Firma digital

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Firma digital

Miren le manda un mensaje a Iker usando un sistema de clave pública

Nadie puede leer el mensaje de Miren a Iker pero cualquiera podría haberlo mandado

¿Cómo sabe Iker que se lo ha mandado Miren o que nadie lo ha modificado?

Solución: Miren firma sus mensajes

Firma digital

Sólo el usuario legítimo puede firmar su documento

Nadie podrá falsificar una firma

Cualquiera puede verificar una firma digital

Firma digital

No se puede reutilizar una firma

No se puede modificar una firma

No se puede negar haber firmado un documento

No se puede alterar un documento después de haberlo firmado

Logramos **Autenticidad**, **Integridad** y **No repudio**

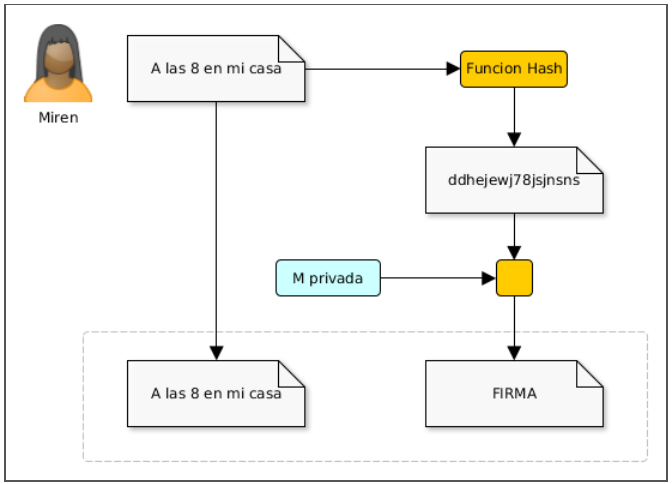
Firma digital

Miren obtiene un resumen criptográfico del mensaje: RC = hash (m)

Miren cifra el resumen criptográfico con su clave privada: Firma = e (RC, $M_{privada}$)

Miren envía el mensaje (cifrado o sin cifrar) y su Firma

Firma digital



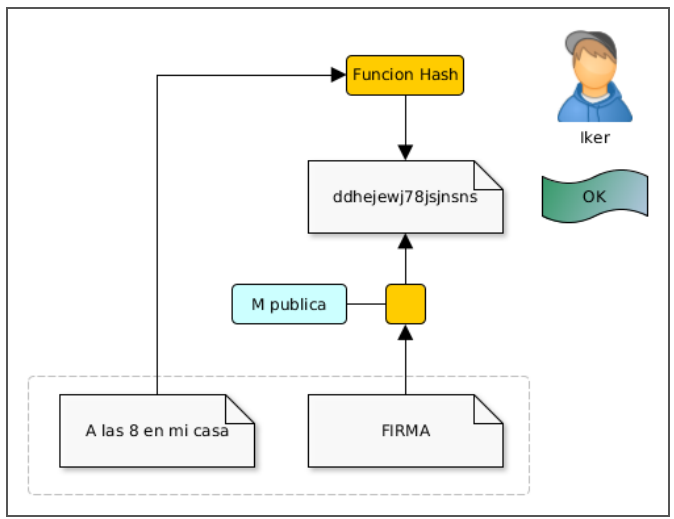
Firma digital

Iker desencripta la Firma usando la clave pública de Miren: RC = (Firma, $M_{pública}$)

Iker obtiene el resumen criptográfico del mensaje: RC’ = hash (m)

Iker compara RC’ con m para asegurarse que no ha sido modificado

Firma digital



Firma digital

Si además de firmarlo, Miren encripta su mensaje sólo Iker podrá leerlo: Se logra **Confidencialidad**, **Autenticidad**, **Integridad** y **No Repudio**

Puede hacerlo usando:

- Un sistema de criptografía asimétrica
- Un sistema de criptografía híbrido

Firma digital

Un sistema de criptografía asimétrica. Enviaría a Iker:

- Criptograma del mensaje cifrado con $M_{privada}$ y con $I_{pública}$
- Su Firma digital (el resumen criptográfico cifrado con $M_{privada}$)

Firma digital

Un sistema de criptografía híbrido. Enviaría a Iker:

- Criptograma del mensaje cifrado con la clave de sesión
- Criptograma con la clave de sesión cifrada con $I_{pública}$
- Su Firma digital (el resumen criptográfico cifrado con $M_{privada}$)

Confianza de firmas

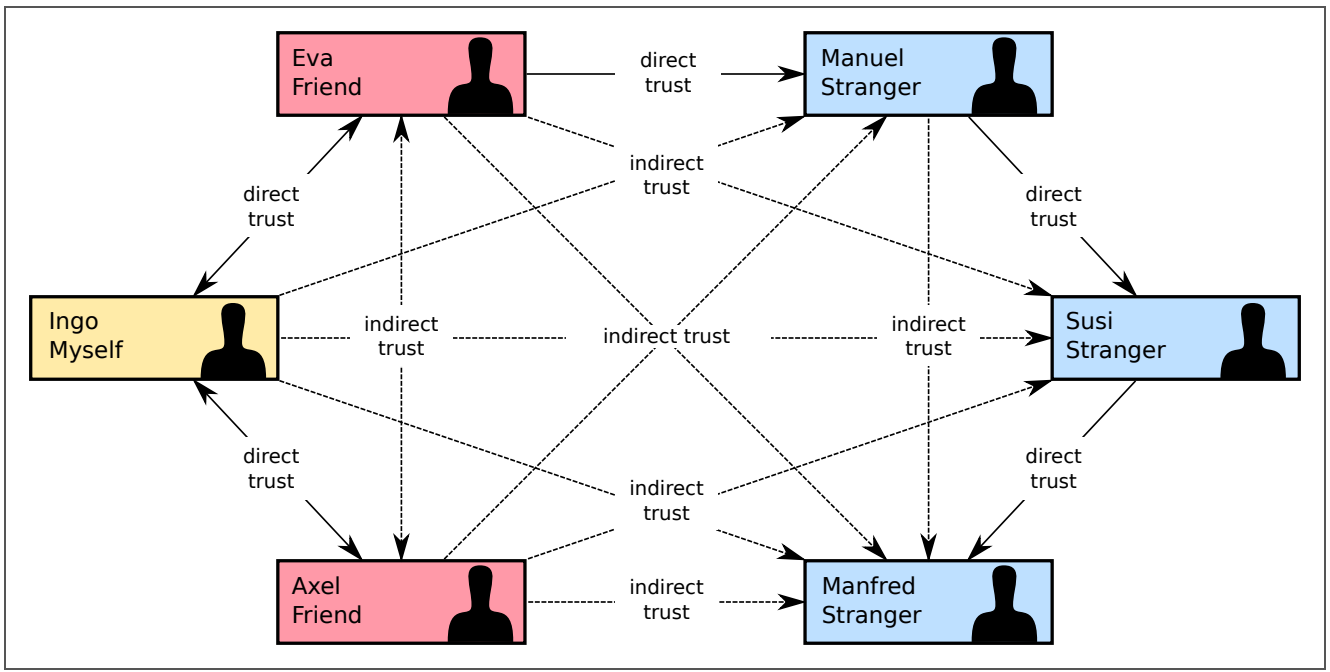
Aunque utilicemos firmas digitales:

- ¿Cómo sabemos que la firma es de quien dice ser?
- ¿Cómo nos asegura una autoridad de certificación que una firma es de quien dice ser?
- ¿No podemos fiarnos de una firma que no esté avalada por una autoridad de certificación?

Confianza de firmas (Web of trust)

- Se usa en PGP, GnuPG y similares
- Un usuario certifica (firmando con su clave privada) que la clave pública de otro usuario es de confianza
- La confianza se propaga según la confianza que demos a los usuarios que firmen las claves

Web of trust



https://commons.wikimedia.org/wiki/File:Web_of_Trust-en.svg

Niveles de confianza

- Desconocido: no nos fiamos de nada que firme ese usuario (por desconocimiento)
- Ninguno: no nos fiamos de nada que firme ese usuario (porque sabemos que lo hace mal)
- Marginal: nos fiamos de las claves firmadas por dos usuarios con confianza marginal
- Absoluto: nos fiamos de todo lo firmado por ese usuario