Digital Certificates. PKI and other TTPs.

3.1

Universidad
Carlos III de Madrid
Grupo SeTI · Dpto. Informática

Digital Certificate

Def. Webster's dictionary:

"A document containing a certified statement, especially as to the truth of something".

In the electronic world:

- Collection of information to which a digital signature has been affixed by an authority that is recognized and trusted by some community of certificate users.

Especially in e-commerce:

- Public-key certificate

Concept of electronic certificate

Law 59/03 Art. 6.1. or

Directive 1999/93/EC Art. 2.9.:

"Certificate"

means an electronic attestation which links signature verification data to a person and confirms the identity of that person.

Public Key Certificate

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

Public Key Certificate

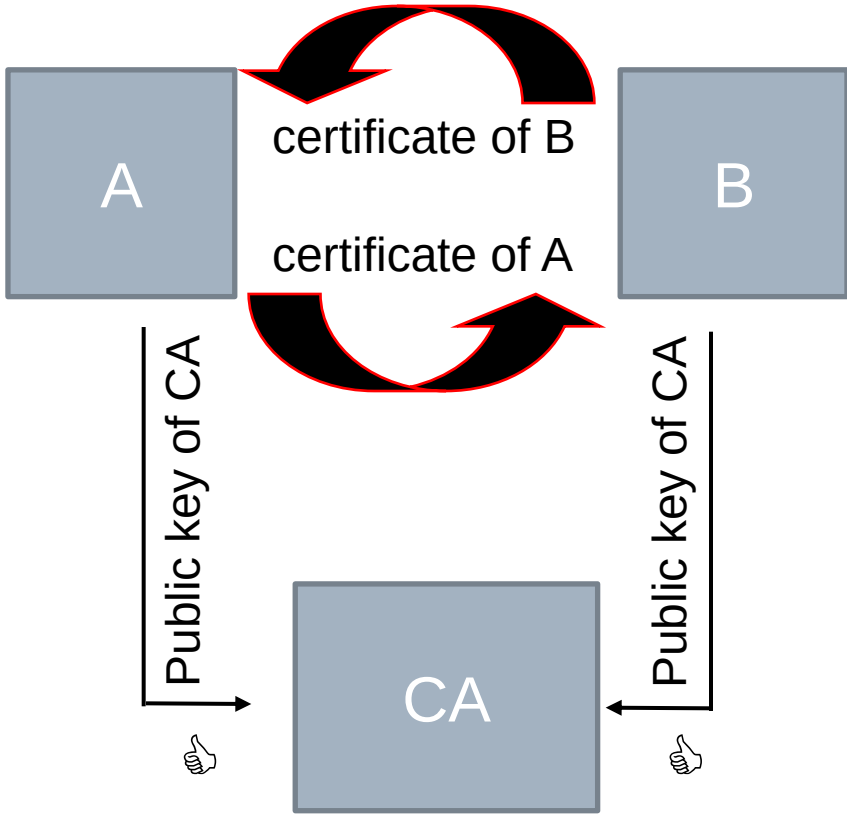
- A data structure consisting of a data part and a signature part:
  - **Data part**: contains cleartext data including, as a minimum, a public key and a string identifying the party (subject entity) to be associated therewith
  - **Signature part**: consists of the digital signature of a certification authority (CA) over the data part, therefore binding the subject entity's identity to the specified public key

Handbook Applied Crypt.

Certification Authority (CA)

- A **Certification Authority** is an entity or organism (TTP) which, according to certain policies and algorithms, certificates - for example - public keys of users or servers

- User **A** sends his certificate to user **B** (public key signed by CA) which checks with this authority its authenticity and validity. The same happens in opposite sense.



Certification Authority CA

Public key certificate types

- There are four kinds of digital certificates used on the Internet:
  - Personal Certificate
  - Server Certificate
  - Software Publisher Certificate
  - Certificate of Certification Authority (CA)

- Description:

http://support.microsoft.com/default.aspx?scid=kb;en-us;195724#XSLTH3180121122120121120120

Uses of public key certificates

- Authentication (entity authentication)
- Data encryption (confidentiality)
- Electronic signature (integrity, data origin authentication, non repudiation)
- Secure e-mail

Public key certificates: Other contents

- a **validity period** of the public key;
- a **serial number** or key identifier identifying the certificate or key;
- **information facilitating verification of the signature** (e.g., a signature algorithm identifier, and issuing CA's name);
- additional information about the subject entity (e.g., street or network address);
- additional information about the key (e.g., algorithm and intended use);
- quality measures related to the identification of the subject entity, the generation of the key pair, or other policy issues (e.g., uses and responsibilities);
- the **status** of the public key.

X.509 Public Key Certificates

- **ITU-T Recommendation X.509** / ISO/IEC 9594-8: Information Technology – Open Systems Interconnection – **The Directory: Public-Key and Attribute Certificate Frameworks (2005)**

X.509 Certificate Format

- issued by a Certification Authority (CA), containing:
  - version (1, 2, or 3)
  - serial number (unique within CA) identifying certificate
  - signature algorithm identifier
  - issuer X.500 name (CA)
  - period of validity (from - to dates)
  - subject X.500 name (name of owner)
  - subject public-key info (algorithm, parameters, key)
  - issuer unique identifier (v2+) , in case of name reuse
  - subject unique identifier (v2+) , in case of name reuse
  - extension fields (v3)
  - signature (of hash of all fields in certificate, encrypted by the private key of the CA)

X.500 Distinguished Names

- X.500 directory distinguished names
- Levels of directory information tree (DIT)
  - Root
  - Country / int. org.
  - Organisation (company or gov. inst.)
  - organisational unit and person

X.500 Distinguished Names

- **X.500 directory names**

  Abbreviations:

  CN = Common Name

  OU = Organization Unit

  O = Organization Name

  L = Locality name

  S = State name

  C = Country

- **Example: O = cities, S = Redmond, C = US**

X.500 Distinguished Names

Other possible naming and addressing formats:

- DNS domain name **`.example.uc3m.es.`**
- E-mail name **`@example.uc3m.es`**
- Universal Resource Identifier (URI) as URL, FTP, HTTP, telnet, mailto, news, and gopher: e.g.:
  `URL=http://.example.uc3m.es`
- Internet Protocol address

X.509 Version 3

- has been recognised that additional information is needed in a certificate
  - email/URL, policy details, usage constraints
- rather than explicitly naming new fields defined a general extension method
- extensions consist of:
  - extension identifier
  - criticality indicator
  - extension value

X.509 Version 3 Certificate Extensions

- key and policy information
  - convey info about subject & issuer keys, plus indicators of certificate policy
- certificate subject and issuer attributes
  - support alternative names, in alternative formats for certificate subject and/or issuer
- certificate path constraints
  - allow constraints on use of certificates by other CA's

Storage of the Private Key and the Public key certificate

- In a file
  - On hard disk
  - On floppy, CD or other removable device
- In a smart card or other smart device

Key and certificate life cycle management

- Certificate generation
  - Trust initialization
  - Generation of user's public/private key
  - Certificate request
  - User enrollment and authentication
  - Certificate issuance
  - Certificate retrieval

Certificate Generation

1st step: trust in CA

A: User, applicant, subscriber

C_{CA}: Certificate for public key of CA

D = Digital fingerprint of C_{CA}

1. A connects to the web of CA
2. CA $\rightarrow$ A (C_{CA})
3. (optional) A verifies D

Certificate Generation

2nd step: certificate request

I_A: Identification of A

RC: Request code

C_A: Certificate for public key of A

k_u, k_v: keys from A

1. A generates k_u and k_v
2. A $\rightarrow$ CA (k_u)
3. CA $\rightarrow$ A (RC)

Certificate Generation

3rd step: enrollment and authentication of A

RA: Registration Authority

CR: Certificate request

1. A presents itself personally in RA with I_A and the RC
2. A signs the CR
3. RA $\rightarrow$ CA (CR)

Certificate Generation

4th step: Obtaining

1. A connects to the web of CA
2. CA $\rightarrow$ A (C_A)

Key and certificate life cycle management

- Certificate renewal
- Certificate update
- Certificate revocation
- Certificate suspension
- Certificate expiration
- Key archival
- Key recovery

Certificate Revocation

- certificates have a period of validity
- may need to be revoked before expiry, eg:
  1. user's private key is compromised
  2. user is no longer certified by this CA
  3. CA's certificate is compromised
- CA's maintain list of revoked certificates
  - the Certificate Revocation List (CRL)

Certificate Revocation List (CRL)

- Issuer name
- Signature algorithm of the CA
- Update Time/Date
- Next update Time/date
- List of:
  - Revoked certificates (serial number)
  - Revocation Time/Date
- Extensions

Certificate Revocation

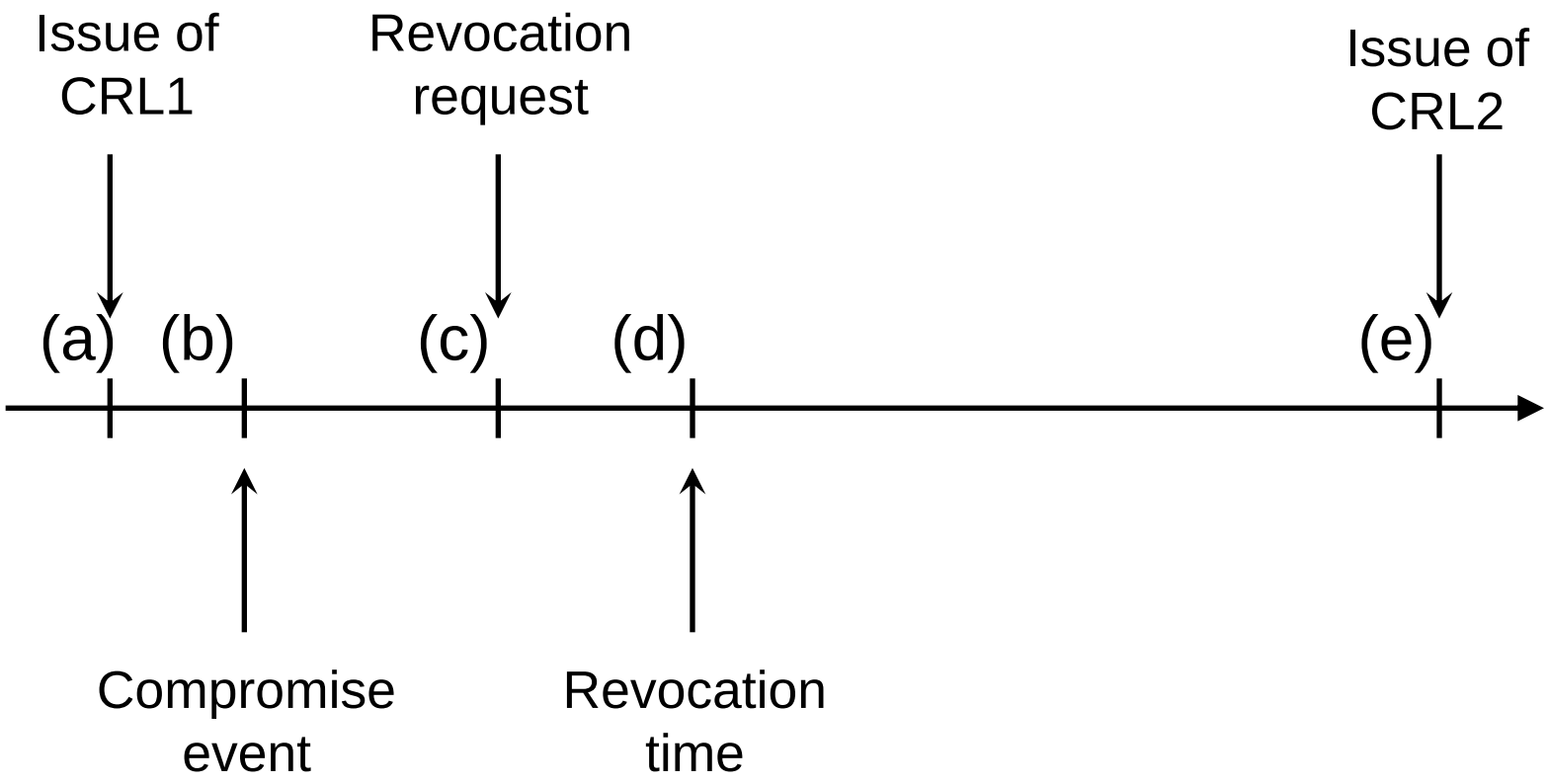
- Requesting revocation
  - Subscriber
  - Officers of CA
  - Others
- Periodic revocation (*pull* method)
  - Time granularity limited to CRL issue period (hourly, daily, weekly…)
  - *Off-cycle*: post immediately
- Broadcast CRLs (*push* method)
  - At the moment new revocations are posted

Certificate Revocation

- Online status checking
  - Confirm validity of a certificate in the moment it is used
  - CA must operate a high-availability online service
  - Secure environment
  - Standard method: Online Certificate Status Protocol (OCSP)
- Short-lived certificates
  - Validation in a *long-term credentials* period
  - Issuing e.g. daily certificates with a lifetime of 25 h
- Other revocation methods

Certificate Revocation

- timeline



Expiry of electronic certificates

Law 59/03 Art. 8.2:

The validity period of electronic certificates will be within the characteristics and technologies employed to generate data for signature creation. In case of qualified certificates, this period can't exceed four years.

Common provisions for expiry and suspension of validity of electronic certificates

Law 59/03 Art. 10.4:

The extinguishment or suspension of an electronic certificate validity is accessible in the certificate expiry enquiry service at least until the date when its validity ends.

Certification Authorities: Tasks

- Generation and issuing of certificates
- Revocation, suspension, renovation and recovery
- Key generation
- Certificate storage
- Certificate revocation information (CRL) maintenance
- Notification of certificates

Registration Authorities: Tasks

- Applicant identification
- Validation of certificate applications → approval or rejection
- Sending information to CA
- Reception of certificates emitted by the CA
- Acceptance and notification of requests for certificate suspension, revocation and attribute changes to CA
- Does NOT issue certificates

Public key certificate validation

- Cryptographically **valid signature** using issuer's public key
- **Validity period**
- Critical extensions
- Intended purpose
- Other policy constraints
- **It has not been revoked**
- + **Validate issuer's public key certificate**

X.509 Attribute Certificates

- Purpose: binding a privilege to a holder
- Two distinct mechanisms:
  - Public-key certificates may contain a **subjectDirectoryAttributes extension** that contains privileges associated with the subject of the public-key certificate
    - CA= Attribute Authority (AA)
    - Validity period of the privilege corresponds to the validity period of the public-key certificate.

X.509 Attribute Certificates

- Two distinct mechanisms:
  - (**subjectDirectoryAttributes extension**)
  - In the more general case, the use of **attribute certificates issued by an AA** provides a flexible solution
    - Entity privileges may have lifetimes different than the validity period for a public-key certificate. Privileges will often have a much shorter lifetime.
    - AA <> CA or multiple AA may exist.
    - There is a relationship between the CA and the AA as the CA is used to authenticate identities of issuers and holders in attribute certificates

X.509 Attribute Certificates Format

- User Identification (holder)
- Name of Attribute Authority (AA)
- Serial number
- Signature algorithm of AA
- Validity period
- Attributes
- Extensions
- Digital signature