



La Firma Electrónica: Conceptos Generales

GENERACIÓN DE UNA FIRMA ELECTRÓNICA

FIRMA ELECTRÓNICA

- ✓ **Herramienta de seguridad** basada en la criptografía asimétrica o de Clave Pública.
- ✓ Algoritmo de cifrado **RSA** y con claves típicamente de **1024 o 2048 bits**.
- ✓ Basada en **Certificados Digitales** emitidos por una **Autoridad de Certificación**.
- ✓ Estándares ampliamente difundidos (**x509 v3**).
- ✓ **Marco regulatorio sólido** en EEUU y la Unión Europea.
- ✓ Se asocian inequívocamente a una persona.
- ✓ Si cumple ciertas propiedades es **equivalente a la firma manuscrita**.
- ✓ Es considerada la **herramienta clave para aportar la seguridad necesaria en la red**.
- ✓ Además de la Firma de mensajes tiene otras importantes aplicaciones: **autenticación, mecanismo de acceso, desarrollo de código seguro, etc.**

CERTIFICADOS DIGITALES

- Representan **identificadores unívocos** de una persona en Internet
- La regulación de la firma conecta directamente con este concepto: la **firma debe basarse en certificado**
- Los certificados permiten diversos usos:
 - Permiten la **identificación de las personas** en Internet
 - Sirven para evitar la retrocesión y garantizan el **“no repudio”**
 - Ofrecen **soporte** a la firma electrónica **con reconocimiento jurídico**
 - Permiten el **envío de mensajes cifrados** al suscriptor del certificado
 - Permiten **ser usados** como mecanismo de acceso (como **“llave”**)

CERTIFICADOS DIGITALES



La Clave Pública del
Certificado la
difunde la AC



**Autoridad de
Certificación**



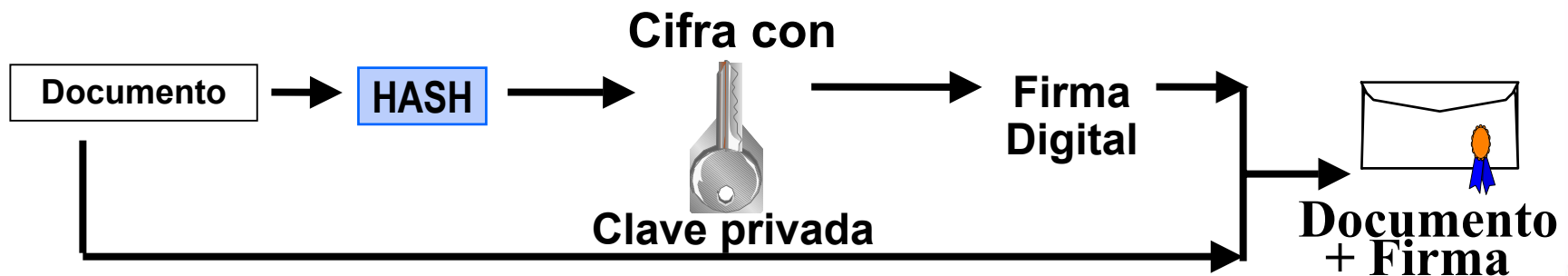
TERCERO

Un tercero puede
comprobar si los
datos del certificado
han sido alterados
respecto a los
firmados por la AC

**CONFIAR EN LA AUTORIDAD DE CERTIFICACIÓN
SUPONE CONFIAR EN LOS DATOS DEL CERTIFICADO**

Firma Electrónica. Generación

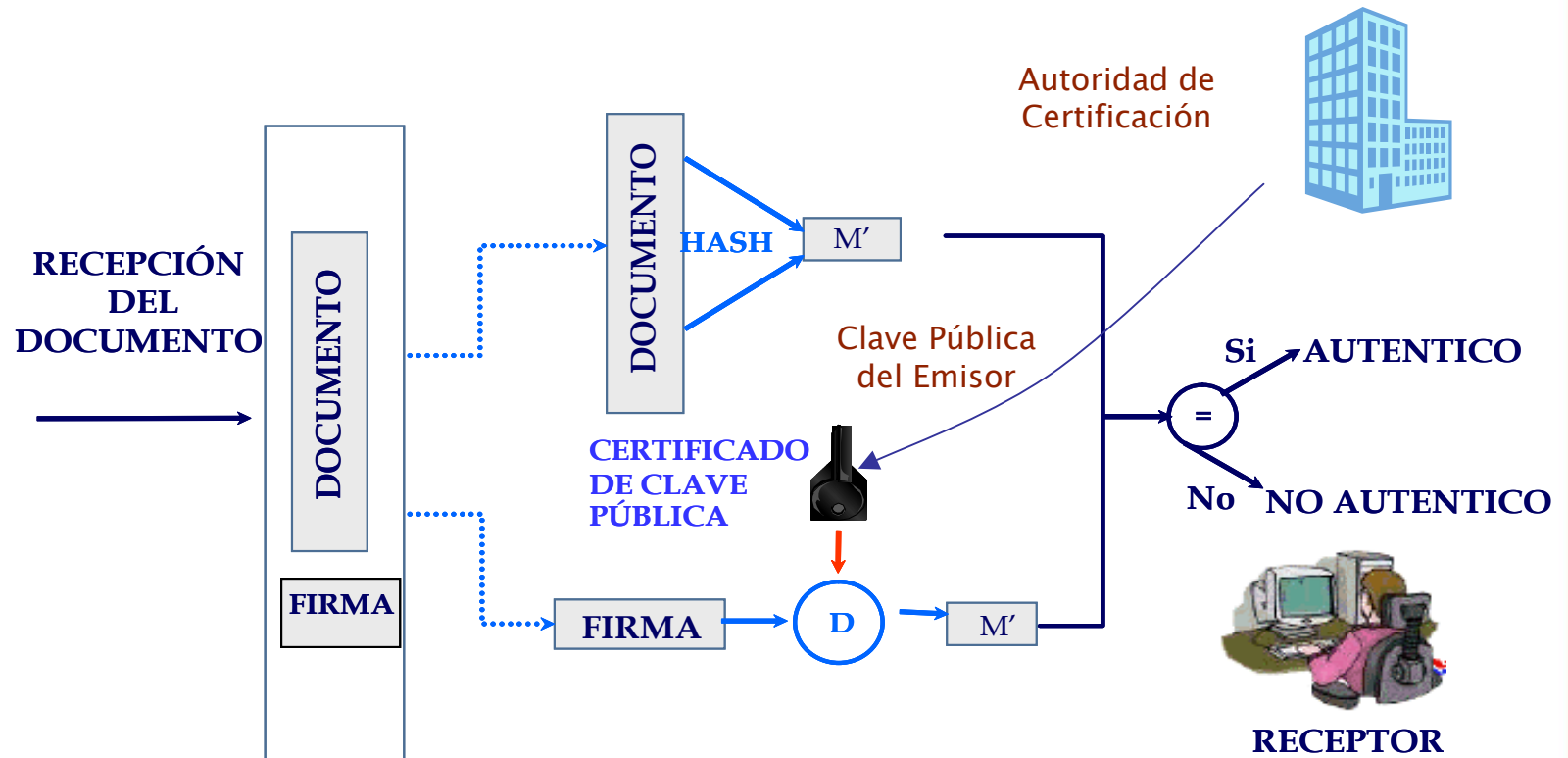
- ¿Cómo se genera una firma electrónica?
 1. Se toma el documento y se calcula un compendio digital (con una función llamada hash -*SHA Secure Hash Algorithm*)
 2. Se emplea la **Clave Privada** del Certificado para cifrar el resumen
 3. Al resultado, se almacena junto con el Documento original en una estructura de datos
 4. Se envía al destinatario, junto al documento o asociada al mismo, a través de un canal



Firma Electrónica. Verificación

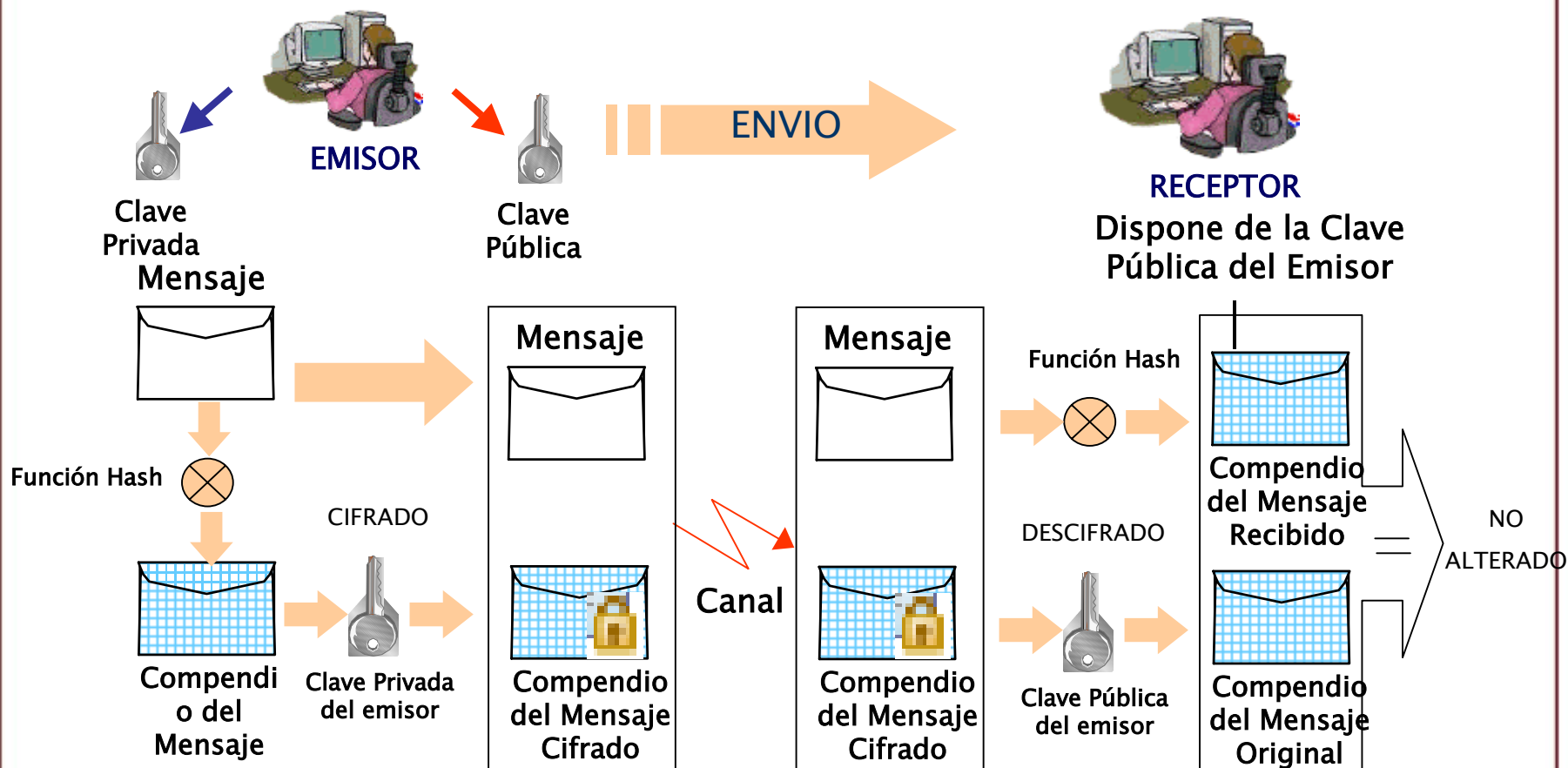
- ¿Cómo se verifica una firma electrónica?
 1. Se recibe el documento y la firma electrónica
 2. Se extrae la firma digital
 3. Se toma el documento y se calcula un nuevo resumen
 4. Se toma el resumen, se toma la firma digital y la clave pública del firmante y se ejecuta una función matemática, que indica si la firma es correcta

VERIFICACIÓN DE UN DOCUMENTO FIRMADO



El proceso de verificación y aviso de autenticidad lo realizan las aplicaciones informáticas sin intervención del usuario

CIRCUITO COMPLETO DE UNA FIRMA ELECTRÓNICA



Una Firma Electrónica consiste en añadir al mensaje original su propio resumen cifrado con la clave privada del emisor