Tema 12

Infraestructuras de clave pública

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Ana I. González-Tablas Ferreres
José M. de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González

uc3m | Universidad Carlos III de Madrid

COSEC

ÍNDICE

- 12. Infraestructuras de clave pública
  - Origen
  - Certificado de clave pública
  - Infraestructura de clave pública (PKI)
  - Certificado X.509
  - Validación de estado de un certificado
  - Otros aspectos
  - Modelo descentralizado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 12. Infraestructuras de clave pública
  - **Origen**
  - Certificado de clave pública
  - Infraestructura de clave pública (PKI)
  - Certificado X.509
  - Validación de estado de un certificado
  - Otros aspectos
  - Modelo descentralizado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Origen

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

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

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Origen

- L. Kohnfelder. ***Toward a Practical Public-Key Cryptosystem.*** 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
    - 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

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Origen

- L. Kohnfelder. ***Toward a Practical Public-Key Cryptosystem***. 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."

ÍNDICE

- 12. Infraestructuras de clave pública
  - Origen
  - **Certificado de clave pública**
  - Infraestructura de clave pública (PKI)
  - Certificado X.509
  - Validación de estado de un certificado
  - Otros aspectos
  - Modelo descentralizado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

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 S y su clave privada $K_{V,AC}$

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

Algoritmo de firma

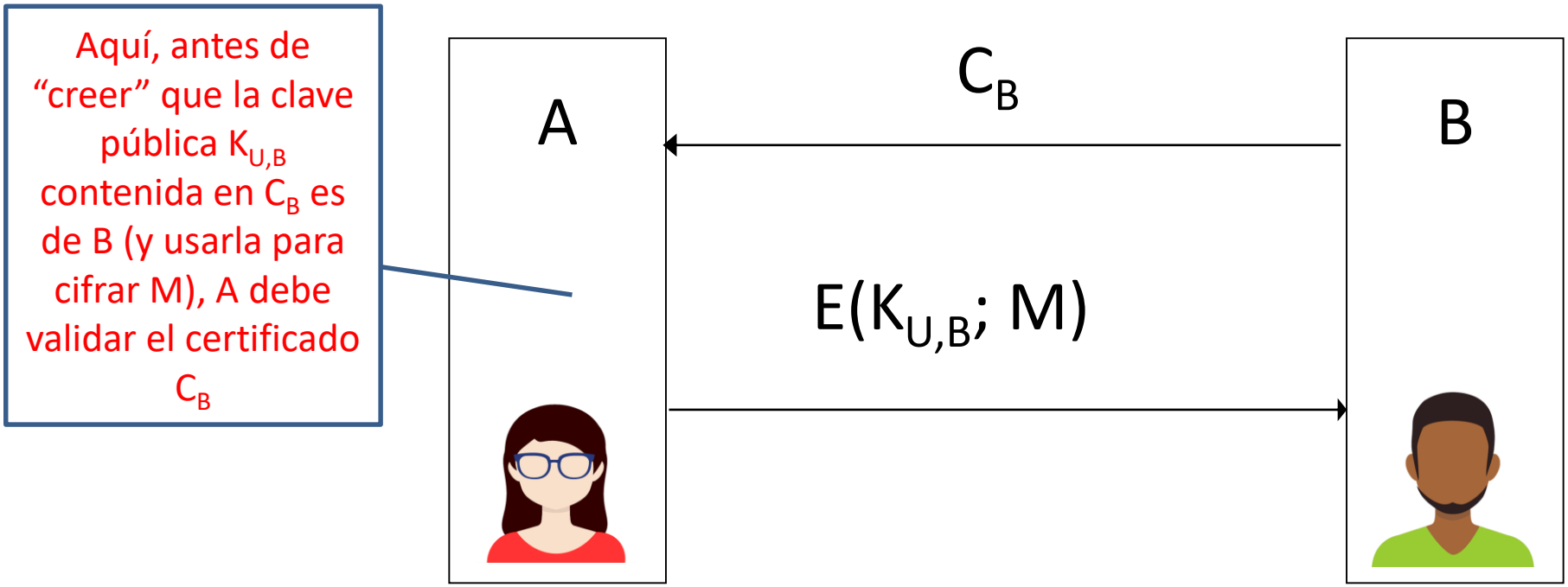
La clave privada que se usa para firmar

Lo que se firma

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Certificado de clave pública. Idea básica

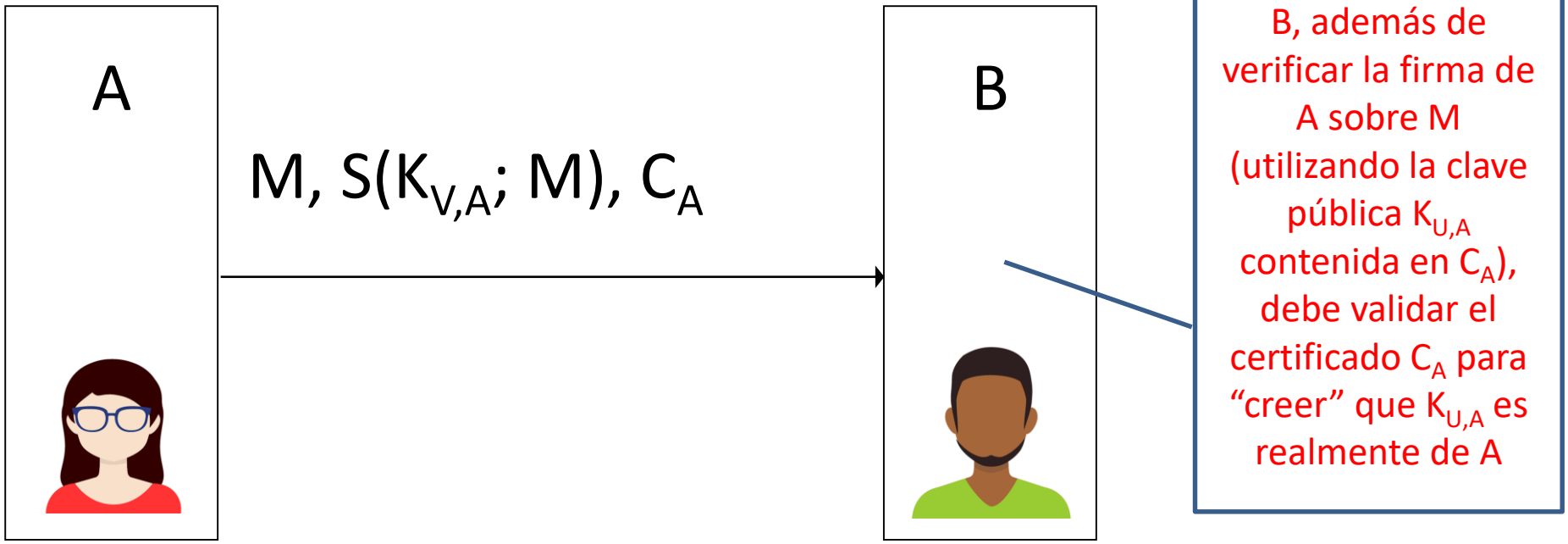
- Si A quiere cifrar un mensaje para B, B le envía su certificado de clave pública C_B para que A sepa seguro que esa es la clave pública de B



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Certificado de clave pública. Idea básica

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



Certificado de clave pública. Periodo de validez, estado y usos

- Periodo de validez
  - Acotado (medida preventiva)
  - Dependiente de la longitud de las claves y de su uso
- Estado
  - Válido
  - Suspendido
  - Revocado
  - …
- Usos permitidos

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Certificado de clave pública. Verificación

- Obtengo una copia confiable de $K_{U,AC}$, la clave pública de la AC, e.g., obteniendo su certificado de clave pública C_{AC}
- ¿Es confiable este certificado? ¡Paradoja del huevo y la gallina!
  - ¡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?
- Verifico
  - La firma emitida por la AC que hay en el certificado, utilizando $K_{U,AC}$ confiable
  - La fecha de uso del certificado está dentro del periodo de validez del mismo
  - El estado del certificado (i.e., que no ha sido revocado)
  - Verifico que entre los usos de dichas claves está el de emitir certificados

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 12. Infraestructuras de clave pública
  - Origen
  - Certificado de clave pública
  - **Infraestructura de clave pública (PKI)**
  - Certificado X.509
  - Validación de estado de un certificado
  - Otros aspectos
  - Modelo descentralizado

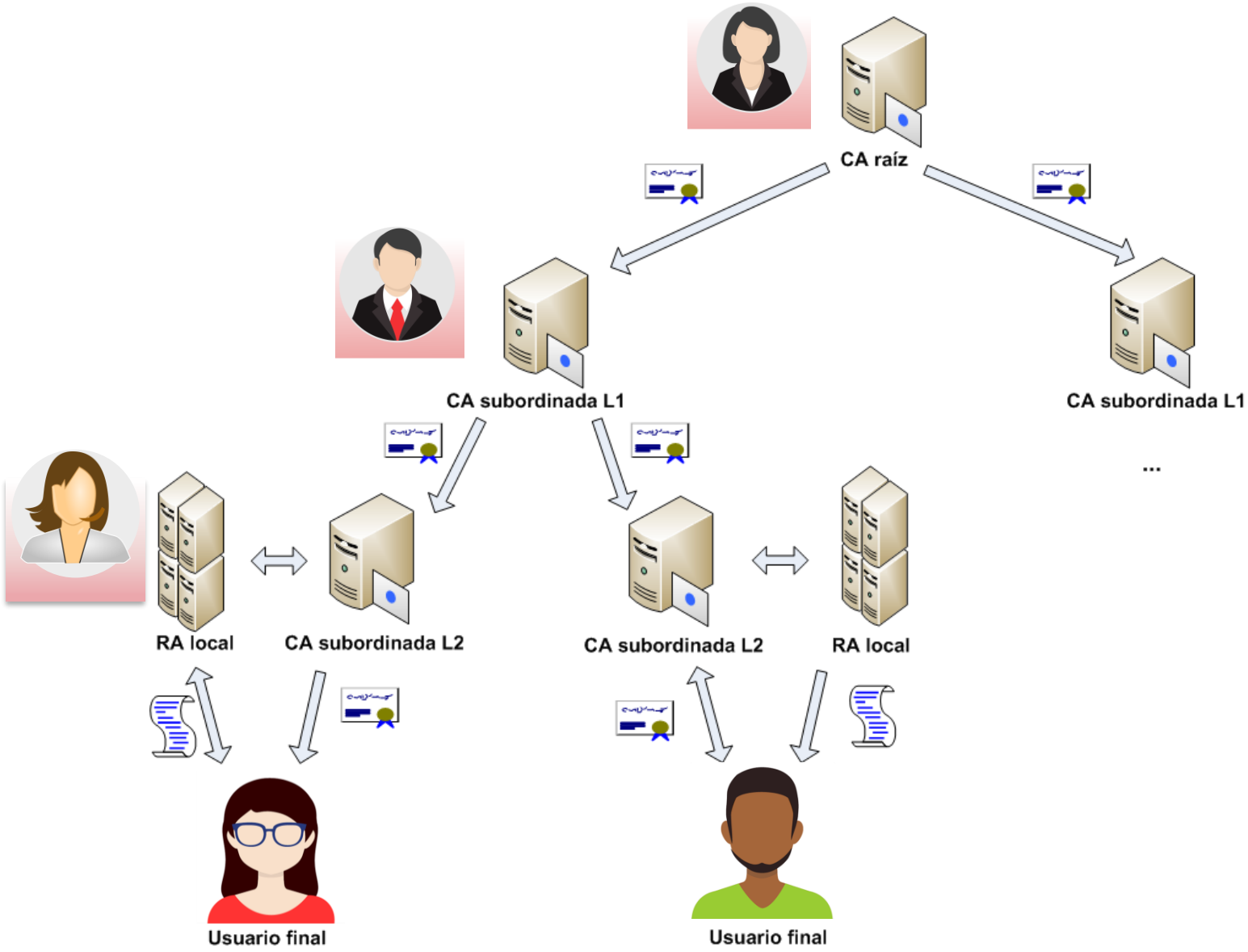
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Infraestructura de Clave Pública (PKI)

- Conjunto de estándares internacionales (ITU-T, IETF)
- Define la estructura de los certificados X.509 y de las listas de certificados revocados (CRL) [RFC 5280]
- Define un **modelo jerárquico** de Autoridades de Certificación [RFC 5280] y Autoridades relacionadas
  - Autoridad de Registro
- Define el conjunto de protocolos operacionales y de gestión [RFC 4210 CMP, RFC 4211 CRMF, RFC 3647 CP/CPS…]

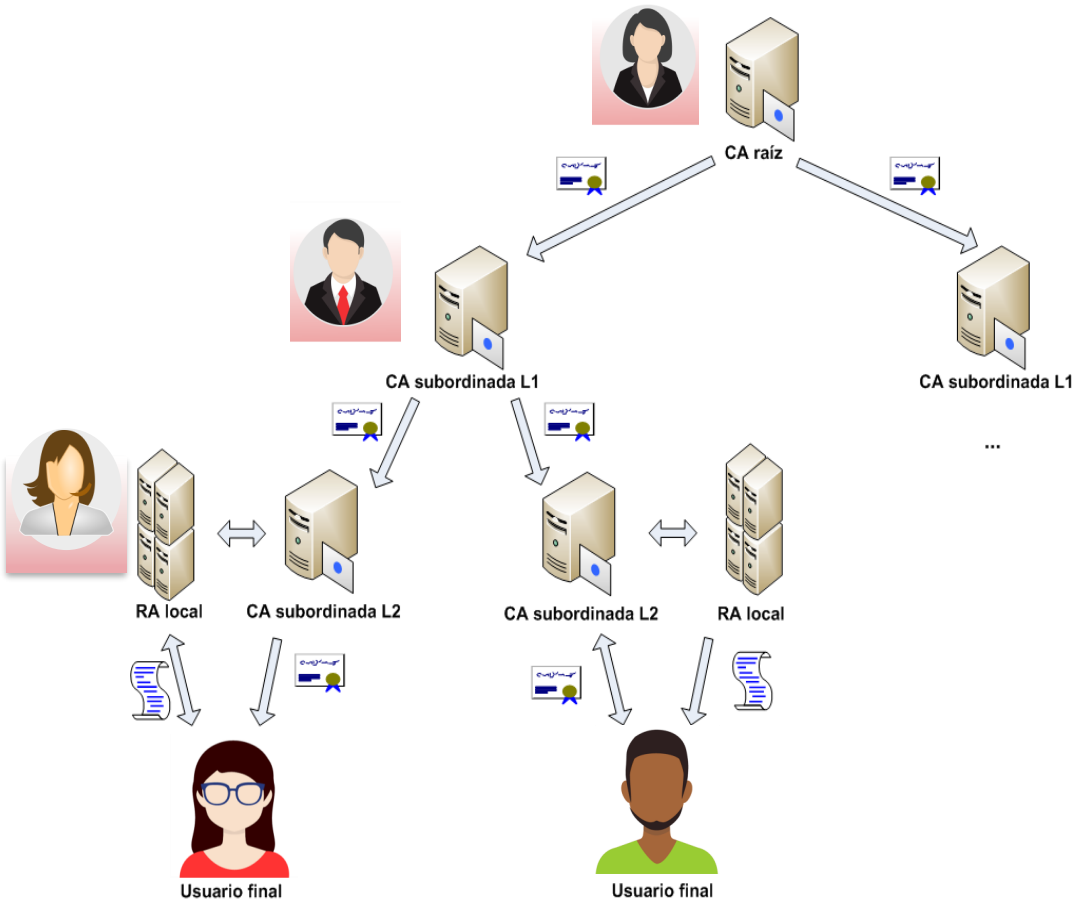
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Infraestructura de Clave Pública (PKI)



Infraestructura de Clave Pública (PKI)

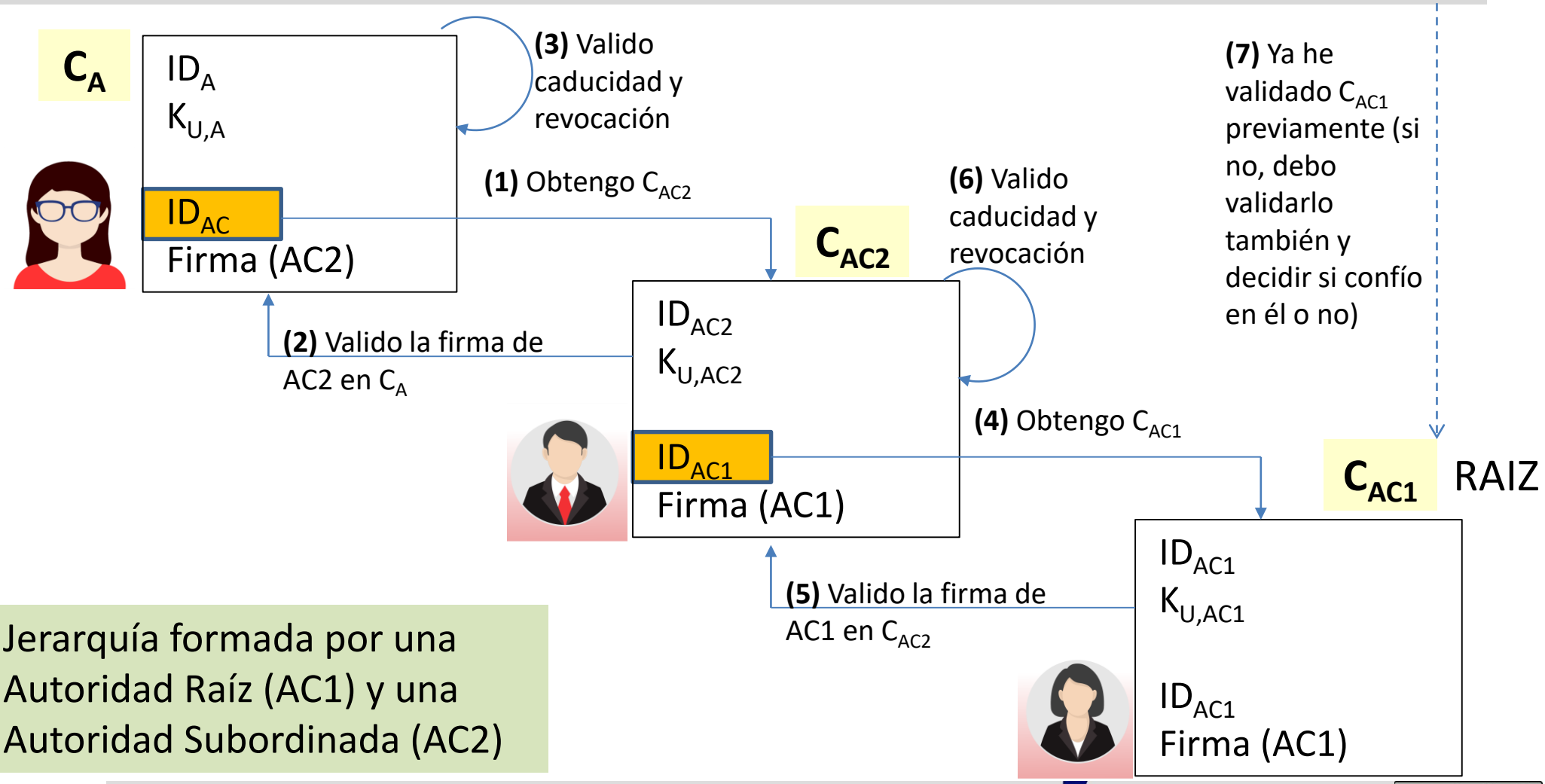
- CA raíz emite el certificado a sí misma y a sus autoridades subordinadas de primer nivel
  - CA subordinadas L1
- CA subordinadas L1 emiten el certificados a sus autoridades subordinadas de segundo nivel
  - CA subordinadas L2
- En este escenario, CA subordinadas L2 emiten certificados a usuarios finales, ayudadas por autoridades de registro



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Infraestructura de Clave Pública (PKI). Cadena de certificación

*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*



Jerarquía formada por una Autoridad Raíz (AC1) y una Autoridad Subordinada (AC2)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Infraestructura de clave pública (PKI). Cadena de certificación

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

B, además de verificar la firma de A sobre M (utilizando la clave pública $K_{U,A}$ contenida en C_A), debe validar el certificado C_A **y toda su cadena de certificación** para "creer" que $K_{U,A}$ es realmente de A

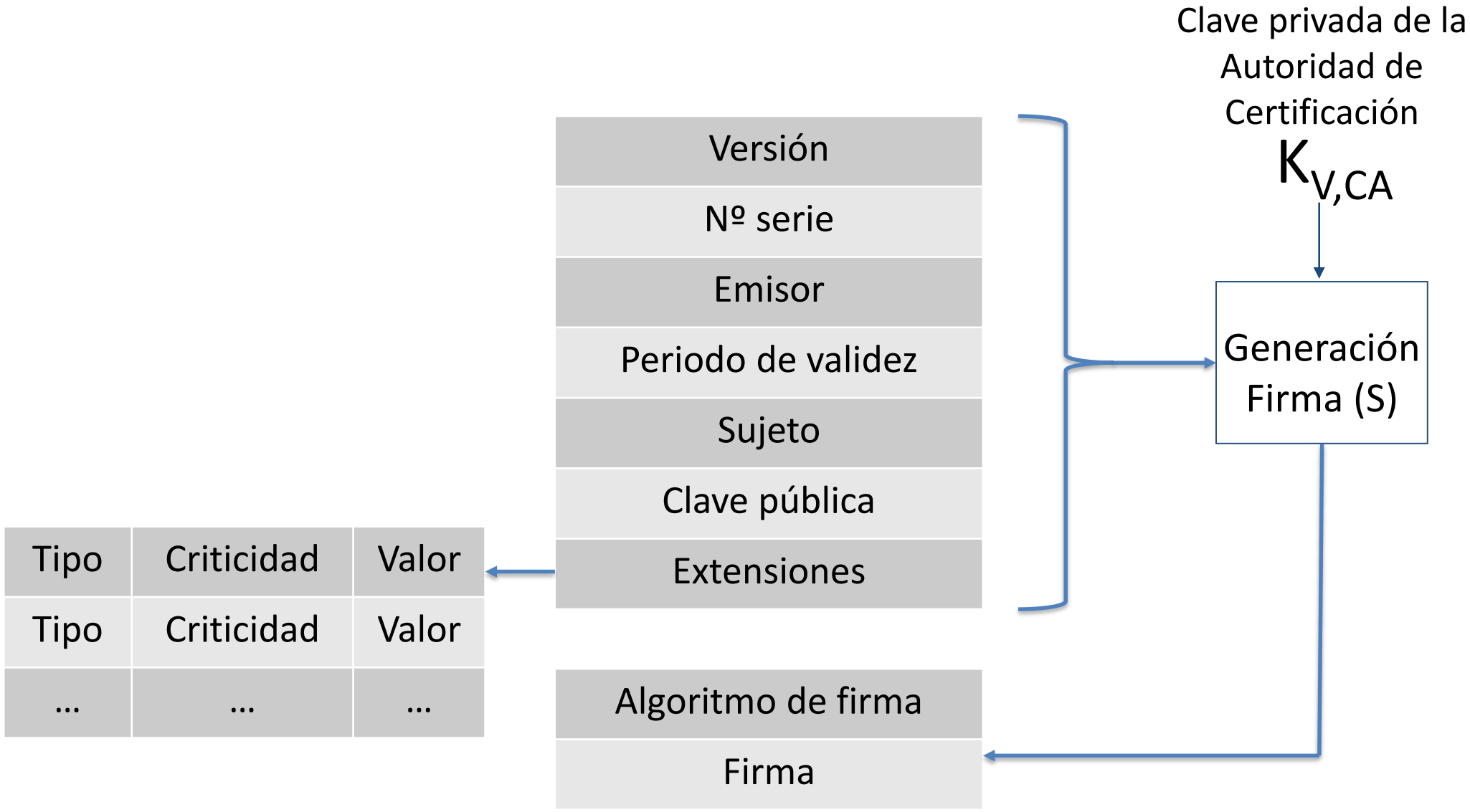
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 12. Infraestructuras de clave pública
  - Origen
  - Certificado de clave pública
  - Infraestructura de clave pública (PKI)
  - **Certificado X.509**
  - Validación de estado de un certificado
  - Otros aspectos
  - Modelo descentralizado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Certificado X.509



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Certificado X.509

- Versión actual: 3
- Nº 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

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

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 ad-hoc 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.

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Certificado X.509

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

ÍNDICE

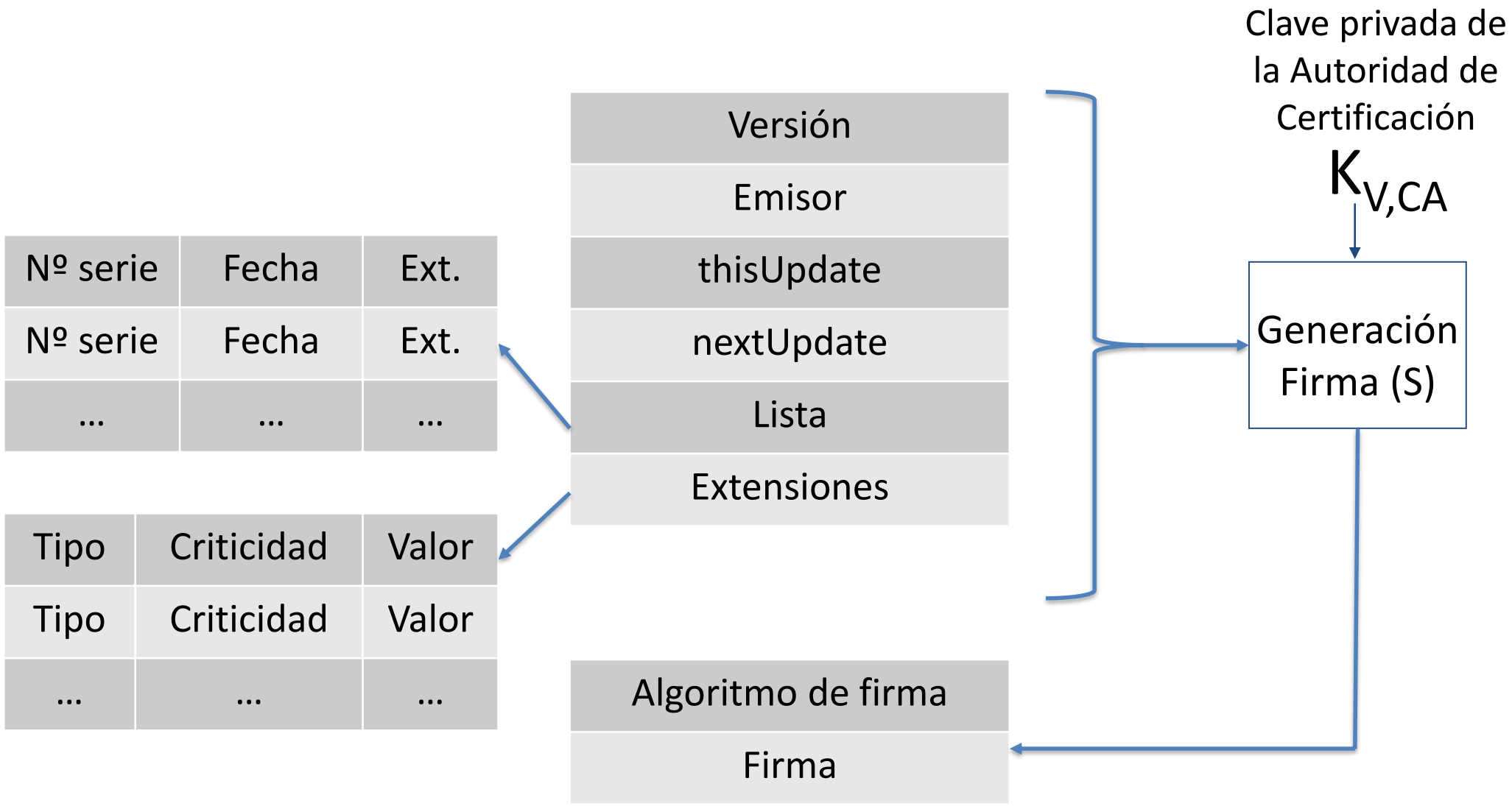
- 12. Infraestructuras de clave pública
  - Origen
  - Certificado de clave pública
  - Infraestructura de clave pública (PKI)
  - Certificado X.509
  - **Validación de estado de un certificado**
  - Otros aspectos
  - Modelo descentralizado

Validación del estado de un certificado

- El estado de revocación de los certificados debe ser accesible
- Métodos de publicación y consulta basados en Listas de Certificados Revocados (*Certificate Revocation List* – 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

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Validación del estado de un certificado. Lista de Certificados Revocados (CRL)



Validación del estado de un certificado. Lista de Certificados Revocados (CRL)

- Publicada por la AC u otra entidad delegada
- Los certificados expirados no se incluyen en la CRL
- *thisUpdate* indica la fecha de emisión de la CRL
- *nextUpdate* indica la fecha límite en la cual el emisor publicará la siguiente CRL actualizada
  - Existe un periodo de tiempo desde que el sujeto solicita la revocación del certificado hasta que dicha revocación se hace efectiva
- Lista de certificados revocados
  - Nº de serie
  - Fecha (de procesamiento de la solicitud de revocación)
  - Extensiones
    - Permite, entre otros, incluir el motivo de la revocación y la fecha de solicitud

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 12. Infraestructuras de clave pública
  - Origen
  - Certificado de clave pública
  - Infraestructura de clave pública (PKI)
  - Certificado X.509
  - Validación de estado de un certificado
  - **Otros aspectos**
  - Modelo descentralizado

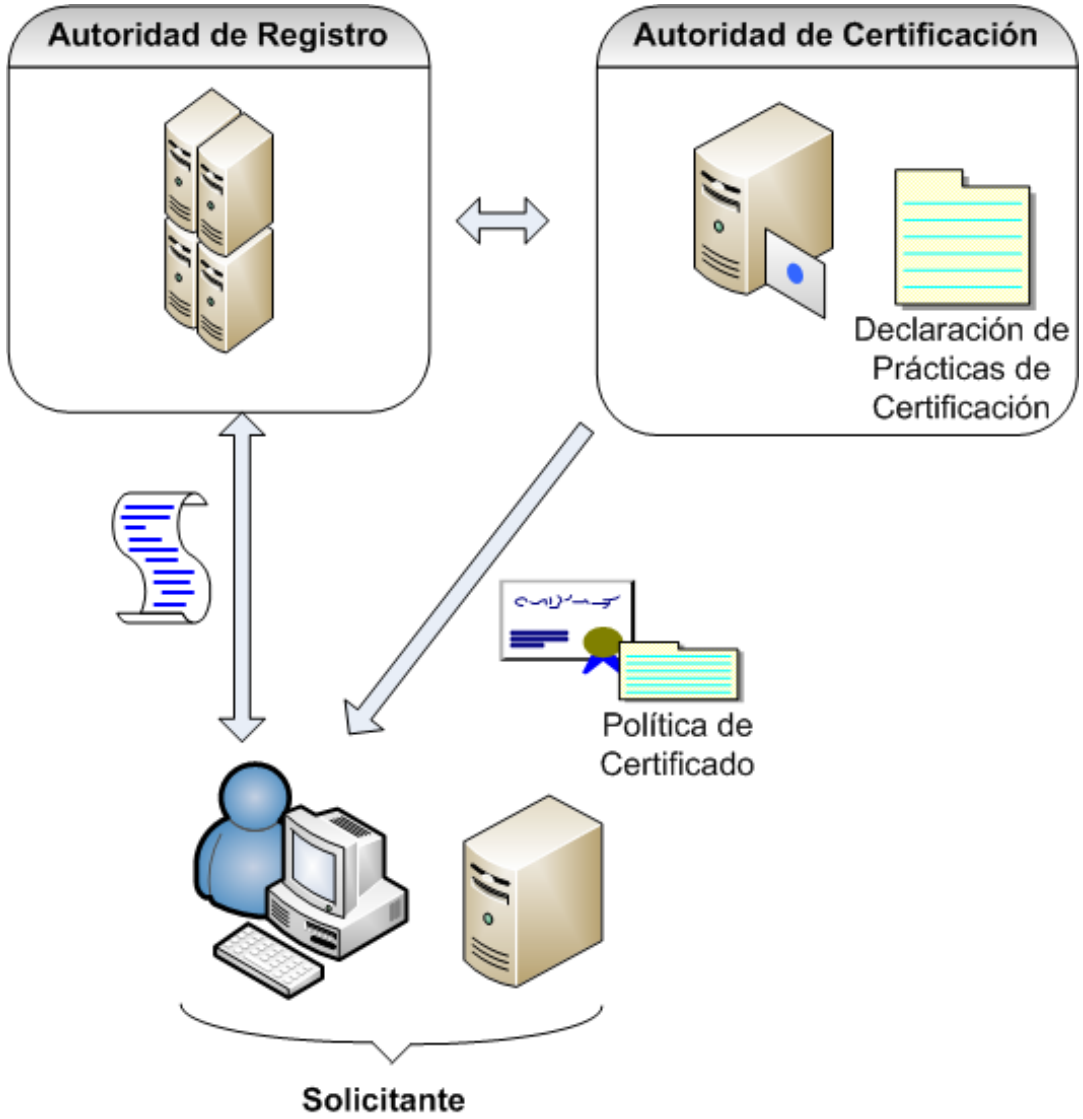
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

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

Generación y almacenamiento de claves

- Generación en el usuario final
  - Librerías, accedidas a través de navegador web o directamente
  - Si es necesario acreditar la identidad física, existirá una Autoridad de Registro
- Generación en una entidad de gestión de claves, que además de generarla, custodia una copia



Generación y almacenamiento de claves

- Almacenamiento de claves privadas
  - Software
    - Repositorio de claves del Navegador Web
    - Fichero específico protegido (PKCS#12, PFX)
  - Hardware
    - Tarjeta Inteligente
    - Token USB
    - Chip TPM
    - HSM

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

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 12. Infraestructuras de clave pública
  - Origen
  - Certificado de clave pública
  - Infraestructura de clave pública (PKI)
  - Certificado X.509
  - Validación de estado de un certificado
  - Otros aspectos
  - **Modelo descentralizado**

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

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)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

COSEC

uc3m | Universidad Carlos III de Madrid