Firma Digital

Ing. Max Alejandro Antonio Cerna Flores

Agenda

Definición

Proceso

Componentes de la Firma Digital

Casos de Uso

Definición

Es un esquema matemático para verificar la autenticidad de mensajes o documentos digitales.

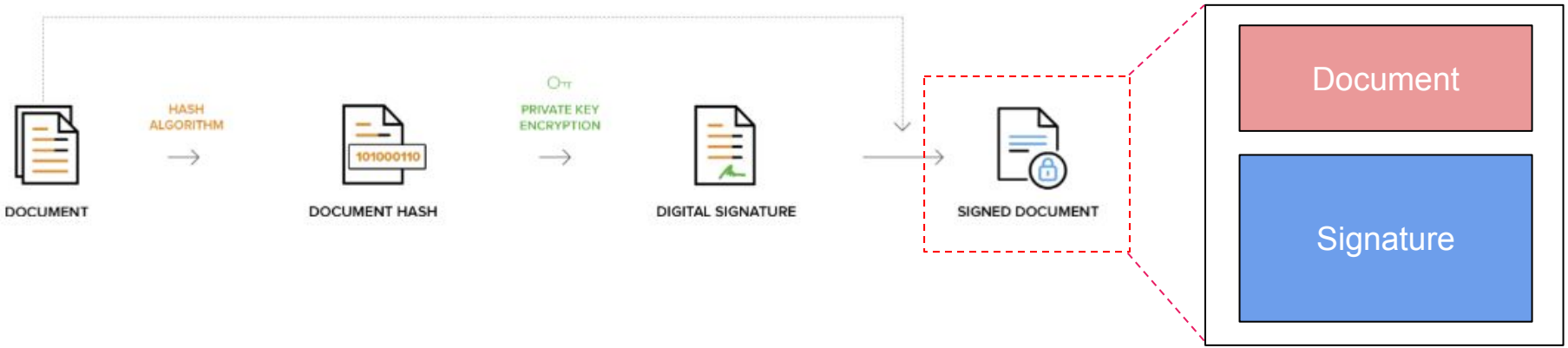
Válida cuando se cumplen los requisitos previos.

Otorga al destinatario una gran confianza en que el mensaje fue creado por un remitente conocido.

Válida que el mensaje no se modificó durante el tránsito.

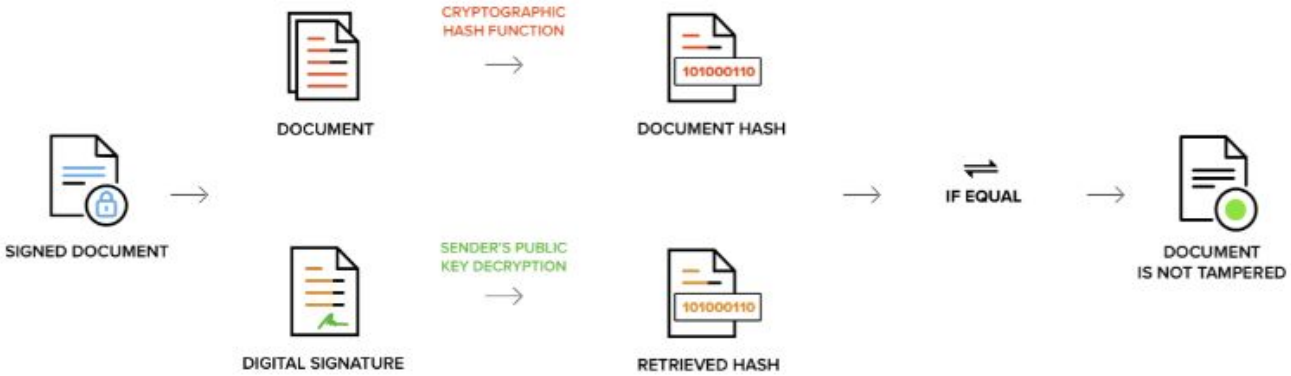
Proceso

Generación de firma

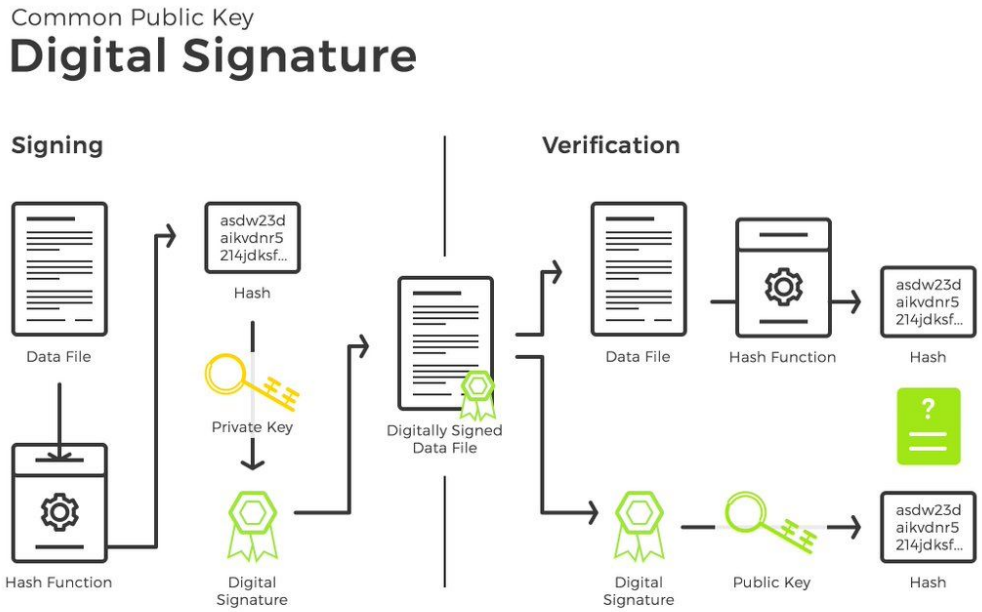


Proceso

Validación de firma



Proceso


Common Public Key
Digital Signature
Signing
Verification
Data File
asdw23d
aikvdnr5
214jdksf...
Hash
Private Key
Hash Function
Digital
Signature
Digitally Signed
Data File
Data File
Hash Function
asdw23d
aikvdnr5
214jdksf...
Hash
?
Digital
Signature
Public Key
asdw23d
aikvdnr5
214jdksf...
Hash

Componentes de la Firma Digital

Un esquema de firma digital normalmente consta de tres algoritmos:

1) Un algoritmo de generación de claves que selecciona una clave privada uniformemente al azar de un conjunto de posibles claves privadas.

   El algoritmo genera la clave privada y una clave pública correspondiente.

Componentes de la Firma Digital

---

2) Un algoritmo de firma que dado el mensaje y una clave privada, produce una firma.

3) Un algoritmo de verificación de firma que dado el mensaje, la clave pública y la firma, acepta o rechaza la afirmación de autenticidad del mensaje.

Casos de Uso

Autenticación

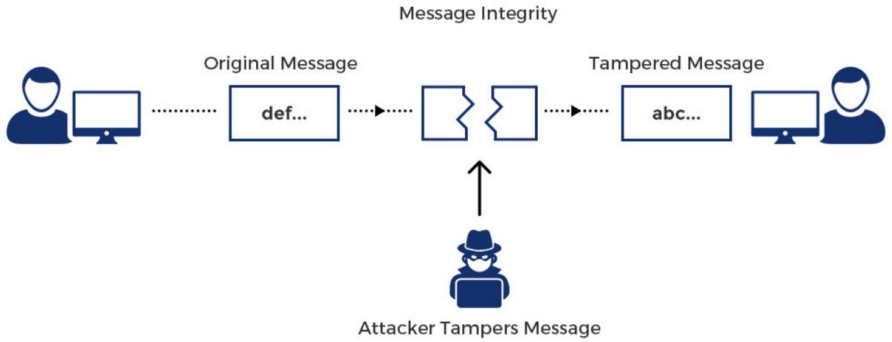
Cuando la propiedad de una clave secreta de firma digital está vinculada a un usuario específico, una firma válida muestra que el mensaje fue enviado por ese usuario.

Caso de Uso

Integridad

Si un mensaje está firmado digitalmente, cualquier cambio en el mensaje después de la firma invalida la firma.

No existe una forma eficiente de modificar un mensaje y su firma para producir un nuevo mensaje con una firma válida, porque la mayoría de las funciones hash criptográficas aún lo consideran computacionalmente inviable.



Caso de Uso

No repudio

Una entidad que ha firmado alguna información no puede en un momento posterior negar haberla firmado.