STI
MEI/MIEBIOM

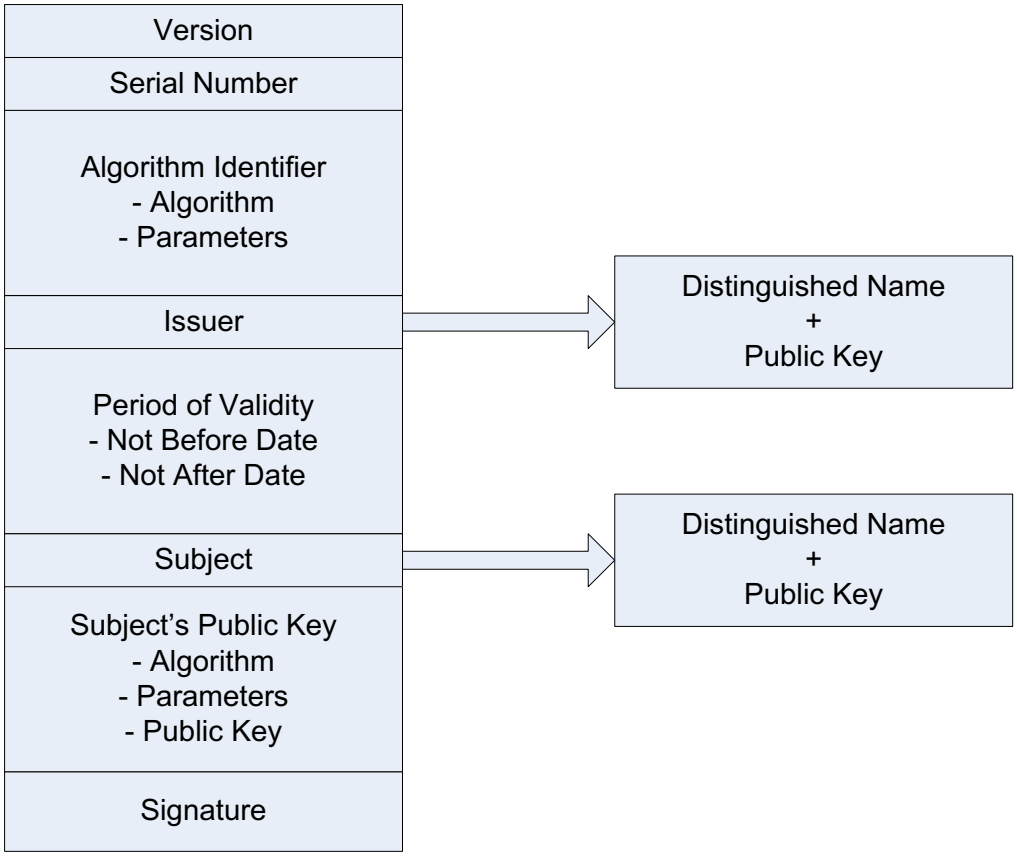
2022/2023

Practical class #2

- Certification authorities using OpenSSL
- Server and client authentication with Apache

X.509 Certificates

A X.509 certificate contains a public-key and also information about a real entity (Subject)



X.509 Certificates

Information about the entity is stored as a DN (Distinguished Name)

Common Name	CN	CN = Joao Luis
Organization	O	O = UC
Organizational Unit	OU	OU = DEI
City / Location	L	L =Coimbra
State / Province	ST	ST = Coimbra
Country	C	C = PT

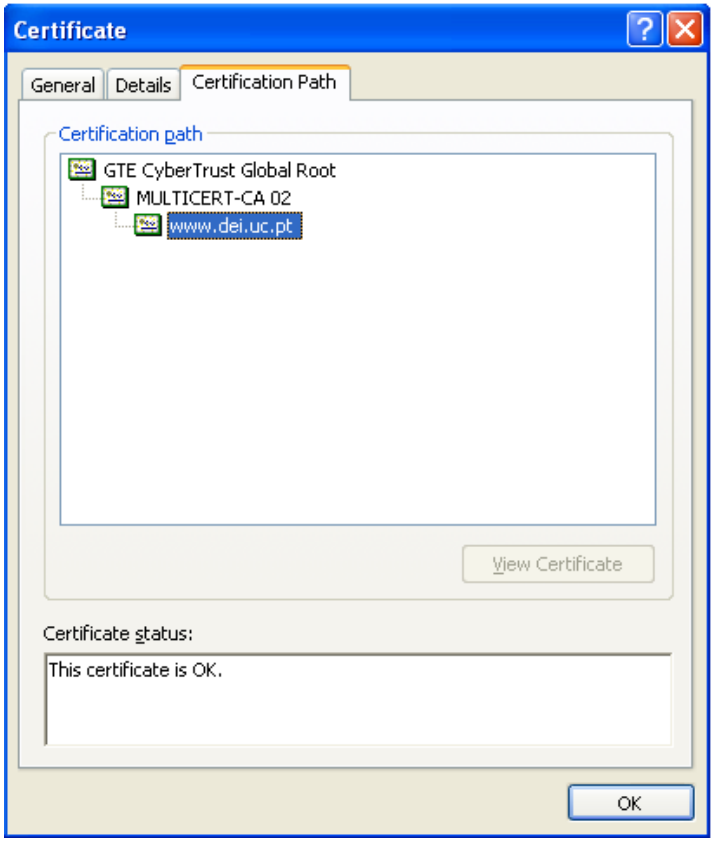
Certification Authorities

- **Verification of CSR (Certificate Signing Request)**
- **Public and Private CA (“self-signed”)**

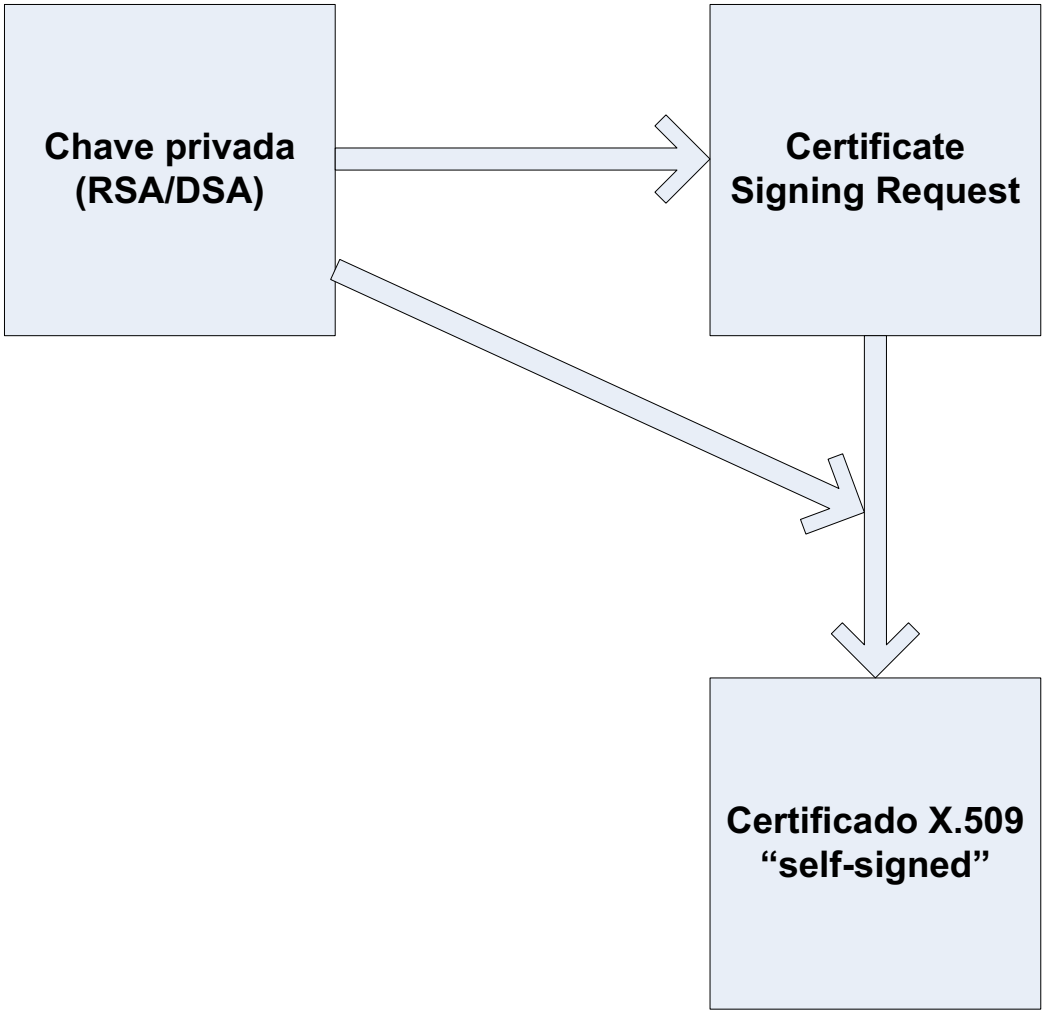
www.verisign.com

www.multicert.pt

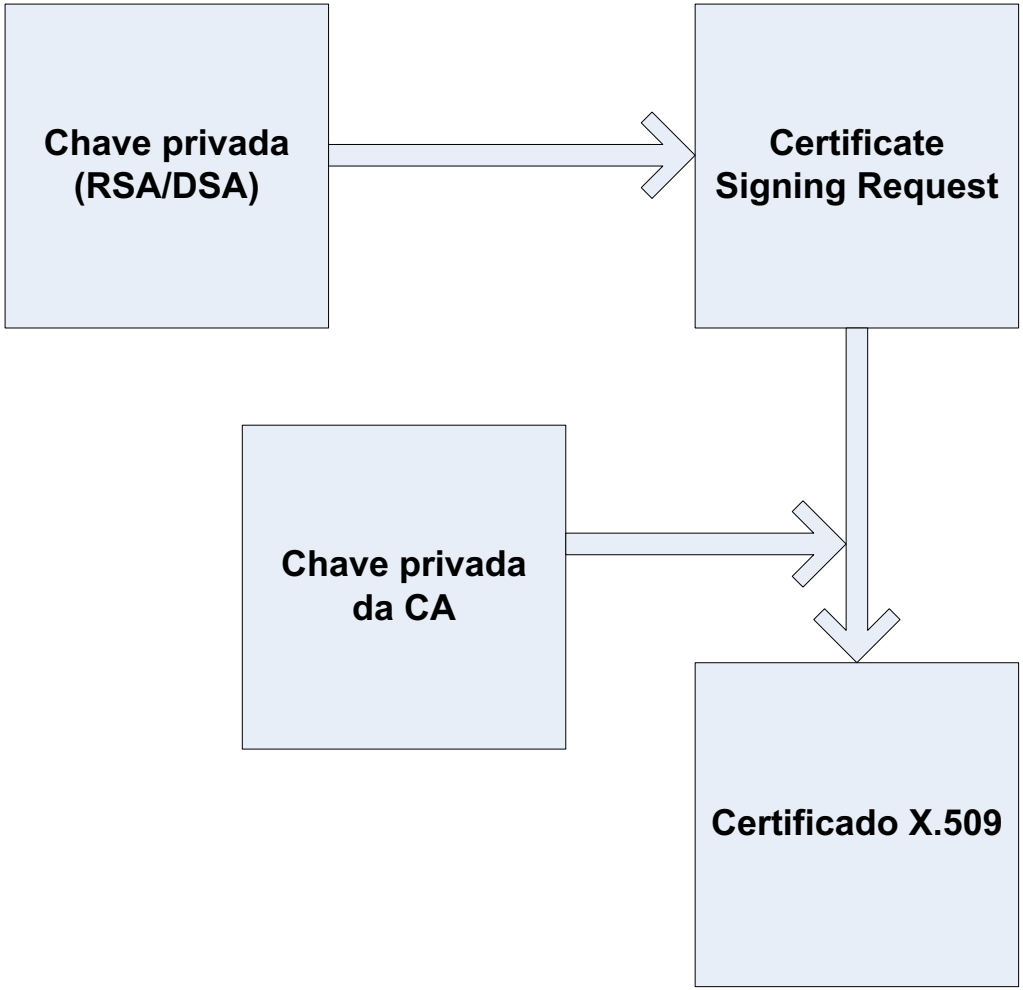
www.thawte.com



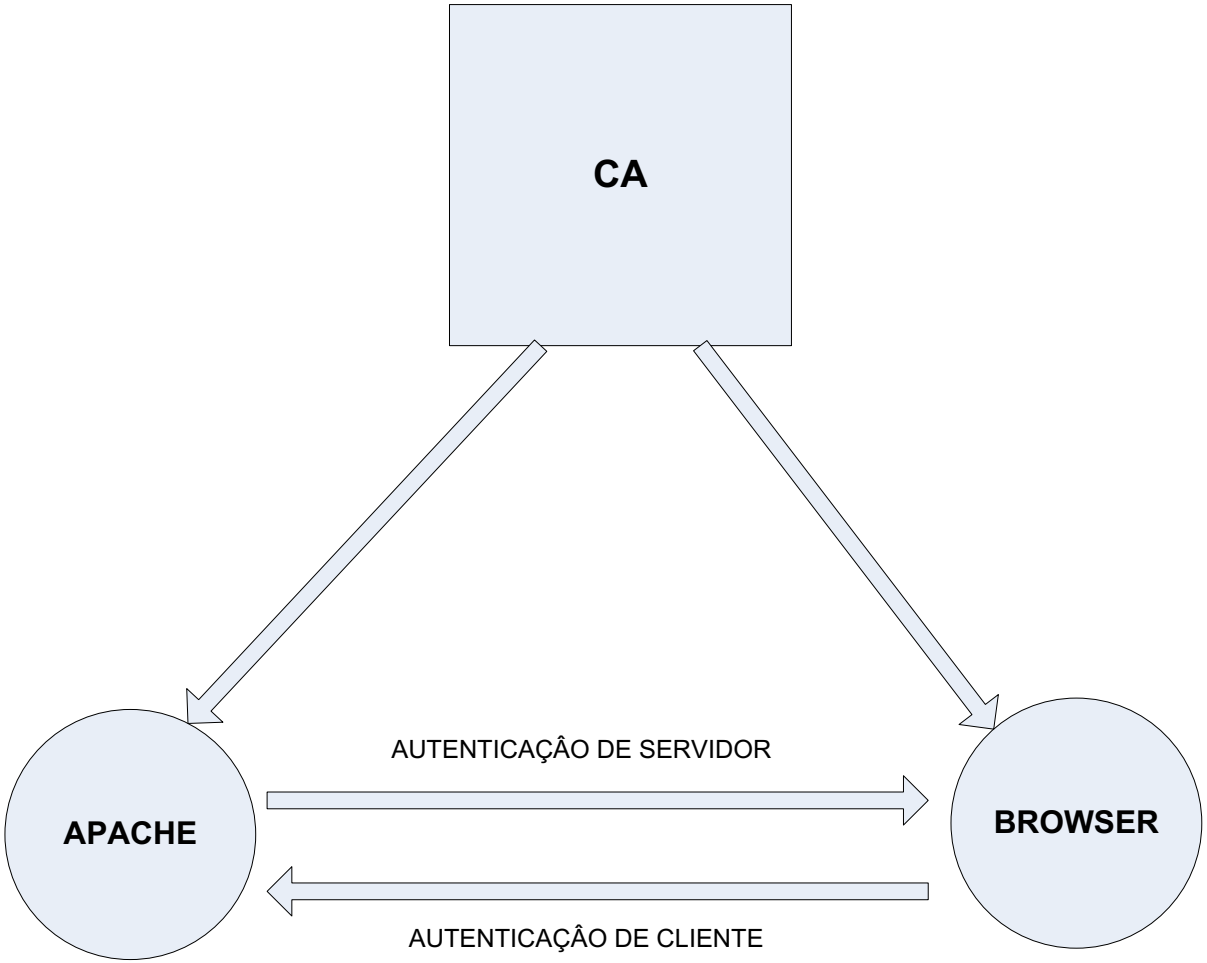
Private CA


Chave privada
(RSA/DSA)
Certificate
Signing Request
Certificado X.509
“self-signed”

Creation of a X.509 certificate



Authentication using X.509 certificates with Apache



Main configuration files (Apache, OpenSSL)

OpenSSL configuration:

/etc/pki/tls/openssl.cnf

Apache with SSL (mod_ssl):

/etc/httpd/conf/httpd.conf

/etc/httpd/conf.d/ssl.conf

OpenSSL usage examples

 # Creation of a 1024-bit public-key (RSA) encrypted with 3DES

openssl genrsa -out xpto.key 1024 -des3

 # Creation of a CSR

openssl req -new -key xpto.key -out xpto.csr

 # Creation of a "self-signed" certificate

openssl x509 -req -days 365 -in xpto.csr -out xpto.crt -signkey xpto.key

 # Viewing the contents of a certificate

openssl x509 -in xpto.crt -text

 # Creation of a x.509 certificate using an existing CA

openssl ca -in cert.csr -cert ca.crt -keyfile ca.key -out cert.crt

 # Converting from PEM to PKCS#12

openssl pkcs12 -export -clcerts -in xpto.crt -inkey xpto.key -out xpto.p12

 # Converting from PEM to DER

openssl x509 -inform PEM -in xpto.crt -outform DER -out xpto.crt.der