Digital Certificates. PKI and other TTPs.

3.2

Universidad Carlos III de Madrid
Grupo SeTI · Dpto. Informática

Public Key Infrastructure (PKI)

Def.:

Set of infrastructural services that support the wide-scale use of public-key-based digital signature and encryption, which include:

- Certification Authorities,
- Registration Authorities,
- Key archival/recovery service,
- Certificate repository,
- Validation service,
- Time stamping service, etc.

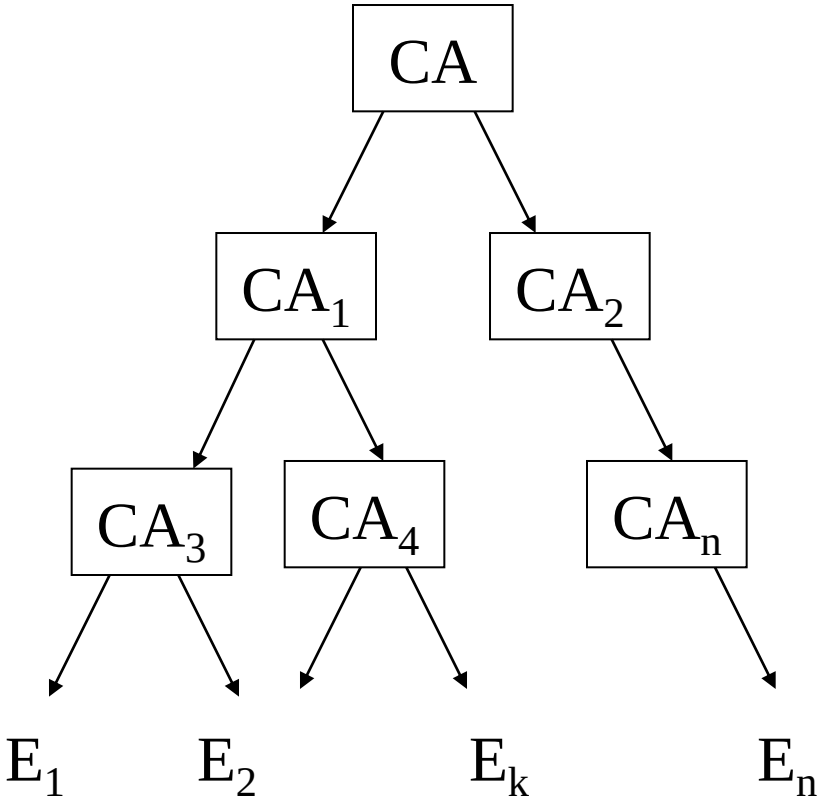
as well as their structuring rules and their methods of key and certificate management, which establish their validity and guarantee their mutual recognition.

Certification Authority Structures

Traditional models

- Hierarchies (trees)
- Forests of trees

Descendent hierarchical structure



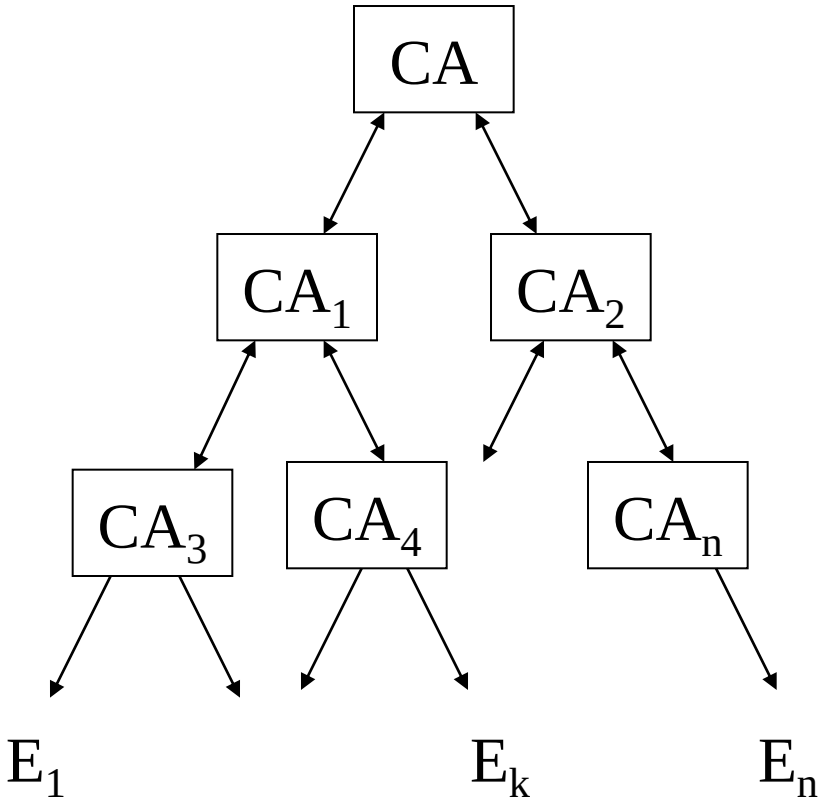
Certificates of certification authorities

- Self-issued: same issuer-subject CA name
  - Self-signed: same issuer-subject CA key
- Cross-certificate: different issuer-subject CA

  Def.

  A certificate issued by one CA to another CA which contains a CA signature key used for issuing certificates

General hierarchical structure



Certification path

Def.

A list of certificates needed to allow a particular user to obtain the public key of another.

Each item in the list is a certificate of the certification authority of the next item in the list.

Alternatively: Source: RFC 2527

An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification path

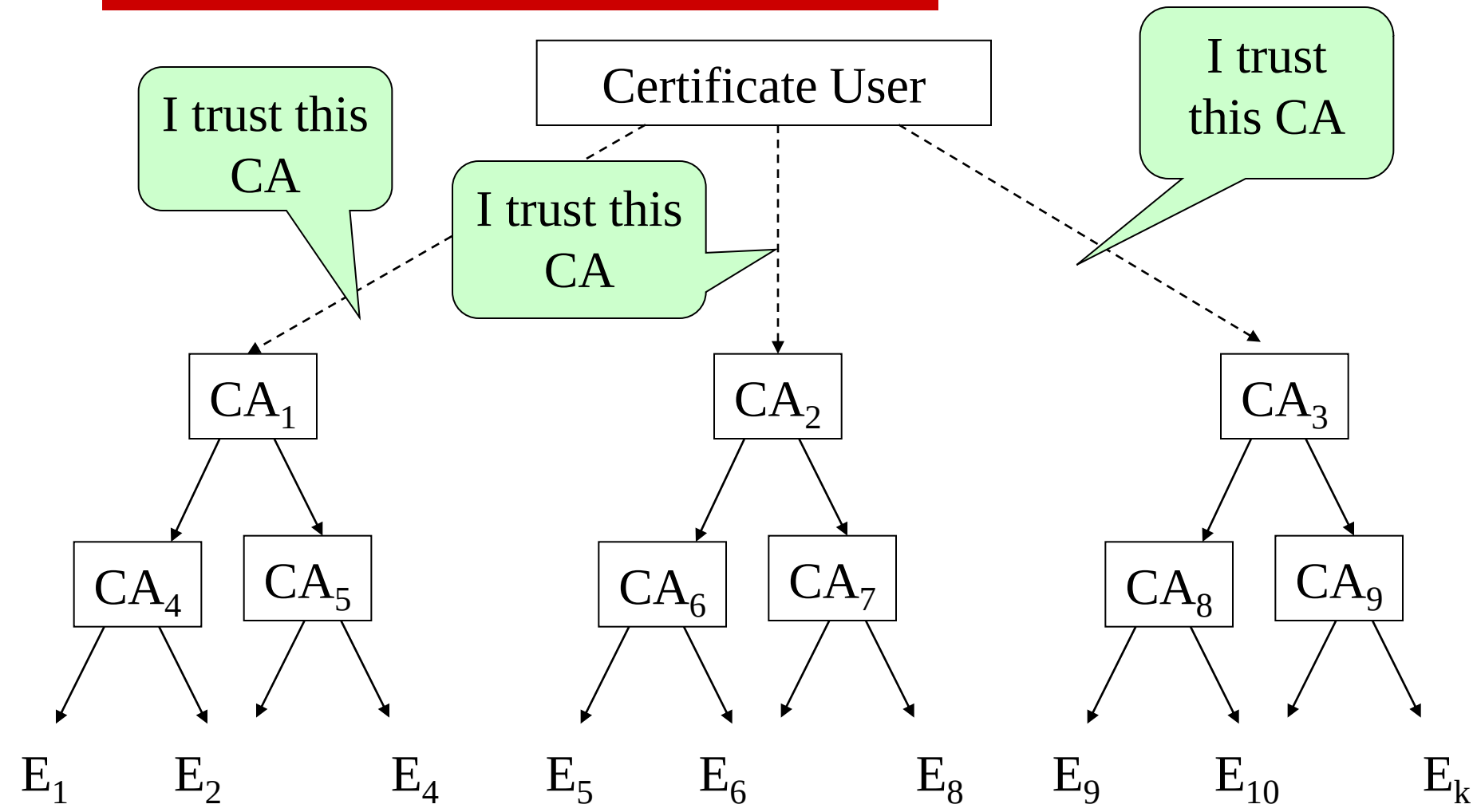
- A certification path from A to B
  - Starts with a certificate produced by CA(A) (the CA of entity A), namely CA(A)<<X1>>

    [Note: This is the TRUST ANCHOR for user A; A trusts CA(A) and possibly knows the authentic public key of CA(A)]
  - Continues with further certificates Xi<<Xi+1>>
  - Ends with the certificate of B

Certification path validation

- Besides validating each certificate within the certification path…
- …the names in the certificates must be consistent with a valid certification path, that is, the subject of every certificate (except the last) is the issuer of the next certificate

Forest of Trees



Certificate Policies

- Certificate Policies
  - Determines the applicability of the **certificate**
- Certification Practice Statement (CPS)
  - Focuses on what a ***CA*** does and **how**

Certificate Policies

Def. (RFC 2527):

A certificate policy is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

- A certificate policy can help a certificate user decide whether a certificate should be trusted in a particular application.

Certificate Policies

- For example purposes, suppose that the International Air Transport Association (IATA) undertakes to define some certificate policies for use throughout the airline industry, in a PKI operated by IATA in combination with PKIs operated by individual airlines. Two CPs might be defined:
  - the IATA General-Purpose CP
  - the IATA Commercial-Grade CP.

RFC 3647

Certificate Policies

- The **IATA General-Purpose CP** could be used by industry personnel for protecting routine information (e.g., casual electronic mail) and for authenticating connections from World Wide Web browsers to servers for general information retrieval purposes. The key pairs may be generated, stored, and managed using low-cost, software-based systems, such as commercial browsers. Under this policy, a certificate may be automatically issued to anybody listed as an employee in the corporate directory of IATA or any member airline who submits a signed certificate request form to a network administrator in his or her organization.

RFC 3647

Certificate Policies

- The **IATA Commercial-Grade CP** could be used to protect financial transactions or binding contractual exchanges between airlines. Under this policy, IATA could require that certified key pairs be generated and stored in approved cryptographic hardware tokens. Certificates and tokens could be provided to airline employees with disbursement authority. These authorized individuals might then be required to present themselves to the corporate security office, show a valid identification badge, and sign a subscriber agreement requiring them to protect the token and use it only for authorized purposes, as a condition of being issued a token and a certificate.

RFC 3647

Certificate Policies

Contents (a set of provisions)

- 1. Introduction
- 2. Publication and Repository
- 3. Identification and Authentication
- 4. Certificate Life-Cycle Operational Requirements
- 5. Facilities, Management, and Operational Controls
- 6. Technical Security Controls
- 7. Certificate, CRL, and OCSP Profile
- 8. Compliance audit
- 9. Other Business and Legal Matters

RFC 3647

Certification Practice Statement (CPS)

Def.:

A Certification Practice Statement is a document published by a CA which comprises the norms, rules and proceedings that rule the life cycle of the issued certificates. Also, it includes the obligations contracted with the certificate owners, and of them with the CA, and the responsibility margins to assume in relation to the entities that accept certificates.

Alternatively **(RFC 2527)**:

A statement of the practices which a certification authority employs in issuing certificates.

Certification Practice Statement (CPS)

Law 59/03 Art. 19.1:

All certification-service providers issue a CPS in which they declare, in detail and in the framework of this law, the obligations they commit regarding signature creation and verification data management, as well as conditions applicable to the requests, issuance, usage, suspension and expiry of certificates, the technical and organisational...

Certification Practice Statement (CPS)

... security measures, the profiles and the information mechanisms about certification expiry, and the possible existence of procedures in coordination with the corresponding public register offices that permit the immediate interchange of information related to the expiration date of powers entitled on certificates and which have to appear mandatory in the mentioned registers.

Certification Practice Statement (CPS)

Law 59/03 Art. 19.2:

The CPS of every service provider will be made available to the public on an easy and accessible way, at least electronically and completely free.

Certification Practice Statement (CPS)

Law 59/03 Art. 19.3:

The CPS will be considered as a security document for the predicted effects on the legislation as regards personal data protection and should contain all the demanded requirements for such a document in the aforementioned legislation.

Certification Practice Statement (CPS)

- A single set of provisions (contents of a CP) with each component addressing the requirements of one or more certificate policies
- An organized collection of sets of provisions. E.g.:
  - a list of certificate policies supported by the CPS
  - for each CP in (a), a set of provisions that contains statements responding to that CP by filling in details not stipulated in that policy or expressly left to the discretion of the CA (in its CPS) ; such statements serve to state how this particular CPS implements the requirements of the particular CP;
  - a set of provisions that contains statements regarding the certification practices on the CA, regardless of CP.

RFC 3647

Resume:

Certificate policy

- Document used to express policy only - "what" but not "how".
- Typically a public document

Certification Practice Statement (CPS)

- Developed by the CA
- It defines "how" a CP is enforced
- It may NOT be a public document (publication of a CPS Abstract)

Certificate Policy (CP) and Certification Practice Statement (CPS)

- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (2003)

- ftp://ftp.rfc-editor.org/in-notes/rfc3647.txt

Name constraints

- Exact specification of names for subsequent certificates in the certification path.
- Restriction of certificate issuance to single or multiple namespaces used within PKI.
- Greater control over which users and computers receive certificates from your qualified subordinate CA.
- Specification of both: permitted and excluded subtrees

PKI - Protocols

- **Certificate Generation** - X.509, PKIX Profile
  - Certificates
  - Cross-certificates
  - CRLs
- **Certificate Distribution** - LDAP, S/MIME
  - LDAP: share cert repositories
  - S/MIME: direct interchange of certs between end users
- **Certificate Management** – PKIX-CMP, PKCS #7/#10
  - Requesting and receiving certificates

PKI - Protocols

Certificate Generation

- The Public Key Infrastructure X.509 (PKIX) was formed by the Internet Engineering Task Force (IETF) to define a model suitable for the Internet.
- Does not support all features of X.509

PKI - Protocols

Certificate Distribution

- LDAP (Lightweight Directory Access Protocol)
  - Repository of certificates issued by the CA
  - Maintenance of the CRL
- S/MIME (Secure / Multipurpose Internet Mail Extensions

PKI - Protocols

Certificate Management

- PKCS (Public-Key Cryptography Standards)
  - Developed by RSA Security
  - #10: Format definition for certification request
  - #7: Format for protecting messages
  - PKCS #10+#7 used for cert request and issuance
- CMP (Certificate Management Protocol)
  - Origin by PKIX (Public-Key Infrastructure (X.509)) Working Group
  - Newest: **CMPv2** by IETF (Internet Engineering Task Force)

Other trust models: PGP's web of trust

- Pretty Good Privacy (PGP)
  - Does not use X.509 certificates
  - Uses OpenPGP certificates (OpenPGP Message Format RFC 4880)
- No concept of CA
- Instead...

"The friends of my friends are my friends, too"

Other trust models: PGP's web of trust

- Other users can certify the binding between a public key and a user
- I can rely on other users ("my friends") to certify other user's public keys
- Trust levels: un-trusted, marginal, complete, ultimate
- No formal structure as a hierarchy of CAs
- Arbitrary certification paths worldwide
- Problems: important decisions for too many individuals → high risk of bad decisions

Multi-enterprise PKI examples

- Privacy enhanced mail (PEM) (1993)
  - Three types (levels) of CA
  - A CA at 3rd level can be certified by more than one CA
  - Three types of certifications (organizational, residential, a persona)
  - Not successful, emergence of MIME
- Secure Electronic Transaction (SET)
  - VISA, MasterCard
  - Includes all parties of a transaction (cardholders, issuers, merchants, acquirers, CAs…)

Multi-enterprise PKI examples

- VeriSign Trust Network http://www.verisign.com/
  - Largest commercial certification authority network:
    - VeriSign Inc. (United States)
    - British Telecommunications
    - KPN Telecom (Netherlands)
    - Telia (Sweden)
    - CIBC (Canada)
    - …
  - Comprises public and private PKI structures