Module 11

# Digital signatures

CRYPTOGRAPHY AND COMPUTER SECURITY COURSE

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
Sergio Pastrana Portillo

uc3m | Universidad Carlos III de Madrid

COSEC

# OUTLINE

- 11. Public Key Infrastructures
  - Introduction
  - Public Key Certificate
  - Public Key Infrastructure (PKI)
  - X.509 Public Key Certificates
  - Public Key Certificate State Validation
  - Other aspects
  - Decentralized model





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

# OUTLINE

- 11. Public Key Infrastructures
  - **Introduction**
  - Public Key Certificate
  - Public Key Infrastructure (PKI)
  - X.509 Public Key Certificates
  - Public Key Certificate State Validation
  - Other aspects
  - Decentralized model





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

# Introduction

- In public key cryptography, public keys are not linked to a certain identity by default
  - We do not know who is the owner of a public key

- At first, models based on Public Key Directories or Public Key Authorities (already seen in previous modules)
  - Need of online access
  - Not scalable





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

# Origen

- L. Kohnfelder. ***Toward a Practical Public-Key Cryptosystem***. Bachelor Thesis, Department of Electrical Engineering, 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."





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

# Introduction

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

  → Proposed the concept of digital certificate and certificate revocation list

  - Binds an identity to a public key
  - Issued by a trusted "Public File"
  - To provide trust on the binding (public key – ID), both data are digitally signed
    - Only the Public File can modify the binding
    - Everybody can verify the binding (everybody knowing the Public File's public key)
  - This model presents several disadvantages: certificate management problems (life cycle), establishing specific key usages, scalability (having several Public Files) vs mutual recognition (certificates issued by different Public Files)





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

# OUTLINE

- 11. Public Key Infrastructures
  - Introduction
  - **Public Key Certificate**
  - Public Key Infrastructure (PKI)
  - X.509 Public Key Certificates
  - Public Key Certificate State Validation
  - Other aspects
  - Decentralized model





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

# Public key certificate. Basic idea

- Subject A's identity ($ID_A$)
- A's public key ($K_{U,A}$)
- Issuer AC's identity ($ID_{AC}$)
- Validity period ($T_1$ , $T_2$)
- Serial number

- Digital signature on the previous fields issued by AC using digital signature algorithm S and AC's private key $K_{V,AC}$

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

Signing algorithm

Private key used to sign

Data to be signed



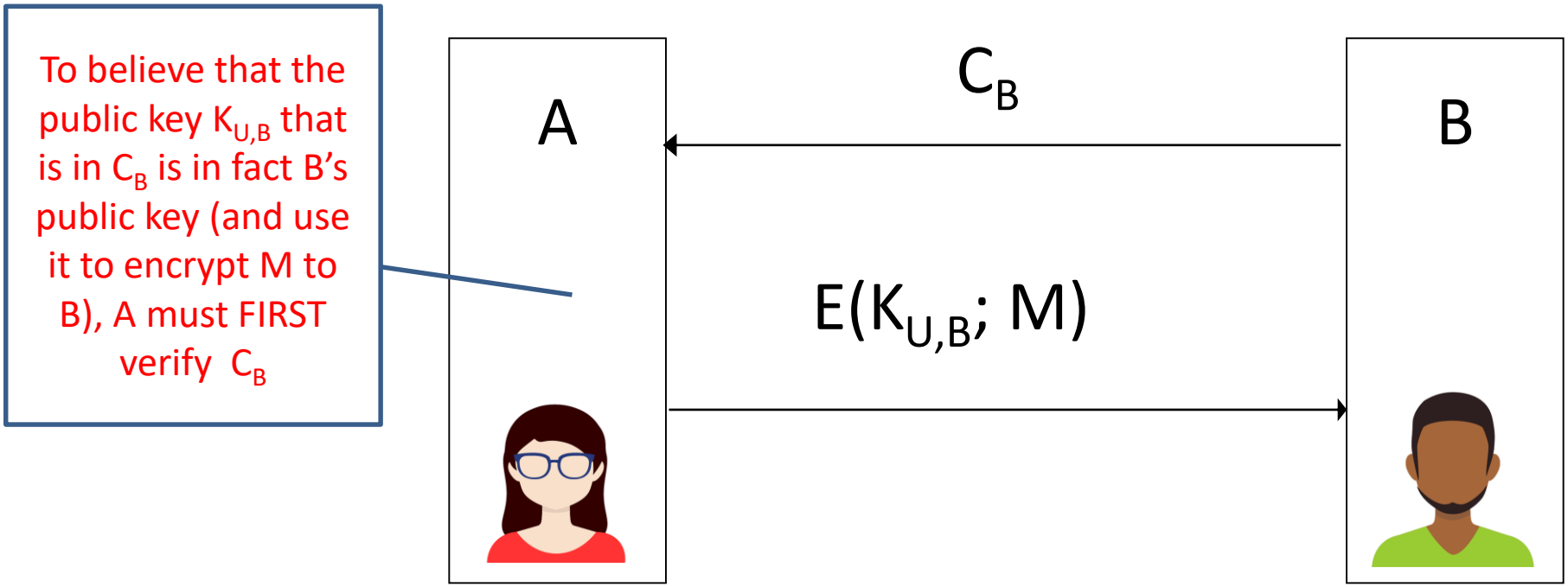




Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

# Public key certificate. Basic idea

- How it is "used": If A wants to encrypt a message to B, first B sends her his public key certificate $C_B$ so A can get to know in a trusted way or verify B's public key





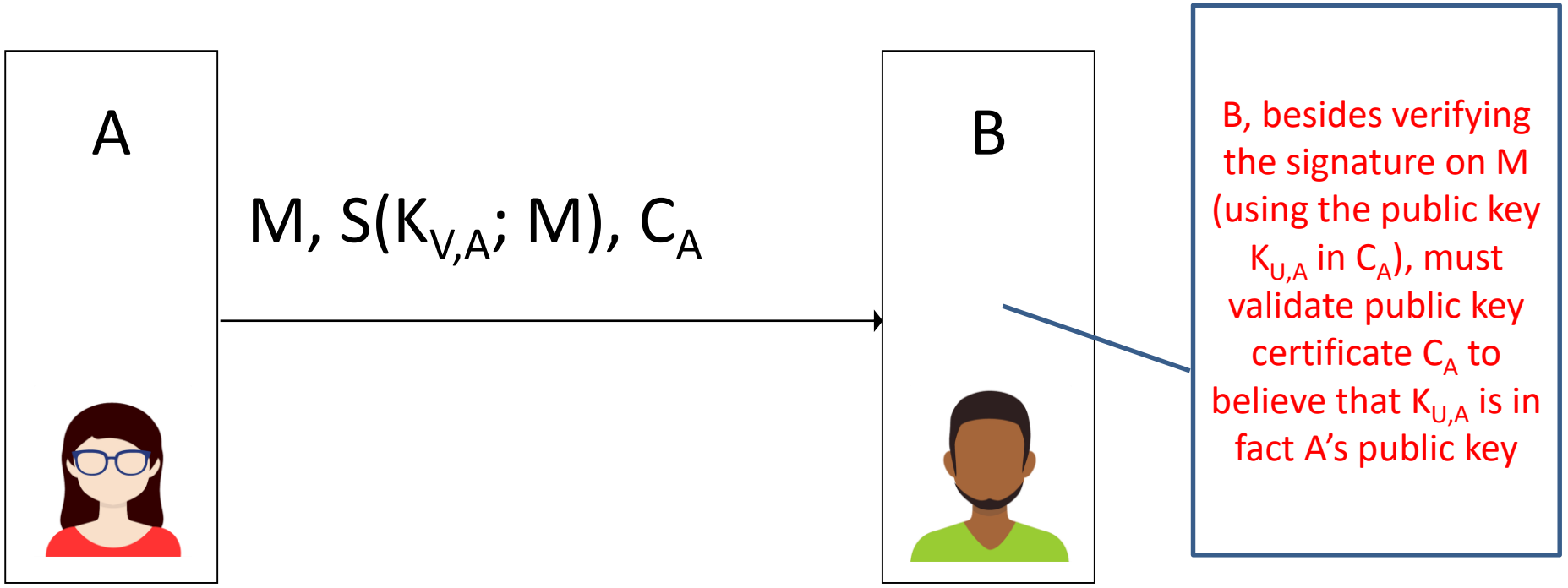





Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

# Public key certificate. Basic idea

- How it is "used": If A wants to sign a message, she concatenates her public key certificate $C_A$ to her signed messages; therefore, everybody can verify who signed the messages, that is, who is the public key legitimate owner







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

# Public key certificate. Validity period, state and usages

- Validity period
  - Bounded (preventive measure)
  - Depends on the length of the keys and their usage
- State
  - Valid
  - Suspended
  - Revoked
  - …
- Allowed usages





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

# Public key certificate. Verification

- First, a trusted copy of $K_{U,AC}$ , AC's public key, is obtained, e.g., by obtaining AC's public key certificate $C_{AC}$
- Is this certificate trusted? How can we check this?
  - It is certified by the AC (it is self-signed)
  - Do we trust the AC? (we must make a decision on this)
  - Have we obtained the certificate trough a secure channel?
- Verification - Checking the following aspects:
  - Verifying the signature in the certificate, generated by AC, using the trusted copy of AC's public key $K_{U,AC}$
  - Verifying that time is within certificate's validity period
  - Verifying that the certificate state is valid (i.e., it has not been revoked)
  - Verifying one of the key usages is issuing certificates





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

# OUTLINE

- 11. Public Key Infrastructures
  - Introduction
  - Public Key Certificate
  - **Public Key Infrastructure (PKI)**
  - X.509 Public Key Certificates
  - Public Key Certificate State Validation
  - Other aspects
  - Decentralized model







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

# Public Key Infrastructure (PKI)

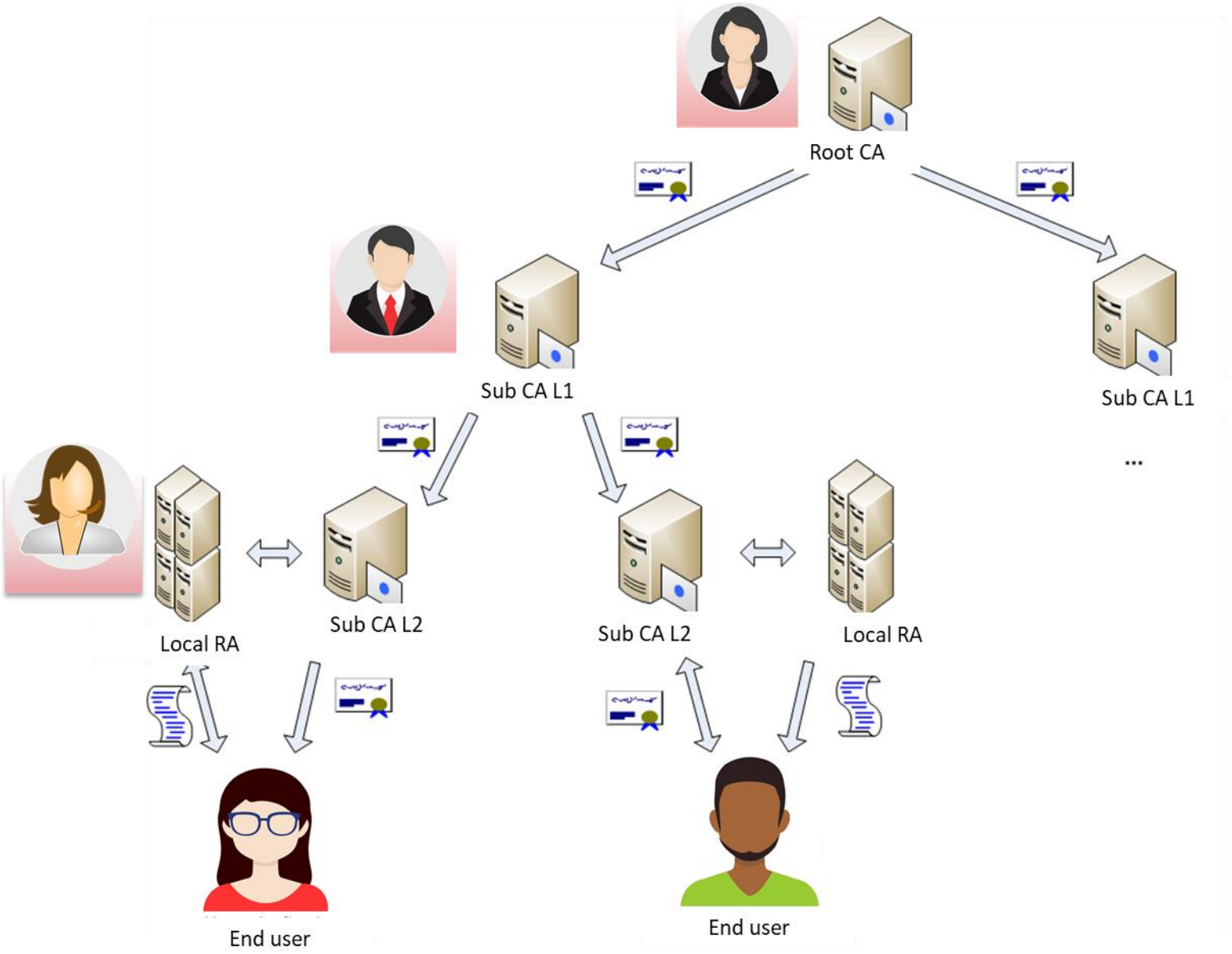
- Set of international standards (ITU-T, IETF)
- Defines the structure of X.509 public key certificates and certificate revocation lists (CRL) [RFC 5280]
- Defines a **hierarchical model** of Certification Authorities [RFC 5280] and related authorities
  - E.g., Registration Authority
- Defines a set of operational and management protocols [RFC 4210 CMP, RFC 4211 CRMF, RFC 3647 CP/CPS…]





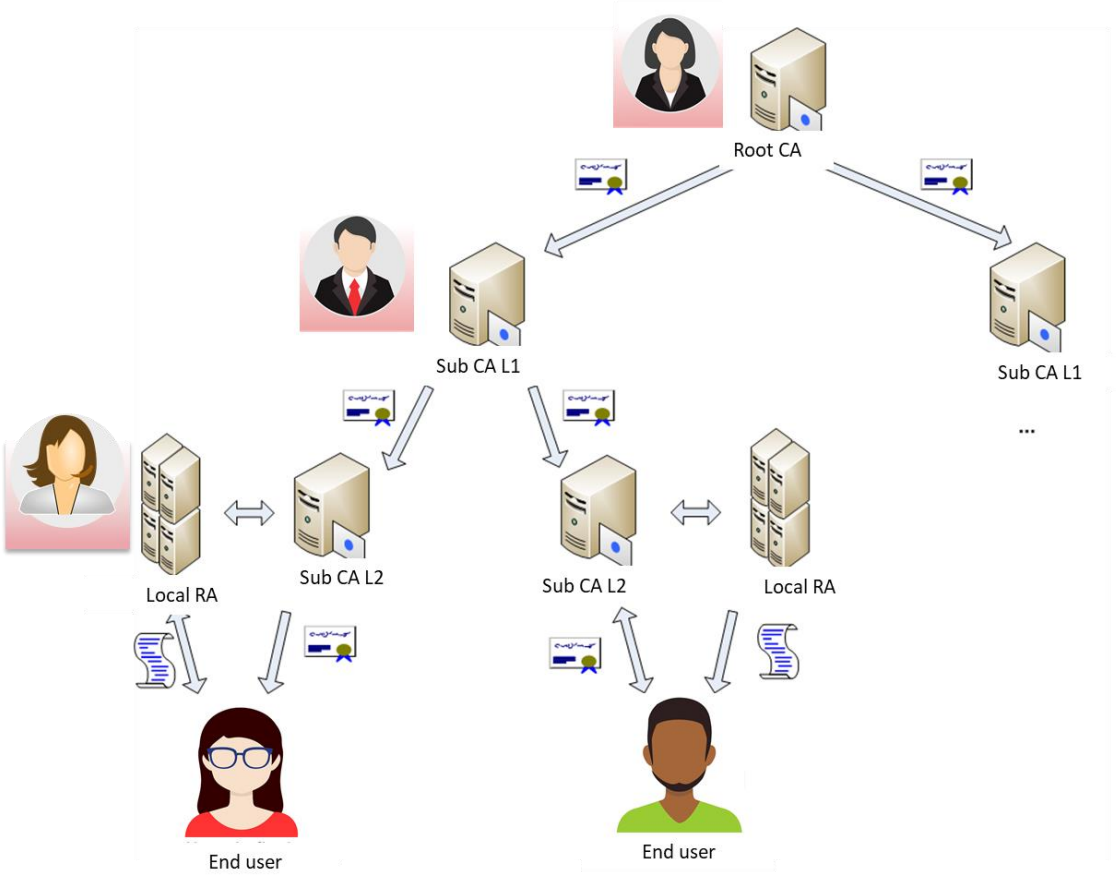
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

# Public Key Infrastructure (PKI)



# Public Key Infrastructure (PKI)

- Root CA issues its own certificate and those of its subordinate CAs (level 1)
  - Subordinate CA L1
- Subordinates CAs Level-1 issue the certificates of their subordinate CAs (level 2)
  - Subordinate CA L2
- In this setting, CAs Level-2 issue the certificates of the end users, with the support of the Registration Authorities





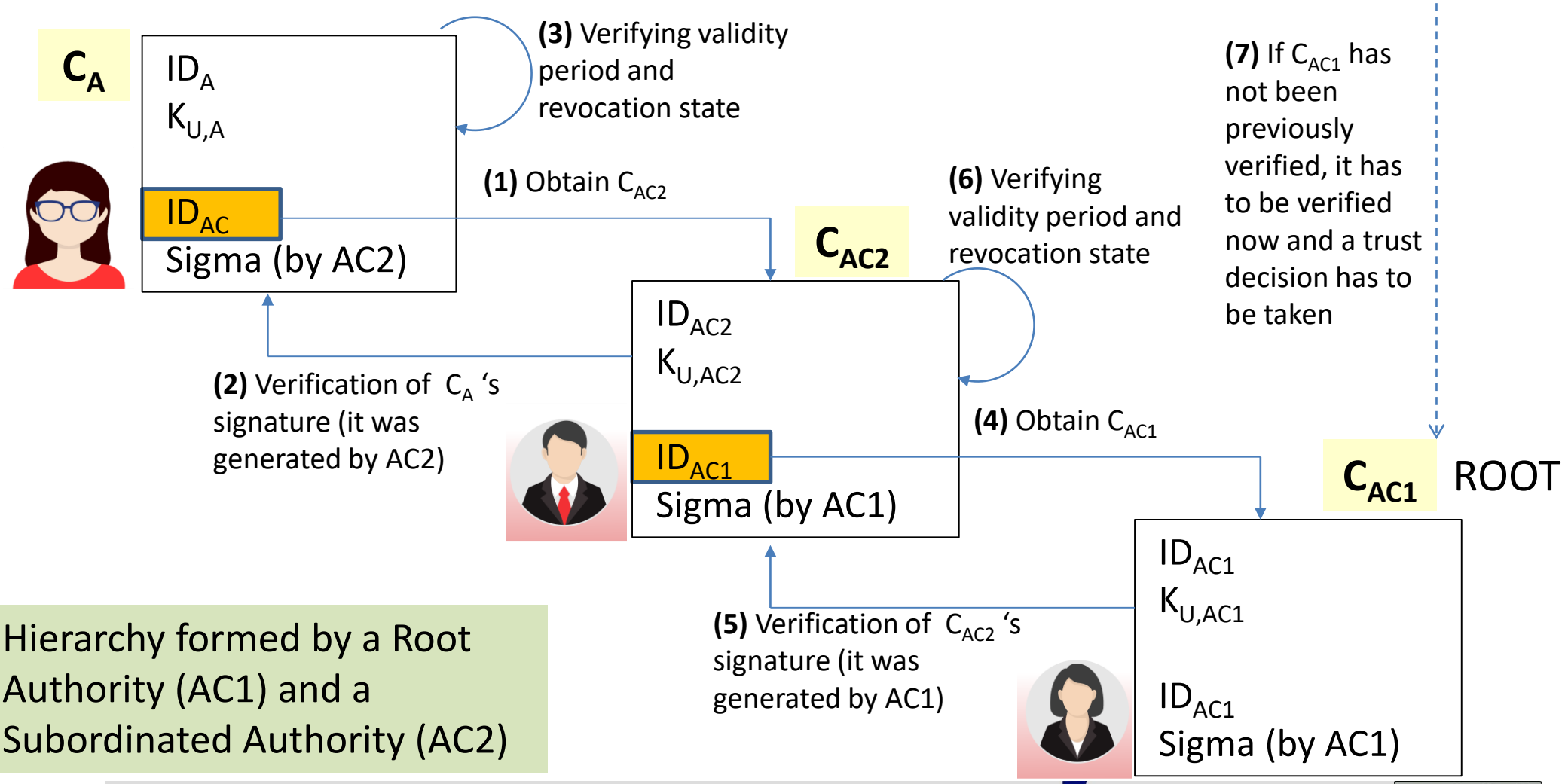





Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

# Public Key Infrastructure (PKI). Certificate chain

*To verify a certificate it is necessary to verify THE WHOLE CERTIFICATE CHAIN until a trusted root (self-signed) certificate is reached*




Hierarchy formed by a Root Authority (AC1) and a Subordinated Authority (AC2)



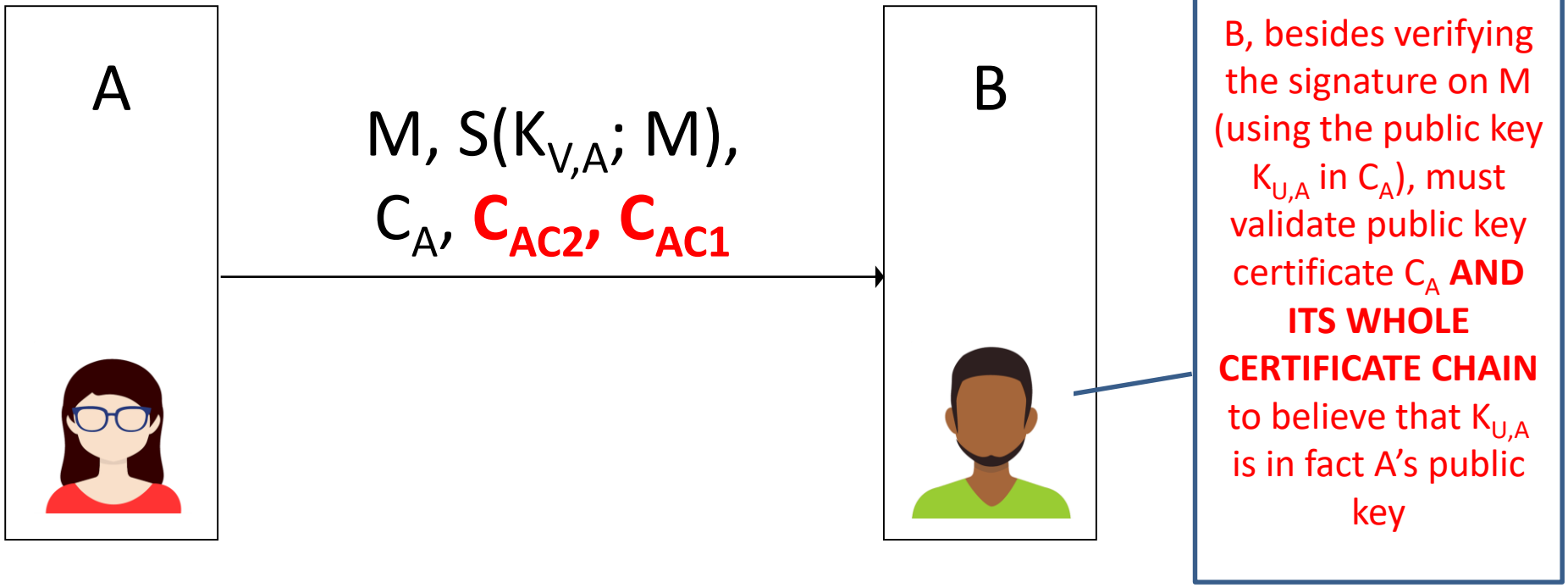




Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

# Public Key Infrastructure (PKI). Certificate chain

- If A wants to sign a message, she must concatenate to the message her public key certificate AND the **whole certificate chain** (…)










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

# OUTLINE

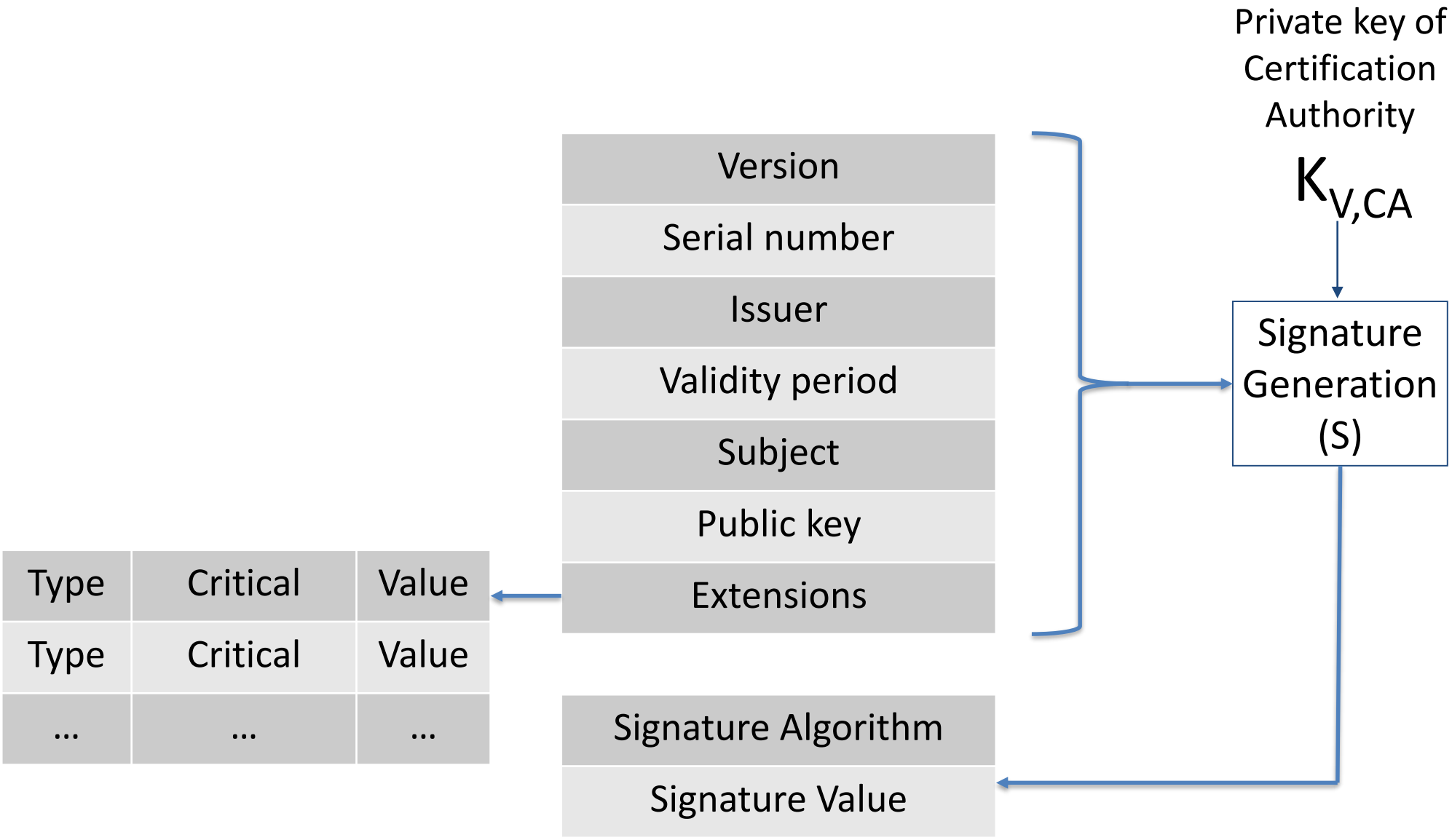
- 11. Public Key Infrastructures
  - Introduction
  - Public Key Certificate
  - Public Key Infrastructure (PKI)
  - **X.509 Public Key Certificates**
  - Public Key Certificate State Validation
  - Other aspects
  - Decentralized model





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

# X.509 certificate



# X.509 certificate

- Current version: 3
- Serial number
  - Uniquely identifies the certificate within the realm of the issuing AC
- Issuer
  - Distinguished name (DN) of the issuing AC (using X.501 standard)
    - Eg: CN = AC DNIE 001, OU = DNIE, O = DIRECCION GENERAL DE LA POLICIA, C = ES
- Validity period: [Not before, Not after]
- Subject
  - Distinguished name (DN) of the subject owner of the certificate
    - 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, Sergio Pastrana Portillo

# X.509 certificate

- Public key
  - Information about the public key in the certificate and the public key algorithm
    - Eg: RSA modulo and public key exponent
  - Extensions
    - They allow the inclusion of additional information
    - Ad-hoc or predefined in the standard
    - Eg: *keyUsage* extension allows to specify the private key intended key usages:
      - Digital signature
      - Non repudiation
      - Key exchange
      - Encryption
      - Etc.





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

# X.509 certificate

- Types of certificates
  - Natural person
  - Legal person
  - SW component  (eg. TLS certificates)
  - Code signing
  - …





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

# OUTLINE

- 11. Public Key Infrastructures
  - Introduction
  - Public Key Certificate
  - Public Key Infrastructure (PKI)
  - X.509 Public Key Certificates
  - **Public Key Certificate State Validation**
  - Other aspects
  - Decentralized model

# Certificate state validation

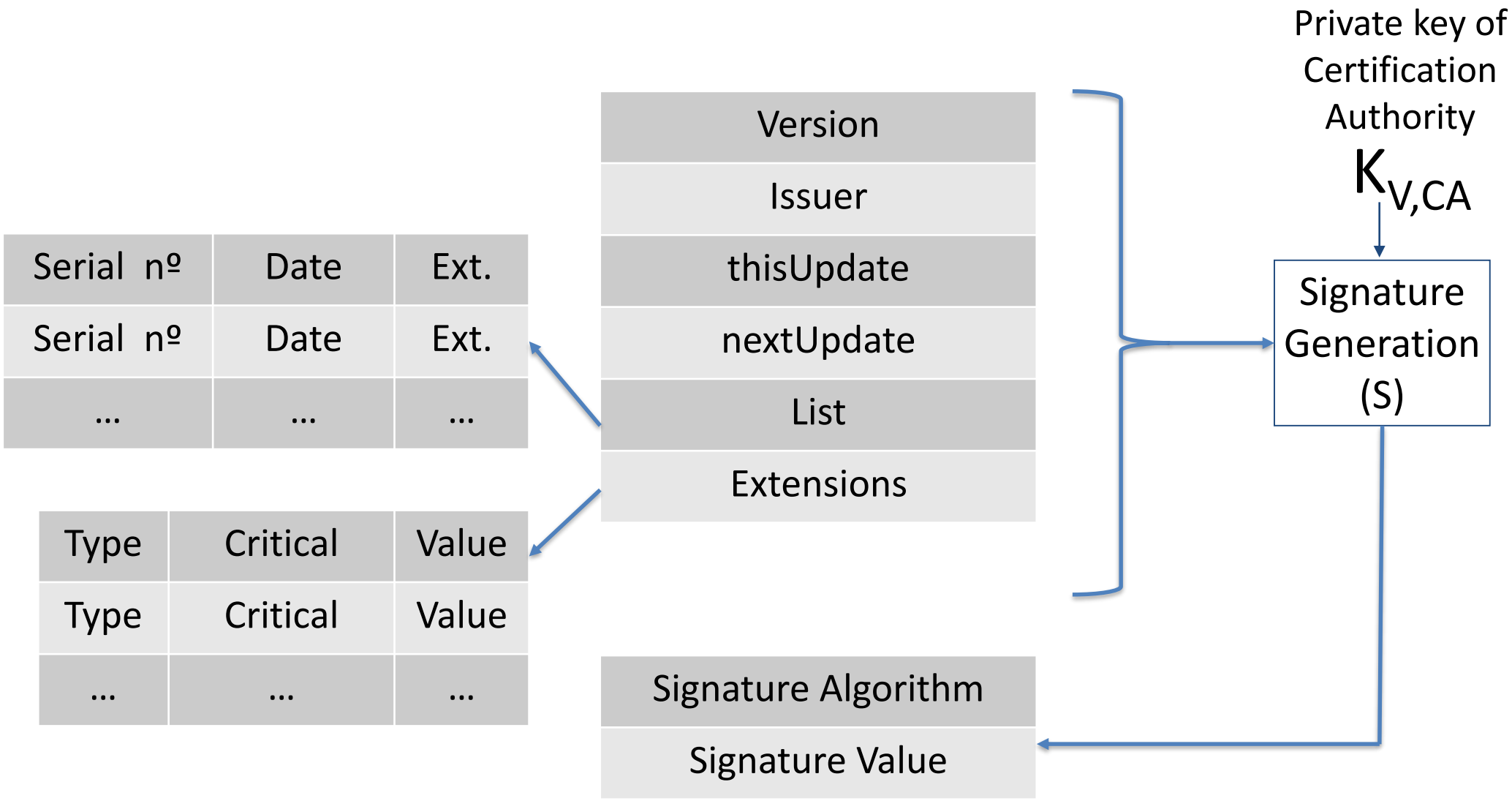
- Certificate revocation state must be accessible
- Certificate state is published using Certificate Revocation Lists (CRL)
  - Periodic update
  - There is an uncertainty period until *nextUpdate* (solution: cautionary period)
  - They have a bandwidth problem (solutions: *over-issued* CRLs, Delta CRLs, segmented CRLs, indirect CRLs…)
- Online Certificate Status Protocol (OCSP)
  - Simple protocol to make queries about the state of a certificate [RFC 2560]
  - They provide the certificate's current state





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

# Certificate state validation. Certificate Revocation List (CRL)










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

# Certificate state validation. Certificate Revocation List (CRL)

- Published by the AC or a delegated entity
- Expired certificates are NOT included in the CRL
- *thisUpdate* refers to the CRL's issuing date
- *nextUpdate* refers to the deadline by which the issuer will publish the next CRL
  - There is a period between the time where the subject requests revocation and the time when the revocation is effective
- Certificate revocation list
  - Serial number
  - Date (when revocation request was processed)
  - Extensions
    - Allows to include revocation reasons and the revocation request date





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

# OUTLINE

- 11. Public Key Infrastructures
  - Introduction
  - Public Key Certificate
  - Public Key Infrastructure (PKI)
  - X.509 Public Key Certificates
  - Public Key Certificate State Validation
  - **Other aspects**
  - Decentralized model





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

# Operational services

- Certificate request
- Registration
- Certificate renewal
- Certificate revocation
- Check the status of a certificate (CRL, OCSP)
- Certificate revocation state publication

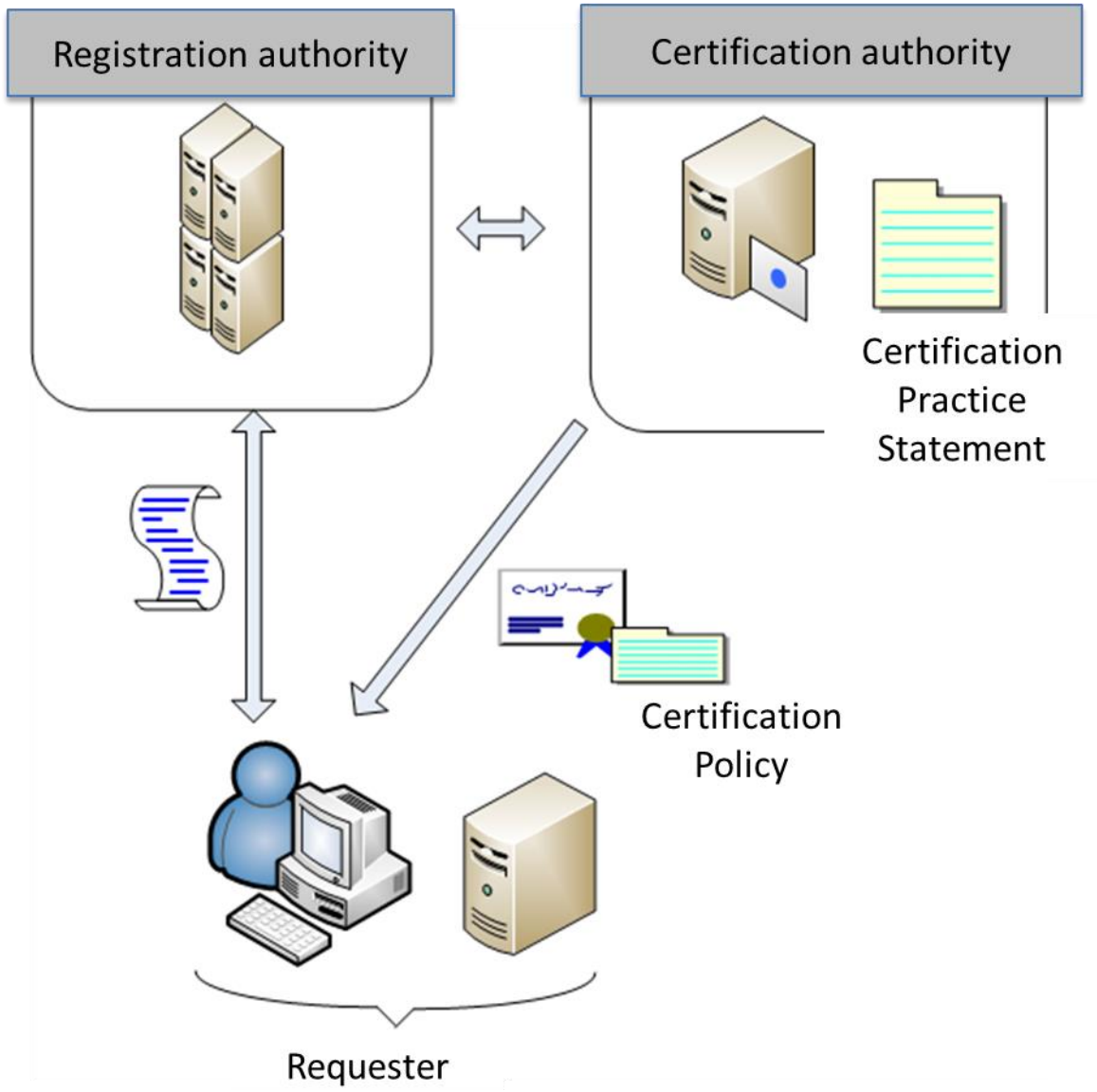




Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

# Key generation and storage

- In the user's system
  - Libraries, called by the browser or directly
  - If it is required to check a person's identity, a Registration Authority will be needed
- A Key Authority may generate them, and keep a copy of the key pair










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

# Key generation and storage

- Private key storage
  - Software
    - Web browser data base
    - Protected key file (PKCS#12, PFX)
  - Hardware
    - Smart Card
    - USB  Token
    - Trusted Platform Module (TPM) Chip
    - Hardware Security Module (HSM)





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

# Certification Practice Statement

- A Certification Practice Statement (CPS) is a document from a certificate authority which describes their practice for issuing and managing public key certificates
- It includes the obligations acquired with the holders of its certificates, and of these with the former, and the margins of responsibility that it assumes in relation to the entities that accept said certificates

# OUTLINE

- 11. Public Key Infrastructures
  - Introduction
  - Public Key Certificate
  - Public Key Infrastructure (PKI)
  - X.509 Public Key Certificates
  - Public Key Certificate State Validation
  - Other aspects
  - **Decentralized model**







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

# Modelo descentralizado

- Decentralized trust model
  - There is no certification authority
  - Each user certifies the keys of the users he/she trusts
  - Trust chains of n-nodes (jumps) can be established
- Advantages
  - Quick and easy deployment, cheaper
- Disadvantages
  - Not scalable
  - Needs to transmit a public key through a secure channel before certifying it
- Example: PGP (Pretty Good Privacy)





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

# CRYPTOGRAPHY AND COMPUTER SECURITY COURSE

COSEC

uc3m | Universidad Carlos III de Madrid