TEMA

Tema 5. Criptografía

Administración de sistemas informáticos en Red

Seguridad y alta disponibilidad

Autor/a: Joaquín Erencia

Linkia FP

Tema 5: Criptografía

¿Qué aprenderás?

- Cuál es la diferencia entre clave y algoritmo
- Cuál es la diferencia entre simétrico y asimétrico
- La importancia de la Firma Electrónica
- Qué es el Phishing

¿Sabías que…?

- En los DNI electrónicos trabajas con certificados y con ellos puedes realizar muchos trámites en entidades oficiales

5.1. Introducción

Seguimos protegiendo lo más importante de nuestro trabajo, los datos. ¿Y cuándo nos damos normalmente cuenta de que tenemos un problema con los datos? Cuando acceden a ellos y los leen. En esta parte vamos a centrarnos en esa parte, "**nos leen los datos**". No quiero que la gente lea mis datos, ni en el lugar que los tengo almacenados ni cuando se los envíe a otra persona.

Vamos a definir la **Criptografía** como la ciencia que estudia los métodos, procesos y técnicas con el fin de guardar, procesar y trasmitir la información en formato digital. En una definición más funcional, podemos determinar que su función es el envió de información secreta.

Este proceso tiene dos partes: el cifrado y la autentificación.

- **Cifrado**, como transformación que aplicamos a la información para que sea secreta. Solo el destinatario de esta es capaz de realizar la transformación inversa y recuperar los datos originales. Para realizar el descifrar un mensaje es necesario el uso de la clave secreta.
- **Autentificación**, como la manera de asegurarnos que solo el destinatario reciba la información.

5.2. Algoritmo

Un **algoritmo** es una estructura de procesos matemáticos que se le aplica a un conjunto de datos para transformarlo en otros. En el mundo de la seguridad, estos pasos se realizan en combinación con un elemento, una palabra o combinación de caracteres, la clave. Este proceso, si es conocido, se puede invertir, pero necesitaremos de esa clave para poder volver a obtener la información original.

Como estos algoritmos son públicos, por lo que la fortaleza depende la su complejidad y de la longitud de la clave empleada.

5.3. Criptografia simética

La criptografía **simétrica** utiliza una clave para cifrar y descifrar el mensaje. Esta clave debe ser conocida por el emisor y el receptor "previamente".

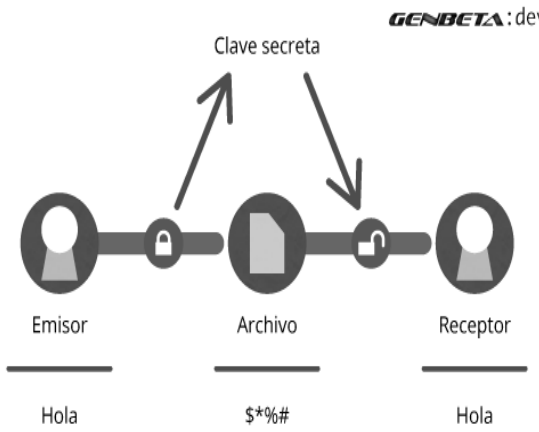


Figura: Comunicación con Cifrado Simétrico

Esta foto de Autor desconocido está bajo licencia CC BY-SA

El problema de este sistema se encuentra en cómo enviamos la clave secreta antes de realizar la comunicación, sin que la intercepten. Será más sencillo interceptar la clave que dedicarnos a averiguarla por **un ataque de fuerza bruta**. Os recomiendo ver la película **Enigma**, donde podéis ver como se utilizó una máquina con un método simétrico encriptaba la información de las comunicaciones alemanas en la Segunda Guerra Mundial.

Otro de los inconvenientes de este sistema se encuentra en que cada comunicación requiere su clave. O sea, si tienes que comunicar un contenido a veinte personas, deberás tener veinte claves diferentes, una para cada persona.

Algoritmos utilizados:

- DES (Data Encryption Standard) – clave de 56 bits
- 3DES (Triple Data Encryption Standard) – clave de 128 bits
- RC5 – clave de 32, 64 o 128 bits
- IDEA – clave de 128 bits (és el más utilizado en la actualidad)
- AES (Advanced Encryption Standard) – clave de 128, 129 y 256 bits (se utiliza en routers con WPA)

5.4. Criptografia asimétrica

La Criptografía Asimétrica se basa en el uso de dos claves; la pública y la privada.

La **clave pública** se puede difundir sin ningún problema a todas las personas con las que tengamos que comunicarnos.

La **clave privada** es secreta y no debe de ser revelada nunca.

El proceso de creación de las dos claves es el siguiente:

1. Mediante un Generador de números aleatorios obtenemos un número aleatorio único.
2. Aplicamos ese número aleatorio al algoritmo de cifrado seleccionado, obteniendo al Clave Privada.
3. Mediante la Clave Privada se genera la Clave Pública.

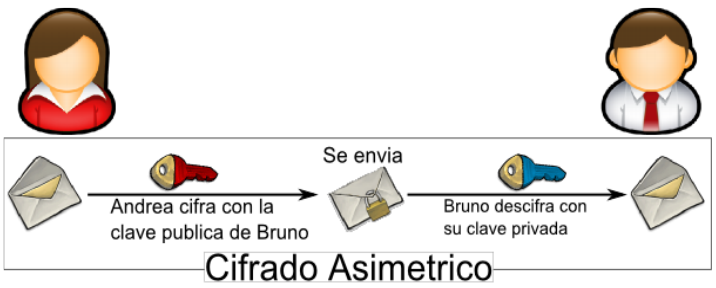
En la comunicación entre varias personas, cada persona tiene una clave privada y una clave pública.

Las parejas de claves tienen la función de cifrar la información, asegurar la integridad de los datos trasmitidos y garantizar la autenticidad del emisor.

Cuando ciframos con la clave pública, necesitamos la clave privada para descifrar, y al revés.

Vamos a ver cómo funciona:

- Dos usuarios (A y B) tienen sus respectivos pares de claves pública y privada.
- El emisor B quiere enviar un mensaje encriptado al receptor A. Para ello lo cifra con la clave pública de A, que todo el mundo conoce y lo firma con su clave pública. De este modo, el receptor A puede verlo y sabe que viene del emisor B.
- El emisor B envía el mensaje sin enviar la clave. (Aumentamos la seguridad)
- El receptor A recibe el mensaje cifrado y lo descifra con la clave privada del receptor A



El inconveniente de este sistema es su **lentitud**.

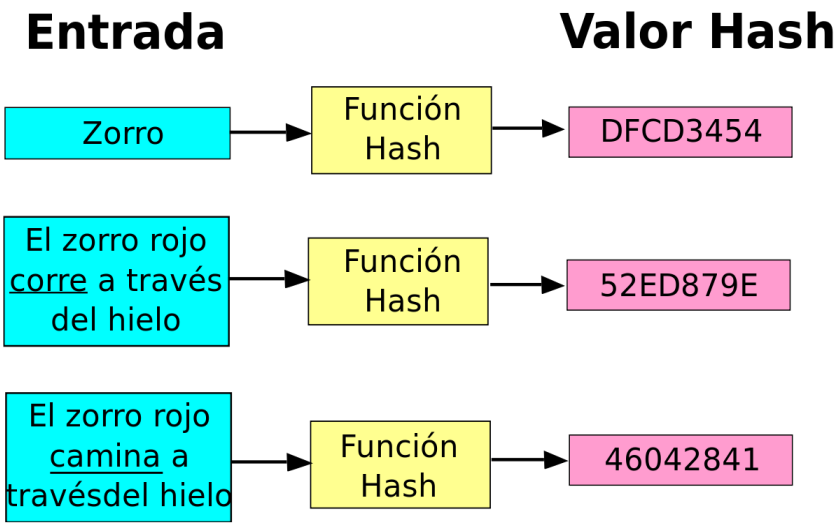
Algoritmos utilizados en este cifrado:

- Diffie-Hellman (poco utilizado)
- RSA
- HASH

El **Algoritmo Hash** es un conjunto de operaciones matemáticas que se aplican sobre un conjunto de datos, sin importarnos el tamaño, de tal forma que se obtiene un conjunto da datos, de tamaño fijo y que está asociado a los datos iniciales. Este conjunto de datos se denomina Resumen Hash y no hay dos Resúmenes Hash iguales.

Tipos de Algoritmo HASH:

- MD5 – resumen a 128 bits (comando md5sum)
- SHA-1 – resumen de 160 bits (comando sha1sum)
- SHA-2 – resumen de 512 bits (SHA-512)

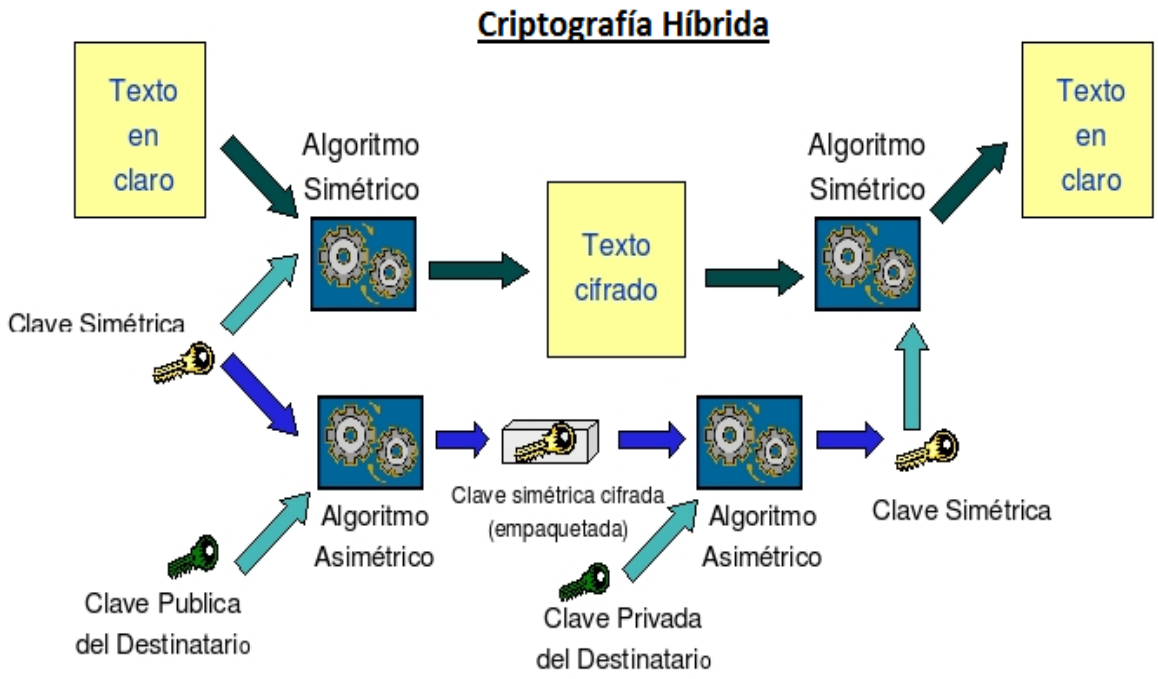


5.5. Criptografía de clave híbrida

Vamos a resolver el problema de lentitud del cifrado asimétrico. Para ello utilizaremos un algoritmo de clave pública junto a uno de clave simétrica.

Vamos a ver cómo funciona:

- El emisor A quiere enviar un mensaje al receptor B. Para ello lo cifra con clave simétrica. Esta clave la llamaremos clave de sesión y se genera aleatoriamente.
- Como es una clave simétrica, hay que enviarla al receptor B, pero como no queremos que nadie la intercepte y la utilice (problema de la criptografía simétrica) lo que hacemos es cifrarla con la clave pública del receptor B (clave asimétrica).
- El receptor B recibe la clave de sesión de sesión cifrada más el mensaje cifrado con esa clave.
- El receptor B descifra la clave de sesión y con esta descifra el mensaje.



5.6. La firma digital

La **Firma Digital** es un método de verificación de la autentificación del origen de la información y su integridad, basándonos en la Criptografía de Clave Pública.

La firma digital se basa en la propiedad de que un mensaje cifrado utilizando la clave privada de un usuario, solo se puede descifrar utilizando la clave púbica asociada al mismo usuario. Por lo tanto, si puede descifrar un mensaje utilizando una clave púbica determinada, me aseguro de que ese mismo mensaje se ha cifrado con una clave privada determinada.

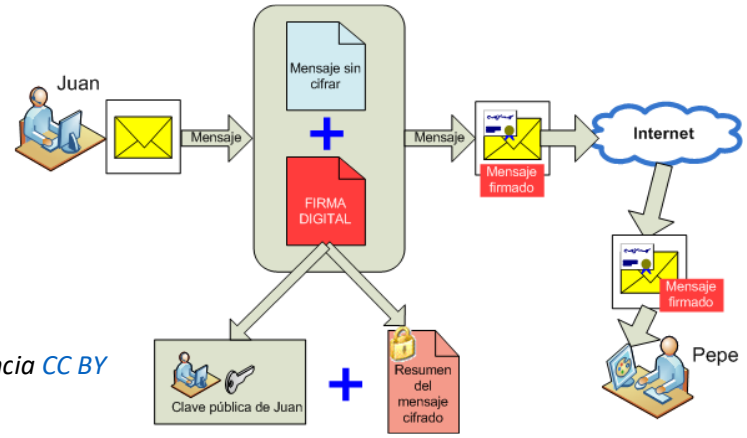
Pero para que este sistema sea viable, tenemos que evitar el problema de la lentitud. La firma digital utiliza los Algoritmos Hash.

Vamos a ver cómo funciona:

- Dos usuarios A y B, tienen sus pares de claves respectivas.
- El usuario A escribe un mensaje a receptor B.
- El usuario A utiliza el Algoritmo Hash y obtiene el Resumen.
- El usuario A cifra el Resumen con su clave privada. Así obtenemos la Firma Digital.
- El usuario A envía el mensaje más la firma
- El receptor B descifra la firma con la clave pública de A y obtiene el Resumen
- El receptor B genera su propio resumen con el Algoritmo Hash y compara los dos resúmenes.

Con este sistema conseguimos:

- **Autentificación**: La firma digital es equivalente a la firma física de un documento
- **Integridad**: El Algoritmo Hash nos asegura que el documento no ha sido modificado
- **No repudio en origen**: El emisor no puede negar que ha enviado el documento



5.7. Certificados digitales

Ante lo que hemos visto anteriormente se nos plantea dos dudas:

¿Estoy seguro de que mi clave privada solo la conozco yo?

¿Estoy seguro de que mi clave pública no es igual a la de otros usuarios?

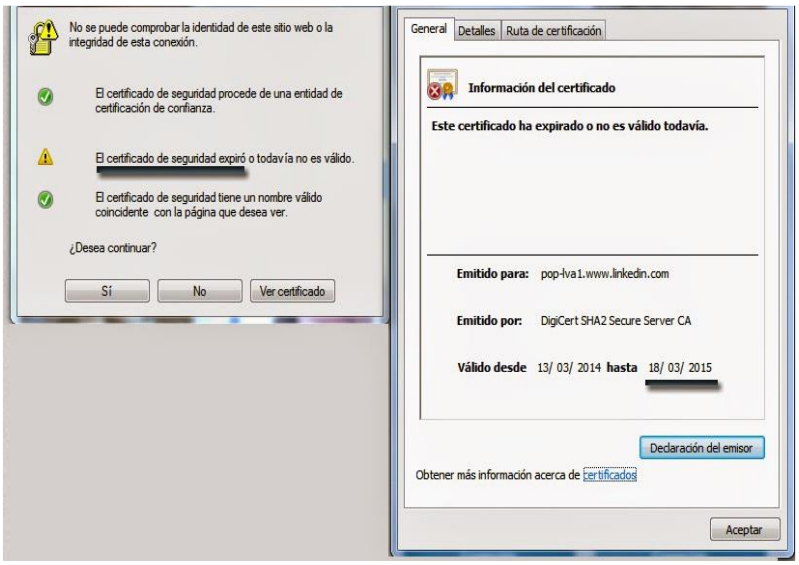
La primera pregunta la podemos responder con el uso de tarjetas personales, biometría, etc.

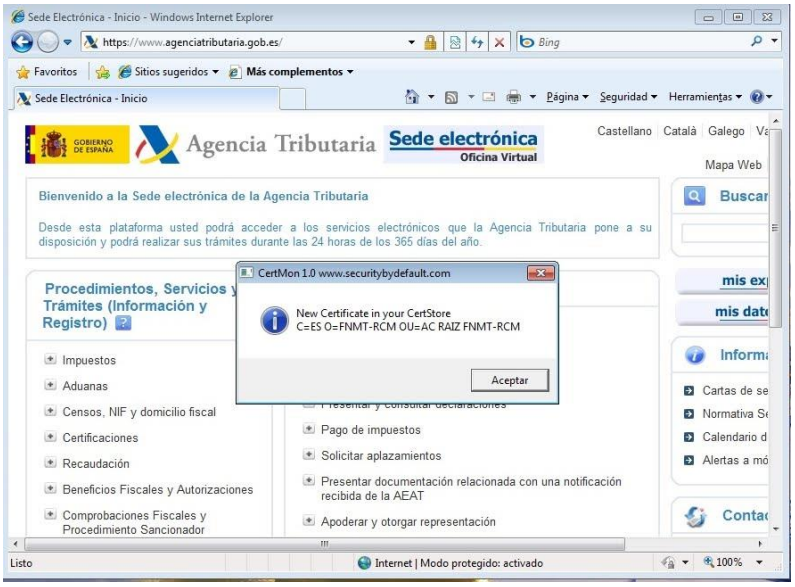
La segunda pregunta la vamos a resolver con el uso de Certificados Digitales.

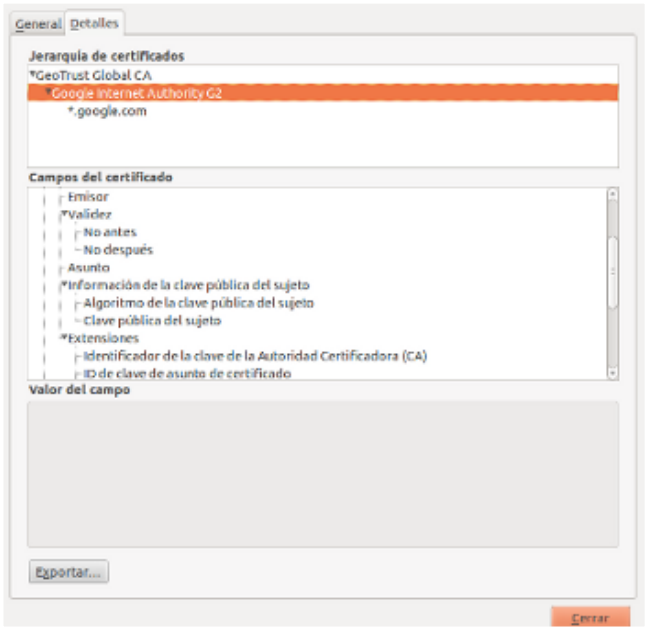
Un **Certificado digital** es un documento electrónico que se asocia la clave pública con la identidad de su propietario. Además, le asociamos el ámbito de utilización, las fechas de inicio y fin de la su validez…

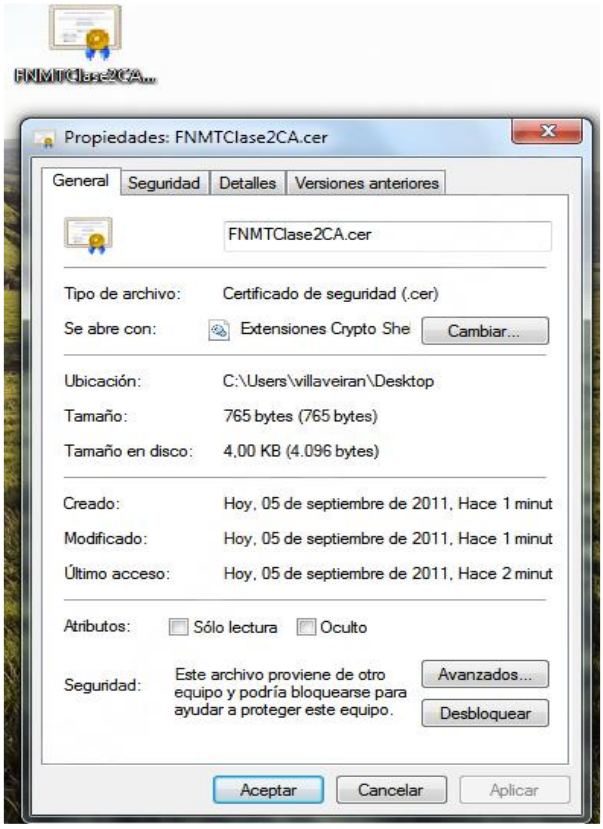
Hasta ahora todo bien, pero ¿quién me dice que el certificado digital es válido? Para responder esto debemos conocer el concepto de confianza en terceras partes.

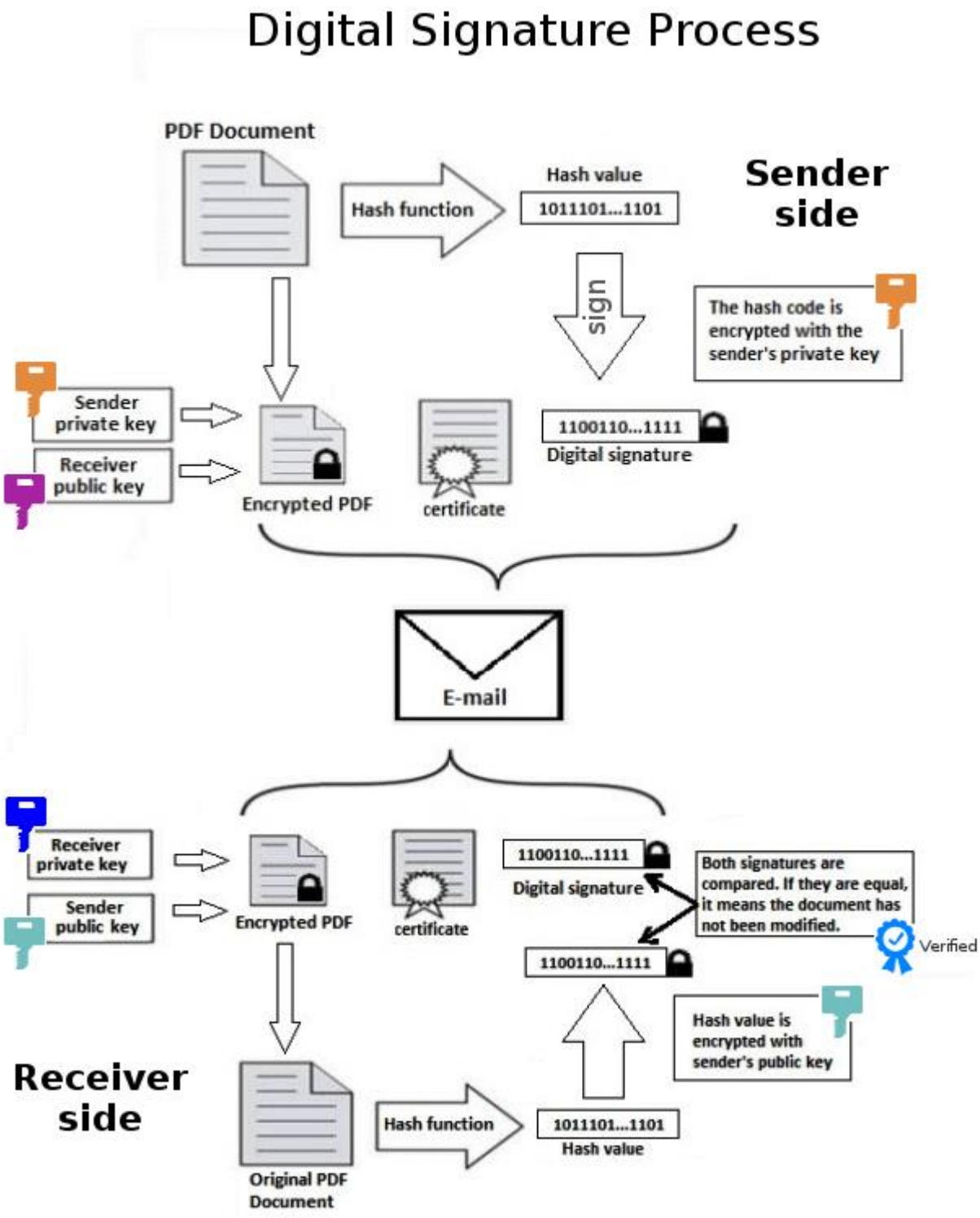
Nosotros vamos a confiar en el certificado digital de una segunda persona a la que no conocemos si dicho certificado está avalado por una tercera persona en la que sí confiamos. Para ello, esa tercera persona se encarga de firmar digitalmente el certificado de esa segunda persona. A esta tercera persona se le conoce como **Autoridad de Certificación** (AC).





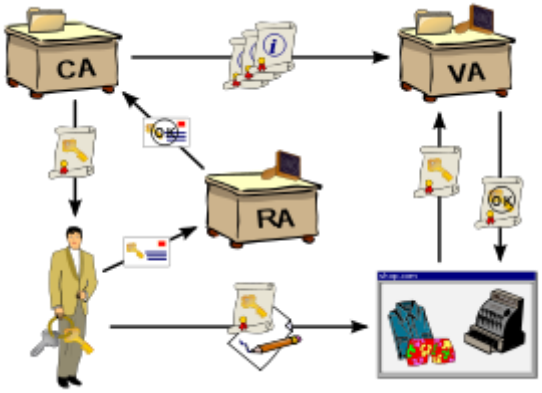






5.8. Infraestructura de clave pública (ICP O PKI)

La Infraestructura de clave pública es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública.



Los servicios que ofrecen son:

- Emitir un certificado para una clave pública
- Cancelación de un certificado previamente emitido
- Publicación de las claves de los usuarios
- Evaluar la confianza en un certificado
- Recuperar las claves de un usuario

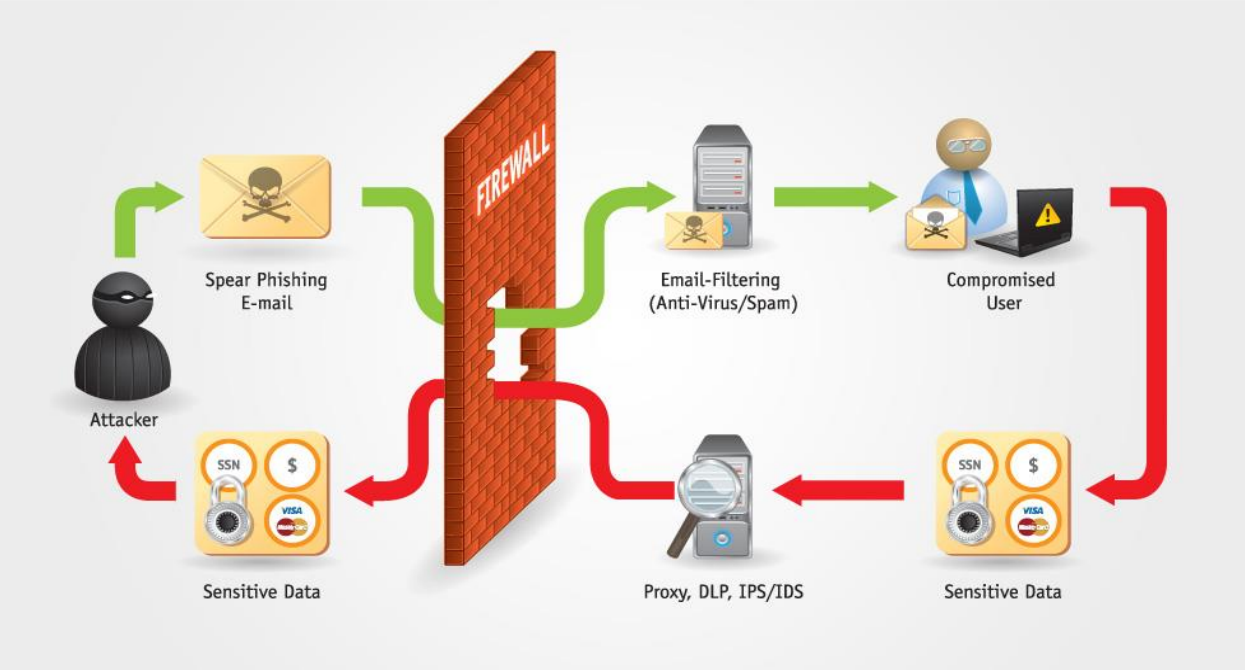
La estructura de estas **PKI** (Public Key Infrastructure) se compone de:

- Autoridad de Certificación (**AC**)
- Autoridad de Registro (**AR**)
- Autoridad de Repositorio
- Autoridad de Registro de Otras Terceras Partes Confiables

5.9. ¿Y para qué todo esto?

¿Alguna vez has enviado un correo electrónico utilizando un remitente falso? Este es el día a día de los estafadores en Internet. Este tipo de acciones criminales son posibles gracias a que muchas empresas renuncian a una instancia de seguridad adicional al enviar facturas y otros documentos sensibles a sus clientes. El llamado **phishing** resulta especialmente peligroso y se ha extendido mucho en los últimos años. Con él, personas sin escrúpulos envían correos electrónicos, supuestamente, en nombre de empresas o remitentes de confianza para acceder a los datos personales o información de pago del destinatario.

La solución para este tipo de fraudes es el uso de firmas digitales. Con el envío de correos firmados electrónicamente, el destinatario puede estar seguro de que el contenido del mensaje que ha recibido no ha sido manipulado y el remitente es, realmente, quien dice ser.



Recursos y enlaces

Cifrado Asimétrico. Linux GPG

Objetivo: En esta práctica vamos a simular dos usuarios que podrían estar en dos máquinas diferentes.

Crearemos la clave pública y privada a uno de ellos. Encriptaremos un archivo y realizaremos los pasos para que el otro usuario pueda leer el contenido cifrado.

- https://youtu.be/A1Pu4rV7hxg

Cifrado Simétrico. Linux y Windows

Objetivo: En esta práctica vas a aprender a cifrar un archivo sin y con cifrado AES. Lo realizaremos en entorno Ubuntu y en Windows.

- https://youtu.be/hOG9dBZYUF8
- https://youtu.be/nfE8c0S6MY8

Cifrado de Información Linux. TrueCrypt

Objetivo: Aprenderás a utilizar el software TrueCrypt para crear una carpeta cifrada en un entorno Linux.

- https://youtu.be/z5vaSkTTol0

Cifrado información Windows. Confidencialidad de la información

Objetivo: En esta práctica podrás cifrar un archivo en entorno Windows y comprobar su seguridad ante otro usuario y ante un Live-DVD de Linux.

- https://youtu.be/Fv4-0DKq-tE

Firma Digital Windows. Kleopatra

Objetivo: En esta práctica trabajaremos la creación y gestión de certificados con Windows y el software Kleopatra.

https://youtu.be/rIr7pvwGRJg

- ¿Cómo usar el ¨DNI-e? https://dnicita.es/dni-electronico-que-es-y-como-usarlo/

- Intypedia http://www.criptored.upm.es/intypedia/index.php?lang=es

- Entidades AC. https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/entidades-de-certificacion

- Descifrando Enigma https://www.filmaffinity.com/es/film617730.html

- Los fisgones https://www.filmaffinity.com/es/film233071.html

Test de autoevaluación

1. A la clave que publicamos para realizar una transacción con cifrado asimétrico, se le denomina.
   a) Popular
   b) Pública
   c) Común
   d) PKI

2. Al cifrado en el que se utiliza una única clave, se le denomina:
   a) Simétrico
   b) Asimétrico
   c) HASH
   d) RSA

3. A la entidad que avala el Certificado de otra empresa se le denomina:
   a) PKI
   b) AR
   c) AC
   d) RSA

4. La clave que solo está a disposición del usuario se denomina:
   a) Simétrica
   b) Password
   c) Pública
   d) Privada

Solucionarios

Test de autoevaluación tema 5

1. A la clave que publicamos para realizar una transacción con cifrado asimétrico, se le denomina.
   a) Popular
   b) Pública
   c) Común
   d) PKI

2. Al cifrado en el que se utiliza una única clave, se le denomina:
   a) Simétrico
   b) Asimétrico
   c) HASH
   d) RSA

3. A la entidad que avala el Certificado de otra empresa se le denomina:
   a) PKI
   b) AR
   c) **AC**
   d) RSA

4. La clave que solo está a disposición del usuario se denomina:
   a) Simétrica
   b) Password
   c) Pública
   d) **Privada**