Protezione e Sicurezza nei Sistemi Operativi:

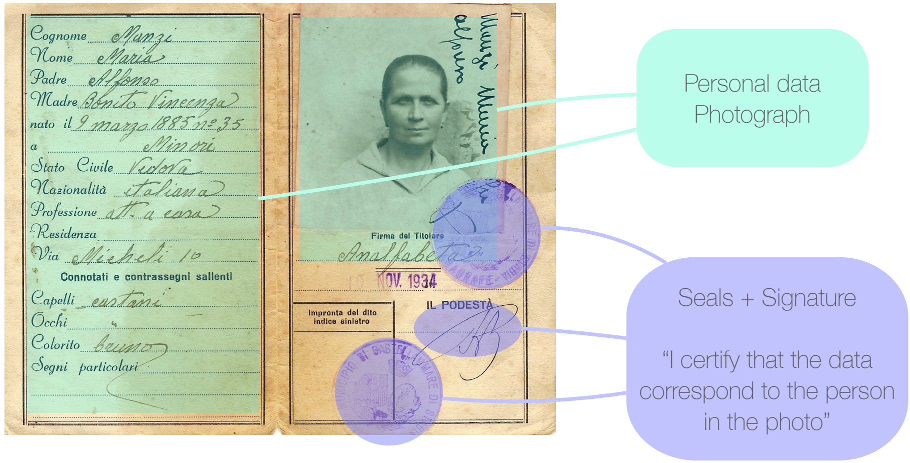
Certificates, Certification Authorities and Public-Key Infrastructures

Ozalp Babaoglu

(Digital) Certificates

- We need to be sure that the public key used to encrypt a message indeed belongs to the destination of the message
- Distributing public keys in a naive manner is subject to possible *man-in-the-middle attacks*
- Distributing public keys using digital *certificates* prevents an intruder from impersonating someone else by substituting their public key

Certificates in the physical world



Cognome Manzi
Nome Maria
Padre Alfonso
Madre Bonito Vincenza
nato il 9 marzo 1885 n° 35
a Minori
Stato Civile Vedova
Nazionalità italiana
Professione att. a casa
Residenza
Via Micheli 10

Connotati e contrassegni salienti

Capelli castani
Occhi "
Colorito bruno
Segni particolari

Manzi Maria alfonso

Firma del Titolare

Analfabeta

10 NOV. 1934

Impronta del dito indice sinistro

IL PODESTÀ

MUNICIPIO DI CASTELLAMMARE DI STABIA

Personal data
Photograph

Seals + Signature

"I certify that the data correspond to the person in the photo"

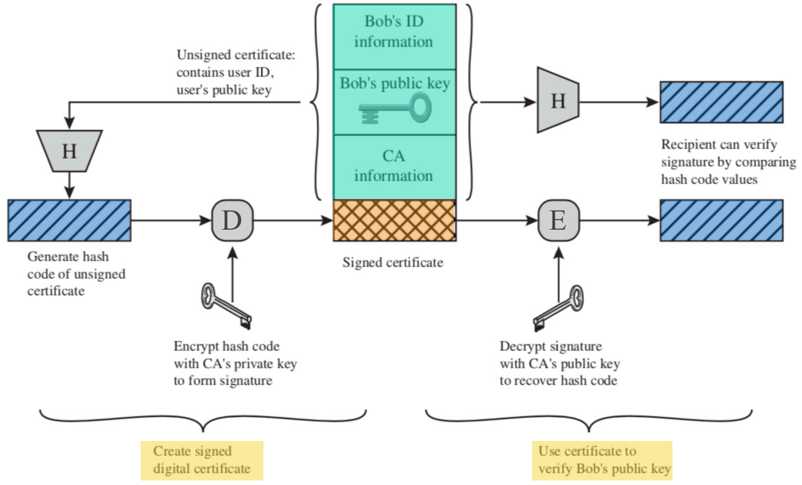
Certificates in the digital world

- Today, we have many examples of *digital certificates* such as the Covid-19 Green Pass
- The autograph signature of the trusted issuer is replaced with their *digital signature*
- Use of the certificate requires that it be *validated* by making sure that it has not expired and that the signature belongs to an entity that is considered and *authority*

Digital Certificates

- In asymmetric cryptography, a digital *certificate* is the form in which public keys are communicated
- It is a ***binding*** between a ***public key*** and ***identity information*** about a subject
- It is ***signed*** by a trusted issuer (CA: ***certification authority***)
- Functions much like a physical certificate
- Avoids *man-in-the-middle* attacks

Digital Certificate use


Unsigned certificate: contains user ID, user's public key
Bob's ID information
Bob's public key
CA information
H
H
Generate hash code of unsigned certificate
D
Signed certificate
E
Recipient can verify signature by comparing hash code values
Encrypt hash code with CA's private key to form signature
Decrypt signature with CA's public key to recover hash code
Create signed digital certificate
Use certificate to verify Bob's public key

Digital Certificate properties

- Any participant can ***read*** a certificate to determine the name and public key of the certificate's owner
- Any participant can ***validate*** a certificate to determine that it originated from a certification authority, that it is not a counterfeit and that it has not expired
- Only the certification authority can ***create*** or ***update*** certificates

X.509 Certificates

X.509 is a standard that specifies digital certificates with the following fields:

Subject: Distinguished Name, Public Key

Issuer: Distinguished Name, Signature

Validity: Not Before Date, Not After Date

Administrative Info: Version, Serial Number

Extended Info: …

X.509 Certificates

- *Distinguished Name Fields* as defined by X.509 Standard

Common Name	CN=Kenneth Lay
Organization or Company	O=Enron
Organizational Unit	OU=Management
City/Locality	L=Houston
State/Province	ST=Texas
Country (ISO Code)	C=US

Certification Authority

- *Certification Authority* (CA) is responsible for ***certification***, ***validation*** and ***revocation*** of certificates
- Many different types of CAs exist: commercial, government, free, etc.
- Examples of CAs: VeriSign, Symantec, GoDaddy, Geotrust, Visa, Actalis, Comodo, Thawte, Taiwan GRCA

Public Key Infrastructure

- The collection of hardware, software, people, policies, and protocols needed to create, manage, store, distribute, and revoke digital certificates constitutes a ***Public Key Infrastructure*** (PKI)

PKI – Certification

- The *subject* generates a (private, public) key pair
- Asks a CA that the (subject_ID, public_key) be certified and transformed into a *certificate*
- The CA ***authenticates*** the subject by verifying that the ID indeed belongs to her
- CA generates the signature for (subject_ID, public_key) using CA's private key
- CA attaches the signature to (subject_ID, public_key) to create the certificate
- CA returns the certificate to the subject (and anyone else who needs it)

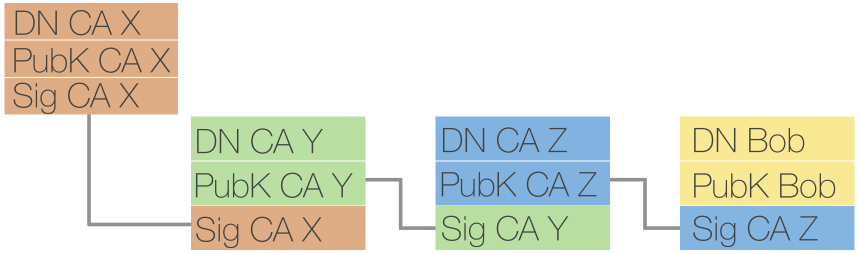
PKI – Authentication

- Out-of-band authentication:
  - performed using traditional methods, such as mail, fax, telephone or face-to-face meeting
- In-band authentication:
  - performed using the PKI itself
  - possible only for certain types of certificates where the ***identity information*** (e.g. email addresses) can indeed be verified

PKI – Certification Authorities

- The certification process is based on trust
  - Users trust the issuing authority to issue only certificates that correctly associate subjects to their public keys
- Only one CA for the entire world?
  - No — would be impractical
- Instead:
  - Most PKI allow one CA to certify another CA
  - One CA is telling its users that they can trust what a second CA says in its certificates

PKI – Certificate Chains



DN CA X
PubK CA X
Sig CA X

DN CA Y
PubK CA Y
Sig CA X

DN CA Z
PubK CA Z
Sig CA Y

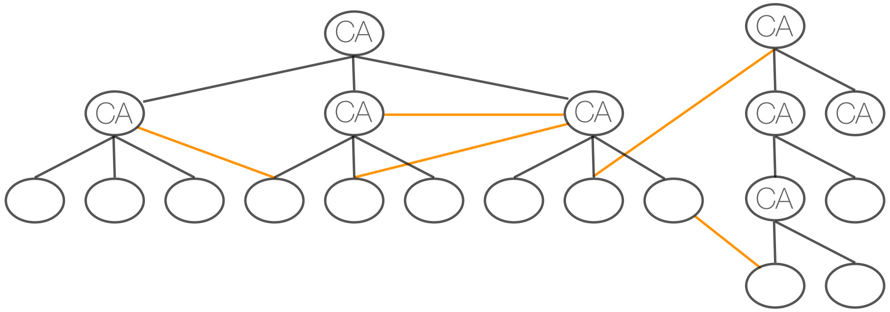
DN Bob
PubK Bob
Sig CA Z

PKI – Certificate Chains

- Certificate chains can be of arbitrary length
- Each certificate in the chain is ***validated*** by the preceding one until the root certificate (which is self validated) is reached
- Different certificates:
  - “Leaf” certificates (end-user)
  - “Intermediate” certificates
  - “Root” certificates

PKI – CA Hierarchies

- CAs can be organized
  - as a rooted tree (X.509)
  - as a general graph (PGP)



Hierarchical Trust (X.509)

- Based on chains of trust forming a rooted tree among entities that are reputed to be CAs
- The (blind) trust we place on root-level CAs must be acquired through reputation, experience, operational competence and other non-technical aspects
- Anyone claiming to be a CA must be a trusted entity and we must believe that it is secure and correct

Web of Trust (PGP)

- In PGP, any user can act as a CA and sign the public key of another user
- A public key is considered valid only if a sufficient number of trusted users have signed it
- As the system evolves, complex trust relations emerge to create a dynamic “web”
- Trust need not be *symmetric* or *transitive*
- (more on PGP later)

PKI – Validation

- *Validation* — need to control that the certificate
  - Is ***current*** — within “not before” and “not after” dates,
  - Has been ***signed*** by a root CA or there is a chain that leads to a root CA,
  - Has not been ***tampered*** with
  - Has not been ***revoked***
- Checking *currency, signature* and *tampering* can be done locally and off-line by the certificate user (like in the *VerificaC19* App for the Green Pass)
- Checking if the certificate has been *revoked* is more complicated

PKI – Revocation

- *Revocation* — the process of breaking the binding between a public key and a subject for various reasons
  - subject’s private key becomes compromised
  - subject identifier information changes (name, URL, email address)
- Since certificates are handed out to clients, it is impossible to physically recall them back
- Revocation can only insert the certificate to be revoked in a *list* of revoked certificates

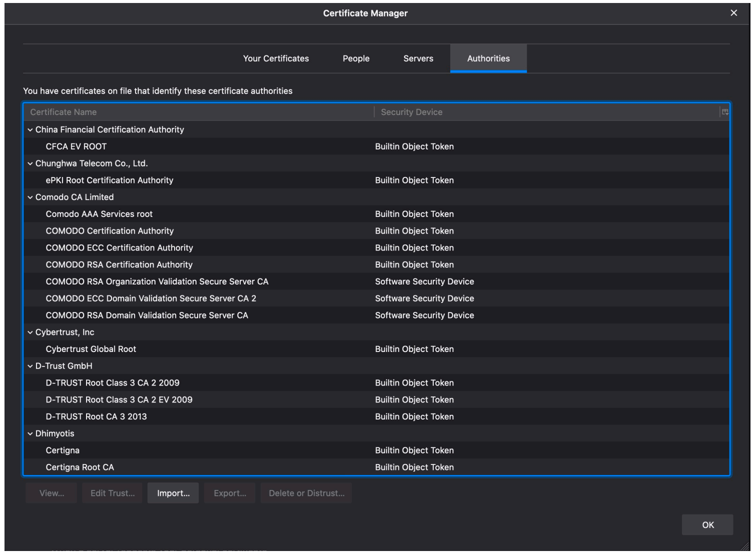
PKI – Revocation

- Controlling if a certificate has been revoked during validation can be performed either
  - On-line
    - consult the centralized database of all revoked certificates
    - *Online Certificate Status Protocol* (OCSP) of X.509 describes how to check validity and revoke certificates
  - Off-line
    - consult a “local copy” of the revoked certificates database
    - since the local copy can be “out-of-date” (missing some recent revocations), there is the risk of validating a certificate (while it is current) that has been revoked

PKI – Revocation

- Certificate Revocation List (CRL)
  - a list of revoked certificate ids constructed, signed and periodically distributed by the CA
  - user must check the latest CRL during validation to make sure that a certificate has not been revoked
  - X.509 includes a CRL profile, describing the format of CRLs
- CRL Problems
  - CRL time-granularity problem — how often to issue CRLs?
  - CRL size — incremental versus bulk

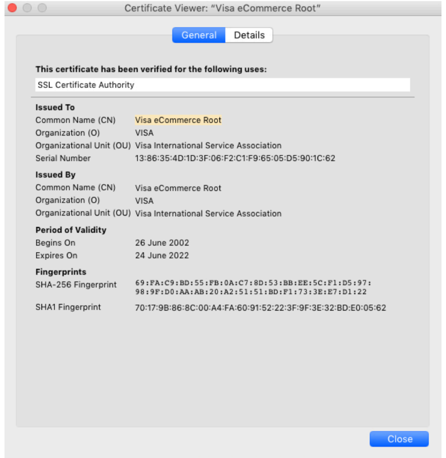
Certificates in Practice: Firefox



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
⌄ China Financial Certification Authority	
CFCA EV ROOT	Builtin Object Token
⌄ Chunghwa Telecom Co., Ltd.	
ePKI Root Certification Authority	Builtin Object Token
⌄ Comodo CA Limited	
Comodo AAA Services root	Builtin Object Token
COMODO Certification Authority	Builtin Object Token
COMODO ECC Certification Authority	Builtin Object Token
COMODO RSA Certification Authority	Builtin Object Token
COMODO RSA Organization Validation Secure Server CA	Software Security Device
COMODO ECC Domain Validation Secure Server CA 2	Software Security Device
COMODO RSA Domain Validation Secure Server CA	Software Security Device
⌄ Cybertrust, Inc	
Cybertrust Global Root	Builtin Object Token
⌄ D-Trust GmbH	
D-TRUST Root Class 3 CA 2 2009	Builtin Object Token
D-TRUST Root Class 3 CA 2 EV 2009	Builtin Object Token
D-TRUST Root CA 3 2013	Builtin Object Token
⌄ Dhimyotis	
Certigna	Builtin Object Token
Certigna Root CA	Builtin Object Token

Certificates in Practice: Firefox



Certificate Viewer: “Visa eCommerce Root”

This certificate has been verified for the following uses:

SSL Certificate Authority

Issued To

Common Name (CN)	Visa eCommerce Root
Organization (O)	VISA
Organizational Unit (OU)	Visa International Service Association
Serial Number	13:86:35:4D:1D:3F:06:F2:C1:F9:65:05:D5:90:1C:62

Issued By

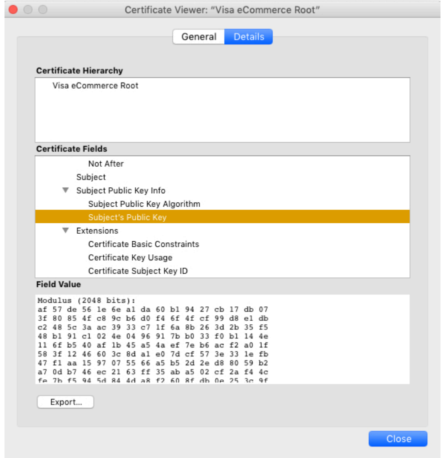
Common Name (CN)	Visa eCommerce Root
Organization (O)	VISA
Organizational Unit (OU)	Visa International Service Association

Period of Validity

Begins On	26 June 2002
Expires On	24 June 2022

Fingerprints

SHA-256 Fingerprint	69:FA:C9:BD:55:FB:0A:C7:8D:53:BB:EE:5C:F1:D5:97: 98:9F:D0:AA:AB:20:A2:51:51:BD:F1:73:3E:E7:D1:22
SHA1 Fingerprint	70:17:9B:86:8C:00:A4:FA:60:91:52:22:3F:9F:3E:32:BD:E0:05:62



Certificate Viewer: “Visa eCommerce Root”

Certificate Hierarchy

Visa eCommerce Root

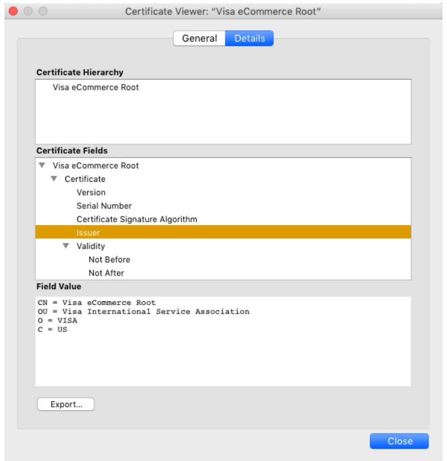
Certificate Fields

```
        Not After
      Subject
    ▼ Subject Public Key Info
        Subject Public Key Algorithm
        Subject's Public Key
    ▼ Extensions
        Certificate Basic Constraints
        Certificate Key Usage
        Certificate Subject Key ID
```

Field Value

```
Modulus (2048 bits):
af 57 de 56 1e 6e a1 da 60 b1 94 27 cb 17 db 07
3f 80 85 4f c8 9c b6 d0 f4 6f 4f cf 99 d8 e1 db
c2 48 5c 3a ac 39 33 c7 1f 6a 8b 26 3d 2b 35 f5
48 b1 91 c1 02 4e 04 96 91 7b b0 33 f0 b1 14 4e
11 6f b5 40 af 1b 45 a5 4a ef 7e b6 ac f2 a0 1f
58 3f 12 46 60 3c 8d a1 e0 7d cf 57 3e 33 1e fb
47 f1 aa 15 97 07 55 66 a5 b5 2d 2e d8 80 59 b2
a7 0d b7 46 ec 21 63 ff 35 ab a5 02 cf 2a f4 4c
fe 7b f5 94 5d 84 4d a8 f2 60 8f db 0e 25 3c 9f
```

Certificates in Practice: Firefox



Certificate Viewer: “Visa eCommerce Root”

Certificate Hierarchy

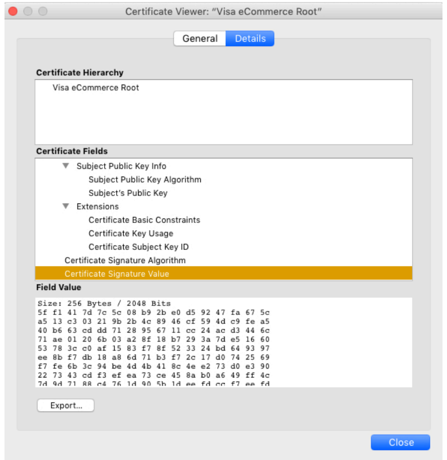
Visa eCommerce Root

Certificate Fields

```
▼ Visa eCommerce Root
  ▼ Certificate
      Version
      Serial Number
      Certificate Signature Algorithm
      Issuer
    ▼ Validity
        Not Before
        Not After
```

Field Value

```
CN = Visa eCommerce Root
OU = Visa International Service Association
O = VISA
C = US
```



Certificate Viewer: “Visa eCommerce Root”

Certificate Hierarchy

Visa eCommerce Root

Certificate Fields

```
    ▼ Subject Public Key Info
        Subject Public Key Algorithm
        Subject's Public Key
    ▼ Extensions
        Certificate Basic Constraints
        Certificate Key Usage
        Certificate Subject Key ID
  Certificate Signature Algorithm
  Certificate Signature Value
```

Field Value

```
Size: 256 Bytes / 2048 Bits
5f f1 41 7d 7c 5c 08 b9 2b e0 d5 92 47 fa 67 5c
a5 13 c3 03 21 9b 2b 4c 89 46 cf 59 4d c9 fe a5
40 b6 63 cd dd 71 28 95 67 11 cc 24 ac d3 44 6c
71 ae 01 20 6b 03 a2 8f 18 b7 29 3a 7d e5 16 60
53 78 3c c0 af 15 83 f7 8f 52 33 24 bd 64 93 97
ee 8b f7 db 18 a8 6d 71 b3 f7 2c 17 d0 74 25 69
f7 fe 6b 3c 94 be 4d 4b 41 8c 4e e2 73 d0 e3 90
22 73 43 cd f3 ef ea 73 ce 45 8a b0 a6 49 ff 4c
7d 9d 71 88 c4 76 1d 90 5b 1d ee fd cc f7 ee fd
```