Criptografía y Firma Digital.

Modulo 3.
Firma Electrónica

Laboratorio de Seguridad de la Información

Mediante el Cifrado de datos, el Hash o resumen de datos y las Firmas Digitales, la criptografía participa directamente en ofrecer los siguientes servicios de seguridad:

- Autenticación de usuario o autenticación de mensaje ¿son el emisor o el destinatario quiénes dicen realmente ser? ¿proviene el mensaje de quién dice provenir?
- Confidencialidad de un mensaje ¿habrá podido alguien, no autorizado, leer o acceder el mensaje o información?
- Integridad de un mensaje ¿ha recibido el remitente realmente la información que le envió su emisor o habrá sido modificada?
- No repudio de un mensaje ¿podrá el remitente negar que ha enviado algo (o el destinatario que lo ha recibido)?

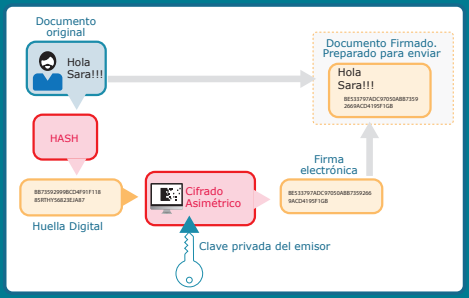
Tipos de Firma electrónica y qué se necesita:

- Firma Electrónica, firma simple: permite identificar al firmante. Por ejemplo, serviría utilizar una imagen pegada de una firma manuscrita.
- Firma Electrónica Avanzada: además de identificar al firmante, proporciona garantía sobre la integridad del documento. Implica que se ha utilizado ya mecanismos técnicos que lo garantizan. Se han utilizado PKIs.
- Firma Electrónica Reconocida: tendría la misma validez jurídica que la Firma Manuscrita. Es una firma electrónica avanzada, pero:
  - ejecutada en un Dispositivo Seguro de Creación de Firma - dispositivos de seguridad especiales (tipo tarjetas criptográficas o smartcards en la mayoría de los casos), homologados específicamente para este uso, y
  - amparada por un certificado reconocido (emitido por una Autoridad de Certificación reconocida, es decir, regulada por el Ministerio de Industria, Energía y Trabajo).

El proceso técnico tanto para realizar como para después verificar una firma electrónica es tedioso, requiere de una serie de cálculos, comprobaciones y verificaciones basados todos en la aplicación de algoritmos criptográficos.

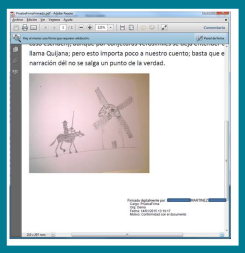
En cambio, las aplicaciones han hecho que el proceso manual que tiene que realizar un usuario para firmar sea tremendamente sencillo (aplicaciones portafirmas).

Cómo se Realiza una Firma:

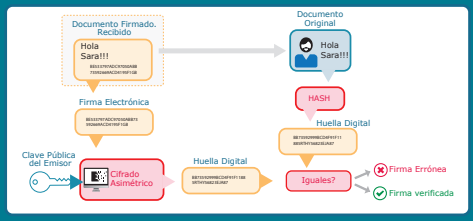


Cómo Firma un Usuario:

- El usuario elige el documento que desea firmar.
- Selecciona el certificado con el que quiere firmar.
- La aplicación adjunta al documento original un anexo con la firma electrónica, listo para distribuir.

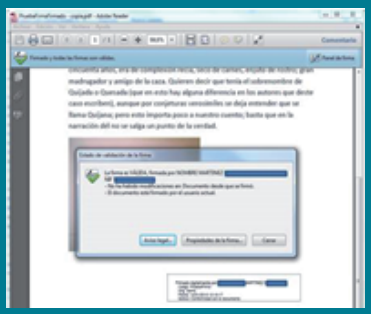


Cómo se Verifica una Firma:



Cómo Verifica una Firma un Usuario:

- Solo tendrá que hacer doble-click sobre la firma para que la aplicación realice todas las comprobaciones técnicas y le muestre el resultado.



XUNTA DE GALICIA
CONSELLERÍA DE SANIDADE
SERVIZO GALEGO de SAÚDE
MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa