Temas pendientes

* Crear certificados con la entidad certificadora AD
* Crear certificados con IIS
* Creación certificados con JAVA
* ¿Que hace que un certificado sea valido?

Objetivos de la criptografía

Es curioso como casi todos los elementos en los que se basa en internet se crearon de una manera más o menos insegura en la que cada elemento viajaba por la red si ningún tipo de protección, libres para que cualquiera pudiera leer su contenido. Esto fue así, hasta que entro en juego la criptografía.

Muchas veces la gente no es consciente de la información personal, privada y secreta que viaja a través de sus computadoras o celular, o si lo es no le da importancia requerida. El tema es que es realmente importancia limitar el acceso a nuestra información, porque nunca sabemos que consecuencia podría tener que un extraño acceda a nuestro teléfono, nuestras fotos o mensajes, lo que para nosotros es inofensivo para otras personas abren posibilidades de extorsión o estafas en contra nuestra.

La criptografía garantica que solo nosotros (u otras personas autorizas) puedan acceder a nuestra información, de forma que sepamos que lo que sale de nuestros dispositivos, está debidamente protegida, y es confidencial.

La criptografía es un conjunto de técnicas y métodos en que los que un mensaje origen (o en claro) con información confidencial, se convierte en otro sin aparente significado y que puede viajar por medios no seguros, con la tranquilidad de que el mensaje original no podrá ser descubierto, sin aplicar los correspondiente métodos criptográficos sobre el mensaje original.

La criptografía existe desde hace muchos siglos, siempre asociada al envió de mensaje secretos entre dos partes. Algunos sistema de criptografía antiguos, se basan en la ocultación del método criptográfico. En los sistemas criptográficos modernos, el método de inscripción es público (o podría serlo sin comprometer la seguridad) y al mismo tiempo poseen una clave de encriptación que debe ser secreta, y que si la cual aunque tengamos el algoritmo y el mensaje cifrado, no conseguiremos tener el mensaje original.

Las herramientas y métodos involucrados en la criptografía se usan en los siguientes aspectos:

## Integridad

Garantiza que la información no ha sido alternada y es tal cual se genero. Este proceso se hace realizando una serie de operaciones matemáticas sobre esta, dando como resultado un número, casi único, al que solo se puede llegar realizando los mismos cálculos. El número resultante de estas operaciones se le conoce como “resumen” o más comúnmente como “hash”, cuanto mayor sea este número, mas seguridad ofrece.

Algunos algoritmos de integridad son:

* **CRC, CRC32, MD5**: Algoritmos actualmente obsoletos que no debiera usarse actualmente.
* **Familia de algoritmos SHA**: Conjunto de algoritmos de hash, que poseen con subfamilias SHA1, SHA2, SHA3, con las siguientes características:
  + **SHA1:** Genera un numero de 160 bits, actualmente considerado no seguro:
  + **SHA256** y **SHA512**: Genera un número de 256 y 512 bits respectivamente, considerados seguros actualmente.

Uno de los problemas de problemas de estos algoritmos son las colisiones esto es el hecho que se puedan genera dos hash iguales para distinta información, lo cual permite “adulterarla”. El otro problema es que se pueda llegar a la información original a través del hash, lo cual puede ser un fallo de seguridad importante en el caso que la información original sea un password, o una clave simétrica de encriptación.

## Confidencialidad

Es la posibilidad de enviar información desde el punto A al punto B garantizando que solo el emisor y el receptor puedan acceder a ella. En un ambiente inseguro desde su concepción como internet, es fundamental poder disponer de herramientas que nos permitan enviar información privada de forma segura. Nuestra información confidencial son datos biométricos y de salud, datos personales como nuestras direcciones, contactos o datos económicos como nuestras tarjetas de crédito. Generalmente se garantiza la confidencialidad mediante la encriptación, la cual se realiza a través de la una seria de transformaciones matemáticas de la información usando una llave de determinados tamaño.

Algoritmos que confidencialidad son:

* **AES:** Usando tamaños de llave de 128, 192 o 256 bits. Se usa la misma llave para encriptar y para desencriptar.
* **RSA:** Usando tamaño de llaves de 1024 (considerado obsoleto), 2048, o 4096. Se usa una llave diferente para encriptar y otra para desencriptar.

## Identidad

Es lo que nos permite garantizar que la persona (o maquina) con la que estamos intercambiando información es realmente quien dice ser.

En estos casos se usa criptografía asimétrica, y principalmente certificados.

La identidad también nos ayuda a implementar el principio de “no repudiación” esto es que la persona o sistema que realiza una operación no puede negar haberla realizado.

Criptografía simétrica

Tanto el recepto del mensaje encriptado, como la persona que encripta, usan la misma clave de encriptación para realizar sus operaciones. Algoritmos que lo usa son por ejemplo AES (Rijndael).

Las ventajas de este método son:

* Es la practica tiene una velocidad aceptable
* Es muy seguro

Las desventajas:

* La principal desventaja es que un usuario genera la clave y tiene que pasársela a otro usuario, lo cual podría comprometer la conexión desde un inicio

El hecho que compartan la misma clave, es un problema, el único que tiene este tipo de criptográfica, porque ¿Cómo se hace que el usuario final y destino tengan la misma clave?, solo enviando la clave por un medio que sea seguro, para garantizar que nadie más la tiene, pero precisamente necesito intercambiar la llave porque no tengo un medio seguro para enviar información.

Criptografía asimétrica

Consta de dos claves, en lugar de una, llamadas clave privada y clave pública, la clave pública sirve para encriptar, y es de libre acceso, la clave privada para desencriptar y solo la tiene una persona (la que genero las claves). Además la privada sirve para firmar mensajes y garantizar que la persona que la usa es el dueño de la clave.

En la práctica funciona así: Una persona genera (a través de un algoritmo) una clave privada y pública (que se complementan entre sí), se queda para sí la clave privada, y distribuye la clave pública (a quien desee), a partir de ese momento, quien desee mandarle un mensaje encriptado, puede hacerlo usando la clave pública, y solo el podrá desencintarlo usando la clave privada. Igualmente si él quiere mandar un comunicado y garantizar su autenticidad, podrá firmarlo con su llave privada, y todo aquel que tenga la llave publica, podrá validar su origen.

Algoritmos que implementan esta tecnología son por ejemplo RSA o DSA.

Las **ventajas** de estos algoritmos son:

* Seguridad en cuanto al custodio de las claves (nunca se difunde la clave privada)
* Seguro en cuanto los mecanismo de inscripción

Las **desventajas:**

* Increíblemente lento

En esta criptografía se resuelve el problema de la llave compartida, puesto que al haber dos llaves, se puede distribuir libremente la llave pública (a cualquier persona) para encriptar, y la permanecer debidamente custodiada la llave privada para desencriptar. Así por ejemplo dos personas (o entes), pueden iniciar una comunicación segura, simplemente intercambiando sus llaves públicas y usando sus llaves privadas para desencriptar.

Debido a que la criptografía asimétrica es realmente lenta, en lugar de encriptar un mensaje completo, se genera una llave simétrica aleatoria, con la que se encripta el mensaje y se envía el mensaje encriptado y adjunto con la llave simétrica encriptada (ahora sí) con la llave asimétrica publica, lo cual garantiza la velocidad y la confidencialidad.

Certificados digital

Cuando recibimos un mensaje firmado con una llave privada, podemos validar su autenticidad con nuestra llave pública. Esto quiere decir que podemos garantizar que la persona que tiene la llave privada es la se está comunicado, con nosotros, puesto que debe coincidir con la llave publica que nos proporcionó.

Hay que agregar que la firma es diferente por cada mensajes, por lo que garantiza no solo que el mensaje fue enviado por quien tiene la llave privada, sino además que el mensaje no ha sido modificado en el cambio.

Un detalle importante es que solo garantiza eso, es decir que el mensaje fue firmado con la llave privada, pero no garantiza que esa firma electrónica pertenezca a una persona en particular. La firma podría ser de cualquier persona, y haberse generado en cualquier momento.

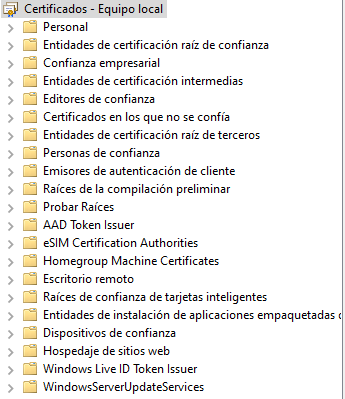
Para garantizar además que la firma privada pertenece a una determinada persona o entidad, se usan los certificados, que bien pueden identificar a una persona o a un ente como una empresa o un banco.

Pero, ¿En qué consiste exactamente un certificado? Imaginemos que yo quiero comunicarme (a través de una computadora) con otra persona o entidad, por ejemplo una tienda. Con el uso de llaves públicas (y privada) garantizo que la comunicación es confidencial entre ambos, pero de ninguna forma garantizo que esa llave pertenezca a la tienda, pero igualmente imaginemos que existe un tercer elemento, un ente en el que confiamos los dos (la tienda y el usuario), que garantice que esa llave privada pertenece a la tienda, ¿Cómo lo puede hacer? Dando por supuesto que yo confió en el tercero, que se llama entidad certificadora, esta firma (con su propia llave privada), la llave publica y demás información de la tienda, posterior a que valide la identidad de la tienda (mediante documentos, escrituras, registros de empresa, visitas en persona). En este punto ya tenemos un certificado, que contiene la llave pública, y que está firmado por alguien en el que confiamos que ha validado correctamente la identidad de la tienda, de esta forma queda ligada la identidad con la llave pública.

¿Quién son esas entidades certificadoras y por qué confiamos en ella? Son grandes empresas cuyo servicio es precisamente ese garantizar la identidad de entes y personas, y son aceptadas a nivel mundial como VERISIGN, o incluso gobiernos o entidades gubernamentales que realizan dicha función.

Elementos involucrados en un certificado

* **Cliente:** Es el ente (maquina, sistema o persona), que desea realizar una operación seguro
* **Servidor:** Es el ente (maquina, sistema o empresa), que está involucrada como destino de una operación.
* **Entidad Certificadora:** Es una entidad (organismo o empresa) conocida y respecta con la capacidad de poder validar y garantizar la identidad de un servidor (o de un persona dado el caso).
* **Entidad Intermedia:** Normalmente la entidad Certificadora no se usa parar generar certificados directamente, ya que podría ser catastrófico si fuera comprometida. Para evitar esto las Entidades Certificadoras generan “Entidades Intermedias” que son las que se usan en la práctica para generar los certificados clientes.
* **Llave privada y pública:** Son el conjunto de claves a usar, la privada pertenece al cliente, la pública es usada por la entidad certificadora.
* **Petición de certificado (archivo .csr):** Es el conjunto de información del cliente, que además está firmada por su clave pública, la entidad certificadora debe validar y garantizar su autenticidad.
* **Certificado público (archivo .cer):** Es el certificado generado por la entidad y firmado por este, que garantiza la identidad del cliente.
* **Certificado privado (archivo .pfx):** Es la unión del certificado público y la llave privada, para ser usado para fines de firmado y autentificación.
* **Almacén de certificados:** Es un lugar seguro donde se guardan los certificados, generalmente un archivo o base de datos protegido por una contraseña o por un parte del sistema operativo, por ejemplo:
* **Alcancen de Windows:**



* **Java KeyStore (archivos JKS):** es un repositorio tanto de certificados públicos como privados, generalmente usados en java.
* **Lista de revocación (archivo .crl):** Es un archivo firmado por la entidad certificadora que almacena los certificados que ya no son validos, generalmente por que su seguridad ha sido comprimida, y ya no es seguro su uso.
* **Online Certificate Status Protocol (OSCP):** Puede consideraras una evolución de los CRL, sirve para consultar la validez de un certificado en línea, parecido a realizar la consulta en una base de datos, con lo cual es más ágil y más rápido.

## proceso para generar un certificado

1. Se genera un par de llaves (pública y privada)
2. Se realiza una petición de generación de certificado en base a la clave pública, y a los datos de la empresa (y los host que queremos certificar).
3. Se envía la petición a una entidad certificara, que realizara los pasos necesarios para garantizar que somos la empresa para la cual estamos pidiendo los certificados, y una vez garantizado nos expedida dicho certificado.
4. En nuestro servidor podemos unir la llave privada con el certificado, y en base a eso configurar nuestros servidores para que lo usen apropiadamente



## Uso de un certificado

Nuestro clientes al conectarse a nuestros servidores descargaran el certificado (con la llave publica), y al estar firmado por la entidad certificadora (en la confiamos), asumiremos que el servidor al que nos estamos conectando es el correcto. Igualmente si no está firmado o lo está por alguien en que no confiamos seremos advertidos de esta situación, y estará en nuestra decisión continuar la comunicación con dicho servidor.



## Autentificación de operaciones

Para poder garantizar que las operaciones son realizadas por un usuario mediante un certificado existen diversos patrones pero todas ellas involucra firmas digitales, y elementos que solo posee el cliente.

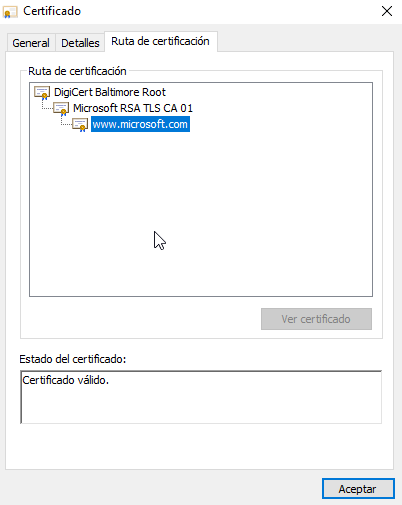
1. El cliente genera una operación
2. En el cliente se genera un hash representativo de la operación.
3. El hash se firma digitalmente con una llave privada.
4. Se envía la operación y la firma (el hash no firmado nunca se envía).
5. En el servidor se toma la operación y se vuelve a genera el hash, notase que el hash nunca se envío. Se debe llegar al mismo hash desde el cliente y desde el servidor, con la información disponible, es decir la misma operación.
6. Se valida el hash obtenido con la firma, si coincide la operación esta integra y además la ha generado el cliente (o por lo menos el que tenga la llave privada).



**Elementos y características de un certificado**

El formato más popular de certificado público es el X.509, que nos permite agrupar una serie de características y valores que han sido verificados y aprobados por una entidad certificadora.

Los certificados se organizan de forma jerárquica, conteniendo una cadena de certificación. El certificado es creado por un certifica intermedia y el certificado intermedio por un certificado raíz (que representa una entidad certificadora).



Los certificados raíces “confían” en sí mismos. No necesita de una entidad superior para ser confiable, generalmente están instalados por defecto en los navegadores y los sistemas operativos (en los que confiamos), si instalamos navegadores o sistemas operativos de dudosa procedencia, pueden instalarse certificados raíz apócrifos y podemos ser víctimas de un ataque por parte de un intruso.

## Elementos de un certificado

* **Fecha de validez:** indica la fecha máxima en la que el certificado es válido.
* **Subject:**

Es la persona, empresa o servicio para el cual se creó el certificado, tiene una estructura en forma de cadena que agrupa elementos como su nombre, su estado, su país, o su correcto electrónico, de la siguiente forma:

* **CN:** Nombre del host o persona sobre la que se esta expidiendo el certificado.
* **OU:** Unidad Organizativa, en una empresa suele ser el departamento al cual pertenece el certificado
* **O:** Organización, o empresa.
* **L:** Ciudad o municipio
* **S:** Estado
* **C:** País

Por ejemplo:

*CN=José Luis Bautista Martin; OU=Desde Las Horas Extras; O=Capicua; L=Guadalajara; S=Jalisco; C=Mexico*

* **CLR y OCSP:** Representan consultas de listas de revocación (para comprobar si el certificado sigue siendo válido).
* **KeyUsage:** Es una lista de opciones que indica de forma general para que se va a usar la clave pública del certificado, los posibles valores son:

|  |  |  |  |
| --- | --- | --- | --- |
| Tipo | Codigo Hexadecimal | Codigo Decimal | Descripción |
| digitalSignature | 80 | 128 |  |
| nonRepudiation | 40 | 64 |  |
| keyEncipherment | 20 | 32 |  |
| dataEncipherment | 10 | 16 |  |
| keyAgreement | 8 | 8 |  |

* **extendedKeyUsage:** Indica de forma más precisa para que se va a usar el certificado :

|  |  |  |
| --- | --- | --- |
| Tipo | Codigo OID | Descripción |
| serverAuth | 1.3.6.1.5.5.7.3.1 | SSL/TLS WWW Server Authentication |
| clientAuth | 1.3.6.1.5.5.7.3.2 | SSL/TLS WWW Client Authentication |
| codeSigning | 1.3.6.1.5.5.7.3.3 | Code Signing |
| emailProtection | 1.3.6.1.5.5.7.3.4 | E-mail Protection (S/MIME) |
| timeStamping | 1.3.6.1.5.5.7.3.8 | Trusted Timestamping |
| OCSPSigning | 1.3.6.1.5.5.7.3.9 | OCSP Signing |
| ipsecIKE | 1.3.6.1.5.5.7.3.5 | ipsec Internet Key Exchange |

Algunos ejemplos de uso de certificados son:

* **Entidad Certificadora**

keyUsage = critical, digitalSignature, cRLSign, keyCertSign

* **Entidad** **Intermedia**

keyUsage = critical, digitalSignature, cRLSign, keyCertSign

* **Certificado de usuario:**

keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment

extendedKeyUsage = clientAuth, emailProtection

* **Certificado de servidor**

keyUsage = critical, digitalSignature, keyEncipherment

extendedKeyUsage = serverAuth

* **Certificado OCSP**

keyUsage = critical, digitalSignature

extendedKeyUsage = critical, OCSPSigning

* **Algoritmo de firma:** es el algoritmo que va a usar el dueño del certificado para firmar, puede ser alguna versión de SHA junto RSA por ejemplo SHA1RSA
* **Clave publica:** Es la clave publico del certificado con la podremos encriptar la información y proporcionársela al dueño del certificado.
* **Nombres alternativos:** En el caso de un servidor, indica todos los nombres por los cuales responde el servidor, este es un campo obligatorio.
* **Microsoft Cryptographic Service Providers:** Los **Cryptographic** Service Providers (CSP) son un conjunto de API de Microsoft con una funcionalidad en concreto, los certificados en Windows se configuran para poder usar o varios CSP.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Provider Name & Type | Description | Purposes | Crypto | Default Microsoft Templates |
| Microsoft Software Key Storage Provider (CNG) | Standard windows software based RSA and ECC provider. | Key Exchange Digital Signature Data Encryption | *RSA ECC SHA1 SHA2* | *OCSP Response Signing (KSP Required, Provider not specific)* |
| Microsoft Smart Card Key Storage Provider (CNG) | Supports smart card key creation and use | Key Exchange Digital Signature Data Encryption | RSA ECC SHA1 SHA2 | None |
| Microsoft Platform Crypto Provider (CNG) | Supports smart card key creation and use | Key Exchange Digital Signature Data Encryption | RSA ECC SHA1 SHA2 | None |
| Microsoft Platform Crypto Provider (CNG) | Generates and stores keys in Trusted Platform Modules. Supports Key Attestation to allow CA to ensure key is created in TPM/Virtual smart card | Key Exchange Digital Signature Data Encryption | RSA ECC SHA1 SHA2 | None |
| Microsoft RSA SChannel Cryptographic Prodvider (CAPI) | Supports hashing, data signing, and signature verification. The algorithm identifier CALG\_SSL3\_SHAMD5 is used for SSL 3.0 and TLS 1.0 client authentication. This CSP supports key derivation for the SSL2, PCT1, SSL3 and TLS1 protocols. | Key Exchange | RSA SHA1 | CEP Encryption Computer Directory Email Replication Domain Controller Domain Controller Authentication IPSec IPSec (Offline) Kerberos Authentication RAS and IAS Server Router (Offline request) Web Server Workstation Authentication |
| Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider (CAPI) | Supports Diffie-Hellman key exchange (a 40-bit DES derivative), SHA hashing, DSS data signing, and DSS signature verification. Derived from Base DSS and Diffie-Hellman Cryptographic Provider. Adds support for RC2/4, DES and 3DES encryption | Digital Signature | RSA SHA1 | Authenticated Session Basic EFS CA Exchange Code Signing EFS Recovery Agent Enrollment Agent Enrollment Agent (Computer) Exchange Enrollment Agent (Offline request) Exchange Signature Only Exchange User Key Recovery Agent Trust List Signing User User Signature Only |
| Microsoft DSS and Diffie-Hellman/Schannel Cryptographic Provider (CAPI) | Supports hashing, data signing with DSS, generating Diffie-Hellman (D-H) keys, exchanging D-H keys, and exporting a D-H key. This CSP supports key derivation for the SSL3 and TLS1 protocols. This CSP supports key derivation for the SSL3 and TLS1 protocols. | Key Exchange | RSA SHA1 | Web Server |
| Microsoft Base Cryptographic Provider (CAPI) | A broad set of basic cryptographic functionality that can be exported to other countries or regions. No 3DES support. RC2/4 limited to 40bits. | Digital Signatures Data Encryption | RSA SHA1 | Administrator Authenticated Session Basic EFS Code Signing EFS Recovery Agent Enrollment Agent Enrollment Agent (Computer) Exchange Enrollment Agent (Offline request) Exchange Signature Only Exchange User Trust List Signing User User Signature Only |
| Microsoft DSS Cryptographic Provider (CAPI) | Provides hashing, data signing, and signature verification capability using the Secure Hash Algorithm (SHA) and Digital Signature Standard (DSS) algorithms. | Digital Signatures | RSA SHA1 | Authenticated Session Code Signing Enrollment Agent Enrollment Agent (Computer) Exchange Enrollment Agent (Offline request) Exchange Signature Only Trust List Signing User Signature Only |

Información de CSP extraída de <https://www.pkisolutions.com/understanding-microsoft-crypto-providers/>