Certificado digital

¿Qué son? - Introducción básica

Son una especie de *clave* digital que permite a una persona, empresa u organización intercambiar datos a traves de la Internet mediante la PKI*.

El mismo evidencia si los datos fueron alterados antes de llegar al destino, así que si un tercero lograse realizar una alteración en esos datos se notará.[2]

Su uso más conocido es en los sitios web donde es preciso que el mismo haya sido certificado para garantizar que sus visitantes no están ante una falsificación y para prevenir que un atacante espíe en los datos de una transacción:

Página oficial de Comodo verificada y bajo conexión segura HTTPS.

También se los conoce como certificado de identidad (*identity certificate*).

¿Qué es la PKI*?[3]

Public Key Infraestructure (Infraestructura de Llave Pública) es una serie de políticas y procedimientos que establecen un intercambio seguro de datos, sus fundamentos se basan en la seguridad en internet:

- **Autenticación:** la importancia de la autenticación es verificar la identidad de los usuarios y máquinas es crucial cuando una organización abre sus puertas en Internet. Unos fuertes mecanismos de autenticidad asegura que los usuarios y máquinas son quienes aseguran ser.
- **Criptografía:** se usan algoritmos de criptografía para asegurar la privacidad de los datos enviados desde un computador a otro (éste mecanismo se le conoce como cifrado de extremo a extremo).
- **No-repudiación:** ninguna de las dos partes puede evitar enviar/recibir un mensaje. Ésto prueba que el usuario hizo determinadas operaciones en un determinado tiempo.
- **Control de acceso:** solo la persona o entidad a la cual está destinada la información puede acceder.

Ésta infraestructura utiliza dos elementos clave: Criptografía de Llave Pública y Autoridades de Certificación (comúnmente conocidos por la sigla CA).

Encriptado y desencriptado

Los beneficios de PKI vienen de la Criptografía de Llave Pública, la cual tiene como aspecto esencial el encriptado y desencriptado de datos digitales.

El encriptado convierte los datos a enviar en código incomprensible, su proceso opuesto es el desencriptado que es la única forma de obtener los datos originales (como "deshacer la conversión").

Llaves Públicas y Llaves Privadas

Se tratan de dos llaves criptográficas únicamente relacionadas (básicamente con un extenso código de caracteres alfanuméricos), aquí un ejemplo de una llave pública mostrado en la fuente Comodo[1]:

```
3048 0241 00C9 18FA CF8D EB2D EFD5 FD37 89B9 E069 EA97 FC20 5E35 F577 EE31 C4FB C6E4 4811 7D86
BC8F BAFA 362F 922B F01B 2F40 C744 2654 C0DD 2881 D673 CA2B 4003 C266 E2CD CB02 0301 0001
```

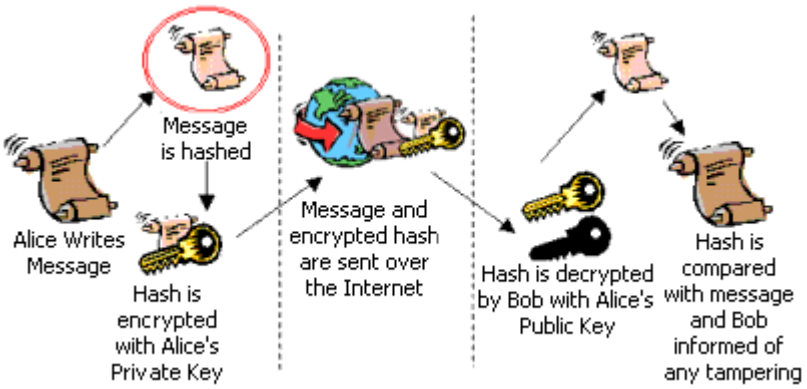
La llave pública es una llave que cualquiera puede acceder, contraria la misma existe la llave privada que pertenece solo a su propietario.

Como ambas están matemáticamente relacionadas se necesitan ambas para desencriptar los datos correspondientes, por ejemplo se tienen datos encriptados con una llave pública, para desencriptarlos se precisa de la llave privada que corresponde.

Aunque las llaves públicas son literalmente públicas existe un proceso que las ofrece de manera segura, mediante pequeños archivos que son los certificados digitales.

¿Cómo crear una firma digital?

Ésta imagen ilustra el proceso resumidamente:



https://www.comodo.com/resources/small-business/digital-certificates3.php

Profundizando un poco sobre los certificados digitales

Son archivos usados para atar criptográficamente la llave pública de una entidad con algunos atributos de la misma que la identifican.

Una entidad puede ser una persona/usuario, una empresa, una organización, ...

Para entender mejor puede ser comparado con una licencia de conducir o un pasaporte que tienen una foto del propietario adjunta.

Certificados Digitales y Autoridades de Certificado

Los certificados digitales son expedidos por Autoridades de Certificado (conocidos por su sigla en inglés "CA" (**C**ertification **A**uthority); son terceros de confianza que aprueban solicitudes de certificados y mantienen la información sobre su estado.

Su objetivo principal es asegurar que otras entidades no consiguen "*copiar*" a la original mediante una verificación por parte de dicho tercero que expidió el certificado a la entidad original.

Algunos ejemplos conocidos: DigiCert, VeriSign, ...

Tipos de certificados digitales

Dependiendo del uso que tendrá (entidad destino) el certificado puede ser del tipo...:

- **Personal:** pertenecen a usuarios, requieren que las transacciones web y de correo electrónico sean seguras.
- **Organización:** similar al del usuario, solo que para los empleados (interno de la organización).
- **Servidor:** prueban la titularidad de un nombre de dominio y establecen conexiones SSL/TLS cliente-servidor.
- **Desarrollador:** para probar la legitimidad e integridad del *software* distribuido.

¿Cómo elegir la mejor CA?

Existen muchos proveedores de certificados digitales, ¿pero cómo saber cuál es el más seguro? ¿cuál me sale más barato? ¿hasta qué punto la veracidad de un servicio es validado (dominio/servidor)? ¿es realmente seguro (fue éste servicio víctima de un hackeo)?, etc.. La adquisición de certificados digitales siempre tiene un costo por "*suscripción*" que varía acorde no solo con su "*calidad*", también se toma en cuenta si valida solo el dominio o también la organización que le corresponde, la demora que existe antes de certificar el sitio (desde inmediatamente hasta 2 días), si admite *wildcards* (comodines) que abarcan los subdominios del sitio web a certificar, etc.

A continuación algunas comparaciones de ejemplo[4]:

SSL Provider	Product Name	1 year price	Type	Validation level	Speed of issuance	Encryption	90 days free PCI scanning	Unlimited Server Licenses	Free trial (single domain)	Site Seal (dynamic/ passive)	Re-issuance policy
Comodo CA	Positive SSL	**$49.95**	One Domain	Domain	Immediate	128 / 256 bit	✓	✓	90 days	Dynamic	Unlimited
Go Daddy	Standard SSL	**$69.99**	One Domain	Domain	Immediate	128 / 256 bit	✗	✓	None	Passive	Unlimited
Comodo CA	Instant SSL	**$99.95**	One Domain	Organization	1-2 days	128 / 256 bit	✓	✓	90 days	Dynamic	Unlimited
Comodo CA	Comodo SSL	**$99.95**	One Domain	Domain	Immediate	128 / 256 bit	✓	✓	90 days	Dynamic	Unlimited
Go Daddy	Deluxe SSL	**$99.99**	One Domain	Organization	2 days	128 / 256 bit	✗	✓	None	Passive	Unlimited
Thawte	Thawte 123	**$149.00**	One Domain	Domain	Immediate	128 / 256 bit	✗	✗	30 days	Passive	Unlimited
Geotrust	Quick SSL Premium	**$149.00**	One Domain	Domain	Immediate	128 / 256 bit	✗	✓	30 days	Passive	Unlimited
Comodo CA	Positive SSL Wildcard	**$149.95**	Wildcard	Domain	Immediate	128 / 256 bit	✗	✓	90 days	Dynamic	Unlimited
Comodo CA	Premium SSL	**$179.95**	One Domain	Organization	1-2 days	128 / 256 bit	✗	✓	90 days	Dynamic	Unlimited
Thawte	SSL Webserver Certificate	**$199.00**	One Domain	Organization	2 days	128 / 256 bit	✗	✗	30 days	Passive	Unlimited

Comparación por precios de cada producto (algunos siendo de una misma CA)

¿Cuál es la mejor CA?

No se debería ir y sacar las conclusiones sin tener en cuenta los numerosos factores en cada uno de los productos, por ejemplo Comodo es de las mejores CA aunque se comenta como la misma fue víctima de un incidente de *hacking*[5].

Por lo que queda en tí tomar acciones como: evaluar los criterios ya mencionados, ver reseñas de otros usuarios, consultar con profesionales, el propósito/público destino de tu sitio web y los servicios/productos que ofrecerás desde él y/o decidir hasta qué punto confías en determinada CA como para comprar uno de sus productos.

Fuentes

Ésto es un trabajo resumido, se recomienda consultar las siguientes fuentes (en inglés) por información en detalles (a lo largo del trabajo se colocaron números en superíndices para indicar la fuente de información, pero generalmente se utilizó como referencia la documentación de Comodo):

1. https://www.comodo.com/resources/small-business/digital-certificates.php (y páginas subsecuentes)
2. https://www.sos.state.tx.us/statdoc/digital.shtml
3. https://docs.oracle.com/cd/B10501_01/network.920/a96582/pki.htm
4. https://www.whichssl.com/compare-ssl-certificates.html
5. https://www.pluralsight.com/blog/software-development/top-reliable-ssl-certificates