad en la red, proporcionando herramientas esenciales para la autenticación, la firma electrónica y el cifrado. La autenticación mediante PKI ofrece una alternativa robusta a los métodos tradicionales basados en nombre de usuario y contraseña, mejorando significativamente la seguridad de las aplicaciones y servicios en línea.

Uso de PKI para autenticación

La autenticación PKI se realiza a través de la verificación de la posesión de una clave privada por parte del usuario, sin la necesidad de transmitir esta clave o su equivalente. Este método es considerablemente más seguro que el uso de contraseñas, especialmente cuando estas últimas pueden ser vulnerables a ataques de fuerza bruta o ingeniería social. La clave privada, que se guarda de manera segura y protegida (a menudo con una frase de paso, medidas biométricas u otros métodos de seguridad adicionales), no se comparte ni se expone durante el proceso de autenticación.

Un ejemplo claro de la aplicación de PKI para la autenticación es el uso del protocolo SSL/TLS, ampliamente utilizado para establecer conexiones seguras en internet. Este protocolo utiliza certificados digitales, que son emitidos por Autoridades Certificadoras (CA) dentro de la PKI, para autenticar la identidad de los sitios web y cifrar los datos transmitidos entre el cliente y el servidor, garantizando la confidencialidad e integridad de la información.

La PKI, al basarse en la criptografía de clave pública, permite no solo autenticar la identidad de los usuarios y dispositivos en una red, sino también asegurar las comunicaciones y validar la integridad y origen de los datos a través de la firma electrónica y el cifrado. Esta infraestructura es esencial en una variedad de aplicaciones, desde la protección de transacciones en línea hasta la autenticación de usuarios en sistemas empresariales y la firma de documentos electrónicos, demostrando su versatilidad y capacidad para mejorar la seguridad en el entorno digital.

Aplicaciones que se apoyan en la existencia de una PKI

Uso de PKI para firmar

La firma digital, una de las aplicaciones más extendidas de las Infraestructuras de Clave Pública (PKI), actúa como un mecanismo matemático para probar la autenticidad de mensajes digitales o documentos. Esta tecnología es fundamental en la firma de documentos, especialmente en formatos como XML, y en la autenticación de correos electrónicos.

Características Principales

- Autenticidad y Verificación: La firma de un mensaje se efectúa con la clave privada del emisor, mientras que la verificación se realiza con la clave pública. El uso de resúmenes criptográficos facilita la comprobación de la integridad del mensaje.
- Seguridad en Transacciones: La firma digital elimina la necesidad de gestiones en papel y mejora la verificación de firmas, ofreciendo una seguridad superior a las firmas manuscritas, que pueden ser fácilmente falsificadas.
- Validación Temporal: La validez de una firma digital depende de la verificación criptográfica y la autenticidad de la cadena de certificación. La caducidad o revocación de cualquier certificado de la cadena puede invalidar la firma.
- Aplicaciones: Los programas de ofimática más comunes permiten la adición de firmas digitales a documentos. Además, existen herramientas especializadas para la firma de documentos PDF, como Sinadura o ClickSign, facilitando la implementación de firmas digitales en entornos empresariales y gubernamentales.

Aplicaciones que se apoyan en la existencia de una PKI

Uso de PKI para firmar

Características Principales

- Firmas Longevas: Para garantizar la validez de las firmas a lo largo del tiempo, se ha desarrollado el concepto de firma longeva, que busca preservar la autenticidad de las firmas frente al avance del tiempo y posibles vulnerabilidades en los algoritmos de cifrado.
- Firma de Código Fuente: Las PKI también son esenciales para la firma de código fuente de programas, asegurando que el software no ha sido alterado desde su creación y que es responsabilidad de la entidad que lo firma. Esto es especialmente relevante para prevenir la distribución de malware.

Consideraciones de Seguridad

La custodia de la clave privada utilizada para firmar es crítica; su compromiso puede poner en riesgo la seguridad de los productos distribuidos por una empresa. Incidentes en los que atacantes han accedido a estas claves privadas subrayan la importancia de una gestión segura y responsable de las claves privadas dentro de las organizaciones.

En conclusión, las PKI y las firmas digitales juegan un rol crucial en la seguridad digital, ofreciendo un método seguro y eficiente para la autenticación de documentos y comunicaciones en el ámbito digital. Su implementación adecuada y gestión cuidadosa son esenciales para mantener la confianza y seguridad en los entornos digitales.

Aplicaciones que se apoyan en la existencia de una PKI

Uso de PKI para cifrado

La Infraestructura de Clave Pública (PKI) es una herramienta esencial para el cifrado de datos, garantizando la confidencialidad de la información transmitida o almacenada. La PKI facilita este proceso al permitir que cualquier usuario cifre datos usando la clave pública del destinatario, asegurando que solo aquellos con la correspondiente clave privada puedan descifrar y acceder a la información.

Principios del Cifrado con PKI

- Confidencialidad: La PKI asegura que los datos cifrados solo puedan ser accesibles por el destinatario previsto, manteniendo la privacidad de la información.
- Claves Asimétricas: Utiliza un par de claves asimétricas; la clave pública se emplea para cifrar los datos, mientras que la clave privada se usa para descifrarlos.
- Seguridad de la Clave Privada: La efectividad del cifrado depende de mantener la clave privada en secreto y protegida.

Aplicaciones del Cifrado PKI

- Tarjetas Inteligentes: Se utiliza para proteger información sensible almacenada, como el PIN de tarjetas de crédito, asegurando que solo el titular de la tarjeta pueda acceder a ella.
- Correo Electrónico: Programas como Thunderbird permiten el cifrado de correos electrónicos, protegiendo la información personal o confidencial compartida a través de esta vía.
- Almacenamiento de Datos: Herramientas como GPG4Win facilitan el cifrado de archivos y carpetas en dispositivos de almacenamiento, protegiendo los datos de accesos no autorizados.

Resumen

Las Infraestructuras de Clave Pública (PKI) son el pilar fundamental para el uso extendido de certificados digitales en Internet, facilitando la autenticación, el cifrado y la firma digital. Estas infraestructuras involucran a autoridades de certificación organizadas jerárquicamente o en red, que emiten, gestionan, almacenan y revocan los certificados digitales. Para obtener un certificado, los usuarios deben generar una Solicitud de Firma de Certificado (CSR), que luego es procesada por estas autoridades.

La verificación de certificados es esencial para confirmar la autenticidad y validez de la cadena de certificación, mientras que la revocación se maneja a través de Listas de Revocación de Certificados (CRL) o el protocolo Online Certificate Status Protocol (OCSP), asegurando que los certificados comprometidos o caducados no se utilicen indebidamente.

Paralelamente, las Infraestructuras de Gestión de Privilegios (PMI) complementan las PKI al administrar los certificados de atributos, que validan los derechos o privilegios del titular, de manera similar a cómo los certificados de clave pública validan la identidad. Esta dualidad entre PKI y PMI subraya la profundidad y complejidad del ecosistema de seguridad digital, proporcionando los medios para una autenticación segura, la integridad de los datos y la privacidad en línea.