Universidad
Carlos III de Madrid

COSEC Lab· Dpto. Informática

TEMA 2. CRIPTOGRAFÍA
T 2.6 Infraestructura de Clave Pública (PKI)

Criptografía y seguridad informática
Seguridad en las tecnologías de la información
@ COSEC

Curso 2016-2017

Origen

Combinación de HW, SW y métodos de seguridad.

- Criptografía de clave pública no permite asociar identidades a claves criptográficas
  - Incertidumbre respecto al origen de una clave pública

- Modelo tradicionalmente basado en Autoridad de Clave Pública o Directorios Públicos
  - Necesidad de acceso online
  - No escalables

Son necesarios
- Usuario, inicia la operación.
- Autoridad, que verifique la pertenencia y garantiza la validez de los certificados
- Destinatario, recibe los datos cifrados o firmados

clave privada, nunca se divulga
" pública, se da a conocer.

Origen

- ***Toward a Practical Public-Key Cryptosystem***. L. Kohnfelder. *Bachelor Thesis, Department of Electrical Engeeniering*, MIT, Cambridge, MA, 1978

  → Propuesta del concepto certificado digital y lista de certificados revocados

  - Vincula una identidad a una clave pública
  - Emitido por un "Fichero Público" de confianza
  - Para ofrecer confianza respecto a la vinculación (clave pública – ID), ambos datos se **firman digitalmente** Aunque pueden aparecer + datos
    - Sólo modificable por el Fichero Público
    - Verificable por terceras partes supuesto que cuentan con la clave pública (certificada) del Fichero Público
  - Presenta problemas de gestión de los certificados (ciclo de vida), particularización de los usos de la clave, escalabilidad versus reconocimiento mutuo

Se basa en la confianza mutua en la Autoridad de certificado

Origen

- ***Toward a Practical Public-Key Cryptosystem***. L. Kohnfelder. *Bachelor Thesis, Department of Electrical Engeeniering*, MIT, Cambridge, MA, 1978
  - *"Public-key communication works best when the encryption functions can reliably be shared among the communicants (by direct contact if possible). Yet when such a reliable exchange of functions is impossible the next best thing is to trust a third party. Diffie and Hellman introduce a central authority known as the Public File(…) Each individual has a name in the system by which he is referenced in the Public File. Once two communicants have gotten each other's keys from the Public File then can securely communicate.* ***The Public File digitally signs all of its transmission so that enemy impersonation of the Public File is precluded."***

¿Qué es hoy un certificado de clave pública? **Idea básica**

- Identidad sujeto A (ID_A)
- Clave pública de A ($K_{U,A}$)
- Identidad emisor AC (ID_{AC})
- Periodo de validez (T_1 , T_2)
- Número de serie

- Firma digital sobre lo anterior emitida por AC con el algoritmo de firma F y su clave privada $K_{V,AC}$

Que contiene:
ID del emisor A
Clave pública de A
ID de la autoridad certif.
Periodos de validez
Nº de serie
Todo lo anterior es firmado por la AC con su clave privada.

Se puede verificar desfirmando con la pública.

$$C_A = ID_A, K_{U,A}, ID_{AC}, T_1 , T_2, F(K_{V,AC}; ID_A, K_{U,A}, ID_{AC}, T_1 , T_2)$$

C_A: Dato, Firma(Datos)

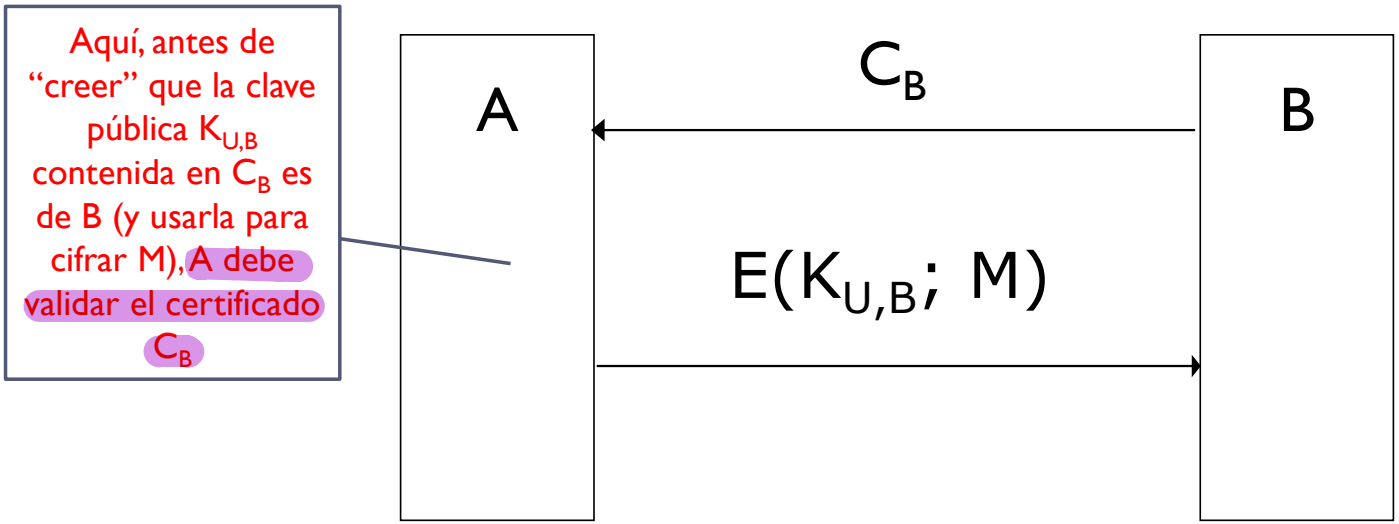
Algoritmo de firma

La clave privada que se usa para firmar

Lo que se firma

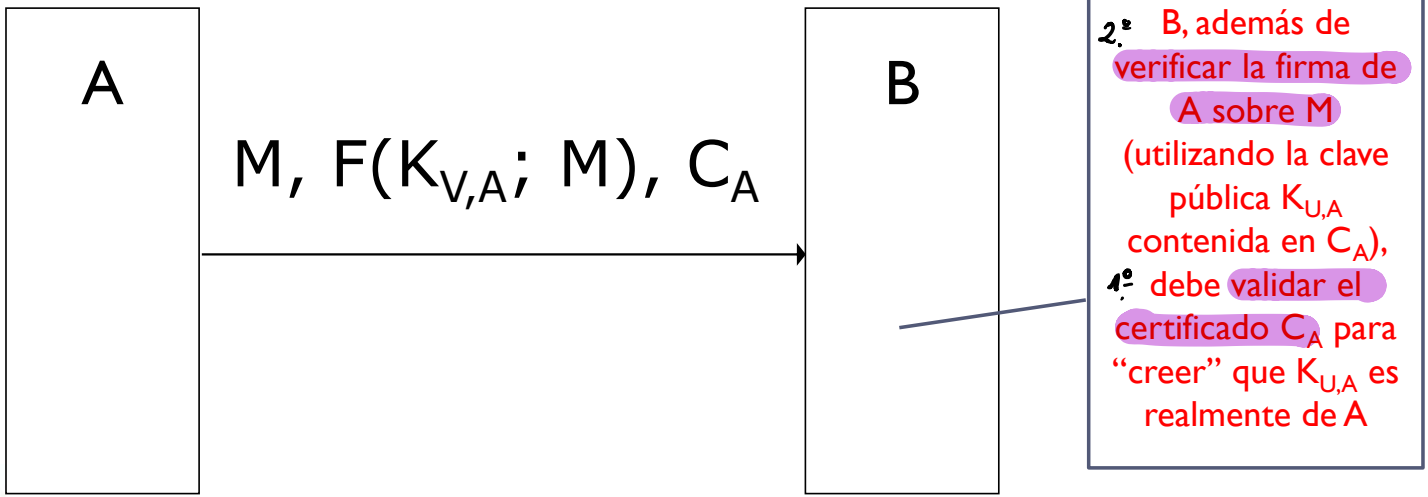
Usos de los certificados de clave pública (1) **Idea básica**

- Si A quiere cifrar un mensaje para B, B le envía su certificado de clave pública C_B para que A sepa seguro que esa es la clave pública de B



Usos de los certificados de clave pública (2) **Idea básica**

- Si A quiere firmar un mensaje, puede adjuntar al mensaje firmado su certificado de clave pública para que todo el mundo que desee verificarlo sepa quién es el legítimo poseedor de esa clave (el emisor de la firma)



¿Cómo validar un certificado de clave pública? **Idea básica**

- Obtengo una copia confiable de $K_{U,AC}$, la clave pública de la AC
  - E.g., obteniendo su certificado de clave pública C_{AC} → K_u, AC
    - ¡Paradoja del huevo y la gallina!: ¿es válido y confiable este certificado? → ¡lo certifica la propia AC!
      - **¿Confianza en AC? (debemos decidir si confiamos en AC o no)**
      - **¿Hemos obtenido una copia del certificado de AC por un canal seguro?**

El problema es como lo validamos hay que dar un primer paso. Canal seguro

Certificado autofirmado, solo en la raiz y debemos confiar para que sea valido

- Verifico la **firma** emitida por la AC que hay en el certificado
  - Utilizando $K_{U,AC}$ confiable (la del punto anterior)

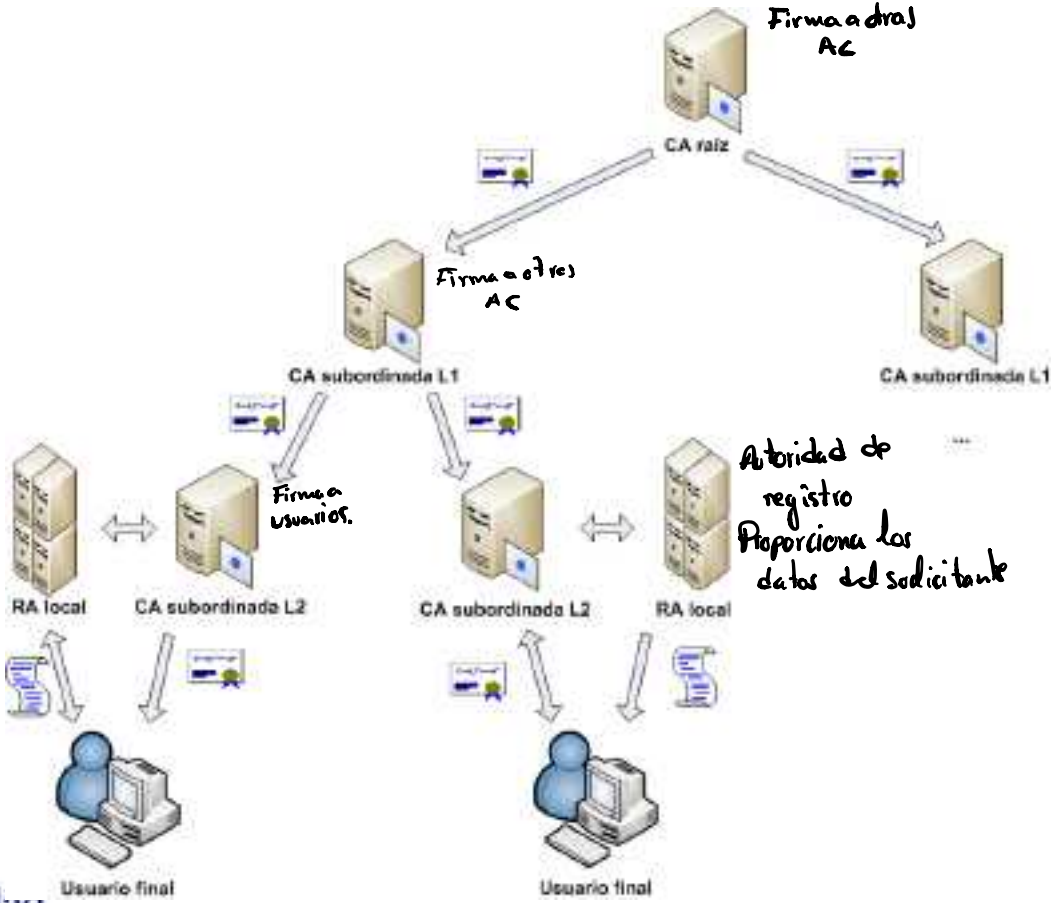
- Verifico que la fecha de uso del certificado está dentro del **periodo de validez** del mismo

- Verifico que el certificado no ha sido **revocado**
  - E.g., consultando la lista de certificados revocados o CRL

Infraestructura de Clave Pública (PKI)

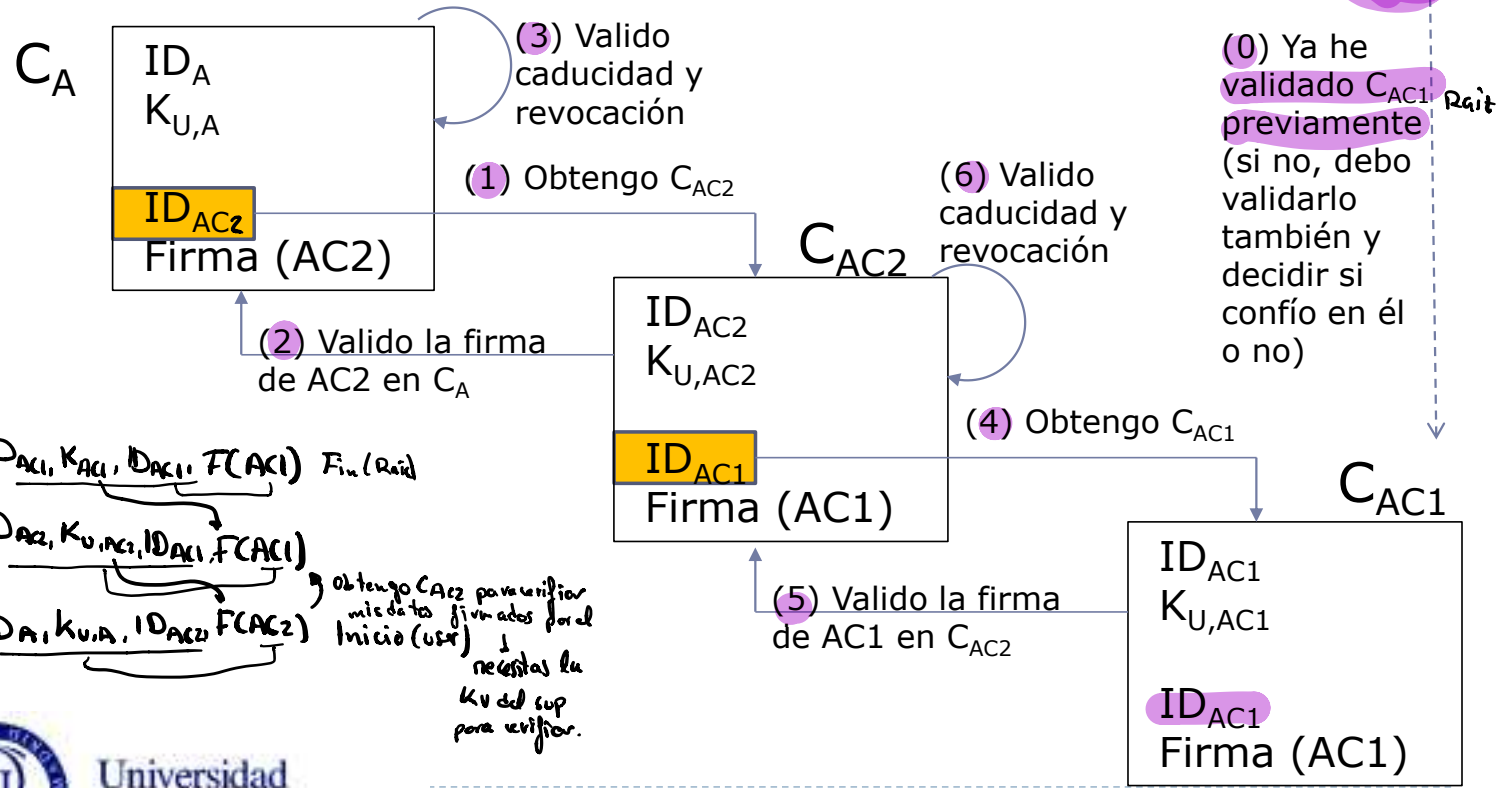
- Conjunto de estándares internacionales (ITU-T, IETF)
- Define la estructura de un certificado X.509 y la Lista de Certificados Revocados (CRL) [RFC 5280]
  La lista de certificados caducados o a punto de.
- Define un modelo jerárquico de Autoridades de Certificación [RFC 5280]
- Define el conjunto de protocolos operacionales y de gestión [RFC 4210 CMP, RFC 4211 CRMF, RFC 3647 CP/CPS…]

Infraestructura de Clave Pública (PKI) – Modelo jerárquico



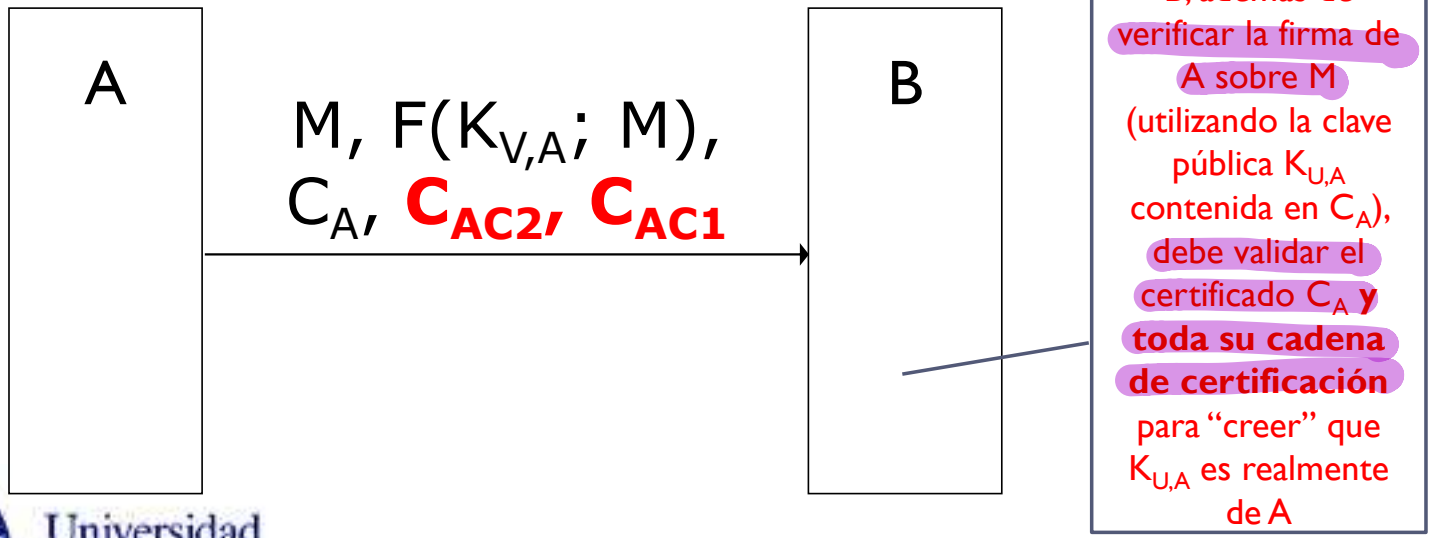
Infraestructura de Clave Pública (PKI) – Modelo jerárquico

*Para validar un certificado se debe validar también toda su **cadena de certificación** hasta llegar a un certificado raíz (autofirmado) en el que se confíe*



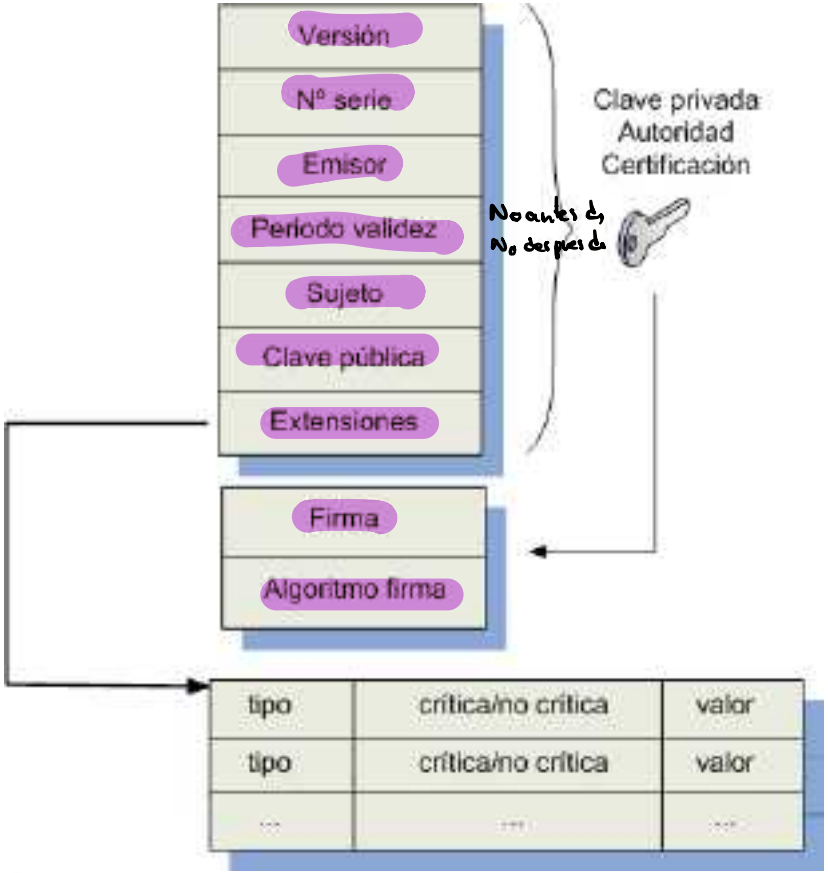
Ampliación: Usos de los certificados de clave pública (2) **Idea básica**

- Si A quiere firmar un mensaje, puede adjuntar al mensaje firmado su certificado de clave pública y **toda su cadena de certificación** (…)



Infraestructura de Clave Pública (PKI) – Certificado X.509

Datos
+
Firma(Data)



Infraestructura de Clave Pública (PKI) – Certificado X.509

- Versión actual: 3
- N° de serie
  - Identifica de manera única al certificado dentro del ámbito de la AC
- Emisor
  - *Distinguished name* (DN) de la AC que ha emitido el certificado (X.501)

    Ej: CN = AC DNIE 001, OU = DNIE, O = DIRECCION GENERAL DE LA POLICIA, C = ES
- Periodo de validez: [No antes, No después]
- Sujeto
  - *Distinguished name* (DN) del sujeto propietario del certificado

    Ej: CN = Español Español Juan, SerialNumber = 12345678A, C = ES

Infraestructura de Clave Pública (PKI) – Certificado X.509

- Clave pública
  - Información de la clave pública contenida en el certificado y algoritmo de clave pública

    Ej: módulo y exponente público RSA
- Extensiones
  - Facilitan la inclusión de información adicional en el certificado
  - Pueden ser adhoc o utilizar extensiones predefinidas en el estándar

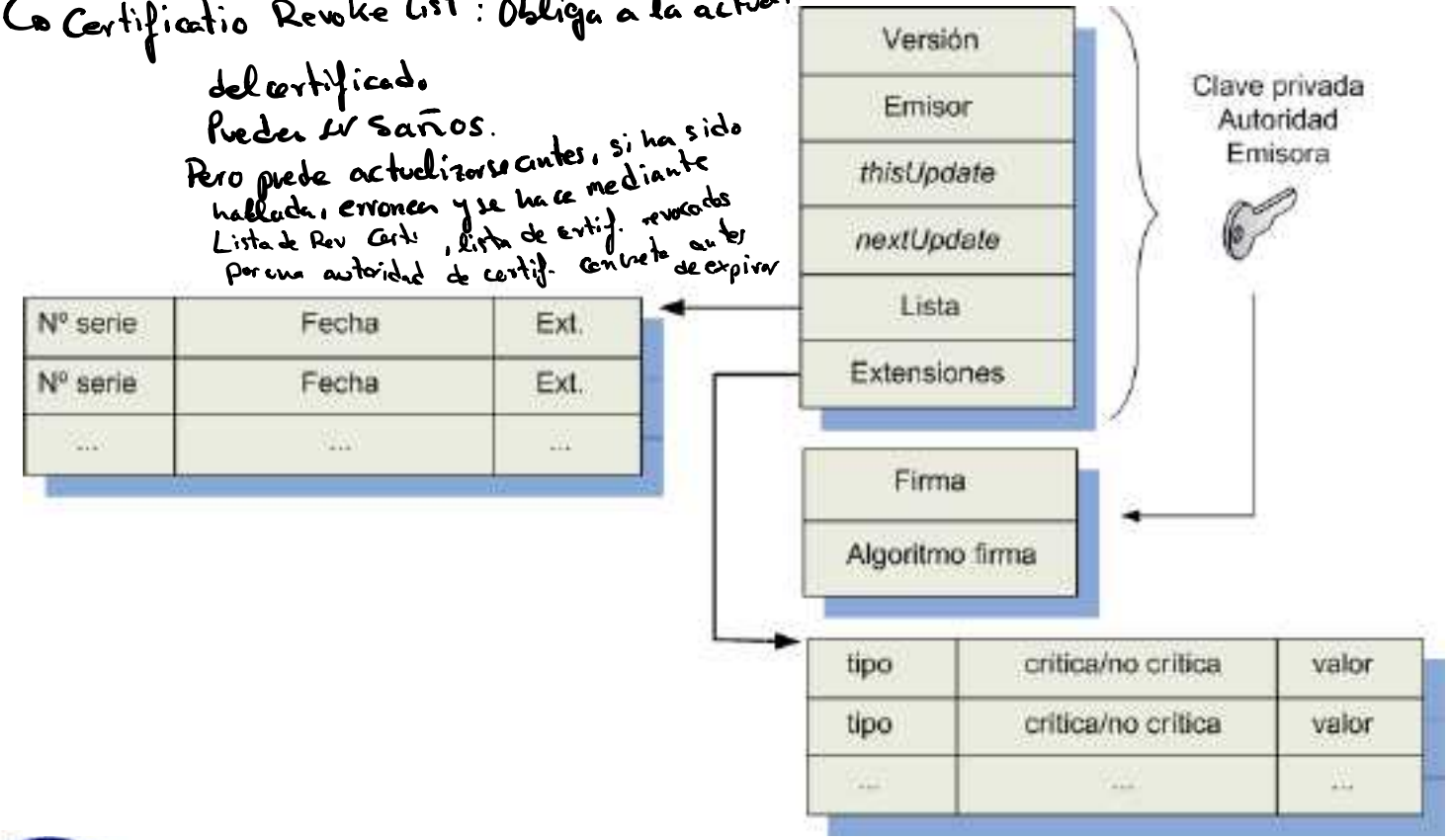
    Ej: Extensión *keyUsage* define los propósitos para los cuales puede emplearse la clave privada asociada:
    - *Firma digital*
    - *No repudio*
    - *Intercambio de claves*
    - *Cifrado*
    - *Etc.*

Infraestructura de Clave Pública (PKI) – Certificado X.509

- Tipos de Certificados
  - Persona física
  - Persona jurídica
  - Componente (p. e. servidor Web)
  - Firma de código
  - …etc

Infraestructura de Clave Pública (PKI) - CRL

Certificatio Revoke List: Obliga a la actualización del certificado.
Pueden ser años.
Pero puede actualizarse antes, si ha sido hallada, errónea y se hace mediante Lista de Rev Certs, lista de certif. revocados por una autoridad de certif. contra de expirar



Infraestructura de Clave Pública (PKI) – CRL

- Publicada por la AC u otra entidad delegada
- La AC puede eliminar de la CRL los certificados expirados
  - Evita un crecimiento descontrolado de la CRL
- *thisUpdate* indica la fecha de emisión de la CRL

  nextUpdate indica la fecha límite en la cual el emisor publicará la CRL actualizada
  - Existe un periodo de tiempo desde que el sujeto solicita la revocación del certificado hasta que dicha revocación se hace efectiva
- Fecha
  - Indica la fecha de procesamiento de la solicitud de revocación
- Ext.
  - Permite, entre otros, incluir el motivo de la revocación y la fecha de solicitud

Infraestructura de Clave Pública (PKI) – Declaración de Prácticas de Certificación (DPC)

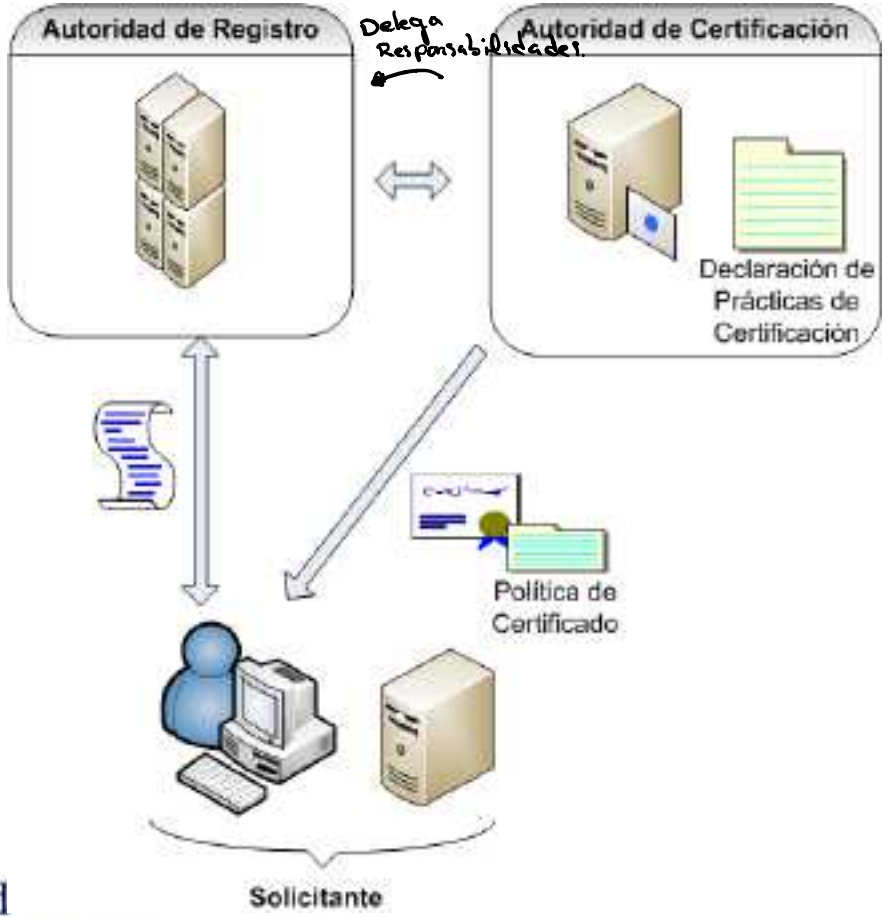
- Documento publicado por una AC que comprende las normas, reglas y procedimientos que rigen el ciclo de vida de los certificados que expide

- Incluye las obligaciones que contrae con los titulares de sus certificados, y de éstos con aquélla, y los márgenes de responsabilidad que asume frente a las entidades que aceptan dichos certificados

Infraestructura de Clave Pública (PKI) – Servicios operacionales

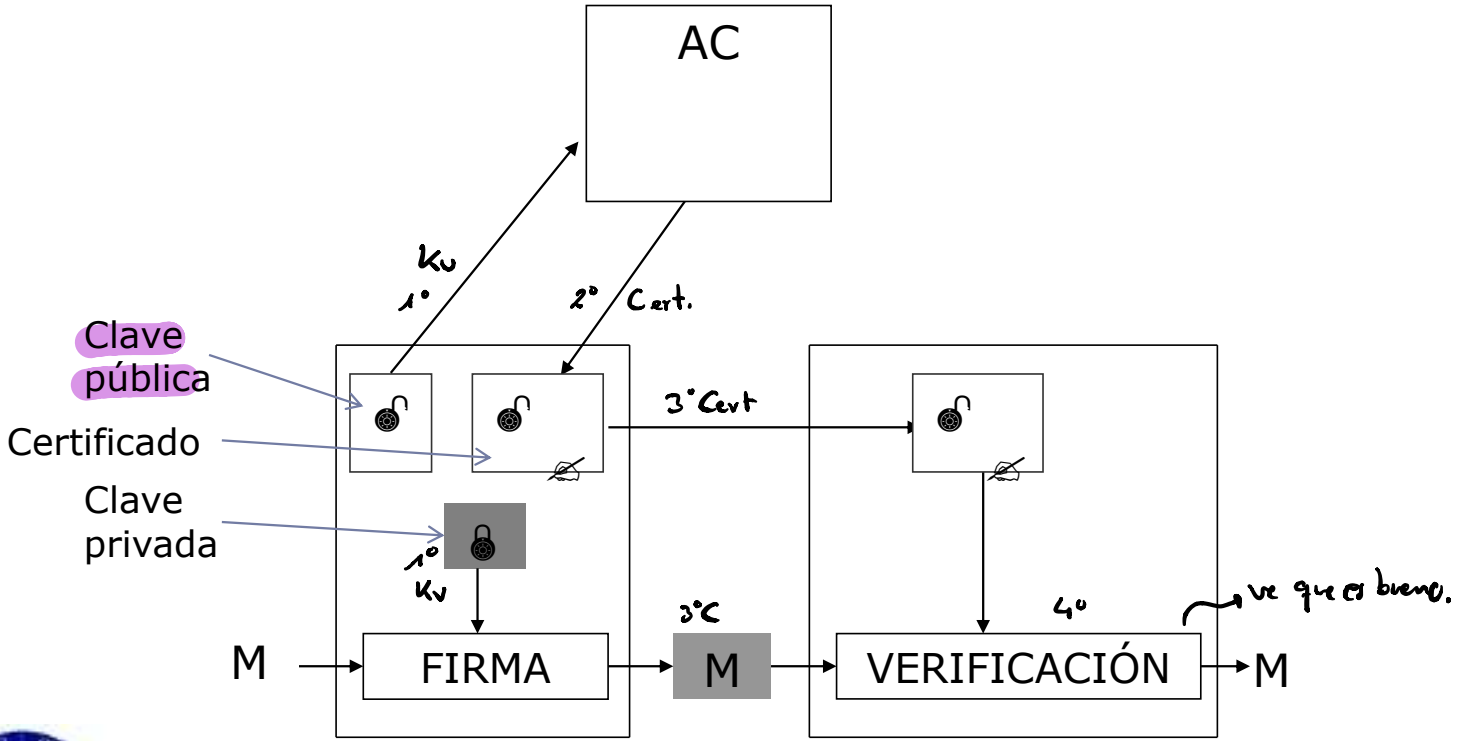
- Solicitud de un certificado
- Registro
- Renovación de un certificado
- Revocación de un certificado
- Consulta del estado de un certificado (CRL, OCSP)
- Publicación del estado de revocación de los certificados

Infraestructura de Clave Pública (PKI) – Solicitud de un certificado + registro (I)



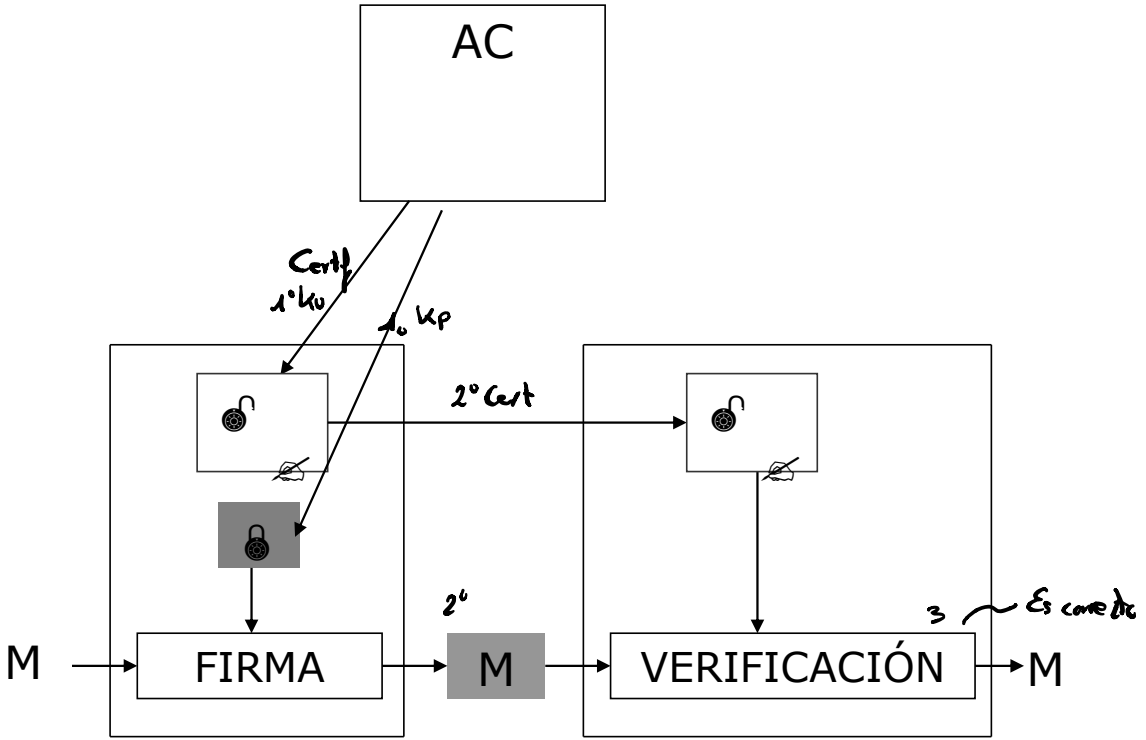
Infraestructura de Clave Pública (PKI) – Solicitud de un certificado + registro (II)

- Generación de claves en cliente



Infraestructura de Clave Pública (PKI) – Solicitud de un certificado + registro (III)

- Generación de claves en la AC



Infraestructura de Clave Pública (PKI) – Solicitud de un certificado + registro (IV)

- Soporte de almacenamiento de la clave privada
  - Software
    - Repositorio de claves del Navegador Web
    - Fichero específico protegido (PKCS#12, PFX)
  - Hardware
    - Tarjeta Inteligente
    - Token USB
    - Chip TPM
    - HSM

Es el unico formato que permite exportar el certificado y su clave publica

Formato

Extension

Circuito o chip programado

Infraestructura de Clave Pública (PKI) – Validación del estado de un certificado

- El estado de revocación de los certificados debe ser accesible
- Métodos de publicación y consulta basados en CRL
  - Actualización periódica
  - Generan periodo de incertidumbre hasta *nextUpdate* (solución: periodo de precaución)
  - Generan problemas de consumo de ancho de banda (soluciones: over-issued CRLs, Delta CRLs, CRLs segmentadas, CRLs indirectas)
- Método de consulta OCSP (*Online Certificate Status Protocol*)
  - Facilita la consulta mediante un protocolo sencillo [RFC 2560]
  - Pueden proporcionar el estado actualizado en todo momento

Modelo descentralizado

- Modelo de confianza descentralizado
  - No existe autoridad de certificación
  - Cada usuario certifica las claves de los usuarios en los que confía
  - Se pueden establecer cadenas de confianza de n saltos
- Ventajas
  - Rápida implantación, sencillez, menores costes
- Desventajas
  - No escalable
  - Necesidad de transmitir una clave pública por un canal seguro antes de certificarla
- Ejemplo: PGP (*Pretty Good Privacy*)

Cualquiera puede firmar y atestiguar la validez de certificados de otros.
Es un criptosistema híbrido, simetrica y asimetrica rapido cano cog.
Garantiza el no repudio y suplantacion.
Fortalece la seguridad criptografica.
1° Comprime, ahorra espacio y fortalece la seguridad criptografica.
2° Crea clave de sesión unica, segura teclado y raton