Material de Lectura. Conceptos del Certificado Digital

Sandra Catalán Pallarés y Vicente R. Tomás López

2023

ÍNDICE

01 Introducción a los Certificados Digitales

Los certificados digitales son una piedra angular de la seguridad en línea. En un mundo cada vez más digitalizado, donde las transacciones, la comunicación y el acceso a recursos confidenciales se realizan en el ciberespacio, los certificados digitales desempeñan un papel esencial en la autenticación, la privacidad y la integridad de los datos. En este capítulo, profundizaremos en lo que son los certificados digitales y por qué son cruciales en el mundo digital actual.

¿Qué es un certificado digital?

En términos sencillos, un certificado digital es un documento electrónico utilizado para verificar y autenticar la identidad de una entidad en línea. Esta entidad puede ser una persona, una organización, un dispositivo o incluso un servicio web. Al igual que el carné de identidad o un pasaporte físico, un certificado digital atestigua quién es el titular, y se emite a través de una entidad de confianza conocida como Autoridad de Certificación (CA, del inglés Certification Authority).

Componentes Clave de un Certificado Digital

Antes de comenzar a comentar los componentes de un certificado digital, conviene entender los conceptos de clave pública y privada. La clave pública y privada son componentes básicos de la criptografía asimétrica[1]. La clave pública se comparte abiertamente y se utiliza para cifrar datos y verificar firmas digitales, mientras que la clave privada se mantiene en secreto y se utiliza para descifrar información cifrada y firmar documentos.

La clave privada no es un componente del certificado digital, no se almacena en él, pero sí un elemento fundamental en la utilización del certificado digital. La clave privada es generada

[1] La criptografía asimétrica implica el uso de dos claves distintas, pero relacionadas entre ellas: una clave pública para cifrar y verificar, y una clave privada para descifrar y firmar.

por el titular del certificado. Y es necesaria para firmar digitalmente documentos o datos, así como para descifrar información cifrada con la clave pública asociada.

Los componentes clave de un certificado digital son:

Información del titular: Esta sección del certificado digital contiene información detallada sobre el titular, como su nombre, dirección, dirección de correo electrónico y otros datos identificativos. Estos detalles son fundamentales para verificar la identidad del usuario o entidad que posee el certificado. Además, esta información permite a las partes participantes en la comunicación confiar en la identidad del titular al realizar transacciones o establecer comunicaciones en línea.

Clave pública: La clave pública forma parte de un par de claves criptográficas junto con la clave privada. La clave pública se utiliza para cifrar datos de manera segura durante las comunicaciones en línea. Es importante destacar que cualquier información cifrada con la clave pública solo puede descifrarse utilizando la clave privada correspondiente. La clave pública se comparte libremente con otros usuarios y es esencial para garantizar la confidencialidad de la información transmitida de manera segura.

Firma digital: La firma digital es un valor criptográfico generado utilizando la clave privada del titular del certificado. Se utiliza para firmar digitalmente documentos, mensajes y transacciones. La firma digital cumple dos funciones críticas: garantiza la integridad del contenido, lo que significa que el documento no ha sido alterado desde que se firmó, y verifica que el documento fue creado por el titular del certificado. La firma digital es una prueba irrefutable de la autenticidad del documento o mensaje.

Validez: Cada certificado digital tiene una fecha de inicio y una fecha de vencimiento. La fecha de inicio marca el momento en que el certificado se vuelve válido y confiable para su uso. Por otro lado, la fecha de vencimiento indica cuándo el certificado dejará de ser válido. Este aspecto asegura que los certificados tengan un período de vida útil limitado y no se puedan

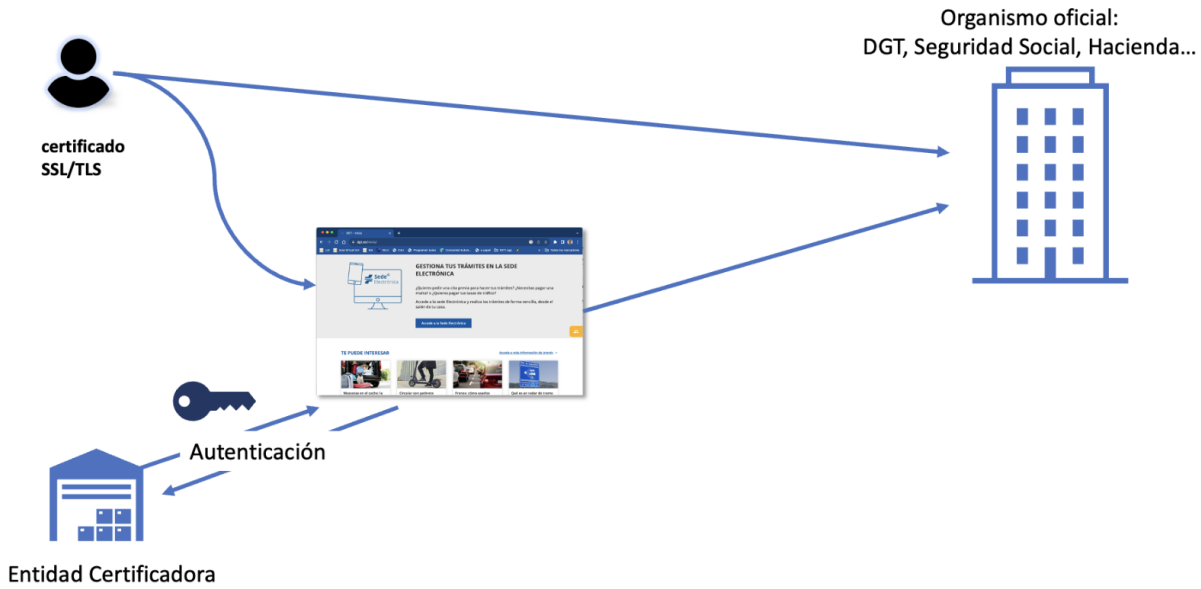
utilizar indefinidamente. Cuando un certificado expira, es necesario renovarlo para mantener su validez y continuar utilizando los servicios en línea de manera segura.

Si un certificado se pierde, ha sido robado o la clave privada del titular del certificado ha sido comprometida, la CA tiene la responsabilidad de revocar el certificado correspondiente y por lo tanto, ese certificado ya no puede utilizarse y debe renovarse.

Importancia de los Certificados Digitales

Los certificados digitales son indispensables en una serie de aplicaciones y contextos en línea, donde la seguridad y la autenticación son críticas. Algunas aplicaciones que hacen uso de los certificados digitales son las siguientes:

Seguridad en transacciones financieras: Los certificados digitales se utilizan para garantizar la seguridad en las transacciones financieras en línea, como las compras en sitios web de comercio electrónico y las transacciones bancarias electrónicas. La autenticación del usuario y la protección de los datos financieros son de máxima importancia en estos casos.



Comunicaciones seguras: Los certificados digitales permiten la comunicación segura y privada a través de canales en línea. Las firmas digitales garantizan que los mensajes y documentos no se modifiquen durante la transmisión y que provengan de la fuente esperada.

Acceso a recursos confidenciales: En organizaciones, tanto públicas como privadas, los certificados digitales se utilizan para controlar el acceso a recursos y datos confidenciales. Los empleados y usuarios autorizados pueden autenticarse utilizando sus certificados digitales.

Firma electrónica de documentos legales: La firma digital basada en certificados digitales es legalmente vinculante en muchos países y se utiliza para firmar electrónicamente contratos, acuerdos y otros documentos legales.

Protección de la integridad de los datos: Los certificados digitales garantizan que los datos no se alteren ni manipulen durante la transmisión o el almacenamiento. Esto es necesario en aplicaciones donde la integridad de los datos es crítica, como la atención médica y la administración de registros.

Ejemplos de Certificados Digitales

Los certificados digitales se usan en ámbitos muy distintos por lo que, en este apartado, se describen algunos de los más utilizados en España a modo de ejemplo.

DNI Electrónico (eDNI)

El DNI electrónico, ampliamente utilizado en España, es un ejemplo de certificado digital emitido por el gobierno. Este certificado permite a los ciudadanos españoles autenticarse en línea y firmar electrónicamente documentos, declaraciones fiscales y trámites administrativos. Contiene información personal del titular, como nombre, fecha de nacimiento y número de identificación, junto con una firma digital que respalda su autenticidad.

Certificado de la FNMT

La Fábrica Nacional de Moneda y Timbre (FNMT) emite certificados digitales en España utilizados en una variedad de aplicaciones. Este certificado incluye una clave pública que permite cifrar y verificar documentos electrónicos firmados digitalmente. Es comúnmente utilizado en transacciones en línea, comunicaciones seguras y autenticación en sitios web gubernamentales.

Certificado de la Generalitat Valenciana (GVA)

La Generalitat Valenciana emite certificados digitales que permiten a los ciudadanos y empresas de la Comunidad Valenciana autenticarse en línea y firmar documentos de manera electrónica. Estos certificados se utilizan en aplicaciones gubernamentales, como la presentación de documentos ante la administración pública y la firma electrónica de formularios oficiales.

Estos son solo algunos ejemplos, pero permiten ilustrar cómo los certificados digitales desempeñan un papel crucial en la autenticación y la seguridad en línea en una variedad de contextos, desde la identificación de ciudadanos hasta la firma electrónica de documentos legales.

02 Funciones de la Autoridad de Certificación y la Infraestructura de Clave Pública

Autoridad de Certificación

Las CA son actores clave en el ecosistema de la seguridad digital. Su papel en la emisión y gestión de certificados digitales es esencial para garantizar la autenticidad y la confiabilidad de las comunicaciones y transacciones en línea. En este capítulo, exploraremos en profundidad las funciones y responsabilidades de una CA y su importancia en la protección de la identidad y la integridad de los datos en el ciberespacio.

Funciones de la CA

Las CA desempeñan varias funciones esenciales en la emisión y gestión de certificados digitales:

Emisión de certificados: La función principal de una CA es emitir certificados digitales a los solicitantes que han sido debidamente verificados. Esto implica un proceso riguroso de validación de la identidad del solicitante y la generación del certificado digital que atestigua dicha identidad. La CA debe asegurarse de que los certificados emitidos sean precisos y confiables.

Revocación de certificados: En caso de pérdida, robo o compromiso de la clave privada del titular de un certificado, la CA tiene la responsabilidad de revocar el certificado correspondiente. La revocación garantiza que el certificado no pueda ser utilizado de manera fraudulenta para realizar transacciones o acceder a recursos confidenciales. Este proceso de revocación es crítico para mantener la integridad de la infraestructura de seguridad en línea.

Mantenimiento de la infraestructura de clave pública: Las CA son responsables de mantener una infraestructura de clave pública sólida y segura. Esto implica la generación y gestión de sus propias claves criptográficas, así como la protección de la integridad de los certificados

emitidos. La seguridad de la infraestructura de clave pública es esencial para garantizar la confianza en los certificados digitales emitidos por la CA.

Confianza en una CA

La confianza en una CA es un pilar fundamental de la seguridad en línea. Los navegadores web, sistemas operativos y aplicaciones confían en las CA para verificar la autenticidad de los certificados presentados por sitios web seguros y otros servicios en línea. Si una CA no es de confianza o su seguridad se ve comprometida, esto puede tener graves implicaciones para la seguridad de las comunicaciones en línea.

Infraestructura de Clave Pública

La Infraestructura de Clave Pública (PKI, del inglés Public Key Infrastructure) es un marco que respalda la emisión y gestión de certificados digitales. La PKI proporciona un conjunto de estándares, políticas y procedimientos que garantizan la seguridad y la confianza en los certificados digitales. En este capítulo, exploraremos cómo funciona la PKI y cómo proporciona una base sólida para la seguridad en línea.

Componentes de la PKI

La PKI consta de varios componentes interconectados que trabajan juntos para garantizar la confiabilidad de los certificados digitales:

Autoridades de certificación: Las CA son el componente central de la PKI. Son las entidades encargadas de emitir certificados digitales y verificar la identidad de los solicitantes. La confianza en una CA es esencial, ya que su papel es certificar que un titular de certificado es quien dice ser.

Repositorios de certificados: Los repositorios de certificados son bases de datos o servicios en línea donde se almacenan los certificados digitales emitidos por las CA. Estos repositorios

permiten a las partes interesadas buscar y recuperar certificados públicos. Es importante que los repositorios estén protegidos y sean accesibles para mantener la integridad de la PKI.

Mecanismos de revocación de certificados: Los mecanismos de revocación, como las Listas de Certificados Revocados (CRL, del inglés Certificate Revocation List) y los Protocolos de Estado de Certificado Online (OCSP, del inglés Online Certificate Status Protocol), permiten a las CA y a los usuarios verificar si un certificado ha sido revocado antes de confiar en él. Esto es esencial para mantener la seguridad y la confiabilidad de los certificados digitales.

La PKI establece un marco de confianza en el que las CA desempeñan un papel central en la emisión y gestión de certificados digitales. Este marco es la base para garantizar que los certificados digitales sean auténticos y que las comunicaciones en línea sean seguras y privadas.

03 Proceso de Generación de un Certificado Digital

Solicitud

El proceso de generación de un certificado digital comienza con la solicitud por parte de un usuario o entidad que desea obtener un certificado que respalde su identidad en el mundo digital. En este capítulo, exploraremos en detalle el proceso de solicitud y cómo se inicia la creación de un certificado digital.

Contenido de una Solicitud de Certificado

Una solicitud de certificado generalmente contiene información personal del solicitante, que es fundamental para establecer su identidad de manera confiable. Los elementos clave que se encuentran en una solicitud de certificado incluyen: *la información del titular* y *la clave pública,* que formarán parte del certificado.

Importancia de la Verificación de Identidad

La verificación de la identidad del solicitante es una parte crítica del proceso de solicitud. Las CA deben asegurarse de que el solicitante sea quien afirma ser antes de emitir un certificado. Esto se logra a través de una serie de métodos, que pueden incluir la presentación de documentos de identificación, la validación de información personal o incluso entrevistas en persona. La rigurosidad de la verificación es esencial para mantener la confianza en los certificados digitales.

Emisión

Una vez que la CA ha recibido y verificado la solicitud de certificado, procede a la emisión del certificado digital. En esta sección, exploraremos los pasos involucrados en el proceso de emisión y cómo se genera el certificado que será utilizado para autenticar al titular en línea.

Contenido de un Certificado Digital

Como ya se ha comentado, el certificado digital emitido contiene la información esencial que respalda la identidad del titular, así como la clave pública y la fecha de validez (fecha de inicio y vencimiento). Además, contiene la información de la CA emisora. Esto es, dispone de la información de la CA que emitió el certificado. Esto permite a otras partes verificar la autenticidad del certificado al comprobar la confiabilidad de la CA emisora.

Rol de la CA en la Emisión

La CA juega un papel fundamental en la emisión de certificados digitales. Su función no se limita a validar la identidad del solicitante, sino que también abarca:

Garantizar la integridad: La CA debe asegurarse de que el proceso de emisión sea seguro y que los certificados emitidos sean confiables y no hayan sido modificados durante su creación.

Proteger la clave privada: La CA debe tomar medidas rigurosas para proteger la clave privada que corresponde a la clave pública incluida en el certificado. La clave privada es secreta y es esencial para garantizar la seguridad y autenticidad de las comunicaciones en línea.

Renovación

Los certificados digitales tienen una vida útil limitada y deben renovarse antes de su fecha de vencimiento para mantener su validez. En esta sección, profundizaremos en el proceso de renovación y su importancia en la seguridad en línea.

Renovación y Clave Privada

Durante el proceso de renovación, se emite un nuevo certificado con la misma clave pública que el certificado anterior. La clave privada, que se mantiene en secreto y es conocida solo por el titular del certificado, no cambia en el proceso de renovación. Esto garantiza la continuidad de la confidencialidad y autenticidad de las comunicaciones en línea, ya que las

partes que confiaban en la clave pública anterior pueden seguir haciéndolo con el nuevo certificado.

La renovación oportuna es indispensable para evitar interrupciones en la capacidad del titular para autenticarse y participar en transacciones seguras en línea. La gestión adecuada de los certificados digitales y su renovación aseguran que la identidad digital del titular se mantenga actualizada y funcione de manera continua en el mundo digital.

En resumen, el proceso de generación de un certificado digital es un viaje que comienza con la solicitud, continúa con la emisión y se mantiene a lo largo de la vida útil del certificado mediante la renovación. Comprender este proceso es esencial para obtener el certificado digital y garantizar su disponibilidad en cualquier momento.

04 Formatos de Certificados Digitales

Los certificados digitales adoptan diversos formatos para cumplir con estándares y garantizar la interoperabilidad en entornos digitales. En este capítulo, describiremos algunos de los formatos más comunes de certificados digitales y proporcionaremos ejemplos prácticos de su implementación.

Formatos de Certificados Digitales

Algunos de los formatos más frecuentes usados en los certificados digitales son los siguientes:

X.509: Este es el formato estándar ampliamente utilizado para certificados de clave púbica. Los certificados X.509 siguen un conjunto de normas definidas en la Internet Engineering Task Force (IETF) y son compatibles con varios protocolos, como TLS/SSL. Cuando visitas un sitio web seguro (HTTPS), tu navegador utiliza certificados X.509 para establecer una conexión segura. Los certificados X.509 también se utilizan en sistemas de correo electrónico seguro (S/MIME) y otros protocolos.

PKCS#12 (PFX): Este formato se utiliza para almacenar certificados y claves privadas en un único archivo. Es comúnmente utilizado en entornos que requieren la exportación e importación de certificados y claves en un solo paquete.

PEM (Privacy Enhanced Mail): Aunque es más conocido por su uso en archivos de clave privada, el formato PEM también se utiliza para certificados digitales. Los archivos PEM son archivos de texto codificados en Base64 que contienen secciones claramente delimitadas para el certificado. Por ejemplo, Un archivo PEM podría contener la clave pública de un servidor web como se muestra a continuación:

```
-----BEGIN CERTIFICATE-----
MIICizCCAfQCCQCY8tKaMcOwDQYJKoZIhvcNAQEFBQAwgZQxCzAJBgNVBAYTAlVT
...
AQH/7kyPj4t/YnfyV6sJgPqzPXgXGx
-----END CERTIFICATE-----
```

DER (Distinguished Encoding Rules): Es un formato binario utilizado para codificar estructuras de datos, incluidos los certificados X.509. A menudo, los certificados en formato DER tienen la extensión .cer o .der. Puedes ver un ejemplo a continuación:

```
25e7 505b 33c5 2719 da00 19b7 4d9a 2466
7469 6f6e 3117 3015 060b 2b06 0104 0182
335a 3081 bd31 0b30 0906 0355 0406 1302
3082 07fd 3082 05e5 a003 0201 0202 1068
```

PKCS # 7 (o P7B): Es un formato para certificados digitales que se encuentra con mayor frecuencia en contextos de servidor de Windows y Java, y generalmente tiene la extensión .p7b. Los archivos PKCS # 7 no se utilizan para almacenar claves privadas.

El formato del certificado a utilizar dependerá de la información a almacenar en el archivo y de las características de la aplicación en las que se va a utilizar el certificado, pudiendo modificar el formato, mediante la utilización de herramientas específicas.

UNIVERSITAT JAUME I

#ProDigital