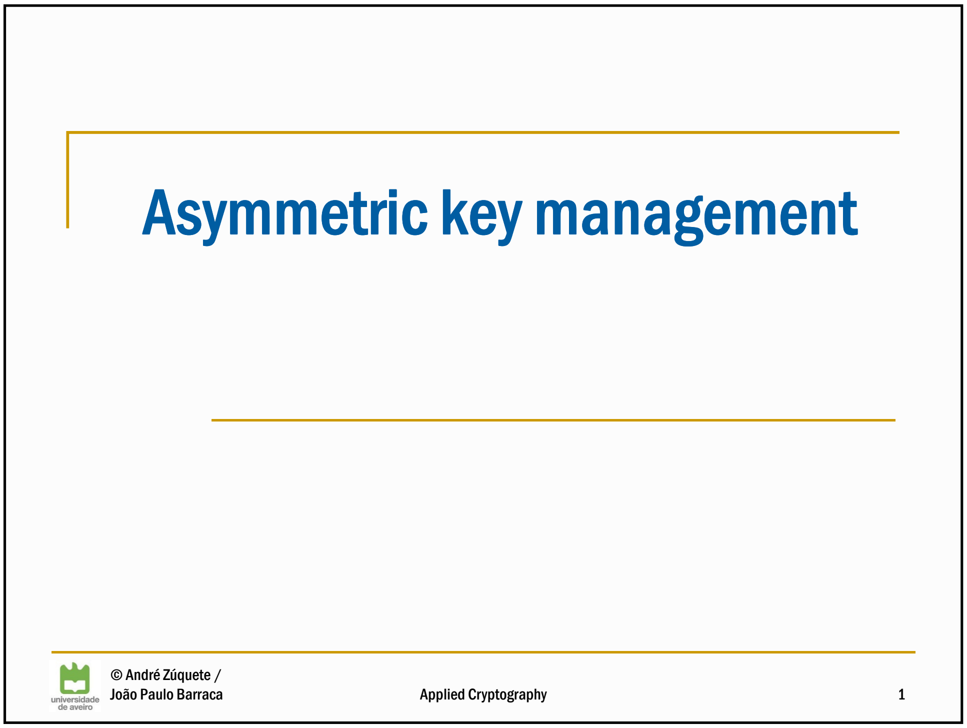
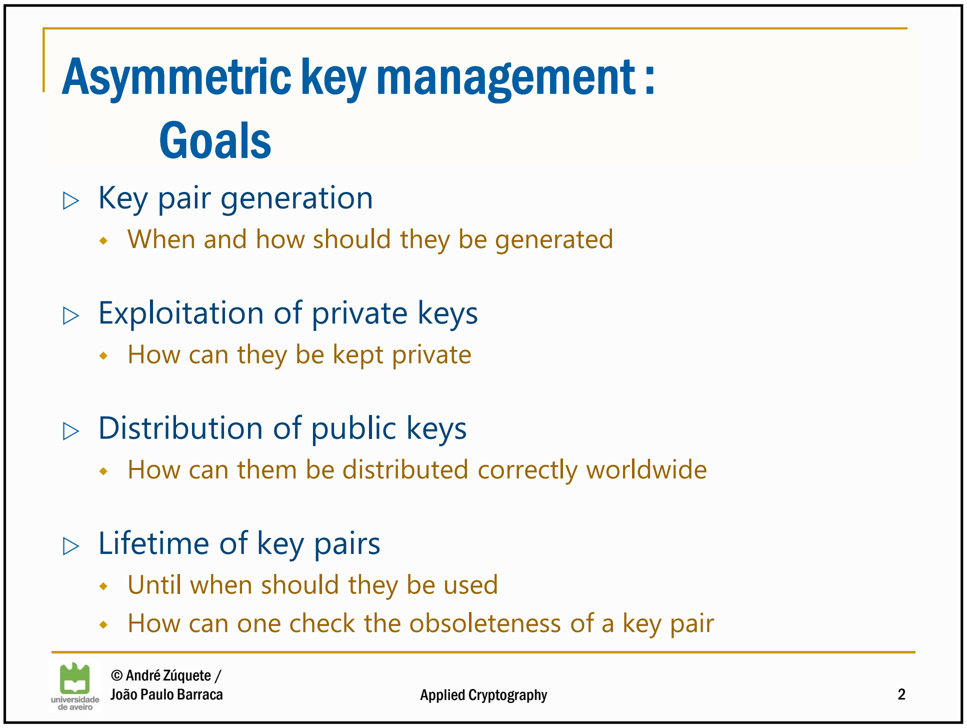
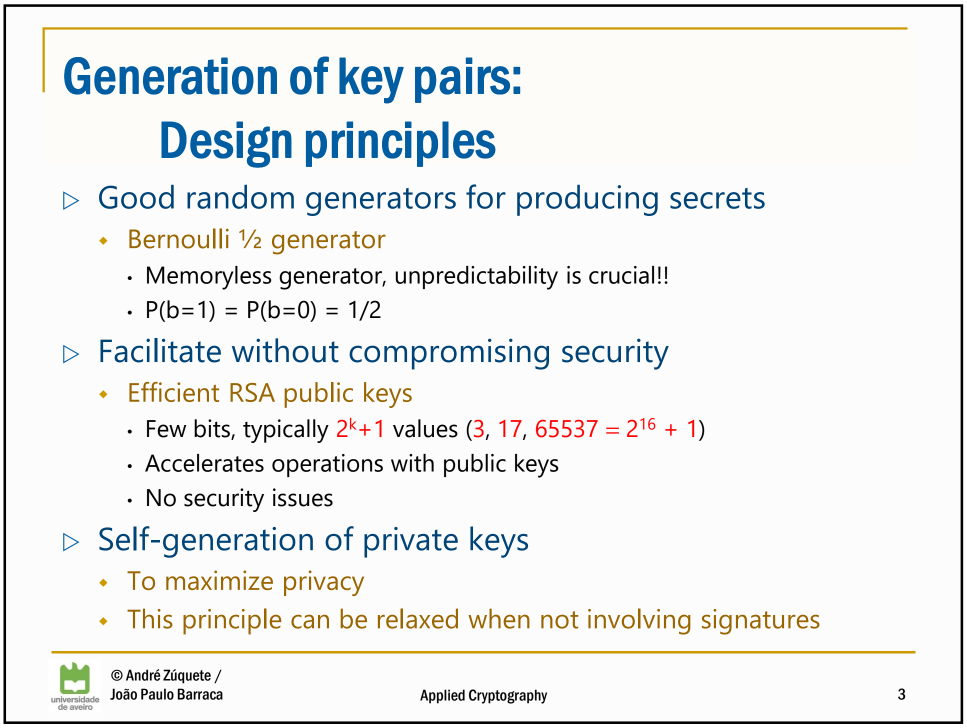


# Asymmetric key management



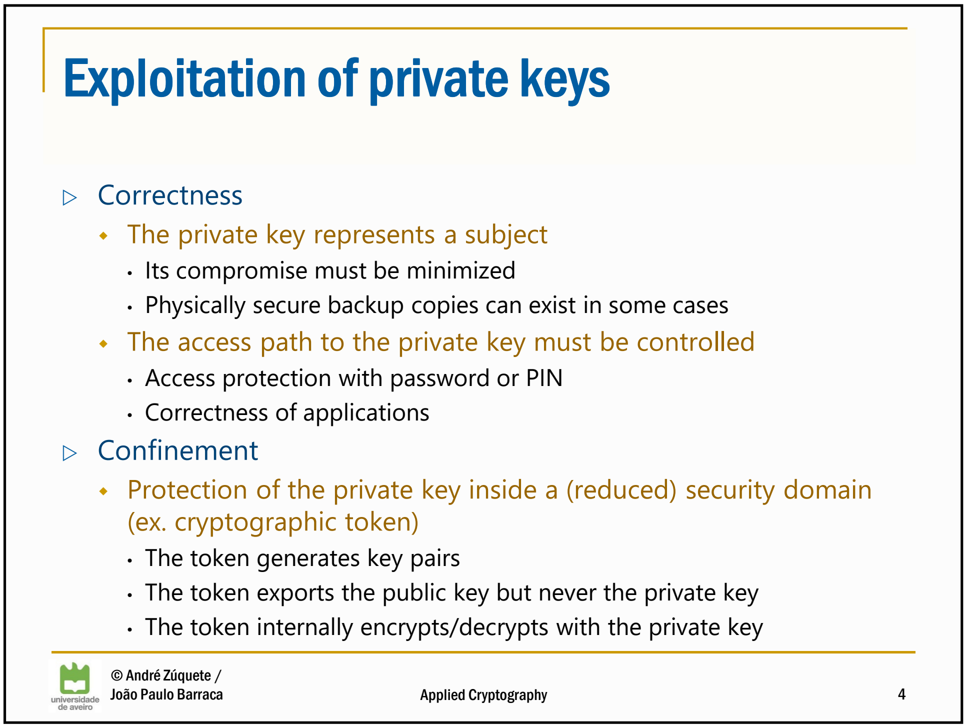
## Asymmetric key management : Goals

- ▷ Key pair generation
  - When and how should they be generated
- ▷ Exploitation of private keys
  - How can they be kept private
- ▷ Distribution of public keys
  - How can them be distributed correctly worldwide
- ▷ Lifetime of key pairs
  - Until when should they be used
  - How can one check the obsoleteness of a key pair



## Generation of key pairs: Design principles

- ▷ Good random generators for producing secrets
  - Bernoulli ½ generator
    - Memoryless generator, unpredictability is crucial!!
    - P(b=1) = P(b=0) = 1/2
- ▷ Facilitate without compromising security
  - Efficient RSA public keys
    - Few bits, typically $2^k+1$ values (3, 17, $65537 = 2^{16} + 1$)
    - Accelerates operations with public keys
    - No security issues
- ▷ Self-generation of private keys
  - To maximize privacy
  - This principle can be relaxed when not involving signatures



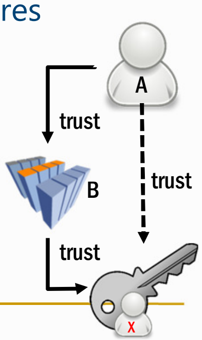
## Exploitation of private keys

- ▷ Correctness
  - The private key represents a subject
    - Its compromise must be minimized
    - Physically secure backup copies can exist in some cases
  - The access path to the private key must be controlled
    - Access protection with password or PIN
    - Correctness of applications
- ▷ Confinement
  - Protection of the private key inside a (reduced) security domain (ex. cryptographic token)
    - The token generates key pairs
    - The token exports the public key but never the private key
    - The token internally encrypts/decrypts with the private key

# Distribution of public keys

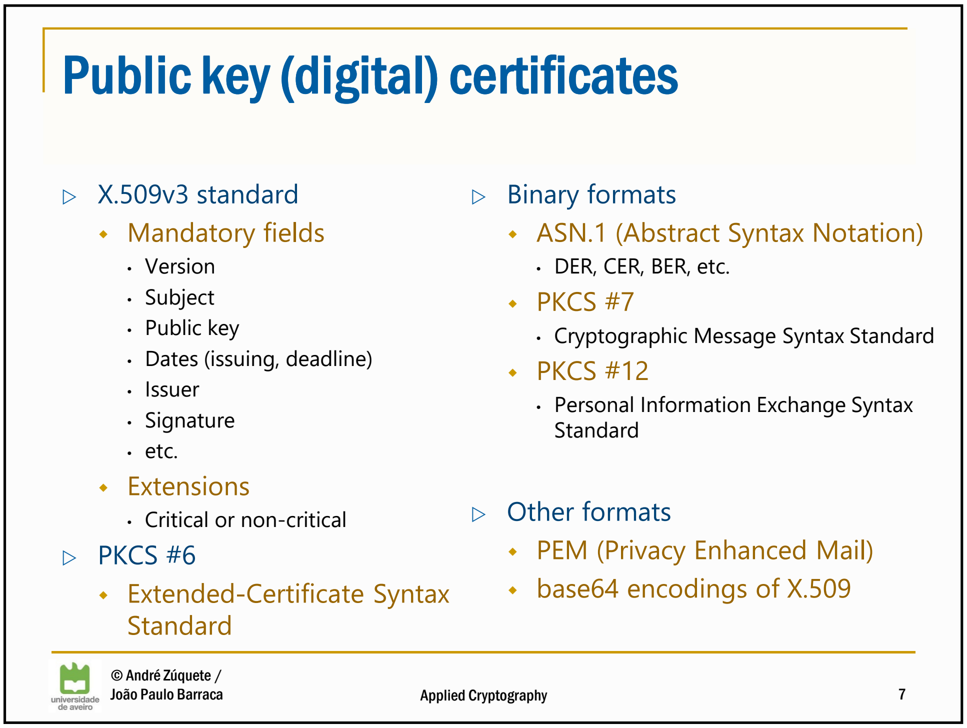
- Distribution to all **senders** of confidential data
  - Manual
  - Using a shared secret
  - Ad-hoc using digital certificates
- Distribution to all **receivers** of digital signatures
  - Ad-hoc using digital certificates
- Trustworthy dissemination of public keys
  - Transitive trust paths / graphs

    If entity A trusts entity B and B trust in $K_X^+$, then A trusts in $K_X^+$
  - Certification hierarchies / graphs



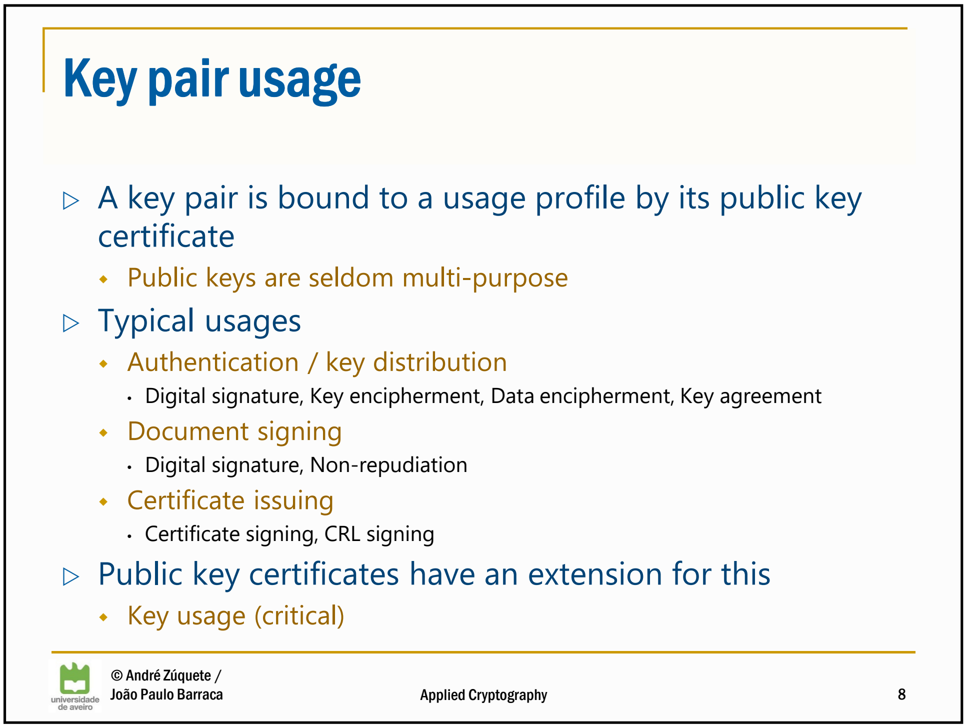
# Public key (digital) certificates

- Documents issued by a Certification Authority (CA)
  - Bind a public key to an entity
    - Person, server or service
  - Are public documents
    - Do not contain private information, only public one
  - Are cryptographically secure
    - Digitally signed by the issuer, cannot be changed
- Can be used to distribute public keys in a trustworthy way
  - A certificate receiver can validate it
    - With the CA's public key
  - If the signer (CA) public key is trusted, and the signature is correct, then the receiver can trust the (certified) public key
    - As the CA trust the public key, if the receiver trusts on the CA public key, the receiver can trust on the public key



# Public key (digital) certificates

- X.509v3 standard
  - Mandatory fields
    - Version
    - Subject
    - Public key
    - Dates (issuing, deadline)
    - Issuer
    - Signature
    - etc.
  - Extensions
    - Critical or non-critical
- PKCS #6
  - Extended-Certificate Syntax Standard
- Binary formats
  - ASN.1 (Abstract Syntax Notation)
    - DER, CER, BER, etc.
  - PKCS #7
    - Cryptographic Message Syntax Standard
  - PKCS #12
    - Personal Information Exchange Syntax Standard
- Other formats
  - PEM (Privacy Enhanced Mail)
  - base64 encodings of X.509



# Key pair usage

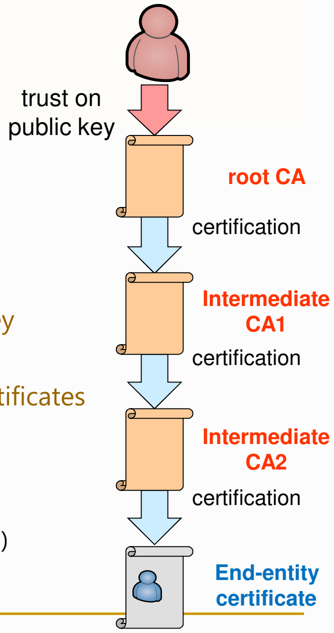
- A key pair is bound to a usage profile by its public key certificate
  - Public keys are seldom multi-purpose
- Typical usages
  - Authentication / key distribution
    - Digital signature, Key encipherment, Data encipherment, Key agreement
  - Document signing
    - Digital signature, Non-repudiation
  - Certificate issuing
    - Certificate signing, CRL signing
- Public key certificates have an extension for this
  - Key usage (critical)

# Certification Authorities (CA)

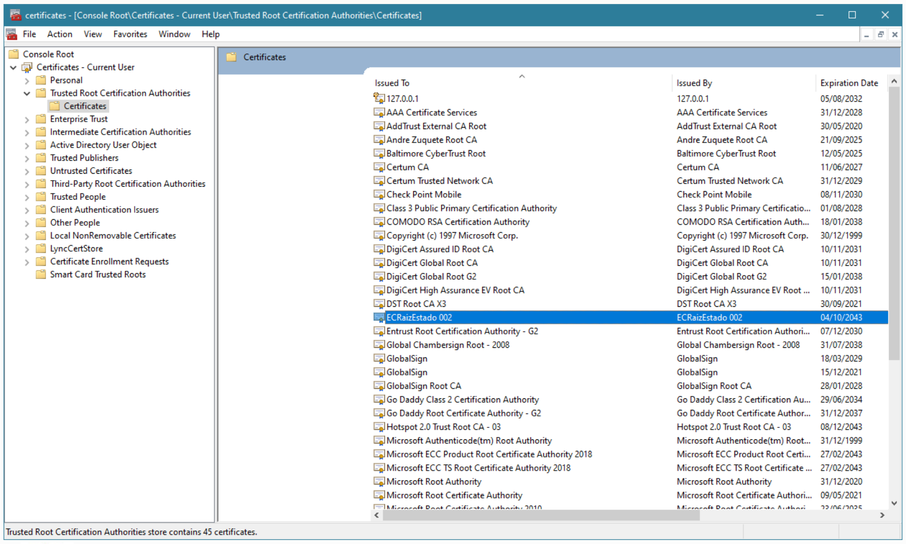
- Organizations that manage public key certificates
- Define policies and mechanisms for
  - Issuing certificates
  - Revoking certificates
  - Distributing certificates
  - Issuing and distributing the corresponding private keys
- Manage certificate revocation lists
  - Lists of revoked certificates

# CA types

- Intermediate CAs
  - CAs certified by other Cas
- Root CAs
  - CAs for which one has a trusted public key
  - Trust anchor
  - Usually implemented by self-certified certificates
    - Issuer = Subject
    - Self-certification is not a reason for trusting!
  - Manual distribution
    - Tools' repositories (Firefox, Thunderbird, etc.)
    - Operating systems' repositories



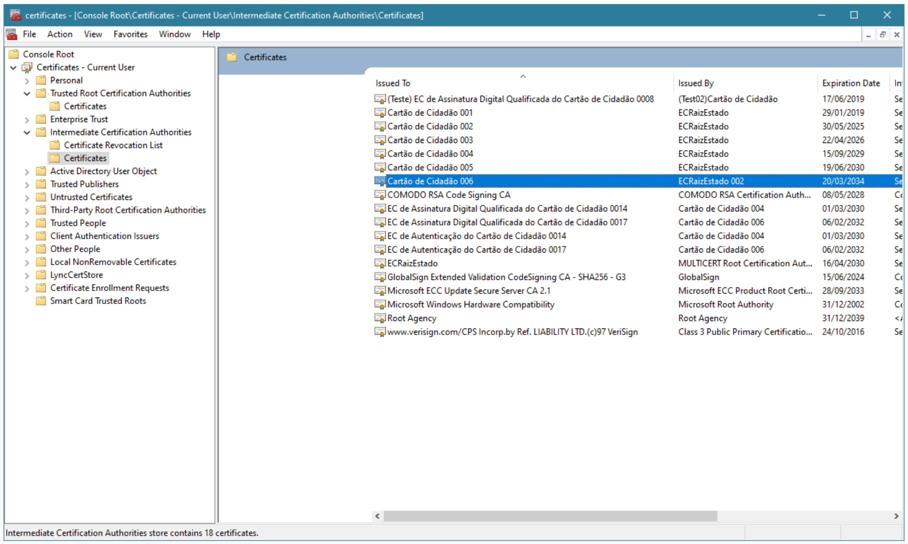
# Certificates of Root CAs: Windows 10


certificates - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Other People
Local NonRemovable Certificates
LyncCertStore
Certificate Enrollment Requests
Smart Card Trusted Roots
Certificates

| Issued To | Issued By | Expiration Date |
|---|---|---|
| 127.0.0.1 | 127.0.0.1 | 05/08/2032 |
| AAA Certificate Services | AAA Certificate Services | 31/12/2028 |
| AddTrust External CA Root | AddTrust External CA Root | 30/05/2020 |
| Andre Zuquete Root CA | Andre Zuquete Root CA | 21/09/2025 |
| Baltimore CyberTrust Root | Baltimore CyberTrust Root | 12/05/2025 |
| Certum CA | Certum CA | 11/06/2027 |
| Certum Trusted Network CA | Certum Trusted Network CA | 31/12/2029 |
| Check Point Mobile | Check Point Mobile | 08/11/2030 |
| Class 3 Public Primary Certification Authority | Class 3 Public Primary Certificatio... | 01/08/2028 |
| COMODO RSA Certification Authority | COMODO RSA Certification Auth... | 18/01/2038 |
| Copyright (c) 1997 Microsoft Corp. | Copyright (c) 1997 Microsoft Corp. | 30/12/1999 |
| DigiCert Assured ID Root CA | DigiCert Assured ID Root CA | 10/11/2031 |
| DigiCert Global Root CA | DigiCert Global Root CA | 10/11/2031 |
| DigiCert Global Root G2 | DigiCert Global Root G2 | 15/01/2038 |
| DigiCert High Assurance EV Root CA | DigiCert High Assurance EV Root ... | 10/11/2031 |
| DST Root CA X3 | DST Root CA X3 | 30/09/2021 |
| ECRaizEstado 002 | ECRaizEstado 002 | 04/10/2043 |
| Entrust Root Certification Authority - G2 | Entrust Root Certification Authori... | 07/12/2030 |
| Global Chambersign Root - 2008 | Global Chambersign Root - 2008 | 31/07/2038 |
| GlobalSign | GlobalSign | 18/03/2029 |
| GlobalSign | GlobalSign | 15/12/2021 |
| GlobalSign Root CA | GlobalSign Root CA | 28/01/2028 |
| Go Daddy Class 2 Certification Authority | Go Daddy Class 2 Certification Au... | 29/06/2034 |
| Go Daddy Root Certificate Authority - G2 | Go Daddy Root Certificate Author... | 31/12/2037 |
| Hotspot 2.0 Trust Root CA - 03 | Hotspot 2.0 Trust Root CA - 03 | 08/12/2043 |
| Microsoft Authenticode(tm) Root Authority | Microsoft Authenticode(tm) Root... | 31/12/1999 |
| Microsoft ECC Product Root Certificate Authority 2018 | Microsoft ECC Product Root Certi... | 27/02/2043 |
| Microsoft ECC TS Root Certificate Authority 2018 | Microsoft ECC TS Root Certificate ... | 27/02/2043 |
| Microsoft Root Authority | Microsoft Root Authority | 31/12/2020 |
| Microsoft Root Certificate Authority | Microsoft Root Certificate Authori... | 09/05/2021 |
| Microsoft Root Certificate Authority 2010 | Microsoft Root Certificate Authori... | 23/06/2035 |

Trusted Root Certification Authorities store contains 45 certificates.

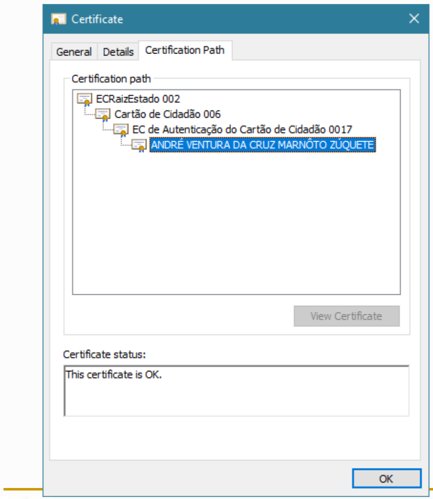
# Certs. of Intermediate CAs: Windows 10


certificates - [Console Root\Certificates - Current User\Intermediate Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Certificate Revocation List
Certificates
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Other People
Local NonRemovable Certificates
LyncCertStore
Certificate Enrollment Requests
Smart Card Trusted Roots
Certificates

| Issued To | Issued By | Expiration Date | In |
|---|---|---|---|
| (Teste) EC de Assinatura Digital Qualificada do Cartão de Cidadão 0008 | (Test02)Cartão de Cidadão | 17/06/2019 | Se |
| Cartão de Cidadão 001 | ECRaizEstado | 29/01/2019 | Se |
| Cartão de Cidadão 002 | ECRaizEstado | 30/05/2025 | Se |
| Cartão de Cidadão 003 | ECRaizEstado | 22/04/2026 | Se |
| Cartão de Cidadão 004 | ECRaizEstado | 15/09/2029 | Se |
| Cartão de Cidadão 005 | ECRaizEstado | 19/06/2030 | Se |
| Cartão de Cidadão 006 | ECRaizEstado 002 | 20/03/2034 | Se |
| COMODO RSA Code Signing CA | COMODO RSA Certification Auth... | 08/05/2028 | Co |
| EC de Assinatura Digital Qualificada do Cartão de Cidadão 0014 | Cartão de Cidadão 004 | 01/03/2030 | Se |
| EC de Assinatura Digital Qualificada do Cartão de Cidadão 0017 | Cartão de Cidadão 006 | 06/02/2032 | Se |
| EC de Autenticação do Cartão de Cidadão 0014 | Cartão de Cidadão 004 | 01/03/2030 | Se |
| EC de Autenticação do Cartão de Cidadão 0017 | Cartão de Cidadão 006 | 06/02/2032 | Se |
| ECRaizEstado | MULTICERT Root Certification Aut... | 16/04/2030 | Se |
| GlobalSign Extended Validation CodeSigning CA - SHA256 - G3 | GlobalSign | 15/06/2024 | Co |
| Microsoft ECC Update Secure Server CA 2.1 | Microsoft ECC Product Root Certi... | 28/09/2033 | Se |
| Microsoft Windows Hardware Compatibility | Microsoft Root Authority | 31/12/2002 | Co |
| Root Agency | Root Agency | 31/12/2039 | <A |
| www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign | Class 3 Public Primary Certificatio... | 24/10/2016 | Se |

Intermediate Certification Authorities store contains 18 certificates.

# Certification hierarchies (or chains, paths): Cartão de Cidadão example

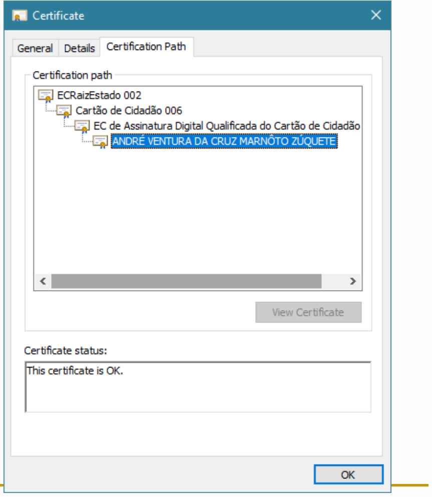


Certification path

- ECRaizEstado 002
  - Cartão de Cidadão 006
    - EC de Autenticação do Cartão de Cidadão 0017
      - ANDRÉ VENTURA DA CRUZ MARNÔTO ZÚQUETE

Certificate status:

This certificate is OK.



Certification path

- ECRaizEstado 002
  - Cartão de Cidadão 006
    - EC de Assinatura Digital Qualificada do Cartão de Cidadão
      - ANDRÉ VENTURA DA CRUZ MARNÔTO ZÚQUETE

Certificate status:

This certificate is OK.

# Certification hierarchies: PEM (Privacy Enhanced Mail) model

- Distribution of certificates for PEM (secure e-mail)
  - Worldwide hierarchy (monopoly)
  - Single root (IPRA)
  - Several PCA (Policy Creation Authorities) bellow the root
  - Several CA below each PCA
    - Possibly belonging to organizations or companies
- Never implemented
  - Forest of hierarchies
    - Each with its independent root CA
    - Oligarchy
  - Each root CA negotiates the distribution of its public key along with some applications or operating systems
    - ex. Browsers, Windows

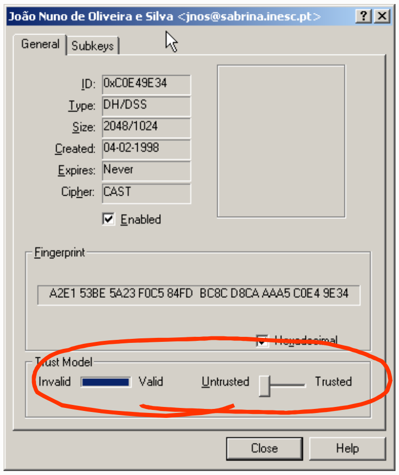
# Certification hierarchies: PGP (Pretty Good Privacy) model

- Web of trust
  - No central trustworthy authorities
    - Each person is a potential certifier
    - Can certify a public key (issue a certificate) and publish it
  - People uses 2 kinds of trust
    - Trust in the keys they know
      - Validated using any means (FAX, telephone, etc.)
    - Trust in the behavior of certifiers
      - Assumption that they know what they are doing when issuing a certificate
- Transitive trust
  - If

    Alice trusts Bob is a correct certifier; and
    Bob certified the public key of Carl,
  - then

    Alice trusts the public key belongs to Carl

# PGP public key certificates: Validity vs. trust

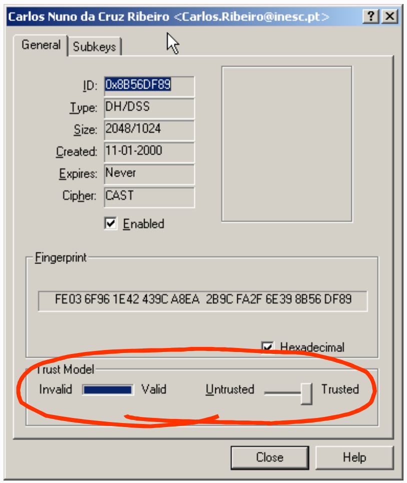


João Nuno de Oliveira e Silva <jnos@sabrina.inesc.pt>

ID: 0xC0E49E34
Type: DH/DSS
Size: 2048/1024
Created: 04-02-1998
Expires: Never
Cipher: CAST
☑ Enabled

Fingerprint: A2E1 53BE 5A23 F0C5 84FD BC8C D8CA AAA5 C0E4 9E34
☑ Hexadecimal

Trust Model: Invalid ▬ Valid; Untrusted ▭ Trusted

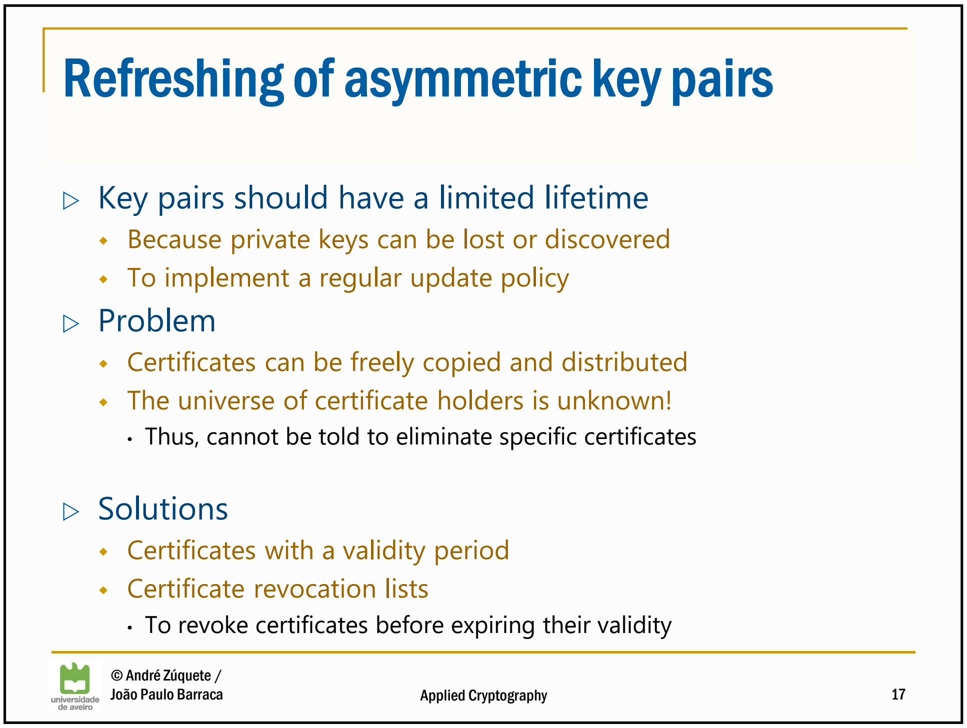


Carlos Nuno da Cruz Ribeiro <Carlos.Ribeiro@inesc.pt>

ID: 0x8B56DF89
Type: DH/DSS
Size: 2048/1024
Created: 11-01-2000
Expires: Never
Cipher: CAST
☑ Enabled

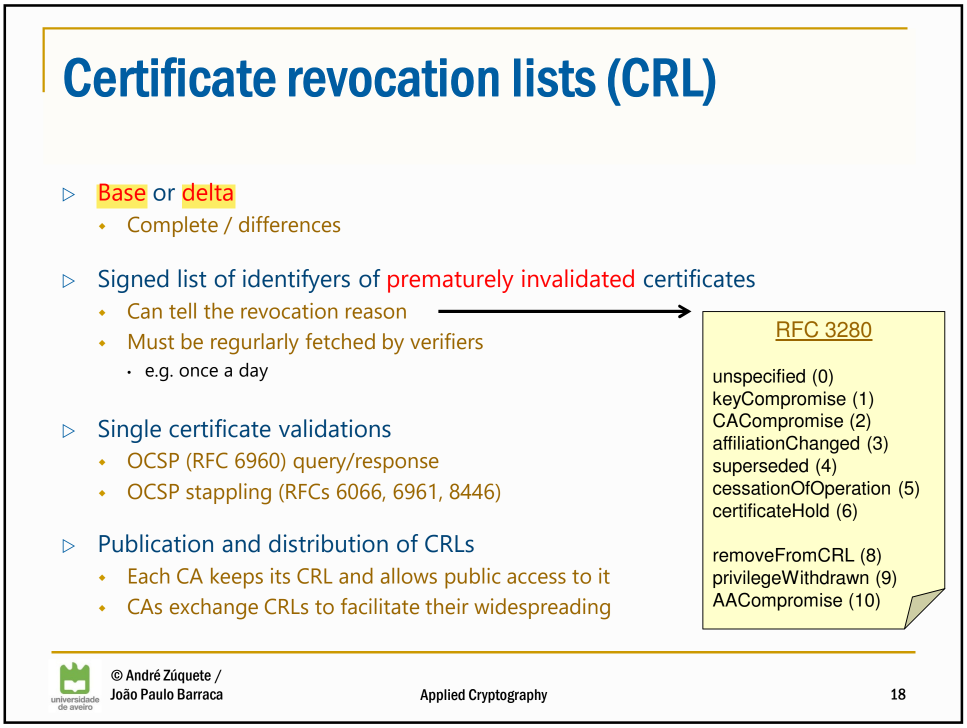
Fingerprint: FE03 6F96 1E42 439C A8EA 2B9C FA2F 6E39 8B56 DF89
☑ Hexadecimal

Trust Model: Invalid ▬ Valid; Untrusted ▭ Trusted



# Refreshing of asymmetric key pairs

- ▷ Key pairs should have a limited lifetime
  - Because private keys can be lost or discovered
  - To implement a regular update policy
- ▷ Problem
  - Certificates can be freely copied and distributed
  - The universe of certificate holders is unknown!
    - Thus, cannot be told to eliminate specific certificates
- ▷ Solutions
  - Certificates with a validity period
  - Certificate revocation lists
    - To revoke certificates before expiring their validity



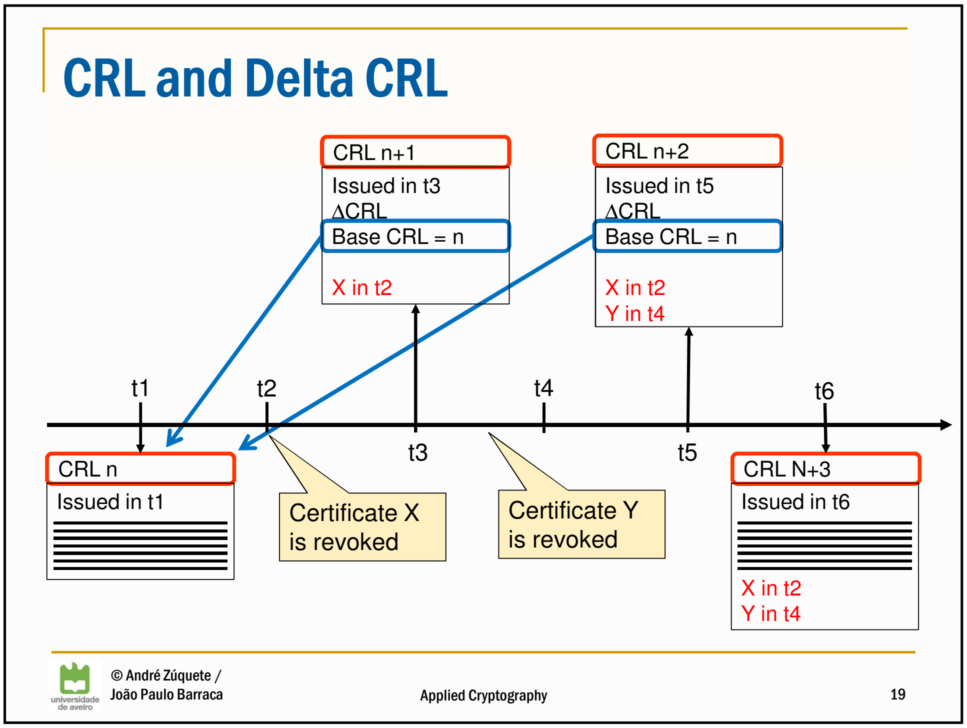
# Certificate revocation lists (CRL)

- ▷ Base or delta
  - Complete / differences
- ▷ Signed list of identifyers of prematurely invalidated certificates
  - Can tell the revocation reason →
  - Must be regurlarly fetched by verifiers
    - e.g. once a day
- ▷ Single certificate validations
  - OCSP (RFC 6960) query/response
  - OCSP stappling (RFCs 6066, 6961, 8446)
- ▷ Publication and distribution of CRLs
  - Each CA keeps its CRL and allows public access to it
  - CAs exchange CRLs to facilitate their widespreading

RFC 3280

unspecified (0)
keyCompromise (1)
CACompromise (2)
affiliationChanged (3)
superseded (4)
cessationOfOperation (5)
certificateHold (6)

removeFromCRL (8)
privilegeWithdrawn (9)
AACompromise (10)



# CRL and Delta CRL

CRL n+1

Issued in t3

ΔCRL

Base CRL = n

X in t2

CRL n+2

Issued in t5

ΔCRL

Base CRL = n

X in t2

Y in t4

CRL n

Issued in t1

Certificate X is revoked

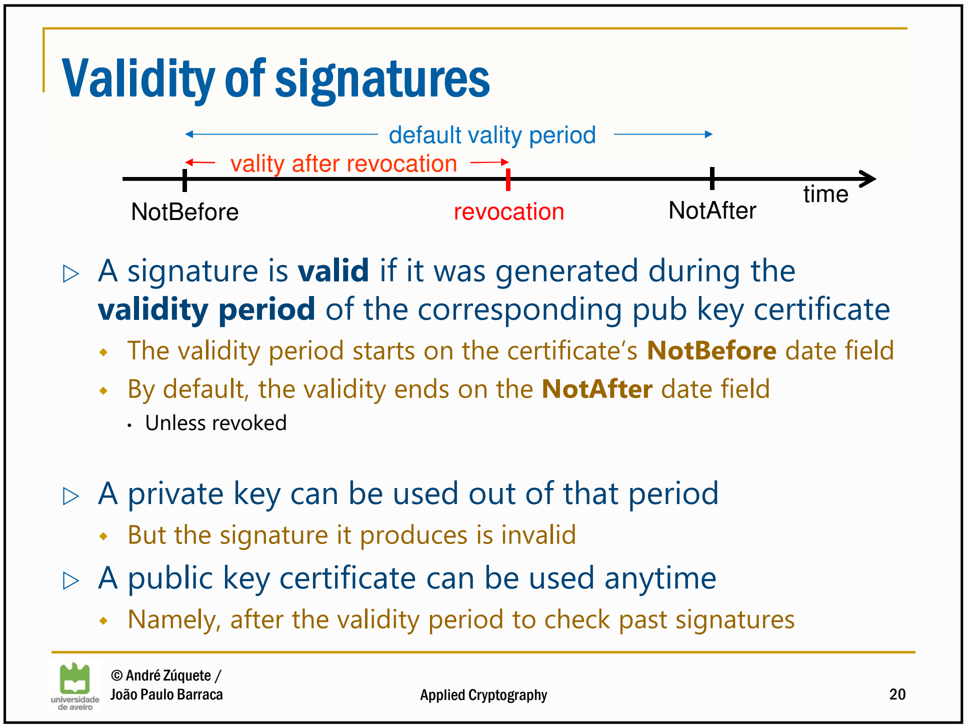
Certificate Y is revoked

CRL N+3

Issued in t6

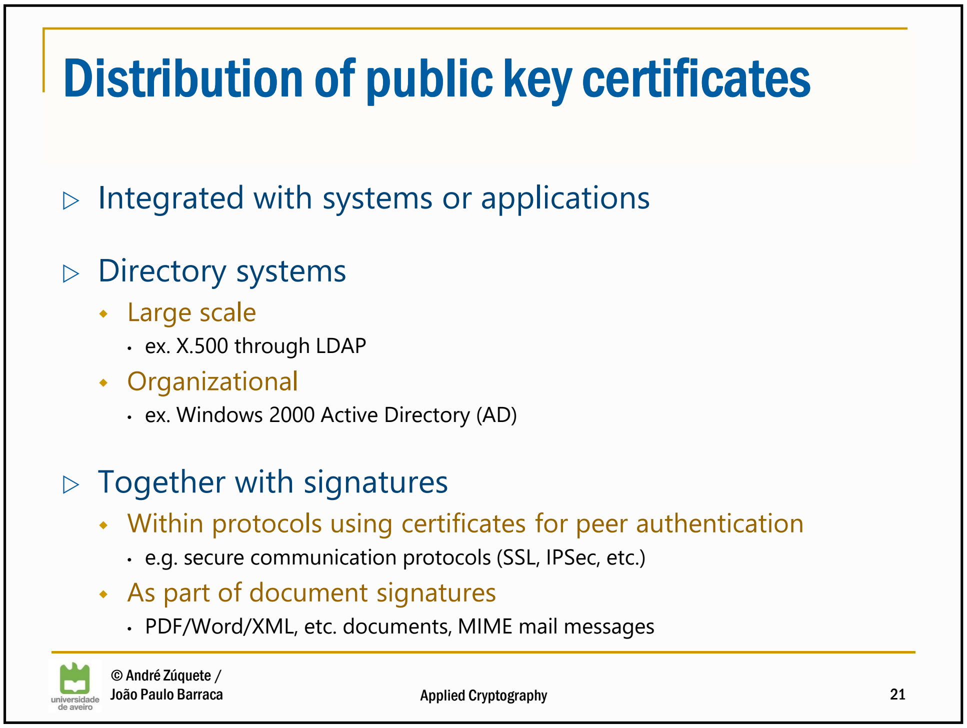
X in t2

Y in t4



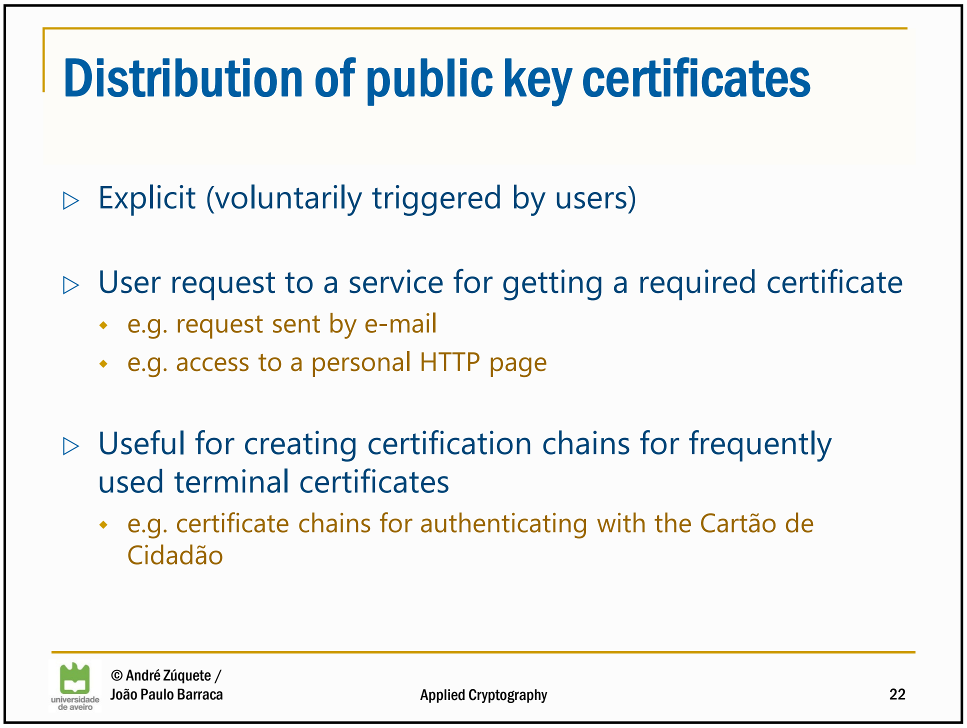
# Validity of signatures

- A signature is **valid** if it was generated during the **validity period** of the corresponding pub key certificate
  - The validity period starts on the certificate's **NotBefore** date field
  - By default, the validity ends on the **NotAfter** date field
    - Unless revoked
- A private key can be used out of that period
  - But the signature it produces is invalid
- A public key certificate can be used anytime
  - Namely, after the validity period to check past signatures



# Distribution of public key certificates

- ▷ Integrated with systems or applications
- ▷ Directory systems
  - Large scale
    - ex. X.500 through LDAP
  - Organizational
    - ex. Windows 2000 Active Directory (AD)
- ▷ Together with signatures
  - Within protocols using certificates for peer authentication
    - e.g. secure communication protocols (SSL, IPSec, etc.)
  - As part of document signatures
    - PDF/Word/XML, etc. documents, MIME mail messages



# Distribution of public key certificates

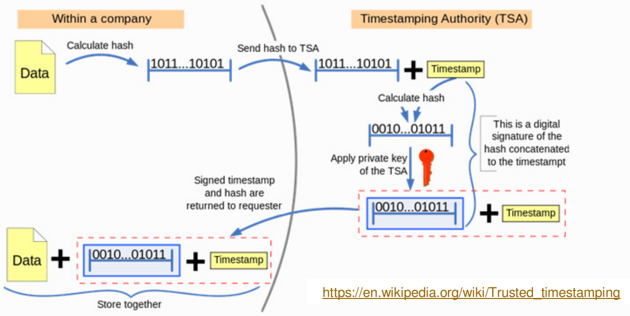
- ▷ Explicit (voluntarily triggered by users)
- ▷ User request to a service for getting a required certificate
  - e.g. request sent by e-mail
  - e.g. access to a personal HTTP page
- ▷ Useful for creating certification chains for frequently used terminal certificates
  - e.g. certificate chains for authenticating with the Cartão de Cidadão

# Time Stamping Authority (TSA)

▷ A service that provides signatures over a timestamp

- Linked with a data digest

Trusted timestamping


Within a company
Timestamping Authority (TSA)
Data
Calculate hash
1011...10101
Send hash to TSA
1011...10101
Timestamp
Calculate hash
0010...01011
This is a digital signature of the hash concatenated to the timestampt
Apply private key of the TSA
0010...01011
Timestamp
Signed timestamp and hash are returned to requester
Data
0010...01011
Timestamp
Store together

https://en.wikipedia.org/wiki/Trusted_timestamping

▷ This is useful for adding trust to a data signature date

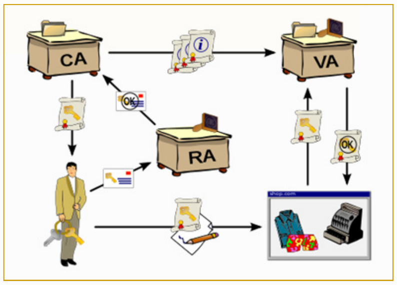
- The signature date becomes linked to the signed data

# PKI (Public Key Infrastructure)

▷ Infrastructure for enabling the use of keys pairs and certificates

- Creation of asymmetric key pairs for each enrolled entity
  - Enrolment policies
  - Key pair generation policies
- Creation and distribution of public key certificates
  - Enrolment policies
  - Definition of certificate attributes
- Definition and use of certification chains (or paths)
  - Insertion in a certification hierarchy
  - Certification of other CAs
- Update, publication and consultation of CRLs
  - Policies for revoking certificates
  - Online CRL distribution services
  - Online OCSP services
- Use of data structures and protocols enabling inter-operation among components / services / people

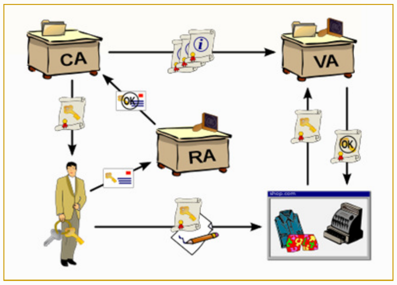
# PKI entities: Registration Authority (RA)



- The actual interface with certificate owners
  - Identification and authentication of certificate applicants
  - Approval or rejection of certificate applications
  - Initiating certificate revocations or suspensions under certain circumstances
  - Processing subscriber requests to revoke or suspend their certificates
  - Approving or rejecting requests by subscribers to renew or re-key their certificates

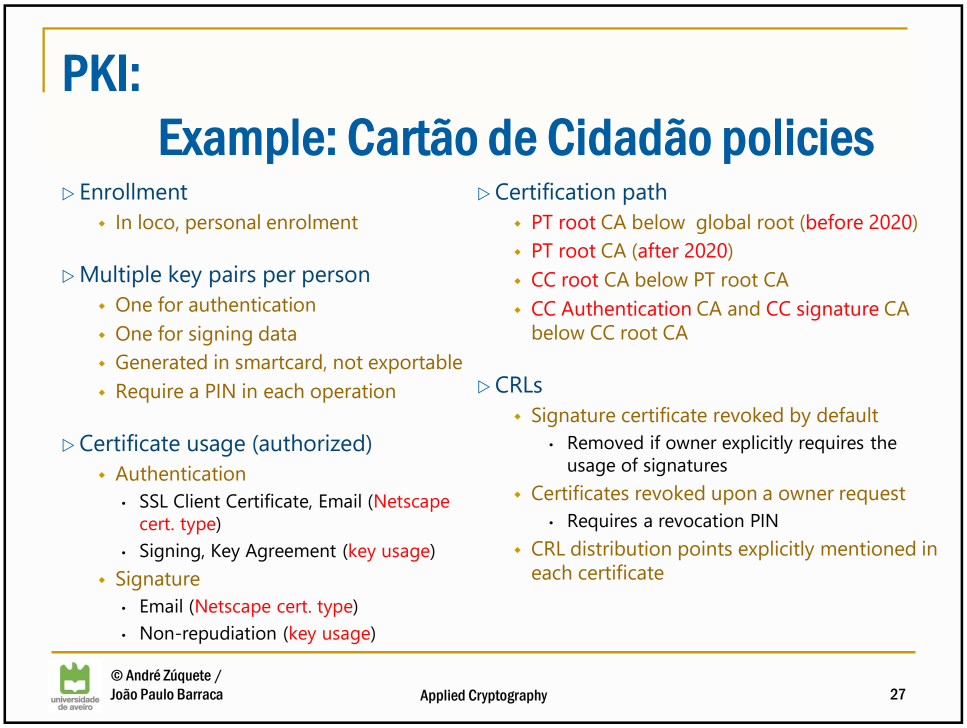
Image src: https://en.wikipedia.org/wiki/Public_key_infrastructure

# PKI entities: Validation Authority (VA)



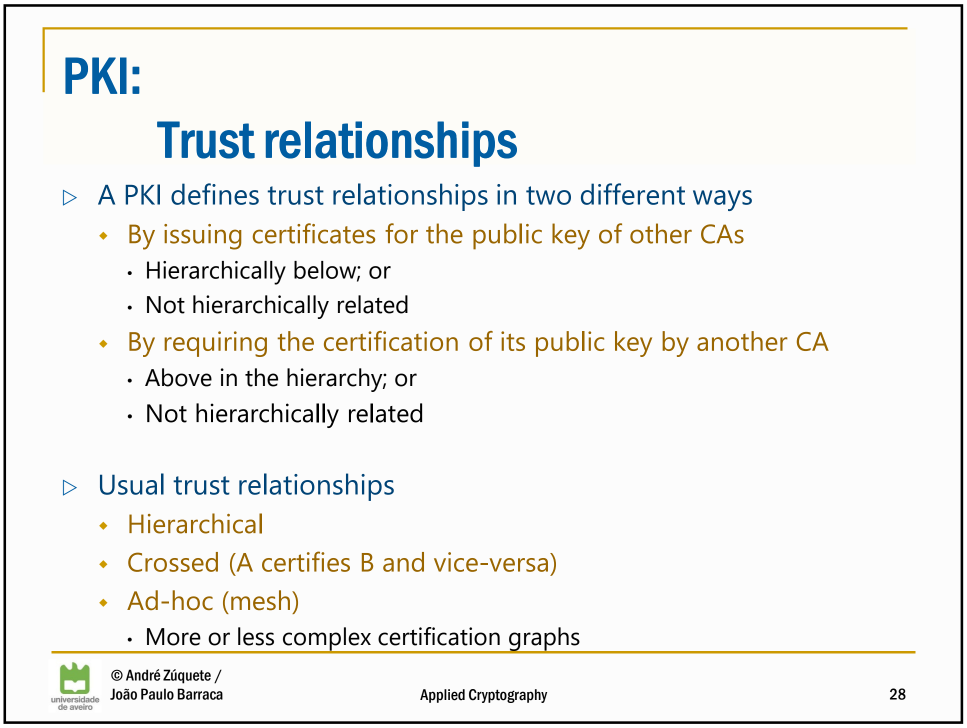
- A service that helps to validate certificates
  - OCSP service

Image src: https://en.wikipedia.org/wiki/Public_key_infrastructure



# PKI:
## Example: Cartão de Cidadão policies

- ▷ Enrollment
  - In loco, personal enrolment
- ▷ Multiple key pairs per person
  - One for authentication
  - One for signing data
  - Generated in smartcard, not exportable
  - Require a PIN in each operation
- ▷ Certificate usage (authorized)
  - Authentication
    - SSL Client Certificate, Email (Netscape cert. type)
    - Signing, Key Agreement (key usage)
  - Signature
    - Email (Netscape cert. type)
    - Non-repudiation (key usage)
- ▷ Certification path
  - PT root CA below  global root (before 2020)
  - PT root CA (after 2020)
  - CC root CA below PT root CA
  - CC Authentication CA and CC signature CA below CC root CA
- ▷ CRLs
  - Signature certificate revoked by default
    - Removed if owner explicitly requires the usage of signatures
  - Certificates revoked upon a owner request
    - Requires a revocation PIN
  - CRL distribution points explicitly mentioned in each certificate

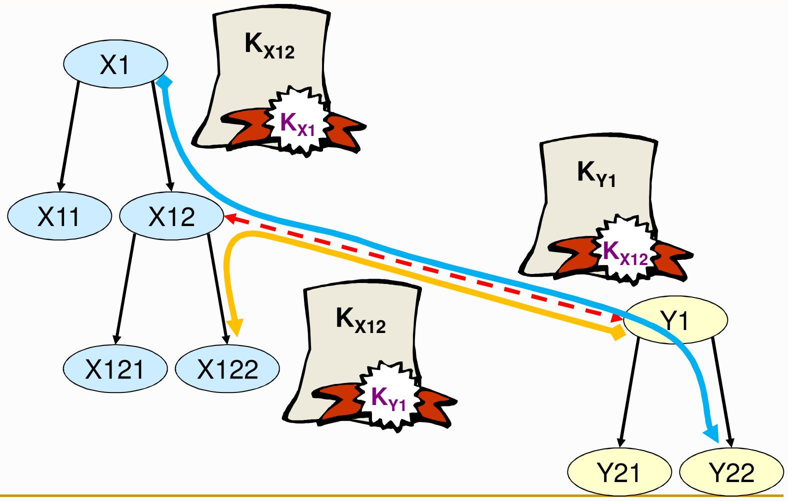


# PKI:
## Trust relationships

- ▷ A PKI defines trust relationships in two different ways
  - By issuing certificates for the public key of other CAs
    - Hierarchically below; or
    - Not hierarchically related
  - By requiring the certification of its public key by another CA
    - Above in the hierarchy; or
    - Not hierarchically related
- ▷ Usual trust relationships
  - Hierarchical
  - Crossed (A certifies B and vice-versa)
  - Ad-hoc (mesh)
    - More or less complex certification graphs

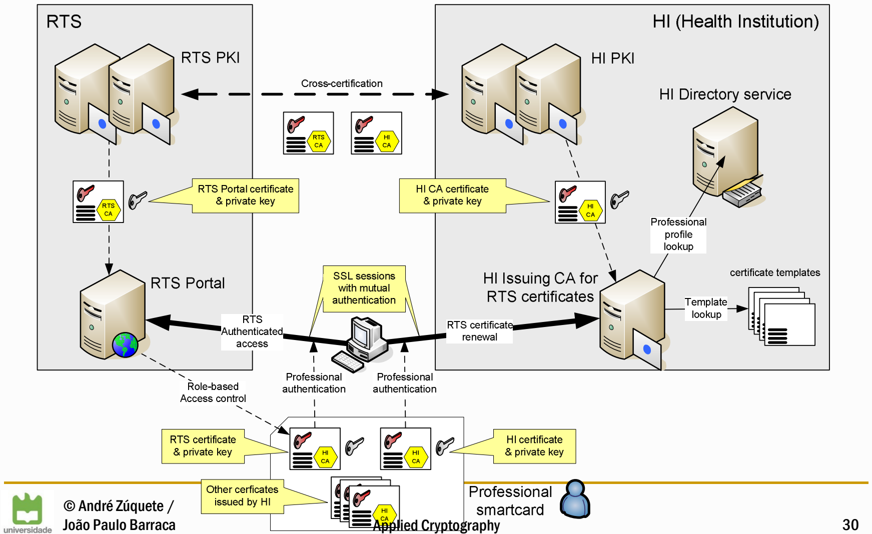
# PKI:

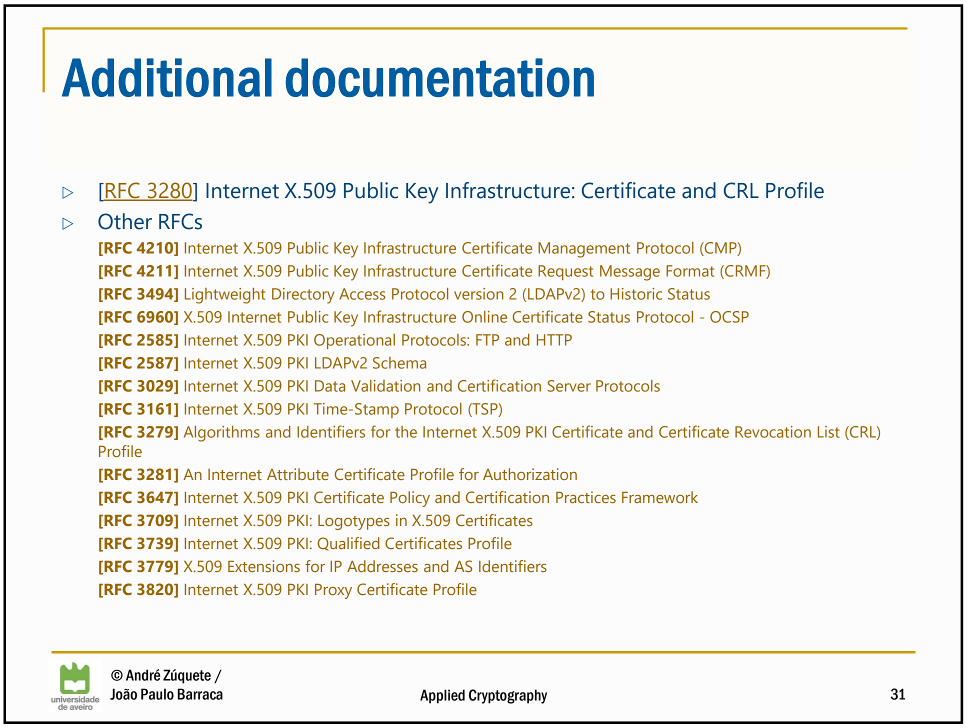
## Hierarchical and crossed certifications



# Cross-certification of PKIs:

## A practical example


RTS
RTS PKI
Cross-certification
RTS CA
HI CA
RTS Portal certificate & private key
RTS CA
RTS Portal
HI (Health Institution)
HI PKI
HI Directory service
HI CA certificate & private key
HI CA
Professional profile lookup
HI Issuing CA for RTS certificates
certificate templates
Template lookup
SSL sessions with mutual authentication
RTS Authenticated access
RTS certificate renewal
Professional authentication
Professional authentication
Role-based Access control
RTS certificate & private key
HI CA
HI CA
HI certificate & private key
Other cerficates issued by HI
HI CA
Professional smartcard



# Additional documentation

- [RFC 3280] Internet X.509 Public Key Infrastructure: Certificate and CRL Profile
- Other RFCs

**[RFC 4210]** Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
**[RFC 4211]** Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)
**[RFC 3494]** Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status
**[RFC 6960]** X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
**[RFC 2585]** Internet X.509 PKI Operational Protocols: FTP and HTTP
**[RFC 2587]** Internet X.509 PKI LDAPv2 Schema
**[RFC 3029]** Internet X.509 PKI Data Validation and Certification Server Protocols
**[RFC 3161]** Internet X.509 PKI Time-Stamp Protocol (TSP)
**[RFC 3279]** Algorithms and Identifiers for the Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile
**[RFC 3281]** An Internet Attribute Certificate Profile for Authorization
**[RFC 3647]** Internet X.509 PKI Certificate Policy and Certification Practices Framework
**[RFC 3709]** Internet X.509 PKI: Logotypes in X.509 Certificates
**[RFC 3739]** Internet X.509 PKI: Qualified Certificates Profile
**[RFC 3779]** X.509 Extensions for IP Addresses and AS Identifiers
**[RFC 3820]** Internet X.509 PKI Proxy Certificate Profile