Firma digital

La firma digital viene a sustituir a la manuscrita en el mundo de la informática. Es decir, si firmamos de forma digital un documenta, le estaremos dando veracidad y como sucede con la firma manuscrita, no podremos decir que no lo hemos firmado nosotras; por lo tanto, seremos responsables de lo que en él se diga.

¿Para qué sirve la firma electrónica?

La firma digital viene a sustituir a la manuscrita en el mundo de la informática.

- Si firmamos de forma digital un documento, le estaremos dando **veracidad**
- No podremos decir que no lo hemos firmado nosotros
- Seremos responsables de lo que en él se diga.

Una firma electrónica es un conjunto de datos electrónicos que:

- Se adjuntan a un documento electrónico determinado
- Identifican al firmante de manera inequívoca
- Certifican la integridad del documento
- Aseguran que el firmante no puede repudiar lo firmado.

Mecanismo

La descripción del mecanismo de firma electrónica es el siguiente texto:

Paso 1. Creamos el documento

```
La firma electrónica es un concepto jurídico, equivalente electrónico al de la
firma manuscrita, donde una persona acepta el contenido de un mensaje electrónico
a través de cualquier medio electrónico válido. Ejemplos:

La firma electrónica a su vez puede tener diferentes técnicas para firmar un
documento, así tenemos las siguientes: Código secreto o de ingreso: es la
necesidad de una combinación determinada de números o letras, que son sólo
conocidas por el dueño del documento, o lo que todos usamos, por ejemplo, en los
cajeros automáticos, es el famoso PIN (Personal Identification Number).

Métodos basados en la Biometría: se realiza el acceso al documento mediante
mecanismos de identificación física o biológica del usuario o dueño del documento.
La forma de identificación consiste en la comparación de características físicas
de cada persona con un patrón conocido y almacenado en una base de datos. Los
lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas
digitales y voz). En el perfeccionamiento del cifrado de mensajes, llegamos a lo
que se conoce como criptografía.
```

Paso 2. Calculamos el hash

Se calcula un valor resumen del documento, conocido como **hash**, utilizando algún algoritmo como el **SHA 256**.

```
8D1DA152769DA821009BBB2D6DD856DE
```

!!! note

```
Al estar calculado con SHA256, el hash tiene 256 bits (0s y 1s), que se pueden
representar con 64 dígitos hexadecimales.
```

Paso 3. Firmamos el hash con nuestra clave privada

Este valor resumen se cifra utilizando nuestra **clave privada**.

!!! note

```
Recordemos que nuestra clave privada nunca sale de nuestro dispositivo, únicamente
la pública.
```

```
MIIBVQIBADANBgkqhkiG9w0BAQEFAASCAT8wggE7AgEAAkEA0CUu5s7oUYtm1k/XLYOtPU0QaBAirTQ8Rc
T/Mn/JQCmyoQh8nrhb3IB93WRR5+mmzaa6WFU7TJyM7J0+VWTm0QIDAQABAkAwMuwRdohFmcpOhl6Fo6BS
Oa466sGc6iOq5FtUDlNED/iu8urdmKi24r+8mnykcGadZIXcnH+ti3GOfdW/dTIhAiEA9uZW7uD1eaVzyH
eLDyswOV1j8bCCSLUQbpWxXp6E488CIQDX0StiAkGhT9Ju9wRsdHDoakUoc2xywoswY+MH1xQTXwIhAMnZ
mJrlCWsxS85JhUOacGuFoW73ehwNA2kVMpQDjutbAiA4/+CiYRAuZ6OfdRQxBMvxRmf/mASThrg2Tpterb
p6pwIhAJMFoBU4zGYBm3UQOjZkRXNtxKZsJODtmNgZWYvdJZkD
```

El resultado de este valor es lo que se conoce como firma digital del documento.

```
sfsvMBz4RdrOOCe1naThF0ZkESDW0fjIpXf3GQchsDpkvc7oI5IowPu6Yefqr3O5LTu5pc0RoHoaJzMN5E
MaHA==
```

Esto permite asegurar que la única persona que ha podido firmar el documento soy yo, el único que conoce la clave privada.

Envío

El documento firmado contendrá:

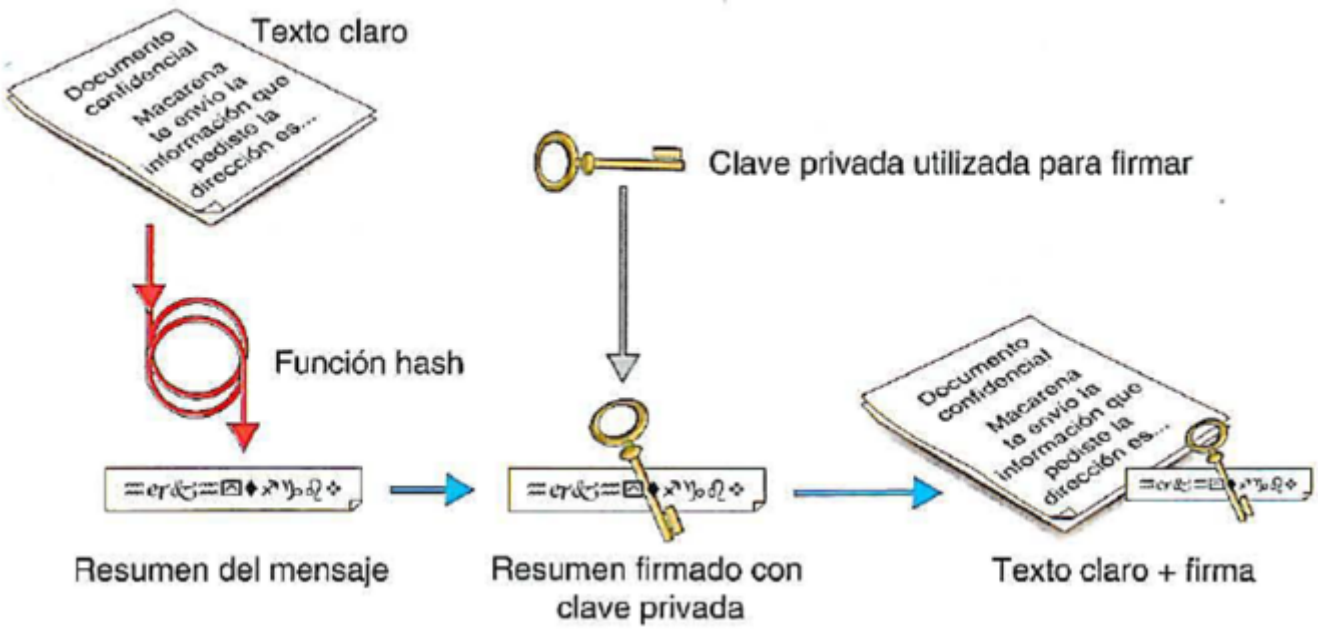
1. El contenido del texto original
2. La clave pública de la persona que ha firmado
3. La firma digital

Con estos 3 elementos, en cualquier momento podemos comprobar que la firma es auténtica.

Firma de documentos electrónicos

Si contamos con un **certificado digital**, podemos comenzar a firmar documentos. La firma electrónica en documentos se puede realizar de dos formas:

- Online, a través de un servicio de verificación y generación de firmas electrónicas como es VALIDe
- A través de aplicaciones de firma electrónica o de ofimática que, tras ser descargadas y ejecutadas en un ordenador, permitirán realizar firmas de documentación sin la necesidad de estar conectado a Internet.



Sellado en el tiempo

Una de las características más útiles que puede ir asociada a la firma electrónica es lo que se conoce como "sellado en el tiempo". Se trata de un método para probar que un conjunto de datos (en este caso, la firma que se ha realizado) existió en un momento determinado (fecha y hora).