Infraestructura Computacional

Seguridad

Francisco Rueda

Sandra Rueda

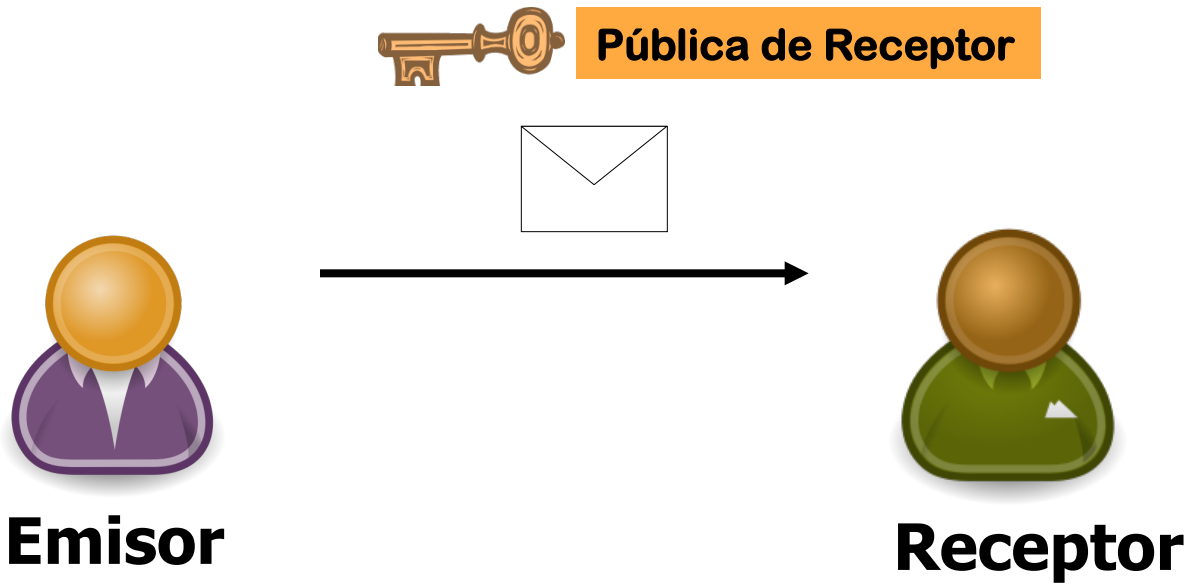
Sobre Digital

- Para evitar que alguien pueda leer la información que se envía, el emisor cifra el mensaje con la llave pública del receptor, es decir, crea un sobre digital

Sobre Digital

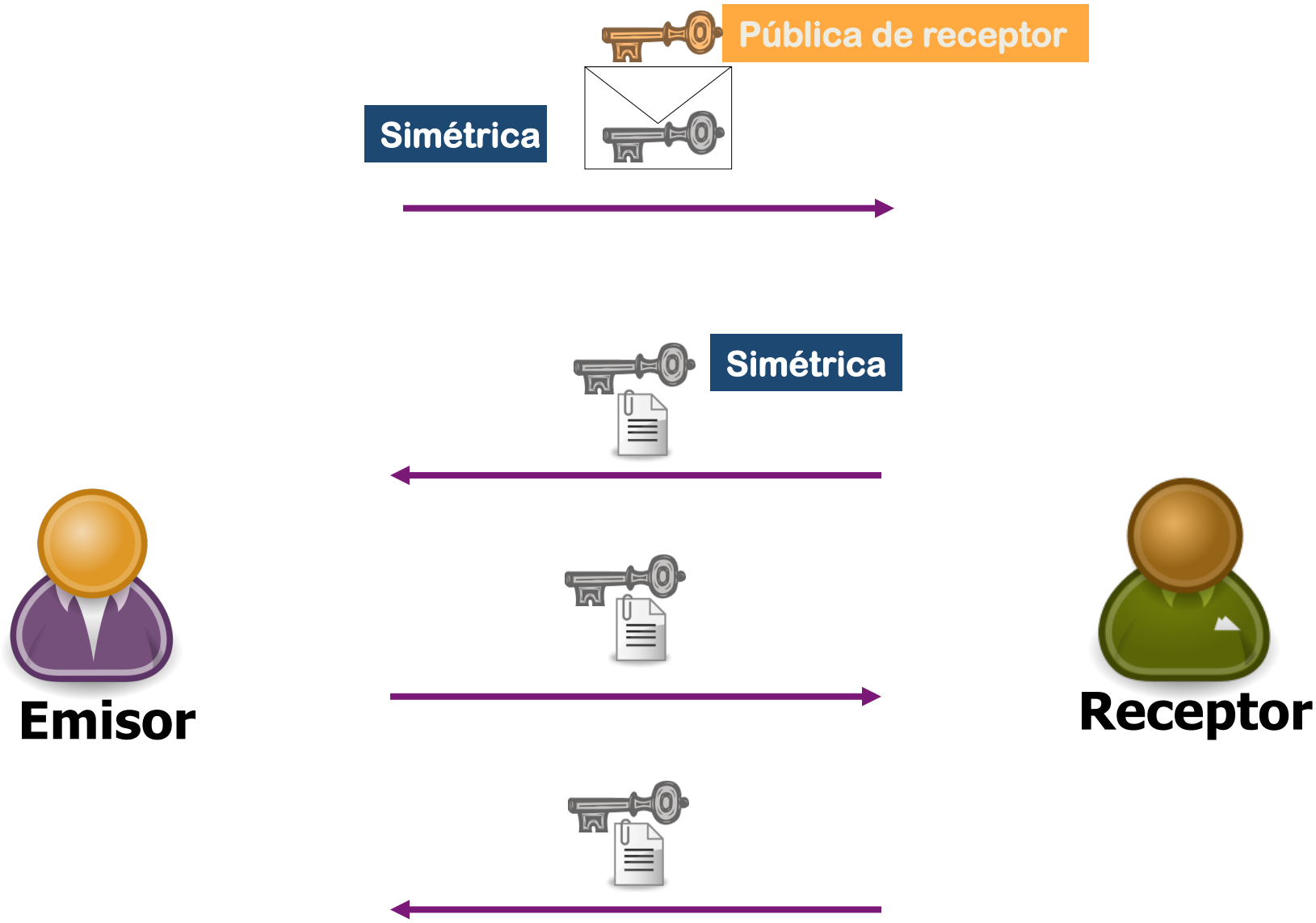
- Para evitar que alguien pueda leer la información que se envía, el emisor cifra el mensaje con la llave pública del receptor, es decir, crea un sobre digital
- ¿ Quién puede descifrar la información?

Sobre Digital



Sobre Digital y Llave de Sesión

- Una vez se cuente con sobres digitales, el emisor puede generar una llave de sesión simétrica y enviarla en un sobre digital
- A partir del momento en el que el receptor recibe la llave de sesión, la usa para las transacciones futuras

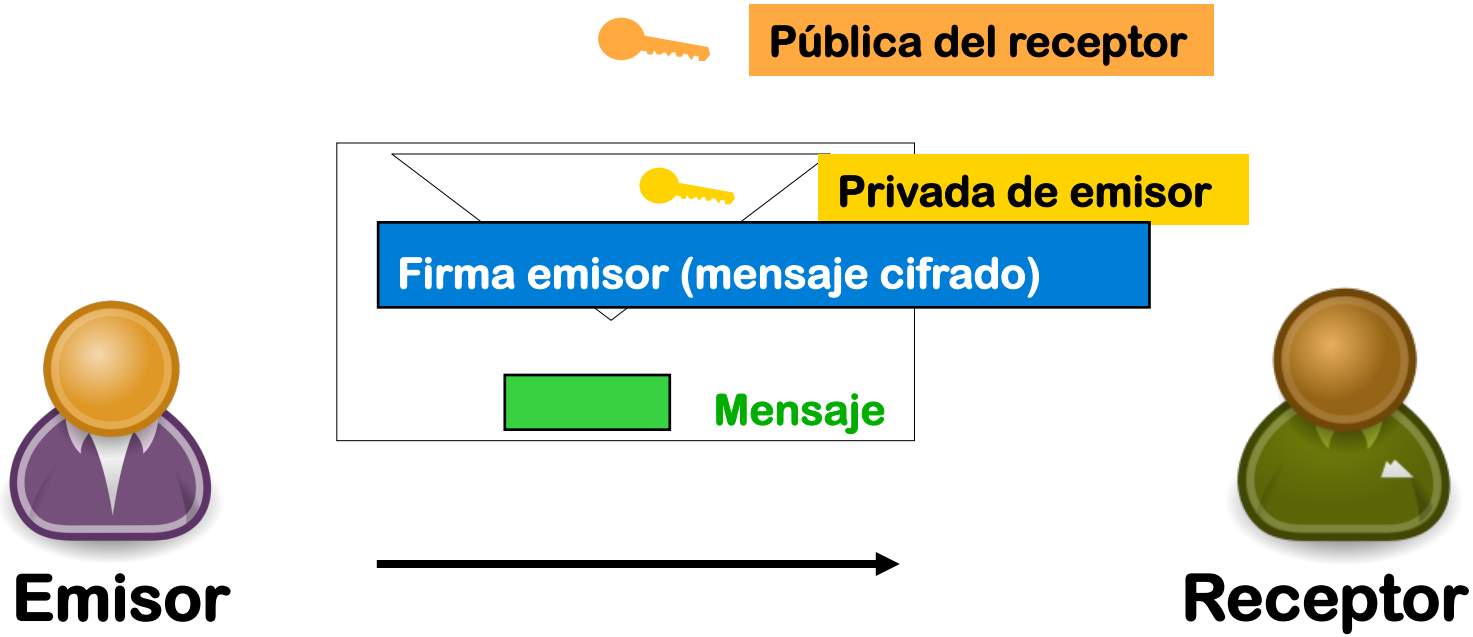

Pública de receptor
Simétrica
Simétrica
Emisor
Receptor

Firma Digital

Firma Digital

- La parte que desea firmar un mensaje lo cifra con su llave privada para obtener la firma y envía el resultado junto con el mensaje
- El receptor obtiene el mensaje y la firma. Al descifrar la firma, con la llave pública del emisor, puede verificar que corresponda al mensaje.

Firma Digital



Garantías

- Con el método anterior :
  - La información no puede ser espiada, pues viaja en un sobre digital
  - El emisor firma el documento, con su llave privada, lo cual permite verificar autenticación de la fuente y no repudio

Garantías

- Con las firmas digitales es posible probar la entidad del emisor (incluso ante la ley)
- Cuando se usan firmas digitales es fundamental proteger adecuadamente la llave privada
- La llave privada se puede almacenar en dispositivos
  - tarjetas inteligentes
  - tokens
  - protegidos por una contraseña o por un mecanismo biométrico

Tiempos

- El tamaño de la llave influye en el tiempo requerido para crear una firma

Processor	Key length (bits)			
	1024	*2048*	*4096*	*8192*
PI-233 MHz	40.3	252.7	1741.7	12,490.0
PIII-500 MHz	14.6	85.6	562.8	3,873.3
PIII-700 MHz	9.2	55.7	377.8	2,617.5
PIII-933 MHz	7.3	43.9	294.7	2,052.0
PIV-1.2 GHz	9.3	58.7	401.2	2,835.0

Table 2: Plain RSA signature timings (ms)

[Ding2007]

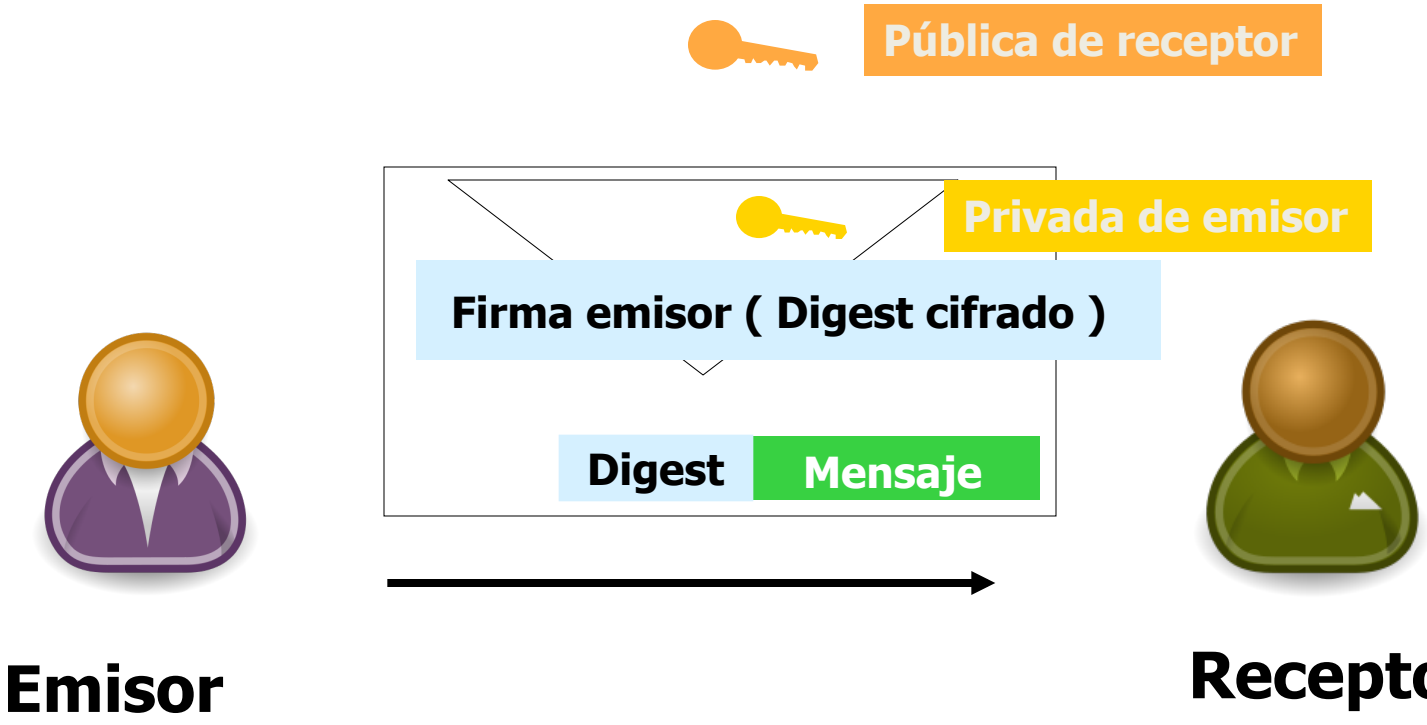
Firma Digital

- Una ventaja de la firma digital es que está asociada con el documento. Si este cambia entonces la firma no coincide.
- Por lo anterior la firma digital sirve también para verificar la integridad.
- La ley 527 reglamenta en Colombia lo relacionado con firmas digitales y otros aspectos.

Firma Digital

- Cuando se usan firmas digitales:
  - El resumen (digest) del mensaje es el que en realidad se cifra con la llave privada, no el mensaje.
  - ¿Qué ventaja tiene firmar el resúmen en vez del mensaje completo?
- Una firma digital, a diferencia de una firma tradicional, está asociada con el documento.
  - Si el documento cambia, la firma ya no coincide.

Digest Firmado



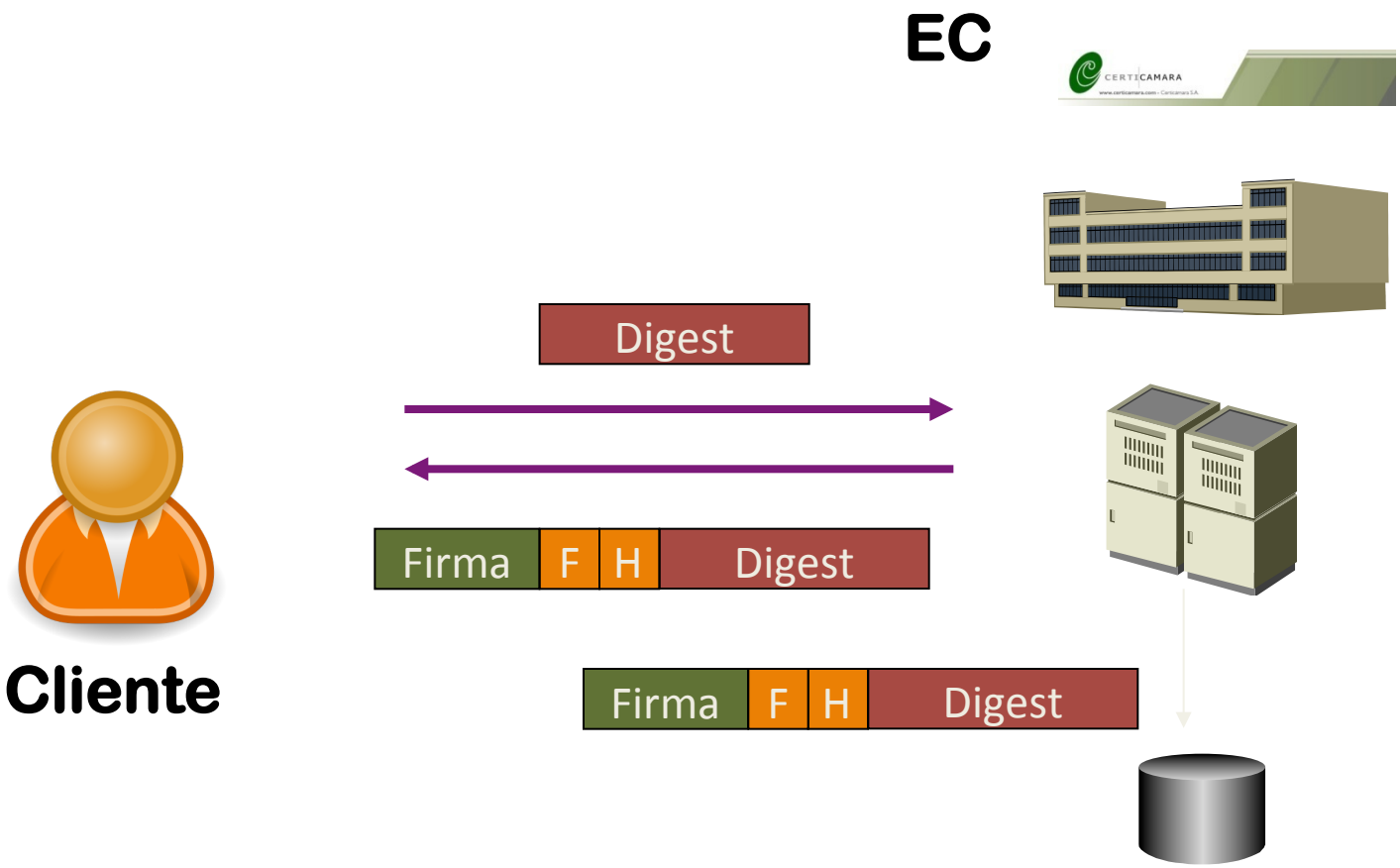
Limitaciones

- Hay dos problemáticas asociadas con las firmas digitales:
  - cómo garantizar su permanencia en el tiempo
  - cómo saber cuándo fue firmado un documento
- Hay algunas dificultades para garantizar la permanencia en el tiempo de un documento firmado

Estampilla Cronológica

- Para saber cuándo fue elaborado un documento se puede usar el estampado cronológico
- El estampado cronológico ".. Es un mensaje de datos firmado.... que permite verificar que otro mensaje de datos generado, transmitido o recibido no ha cambiado desde la fecha y el tiempo del día en que el subscriptor hace la solicitud.." Certicamara

Estampilla Cronológica



Limitaciones

- Otra dificultad se presenta para el uso de firmas digitales en dispositivos móviles, porque tienen capacidad de procesamiento limitada
- Hay varias alternativas:
  - Basada en la tarjeta SIM
  - Tecnologías basadas en el dispositivo
  - Independientes del dispositivo

[Martínez2007]

Alternativas

- Basada en la tarjeta SIM
  - Paquetes SMS con un encabezado que define los parámetros del cifrado
  - SIM Application Toolkit Technology (SAT)
- Tecnologías basadas en el dispositivo
  - Windows Mobile OS: Microsoft Cryptographic System
  - Symbian OS: Symbian OS Security Architecture
  - Java ME: Librerías para manejo de llaves y algoritmos de cifrado

Alternativas

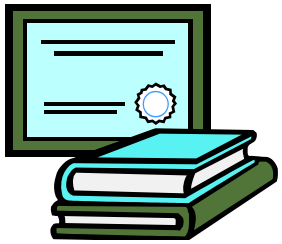
- Independientes del dispositivo
  - Firmas generadas por un servidor
    - SAS, Server-aided Signatures, o SBS ,Server-based signatures.

Marco Legal

- En Colombia, según la ley 527, el uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si incorpora los siguientes atributos:
  - Es única a la persona que la usa
  - Es susceptible de ser verificada
  - Está bajo el control exclusivo de un dueño
  - Está ligado a la información o mensaje, de tal manera que si este es cambiado, la firma es invalidada
  - Está conforme con las reglamentaciones adoptadas por el Gobierno Nacional

Certificados Digitales

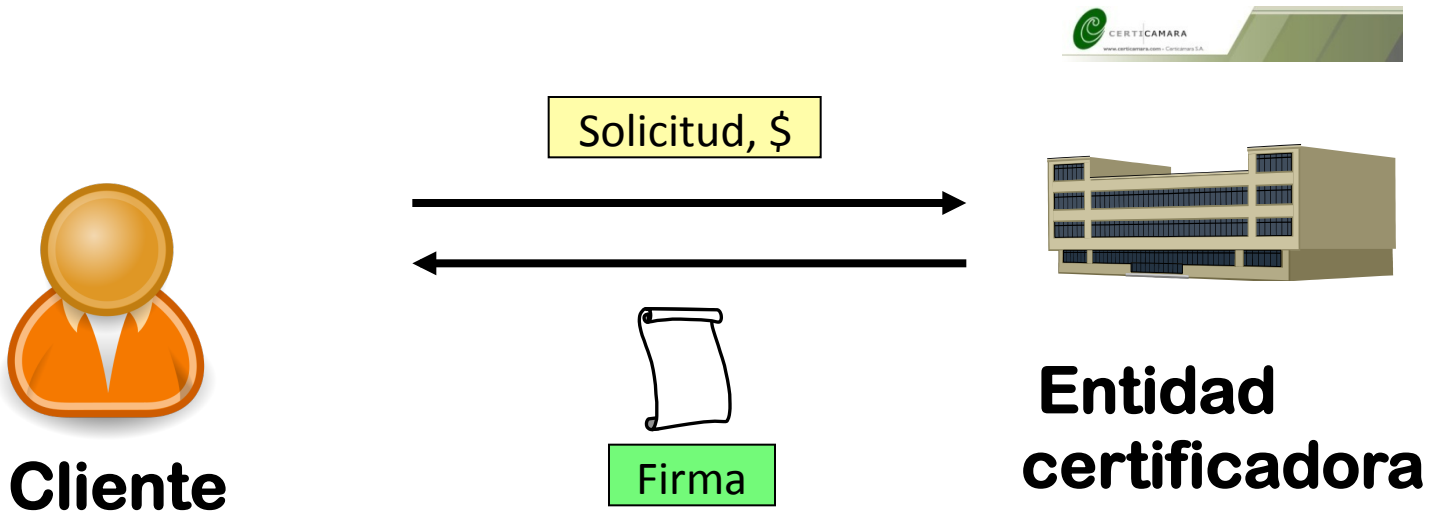
- Los certificados digitales (CD) son generados por una entidad que garantiza a otros la identidad de alguien (persona, programa, servidor,…)
  - El ente que hace la certificación se denomina Entidad certificadora (EC)



CD

- Los CDs contienen información del solicitante, junto con su llave pública, y están firmados por una EC
- Es el método usado para difundir la llave pública (sirve, por ejemplo para verificar una firma)
- Para obtener un CD es necesario primero pedirlo a una EC

CD



CD

- El CD está firmado por la EC y contiene:
  - La firma de la EC
  - Los datos del usuario certificado
  - La llave pública del usuario certificado

EC

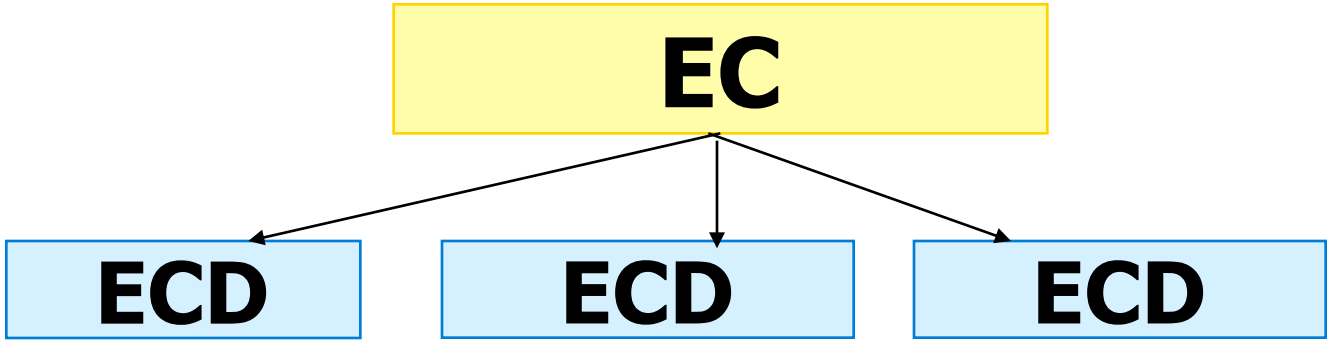
- La EC debe proteger muy bien su llave privada
- El CD puede entregarse por un medio electrónico
  - Si la EC genera la llave privada correspondiente, esta información debería entregarse por un medio seguro
    - Por ejemplo, en un medio físico

EC

- Para que el CD sea confiable se requiere verificación presencial de la identidad del usuario
  - Este mecanismo no escala
  - Es posible establecer una jerarquía de registro asociada a una EC

EC

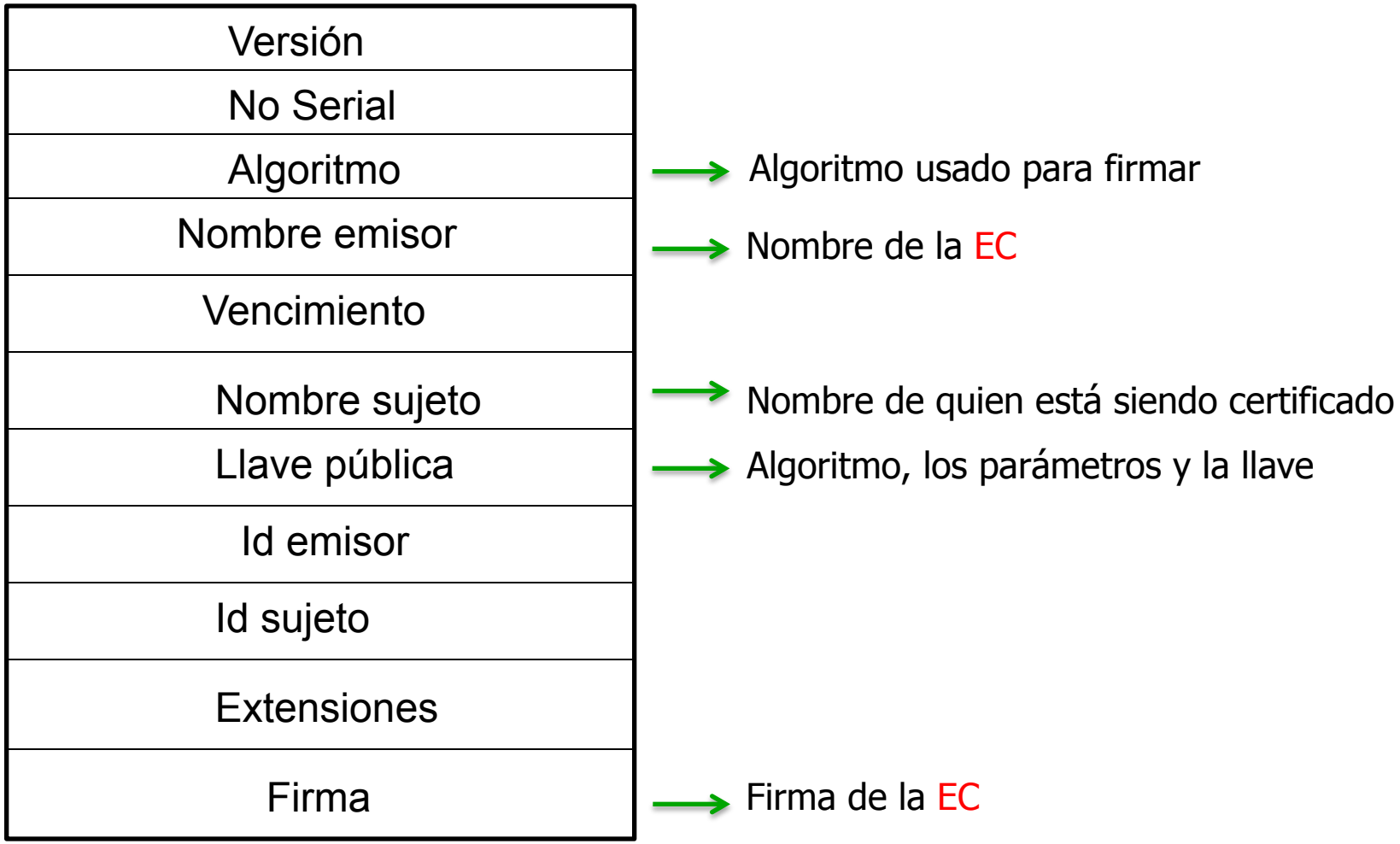
- Jerarquías para facilitar la administración



X509

- Existe un estándar, definido por ITU-T (ITU Telecommunication Standardization Sector) para el manejo de certificados, el X509, en el que se especifica cómo debe ser el servicio de certificados

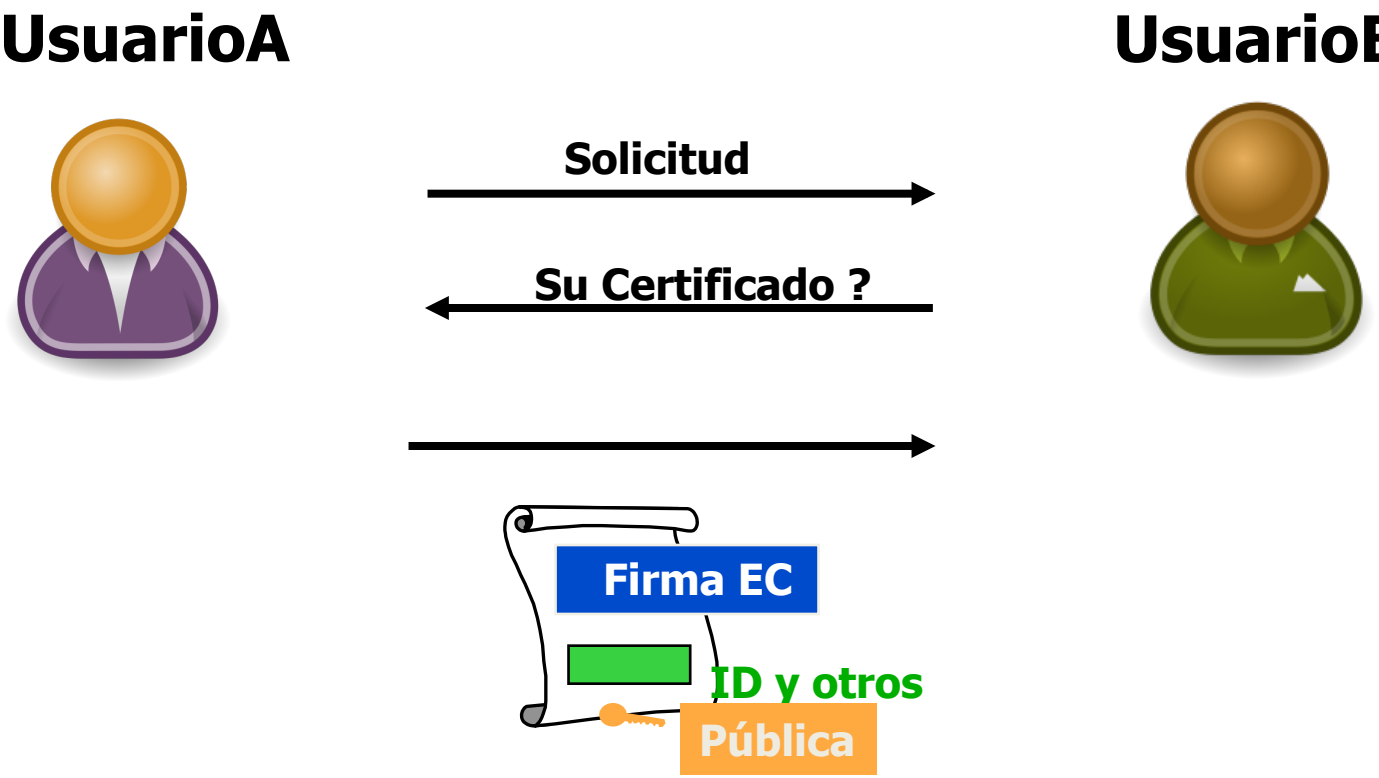
X509


Versión
No Serial
Algoritmo
Nombre emisor
Vencimiento
Nombre sujeto
Llave pública
Id emisor
Id sujeto
Extensiones
Firma
Algoritmo usado para firmar
Nombre de la EC
Nombre de quien está siendo certificado
Algoritmo, los parámetros y la llave
Firma de la EC

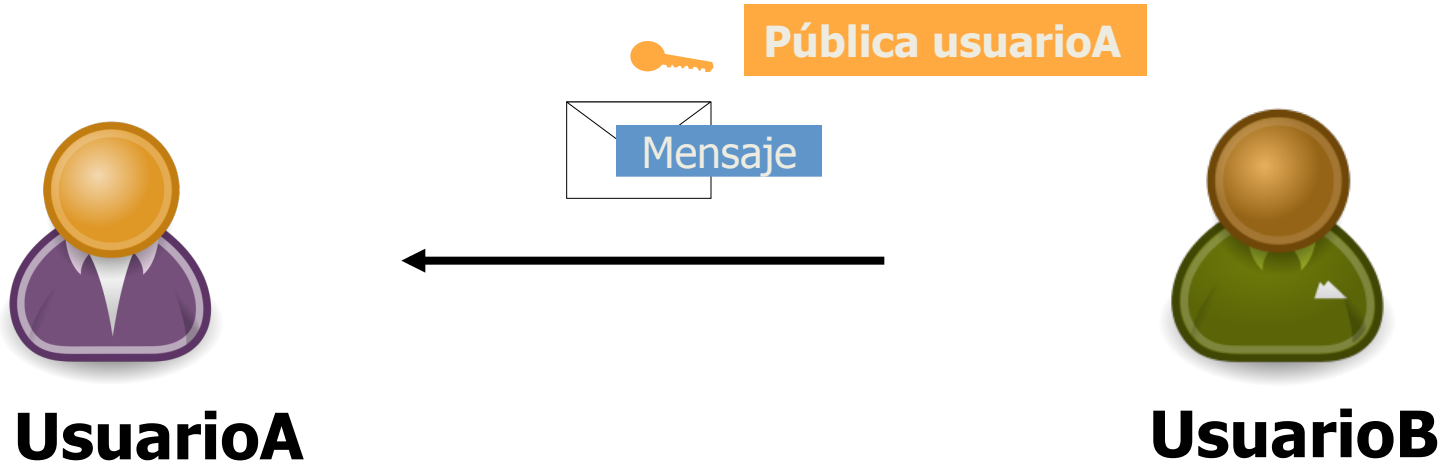
CD

- Cada vez que una parte desea verificar la identidad de otra , le solicita primero su CD
- A partir del CD se puede obtener su llave pública, enviarle sobres digitales y verificar su identidad (para evitar suplantaciones)

CD


UsuarioA
UsuarioB
Solicitud
Su Certificado ?
Firma EC
ID y otros
Pública

CD



CD

Cliente

Solicitud

Certificado servidor seguro

Certificado cliente

Servidor

CD

- Al conocer un CD se le pueden enviar sobres digitales a su dueño
- Existe un problema con la revocatoria de CD

CD

- Los CDs se usan para certificar :
  - Pertenencia a una empresa
  - Representación de empresa
  - Identificación de un servidor
  - Identificación de un programa
  - Identificación de un cliente (caso Grid computing)
  - .....

Referencias

- [NIST2002] *Risk Management Guide for Information Technology Systems*. NIST, 2002.
- [NIST2012] *Recommendation for Key Management*. NIST, 2012.
- [ForoUniandes2012] *Segundo Foro de Computación Móvil*. Uniandes, 2012.
- [Stallings2003] *Cryptography and Network Security*. William Stallings. Prentice Hall, 2003.
- [Swaminatha2003] *Wireless Security and Privacy*. Tara Swaminatha y Charles Elden. Addison-Wesley, 2003.
- [Couloris2005] *Sistemas Distribuidos: conceptos y diseño*. George Coulouris, Jean Dollimore y Tim Kindberg. Addison-Wesley, 2005.
- [Martinez2007] A Survey of Electronic Signature Development in Mobile Devices. Martínez, Sánchez, Ruiz, Gómez. Journal of Theoretical and Applied Electronic Commerce Research. 2007.