

# Public Key Infrastructure

Use of digital signatures in information security

Mihai-Lica Pura  
2020.03.18

# Topics

- ▶ **Information security**
  - Cryptography and its use for accomplishing the goals of information security:
    - Authentication
    - Confidentiality
    - Integrity
    - Non-repudiation
- ▶ **Electronic signatures vs. digital signatures**

# Topics

- ▶ **Symmetric cryptography**
  - Problem with sharing the key between the parties
- ▶ **Asymmetric cryptography**
  - Problem with trusting that a given public key belongs to a certain entity (person, server)
  - Speed problem
- ▶ Solving the speed problem
  - **Asymmetric cryptography for confidentiality**
    - Hybrid cryptography

# Topics

## ▶ Solving the trust problem

- Public Key Infrastructure
  - Certificate issuance flow
  - Trust flow
- Web of trust (PGP)
  - Same as above
- Identity based cryptography
  - Same as above

# Topics

- ▶ **Public Key Infrastructure**
- ▶ **Certificate issuance in PKI**
  - PKCS#12, PEM, DER, X509 v3, ASN.1, OID
- ▶ **Management of certificates in Microsoft Windows**
  - Windows certificate stores, certmgr.msc, mc.exe
- ▶ **Validation of a certificate**
  - Time validity
  - Revocation status
  - Trust
    - Certificate trust path
    - Self-signed CA certificates
    - Microsoft Trusted Root Certificate Program
    - Mozilla CA Certificate Policy

# Topics

- ▶ **Certificate revocation**
  - CRL, OCSP
- ▶ **Certificate search**
  - CA web page manual search, LDAP
- ▶ **Performing a digital signature**
  - Using Microsoft CNG API through certificate stores
    - flow
  - Using PKCS#11
    - flow
  - Remote/cloud/mobile through Cloud Signature Consortium signing protocol
    - flow

# Topics

- ▶ E-signature vs. e-seal
- ▶ Use of digital signed documents
  - ANAF
  - CNAS
  - ONRC
  - UNNPR
  - ITM
  - MySMIS 2014
  - MO
  - etc.

# Topics

- ▶ **Digital signing documents**
  - **Qualified Electronic Signatures**
    - PDF (Adobe Acrobat Reader)
      - Signing PDF files
      - Signing PDF forms with a digital signature field
    - Microsoft Office documents (Microsoft Office software)
    - PKCS#7 (DeskSeal, Prosigner, etc.)
      - Attached, detached, cosignatures
    - XMLDSig
  - **Advanced Electronic Signatures**
    - CAdES, PAdES, XAdES
  - **Time stamping of digital signatures**

# Topics

- ▶ **Digital signing code**
  - Java applets (obsolete)
  - Java Web Start (signed jars for JNLP)
  - Macros (Microsoft Office)
  - Microsoft software installation packages
- ▶ **Digital signing for authentication**
  - Certificate login
- ▶ **Cryptography APIs**
  - High level
  - low level

# The trust problem

- ▶ Asymmetric key cryptography based on two keys:
  - a public key known to anybody,
  - a private key known only by the owner of the pair
  - the two keys are in a mathematical relation
- ▶ How to be sure that a public key really belongs to a certain person or entity?
- ▶ Solutions:
  - Based on certificates
    - 1. Public Key Infrastructure
    - 2. Web of Trust
  - Certificateless
    - Identity based Cryptography

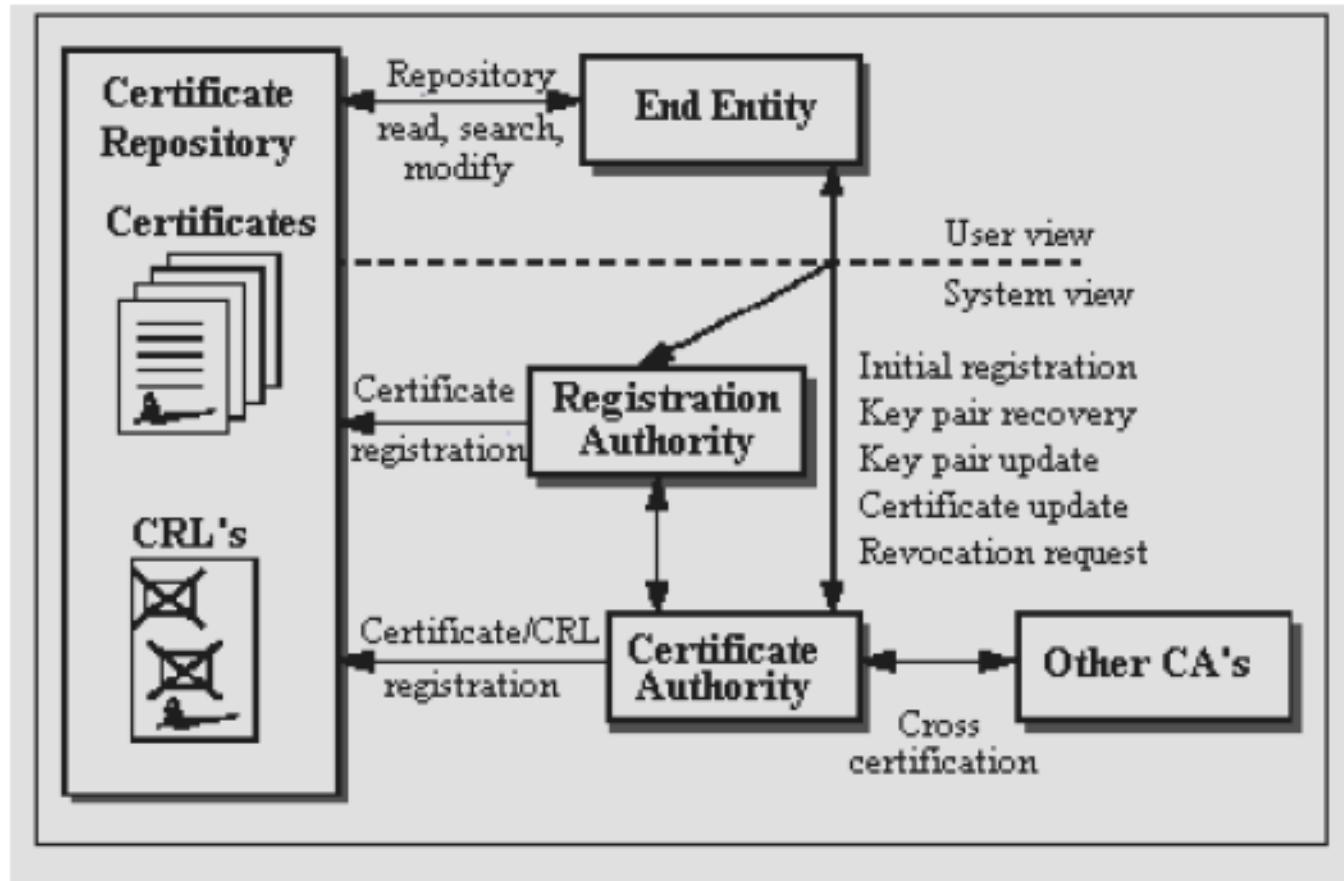
# The trust problem

- ▶ PKI solution
- ▶ The public key is bounded to the identity of the owner through a Certificate Authority (CA)
- ▶ The CA guarantees the identity of the owner of the public key
- ▶ The element that securely proves this bound is the digital certificate

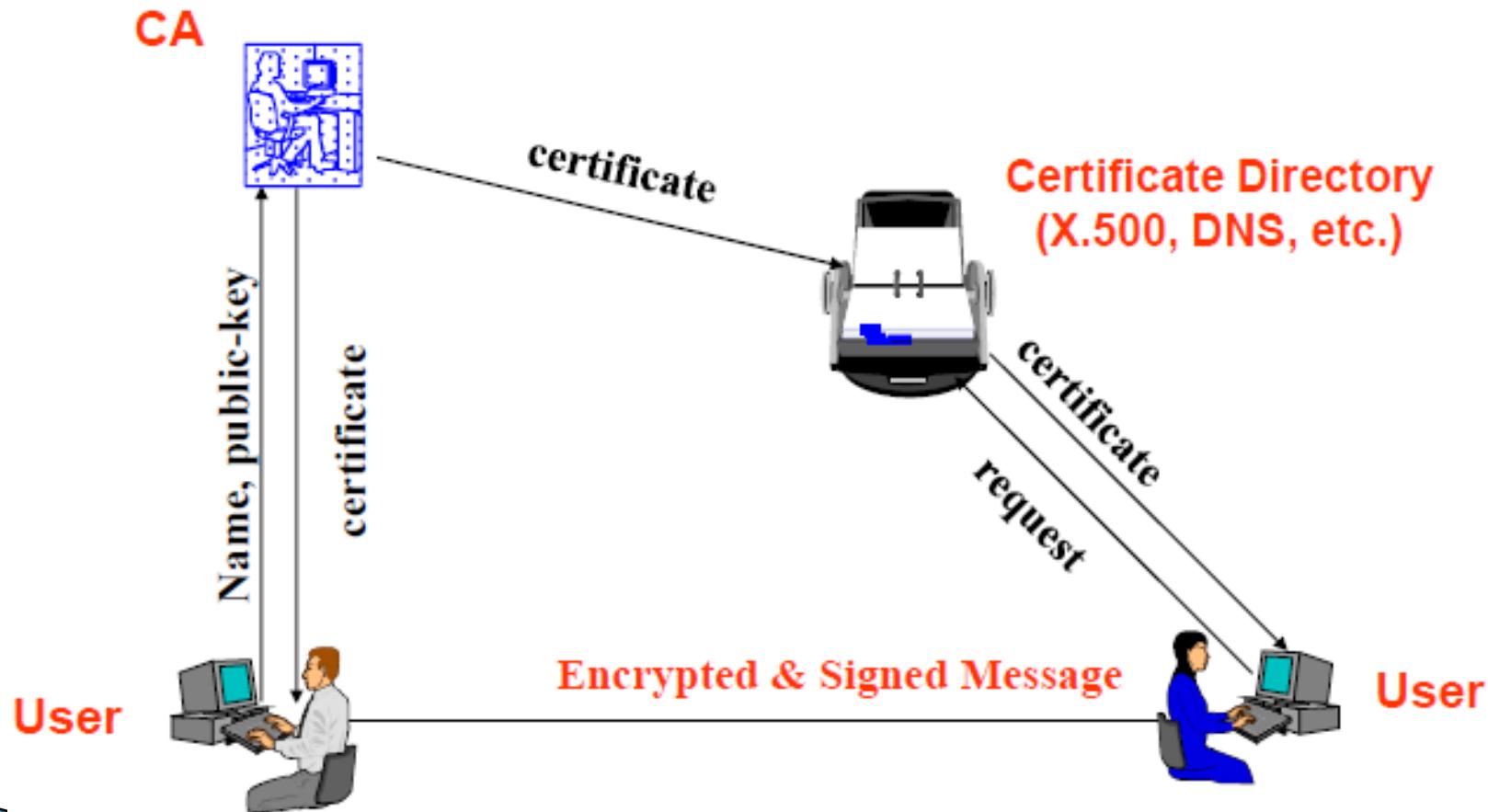
# Public Key Infrastructure

- ▶ PKI
  - set of components (hardware and software) that work together for using public-key technology in a secure manner
- ▶ Components of a PKI
  - The end-entities (EE)
  - The certificate authority (CA)
  - The certificate repository (CR)
  - The registration authority (RA)
  - Digital certificates

# Public Key Infrastructure



# Public Key Infrastructure



# End-entity

- ▶ is defined as a user of PKI certificate and/or end-user system that is the subject of a certificate
- ▶ is a generic term for a subject that uses some services or functions of the PKI system, which may be
  - a certificate owner (human being or organization or some other entities)
  - a requestor (it might be application program) for certificate or CRL

# Certificate Authority

- ▶ CA
  - a trusted authority
  - central administration
  - provides a statement (the digital certificate) that the enclosed public key belongs to the specified entity
    - organization/company to its employees
    - university to its students
    - public CAs to their clients
- ▶ Primary operations
  - certificate issuance
  - certificate renewal
  - certificate revocation

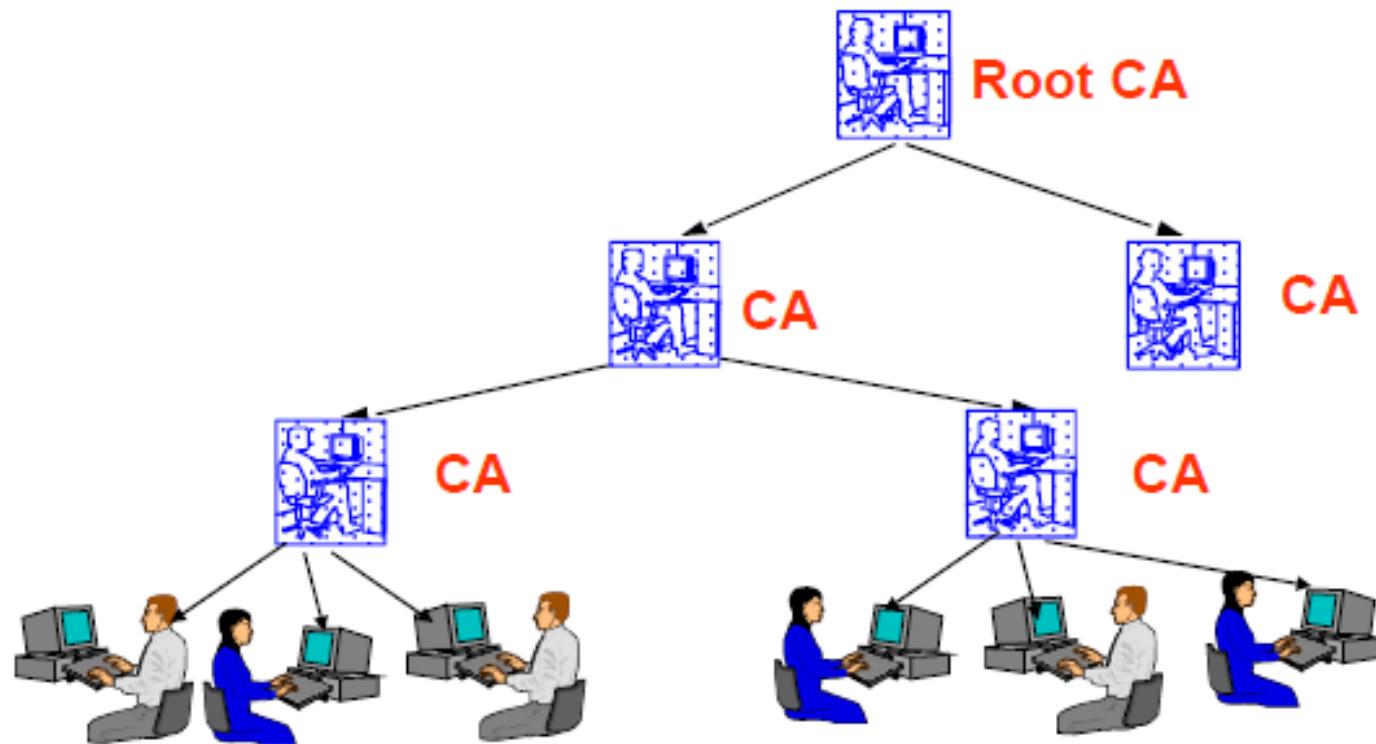
# Certificate Authority

- ▶ Original intent was to certify that a public key really did belong to a given entity
- ▶ Role was later expanded to certify all sorts of other things
  - Are they a bona fide business?
  - Can you trust their web server?
  - Can you trust the code they write?
  - Is their account in good standing?
  - Are they over 18?

# Certificate Authority Hierarchy

- ▶ Each CA issues certificates to its users community
  - *Root-CA* is used to establish TRUST between communities
  - Root certificates (self-signed) are installed/configured as trusted points

# Certificate Authority Hierarchy



# Registration Authority

- ▶ An optional component in a PKI
  - The CA can incorporate the role of an RA
- ▶ When used, the RA is
  - a trusted end-entity certified by the CA
  - acting as a subordinate server of the CA
- ▶ The CA can delegate some of its management functions to the RA
  - personal authentication tasks
  - generate keys
  - archive key pairs
- ▶ The RA, however, does not issue certificates or CRLs

# Certificate Repository

- ▶ Store for certificates and CRLs
- ▶ X.509 certificate format fit to an X.500 directory
- ▶ Best implemented as a directory accessed by Lightweight Directory Access Protocol (LDAP)
- ▶ CR can be accessed with LDAP commands or procedures (bind, search, modify, unbind)

# How to obtain a digital certificate (qualified)

- ▶ <http://www.transped.ro/>
- ▶ <http://ca.transped.ro/Index.aspx?Document=enrol>
- ▶ [http://ca.transped.ro/Index.aspx?Document=UA\\_Form](http://ca.transped.ro/Index.aspx?Document=UA_Form)

# Free digital certificates

- ▶ Getting a free S/MIME digital certificate (personal)
- ▶ [http://kb.mozilla.org/Getting\\_an\\_SMIME\\_certificate](http://kb.mozilla.org/Getting_an_SMIME_certificate)
- ▶ Getting a free SSL/TLS digital certificate (server)
- ▶ <https://geekflare.com/free-ssl-tls-certificate/>

# Free digital certificates (S/MIME)

- ▶ SECTIGO (formerly COMODO CA)
- ▶ <https://www.instantssl.com/ssl-certificate-products/free-email-certificate.html>
- ▶ Actalis
- ▶ <https://www.actalis.it/products/certificates-for-secure-electronic-mail.aspx>

# Free digital certificates (S/MIME)

- ▶ WoSign
  - ▶ [https://www.wosign.com/english/Free\\_Email\\_Certificate.htm](https://www.wosign.com/english/Free_Email_Certificate.htm)
- ▶ GlobalSign
  - ▶ <https://www.globalsign.com/en/personalsign/>
- ▶ secorio
  - ▶ [https://www.secorio.com/en/?S\\_MIME\\_Email\\_Certificates](https://www.secorio.com/en/?S_MIME_Email_Certificates)

# Free digital certificates (S/MIME)

- ▶ Tutorials – COMODO
- ▶ <https://fastersolutions.com/wp-lib/wp-content/uploads/2015/07/comodoinstructions.pdf>
- ▶ <https://support.postbox-inc.com/hc/en-us/articles/202200540-Obtaining-an-S-MIME-Certificate-to-Sign-Emails>
- ▶ <https://www.netwoven.com/2015/07/07/secure-encrypt-emails-in-outlook-with-a-digital-id-certificate/>

# Free digital certificates (SSL/TLS)

- ▶ COMODO
- ▶ <https://ssl.comodo.com/free-ssl-certificate.php>
  
- ▶ Let's encrypt
- ▶ <https://letsencrypt.org/>
- ▶ <https://www.sslforfree.com/>
  
- ▶ ZeroSSL
- ▶ <https://zerossl.com/>

# How to obtain a digital certificate (for testing)

▶ <https://www.certsign.ro>

28-01-2010

Certificatul de server Web emis de certSIGN  
- de încredere pentru cel mai important browser  
Open Source

27-01-2010

Ucraina a ales certSIGN ca furnizor de carduri

## Resurse

- ▶ Ce este un certificat digital?
- ▶ Cum se obtine un certificat digital calificat?
- ▶ Ce este o semnatura electronică extinsă?
- ▶ Ce este un certificat SSL?
- ▶ Cum poti verifica semnatura electronică și marcarea temporală a documentelor?
- ▶ Ce este semnatura electronică legală?
- ▶ LEGE nr. 455/2001 privind semnatura electronică
- ▶ Normele pentru aplicarea Legii nr. 455/2001 privind semnatura electronică

## Testează

- ▶ **Certificat digital** (circled in red)
- ▶ Aplicație clickSIGN Demo
- ▶ Aplicația clickSIGN pdf

Află mai mult ➔

### Certificat digitale



- ▶ Certificate digitale și semnatura electronică
- ▶ Certificate calificate și semnatura electronică extinsă
- ▶ Semnatura electronică extinsă
- ▶ Aplicație gratuită pt a verifica o semnatura electronică

Află mai mult ➔

Află mai mult ➔

### Află cum să utilizezi certificatul digital



- ▶ Utilizarea dispozitivului criptografic (token)
- ▶ Procedura de depunere a declaratiilor fiscale on-line
- ▶ Semnarea documentului de confirmare

Află mai mult ➔

certSIGN furnizează încrederea de care ai nevoie

certSIGN, companie a grupului UTI , dezvoltă integral în România soluții proiectate pe nevoile specifice de business. De la certificate digitale calificate până la soluții complexe de securitate care au trecut teste de interoperabilitate NATO, certSIGN a luat toate măsurile pentru ca informațiile tale să fie în siguranță.

Sistemului de Management a Securității Informației al certSIGN este certificat de către BSI (British Standard Institution) în conformitate cu ISO 27001:2005 iar compania a parcurs cu succes, în premieră pentru România, auditul WebTrust for CA.

# How to obtain a digital certificate

 certSIGN.  
Secure your on-line transactions

[Despre noi](#) [Produse](#) [Servicii](#) [Soluții de securitate](#) [Resurse](#) [Contact](#) [Căutare](#)

**Testează**  
Certificate demo



**Testează**

Certificate demo

[Testează certificat](#) (circled)

[Caută un certificat](#)

[Revocă un certificat](#)

[Listă certificate revocate](#)

**Ghid**

- ▶ Pași pentru obținerea unui certificat digital

**Certificate Demo**

Pentru a te familiariza cu procedurile de obținere a diferitelor tipuri de certificate, precum și cu certificatele însele, îți oferim posibilitatea de a obține imediat un certificat de test din categoriile prezentate mai jos. Certificatele sunt perfect funcționale și pot fi folosite timp de 3 luni, după care expiră.

În plus, poti cunoaște mai bine și alte etape din ciclul de viață al unui certificat : obținerea lui de către o entitate parteneră - acea persoană care dorește să beneficieze de serviciile infrastructurii noastre de chei publice, prin verificarea unei semnături sau prin criptarea unui document/e-mail -, revocarea sau consultarea listei de certificate revocate – CRL.

# How to obtain a digital certificate

**certSIGN.**  
Secure your on-line transactions

Căutare

Despre noi   Produse   Servicii   Soluții de securitate   Resurse   Contact

**Testează**  
Certificate demo



**Testează**  
Certificate demo

**Testează certificat**

Alege tipul dorit de certificat și apasă butonul Continuă pentru a te înregistra și a obține certificatul.

**Alege tipul de certificat dorit:**

Certificat digital simplu personal  
 Certificat digital pentru servere web  
 Certificat digital IPSec

Continuă

**Ghid**

▶ Pași pentru obținerea unui certificat digital

Copyright 2007 certSIGN. Toate drepturile rezervate. [Codul de practici și proceduri \(doc\)](#) | [Politica de certificare \(pdf\)](#) | [Termeni utilizare site](#) | [Sitemap](#)

**Uni**  
GRUP

# How to obtain a digital certificate

## Testează

Certificate demo

### Testează certificat

Caută un certificat  
Revocă un certificat  
Listă certificate revocate

## Ghid

▶ Pași pentru obținerea unui certificat digital

## Testează certificat

Alege tipul dorit de certificat și apasă butonul Continuă pentru a te înregistra și a obține certificatul.

Alege tipul de certificat dorit:

- Certificat digital simplu personal
- Certificat digital pentru servere web
- Certificat digital IPSec

Alege scopul în care dorești să folosești certificatul:

- Pentru semnare și autentificare
- Pentru criptare

Continuă

# How to obtain a digital certificate

## Testează

Certificate demo

### Testează certificat

Caută un certificat  
Revocă un certificat  
Listă certificate revocate

## Ghid

- ▶ Pași pentru obținerea unui certificat digital

## Testează certificat

Alege tipul dorit de certificat și apasă butonul Continuă pentru a te înregistra și a obține certificatul.

**Alege tipul de certificat dorit:**

- Certificat digital simplu personal
- Certificat digital pentru servere web
- Certificat digital IPsec

**Alege scopul în care dorești să folosești certificatul:**

- Pentru semnare și autentificare
- Pentru criptare

**Alege locația unde vrei să păstrezi certificatul:**

- Cu dispozitiv criptografic și cheie generată de client

Ai deja un smart card sau token USB de tipul celor recomandate de noi, sau vei achiziționa unul de la noi. Cheia privată va fi generată de tine prin intermediul procesorului criptografic al dispozitivului și certificatul va fi scris pe dispozitiv tot de sine.

- Fără dispozitiv criptografic și cheie generată de client

Vei genera cheia privată prin mijloace software, direct pe suportul de memorie. Cheia și apoi certificatul vor fi create într-un fișier de tip pkcs #12

Continuă

# How to obtain a digital certificate

## Cerere de certificat Demo!

Ai ales să testezi un **certificat digital simplu personal pentru semnare și autentificare**.

Pentru a putea obține acest tip de certificat trebuie mai întâi să te înregistrezi. Mai multe informații despre pașii de obținere ai unui certificat digital poți obține [aici](#), sau descărcând ghidul de obținere a unui certificat digital.

Numai câmpurile marcate cu **\*** sunt obligatorii.

După ce introduci datele tale, apasă butonul Înregistrează.

### Date de identificare utilizator

Nume: <b>*</b>	Pura	Prenume: <b>*</b>	Mihai
CNP:	<input type="text"/>	Inițiala Tatălui:	<input type="checkbox"/>
Pseudonim:	<input type="text"/> ?		

### Informații despre adresa utilizatorului

Tara:	Romania 		
Județ/Sector:	<input type="text"/>	Localitate:	<input type="text"/>
Strada:	<input type="text"/>	Nr:	<input type="text"/>
Bloc:	<input type="text"/>	Scara:	<input type="text"/>
Apartament:	<input type="text"/>	Cod Poștal:	<input type="text"/>

### Date de contact ale utilizatorului

Telefon:	<input type="text"/>	Fax:	<input type="text"/>
Email: <b>*</b>	puramihai@yahoo.com		
		Web:	<input type="text"/>

### Date despre societate

Organizația:	<input type="text"/>	Departament:	<input type="text"/>
--------------	----------------------	--------------	----------------------

Introdu codul de verificare din imagine în căsuța de mai jos (pentru prevenirea înregistrării automate).

Cod verificare:	<input type="text"/> C5N4K5NR
	

(dacă imaginea este nedată, execută click pe ea pentru a o reîncărca)

# How to obtain a digital certificate

 certSIGN.

Secure your on-line transactions

Căutare

Despre noi   Produse   Servicii   Soluții de securitate   Resurse   Contact

**Testează**  
Certificate demo



## Cerere de certificat Demo!

Pentru a putea revoca certificatul ai nevoie de o parolă. Alege această parolă mai jos și păstrează-o undeva în siguranță pentru situația în care vei avea nevoie de ea.

Pentru a iniția procesul de generare a certificatului, apasă butonul **Generează certificat**.

Parolă Acces Certificat:  (minim 6 caractere)

Confirmă Parolă:  

Nume Certificat:

Dacă în pasul anterior și-ai ales un pseudonim, poți decide acum ca acest pseudonim să apară în certificat în locul numelui.

**Înădoi Generează Certificat**

Copyright 2007 certSIGN. Toate drepturile rezervate. [Codul de practici și proceduri \(doc\)](#) | [Politica de certificare \(pdf\)](#) | [Termeni utilizare site](#) | [Sitemap](#)



# How to obtain a digital certificate

## Cerere de certificat Demo!

Certificatul de test a fost emis. Il poți descărca acum ca fisier P12 sau oricând în format .crt în interval de 3 luni de la data emiterii, urmând linkul [obține certificat](#).

Certificatul este perfect funcțional și este valid timp de 3 luni de la data emiterii.

Serial Certificat:	200605167004010702	
Subiect Certificat:	C=RO, CN=Pura Mihai, Name=Pura Mihai, G=Mihai, SN=Pura	
Valabilitate Certificat:	2010 11 22 09:31:28	2011 02 20 09:31:28
Certificat:	<pre>-----BEGIN CERTIFICATE----- MIIE2TCCA8GgAwIBAgIJIAYFFnAEAQcCMAOGCSqGSIB3DQEBBQUAMEMxCzAJBgNV BAYTA1JPMREwDwYDVQQKEwhjZXJOU01HTjEhMB8GA1UECxMYY2VydFNJR04gRGVt byBDQSEDbGFzcycAxMB4XDTEwMTExMDIyMDA3MzEyOFowVjEL MAkGA1UEBhMCUk8xEzARBgNVBAMMC1B1cmEgTW1oYWkxEzARBgNVBCKMC1B1cmEg TW1oYWkxDjAMBgNVBCoMBU1paGFpMQ0wCwYDVQQEDARQdXjhMIGfMA0GCSqGSIB3 DQEBAQAA4GNADCBiQKBgQDAKchztqkSNkz/ARVXeqeJWA8kzYXJr7edteSmtPNW kGePi4XXmXmY9EMv8Ft6kXfhjbsqwNoNMF5upJeqTSjjZhGpt+o4bbEGfgh8ls FE5QePdt8IFYR7C2stFZwuGgUYM21ZsdliW7QoV9bsnhj fHUUDDQ02jxr/xSISjVm LQIDAQABo4ICPzCCAjswMvYIKwYEBQUHAQEEJzAlMCGCCsGAQUFBzABhhodHRw Oi8vb2NzcC5jZXJ0c2lnbi5ybzaMEgNVHRMBAf8EAjAAMA4GA1UDwEB/wQEawIG wDBsBgNVHSMEZTBjgBTXhtgocLIRJA5GK9e2FizIL+tivaFHpEUwQzELMAkGA1UE BhMCUk8xETAPBgNVBAoTCGN1cnRTSUdOMSEwHwYDVQQLEhxjZXJOU01HTiBEZW1v IENBIEnYXNzIDCCAgSaME0GA1UDgQWBQBhkeV61kLrBrJis3fgxq7eUJvhXBj BgNVHSAEQjBAND4GCysCAQQBgcmNSAQEBMC8wLQYIKwYBBQUHagEWIWh0dHHA6Ly93 d3cuY2VydHNpZ24ucm8vcWwb3NpdG9yeTCBnQYDVQfBIGVMIGSMIGPoIGMoIGJ hiFodHw0i8vY3JzLmN1cnRzaWduLnJvL2NsYXNzMS5jcmYgZCkxYKA6Ly9sZGPw LmN1cnRzaWduLnJvL09VPWN1cnRTSUdOIErlbW8gQ0EgQ2xhc3MgMSxPPWN1cnRT SUdOLEM9Uk8/Y2VydGmaWnhdGVSZX2vY2F0aW9uTG1zdDtiaW5hcnkwQwYDVROR Bdw0qAjBgorBgEEAYI3FAIDoBUMe3B1cmFtaWhhaUB5YWhvby5jb22BE3B1cmFt aWhhaUB5YWhvby5jb20wRQYDVRO1ECIwIAKKwYBBAGCNxQCAgYIKwYBBQUHawIG CCsGAQUFBwMEMAOGCSqGSIB3DQEBBQUAA4IBAQ/k+jBRoAf83jpuPfyPygdht GTPMp+UgwH8eWL2+oM+o65oYKSjwOYLX2Pqc51/UnyzI90M+qNFnshFM4VVVX/i AWDb1tsqm6bYs7/LU+8w3Em6Tjd1GJNabXUpTw0LzT4z6TVYprVxg5kuQemIsJlz wGC5phH/8RHL8sdcsEAzeNpbRVj1CYpFM01vkCbJvWngTVDENjRJ2fm0IHwpVeZW</pre>	

[Înapoi](#) [Download P12](#) [Download PEM](#) [Download DER](#)

# P12

- ▶ P12 – PKCS#12 – Public Key Cryptography Standards 12 –
  - RSA Laboratories standard
  - defines the format of the files used to store a private key together with its corresponding digital certificate
  - encrypted with a symmetric key or a password
  - binary content

# DER

- ▶ DER – Distinguished Encoding Rules
  - message transfer syntax published by ITU in X.690
  - are binary files
  - also used to store digital certificates

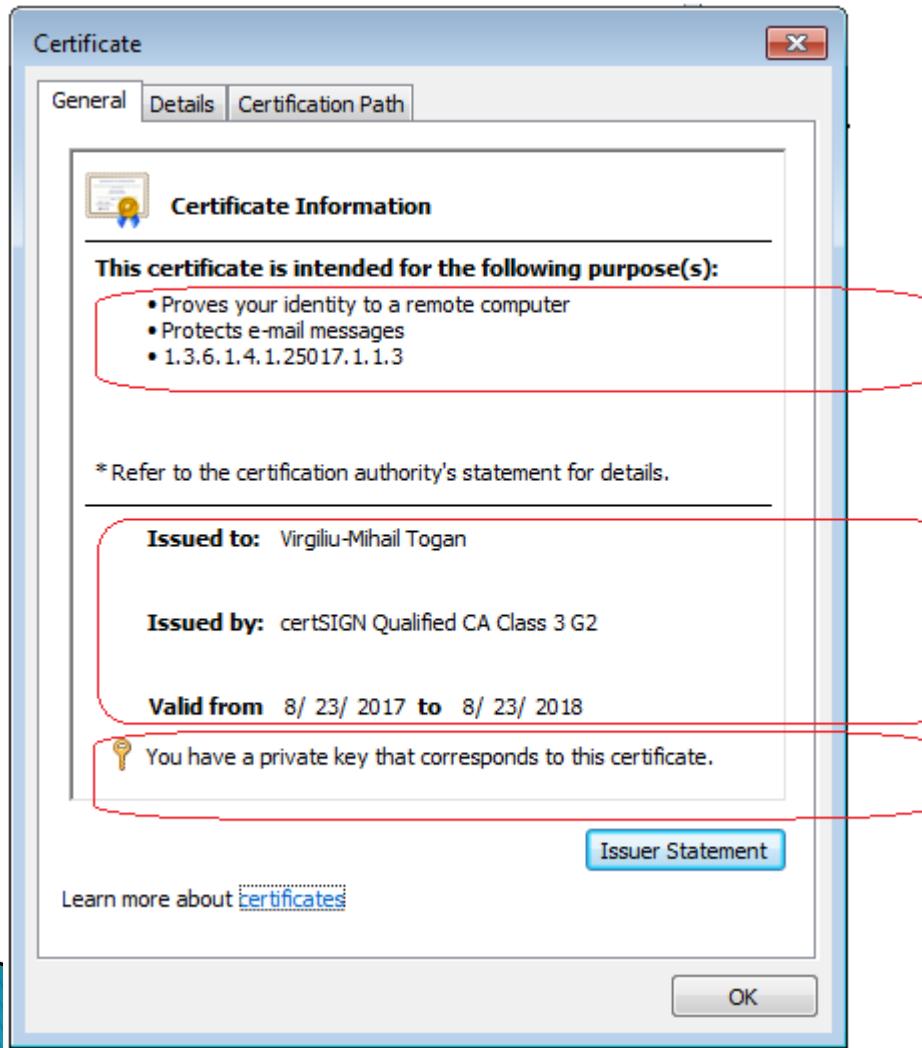
# PEM

- ▶ **PEM – Privacy Enhanced Mail**
  - early standard for securing electronic mail, but never adopted as a widely used Internet Mail Standard
  - text files that contain a US-ASCII representation of a DER digital certificate
    - BASE64 encoding
    - enclosed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"
  - BASE64
    - encoding scheme used to represent binary data in an ASCII string by translating it into radix-64 representation
    - ASCII characters used are "A-Z", "a-z", "0-9", plus two more characters, often "+" and "/"

# Digital certificates

- ▶ A digital certificate
  - a collection of information referring to a public key, digitally signed by the CA
  - conforms to the ITU (IETF) standard X.509 v3
  - the CA signs the information from the digital certificate using its private key

# Digital certificates



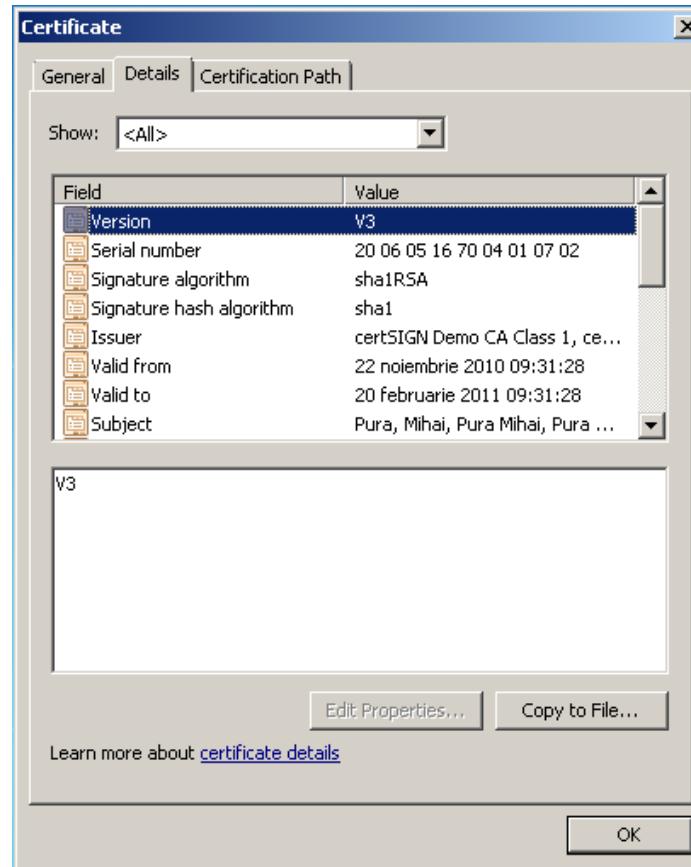
There are several categories of information:

The main scope of certificate

The SUBJECT of certificate  
The ISSUER of certificate  
The validity of certificate

If there is a registered private-key, pairing with this public key

# Digital certificates



# Digital certificates

## ▶ Extensions

- The scope of the certificate, usage policies, constraints, etc.
- X.509 v3 standard extensions
  - 1. key information
    - authority key identifier
    - subject key identifier
    - key usage
    - private key usage period
  - 2. policy information
    - certificate policies
    - policy mappings

# Digital certificates

## ▶ Extensions

- X.509 v3 standard extensions
  - 3. user and CA attributes
    - subject alternative name
    - issuer alternative name
    - subject directory attributes
  - 4. certification path constraints
    - basic constraints
    - name constraints
    - policy constraints

# Digital certificates

## ▶ Extensions

- Authority key identifier extension contains a key identifier, if not necessary the issuer name and the serial number
- CRL distribution points extension contains the location where CRL may be found
- Authority information access extension contains the repository in which the own CA certificate may be found

# Digital certificates

- ▶ End-entity certificates
  - Are issued to subjects that are not CAs
  - Contain public keys used for verifying digital signatures or for performing key management
  - Subject:
    - human user
    - system (Web server or router)
  - two types:
    - User certificates
    - System certificates

# Digital certificates

## ▶ CA certificates

- Are issued to subjects that are CAs
- Are part of certificate paths
- Contain public keys used for
  - verifying digital signatures on certificates and CRLs
- Must contain sufficient information for certificate users to construct certification paths and locate CRLs

# Digital certificates

## ▶ CA certificates

- Subject:
  - other CA in the same enterprise
  - a CA in other enterprise
  - a bridge
- three types
  - CA certificates within an enterprise PKI
  - CA certificates between enterprise PKIs
  - CA certificates in a Bridge CA Environment

# Digital certificates

- ▶ Self-signed CA certificates (self-issued)
  - Issuer and Subject are the same
  - Used to
    - establish trust points
    - distribute a new signing public key
    - modify the certificate policies supported in a PKI

# ASN.1

- ▶ ASN.1 – Abstract Syntax Notation One
  - a standard and notation that describes
    - rules
    - and structures
  - for representing, encoding, transmitting, and decoding data in telecommunications and computer networking
- ▶ ASN.1 decoder:
  - <https://holtstrom.com/michael/tools/asn1decoder.php>
  - <http://phpseclib.sourceforge.net/x509/asn1parse.php>
  - <https://lapo.it/asn1js/>
- ▶ Object Identifier (OID) Repository
  - <http://www.oid-info.com/>

# Digital certificates – ASN.1

## ASN.1 JavaScript decoder

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (127 bit) 116562349437600534260500195073713998130
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.5
      NULL
  SEQUENCE (4 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6
        SET (1 elem)
          SEC(Offset: 52
               Length: 2+3
               Value:
               2.5.4.6
               SET countryName
               SEQUENCE (1 elem)
                 X.520 DN component
                 OBJECT IDENTIFIER 2.5.4.11
                 PrintableString Trans Sped Certification Authority
               SET (1 elem)
                 SEQUENCE (2 elem)
                   OBJECT IDENTIFIER 2.5.4.3
                   PrintableString Trans Sped QCA
             SEQUENCE (2 elem)
               UTCTime 2015-03-12 00:00:00 UTC
               UTCTime 2016-03-11 23:59:59 UTC
  SEQUENCE (5 elem)
```

# Digital certificates – ASN.1

## OID description

- ▶ [Format of this page](#)
- ▶ [Modify this OID](#)
- ▶ [Create a child OID](#)
- ▶ [Create a brother OID](#)
- ▶ [Find similar OIDs](#)

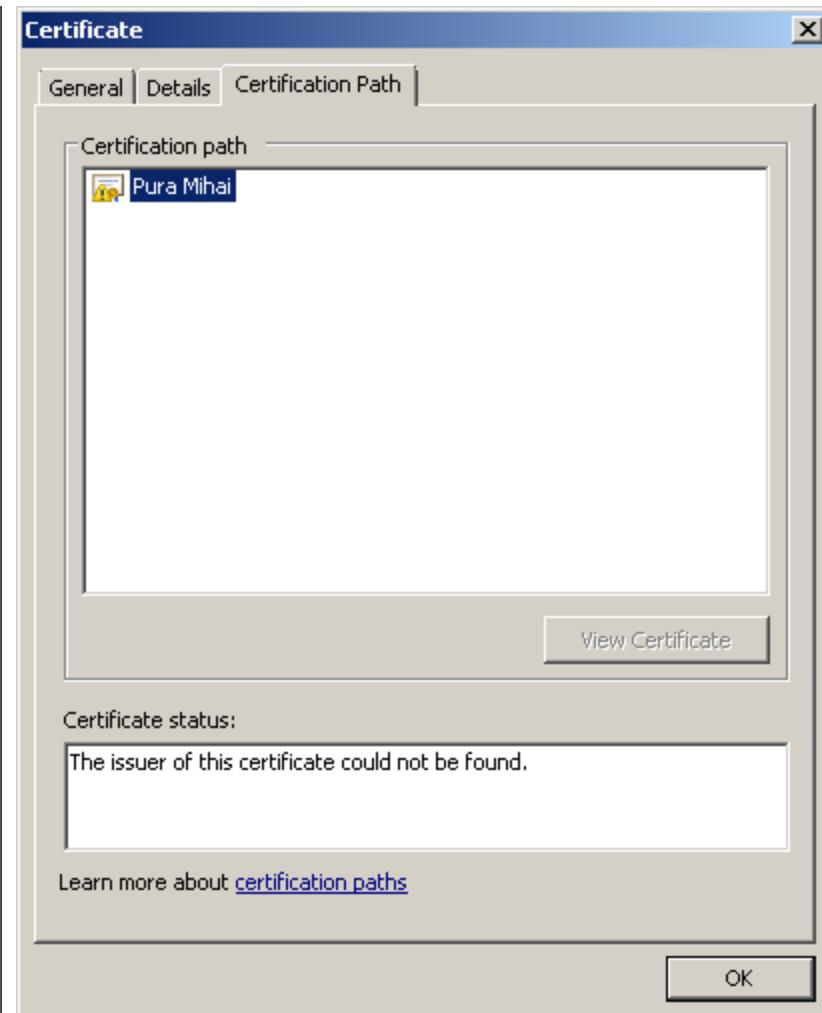
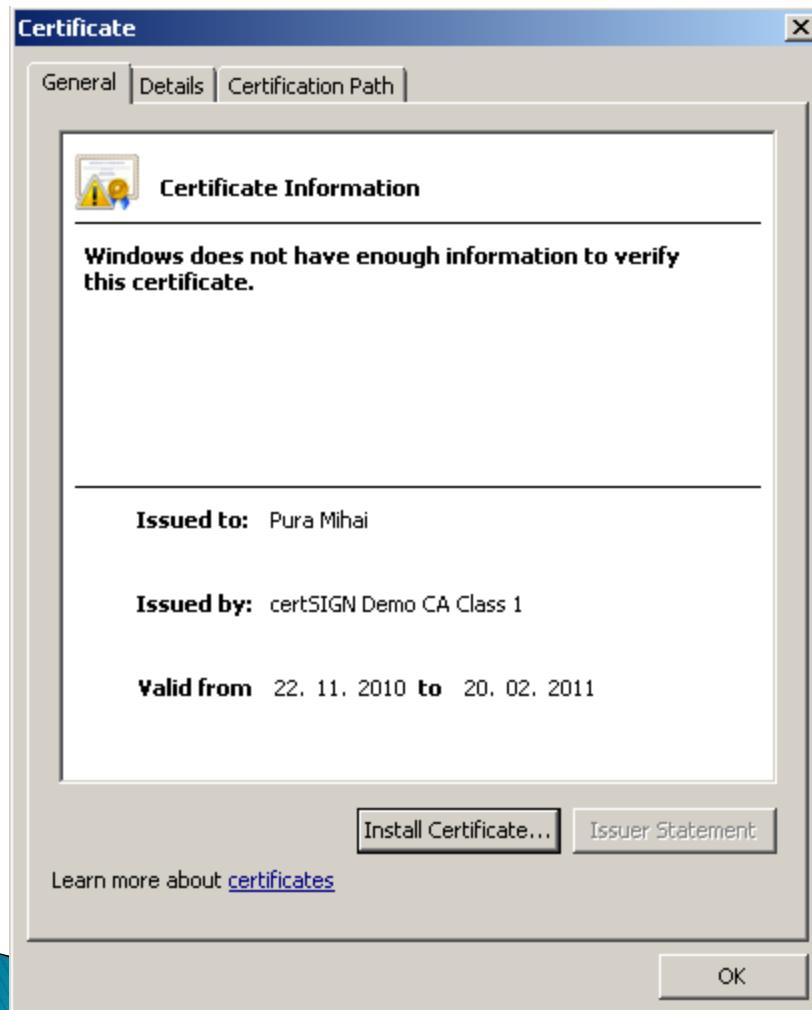
{joint-iso-itu-t(2) ds(5) attributeType(4) countryName(6)}	(ASN.1 notation)
OID: 2.5.4.6	(dot notation)
/Joint-ISO-ITU-T/5/4/6	(OID-IRI notation)
<b>Description:</b> Country name	
<b>Information:</b>	This node is defined in <a href="#">Annex A of Rec. ITU-T X.520 (February 2001)</a> and in <a href="#">ISO/IEC 9594-6: 2001: "The Directory: Selected attribute types"</a> .

Short URL for this page: <http://oid-info.com/get/2.5.4.6>

# Certification Path

- ▶ CA's digital signature on the certificate
  - is the guaranty that the digital certificate is owned by the person whose identification information are contained in it
- ▶ To verify the bond between the public key and the identity of the owner
  - verify the signature of the CA over the certificate
- ▶ The digital certificate of the issuer (a CA) is needed

# Certification Path



# Certification Path

- ▶ Certification path
  - all the digital certificates needed to verify someone's digital certificate
  - each certificate has a *certification path starting from a ROOT-CA*
  - usually, Root-CA certificate is a trusted point in the *system*
- ▶ The root certificate for this path is a self-signed certificate
  - The self-signed certificate cannot be further validated
  - So another verification element is added: the trust in a CA

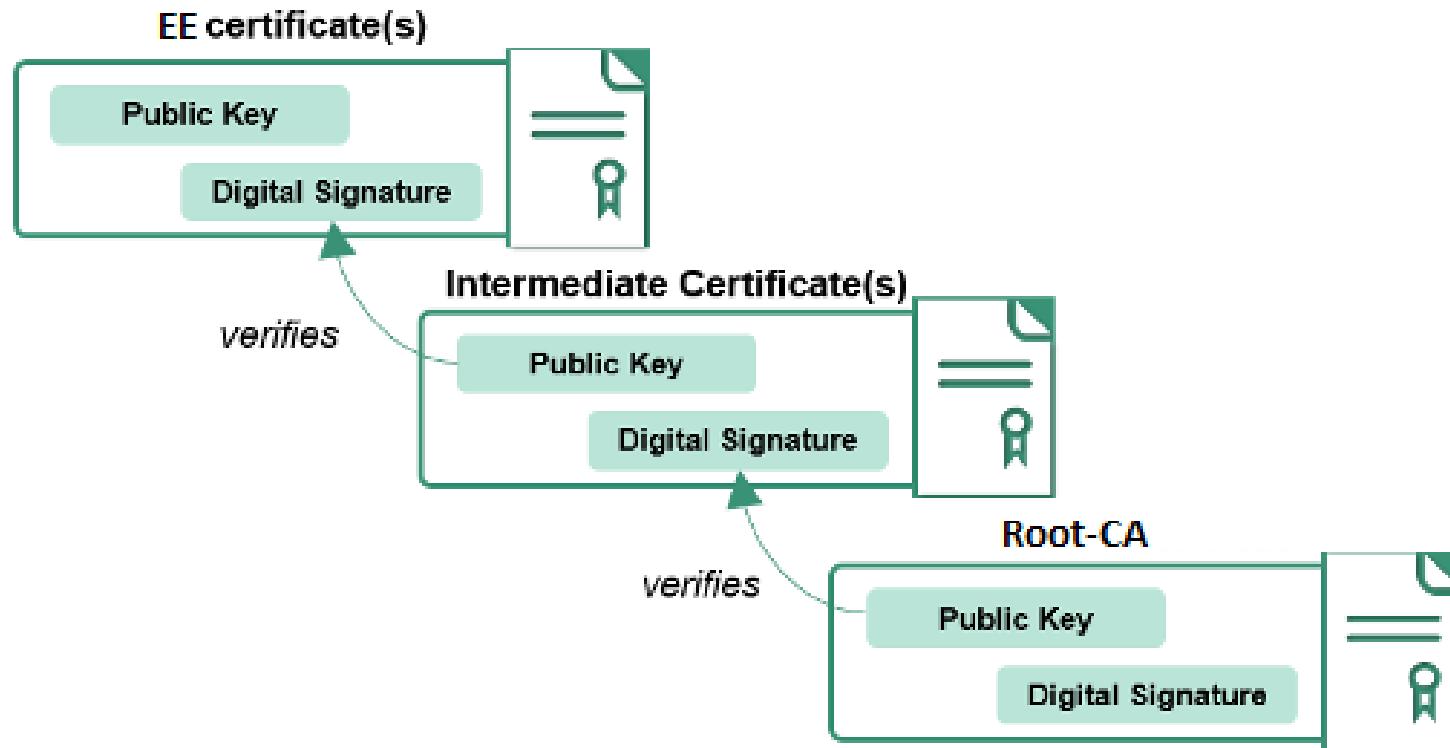
# Certification Path

- ▶ If a CA is trusted it does not matter that it had sign its own certificate
- ▶ If a CA is not trusted, the user will be informed about it
- ▶ The digital certificates of a CA can be downloaded from their web site

# Certification Path

- ▶ An ordered sequence of certificates between
  - the end entity
  - and the trusted point in the hierarchy (Root–CA)
- ▶ The result is a certificate chain that
  - begins at the end entity
  - and ends at the Root–CA

# Certification Path



# Certification Path

**certSIGN.** Căutare

Secure your on-line transactions Despre noi Produse Servicii Soluții de securitate Resurse Contact

**Testează**  
Certificate demo



## Testează

**Certificate demo**

Testează certificat  
Caută un certificat  
Revocă un certificat  
**Listă certificate revocate**

### Ghid

- ▶ Pași pentru obținerea unui certificat digital

## Certificate Demo

Pentru a te familiariza cu procedurile de obținere a diferitelor tipuri de certificate, precum și cu certificatele însele, îți oferim posibilitatea de a obține imediat un certificat de test din categoriile prezentate mai jos. Certificatele sunt perfect funcționale și pot fi folosite timp de 3 luni, după care expiră.

În plus, poți cunoaște mai bine și alte etape din ciclul de viață al unui certificat : obținerea lui de către o entitate parteneră - acea persoană care dorește să beneficieze de serviciile infrastructurii noastre de chei publice, prin verificarea unei semnături sau prin criptarea unui document/e-mail -, revocarea sau consultarea listei de certificate revocate – CRL.

# Certification Path

 certSIGN®

Secure your on-line transactions

[Despre noi](#) [Produse](#) [Servicii](#) [Soluții de securitate](#) [Resurse](#) [Contact](#) [Căutare](#)

**Testează**  
Certificate demo



## Certificate/Crl-uri clase Demo!

Lista cu autoritățile care emit certificate Demo. Poți descărca CRL-ul sau certificatul autorității facând clic pe link-ul corespunzător.

Autoritate	Serial	Stare	Actiuni
certSIGN Demo CA Class 1	049a	Activ	<a href="#">Download CRL</a> <a href="#" style="color: red; border: 2px solid red; border-radius: 50%; padding: 2px;">Certificat</a>

# Certificate stores

- ▶ Microsoft Windows operating systems manages digital certificates through special store places
  - certificate stores
- ▶ To execute operations over these stores, the Certificates snap-in should be used
- ▶ Start, Run: **certmgr.msc**

# MS Windows certificate stores

- ▶ A system store
  - a collection that consists of one or more physical sibling stores
  - for each system store, there are predefined physical sibling stores
- ▶ All certificates in those physical stores are available through the logical system store collection
- ▶ For each system store location, the predefined systems stores are: MY, Root, Trust, CA
- ▶ In CERT\_SYSTEM\_STORE\_CURRENT\_USER, there is also a predefined UserDS store. A smart card store is planned for this location

# MS Windows certificate stores

- ▶ The system stores:
- ▶ CERT\_SYSTEM\_STORE\_CURRENT\_USER
- ▶ CERT\_SYSTEM\_STORE\_LOCAL\_MACHINE
- ▶ CERT\_SYSTEM\_STORE\_CURRENT\_SERVICE
- ▶ CERT\_SYSTEM\_STORE\_SERVICES
- ▶ CERT\_SYSTEM\_STORE\_USERS
- ▶ CERT\_SYSTEM\_CURRENT\_USER\_GROUP\_POLICY
- ▶ CERT\_SYSTEM\_LOCAL\_MACHINE\_GROUP\_POLICY
- ▶ CERT\_SYSTEM\_STORE\_LOCAL\_MACHINE\_ENTERPRISE

# MS Windows certificate stores

- ▶ CERT\_SYSTEM\_STORE\_CURRENT\_USER system stores are at the following registry location:
- ▶ HKEY\_CURRENT\_USER
  - ▶ Software
  - ▶ Microsoft
  - ▶ SystemCertificates
- ▶ The predefined physical stores associated with those system stores are as follows

<http://msdn.microsoft.com/en-us/library/windows/desktop/aa388136%28v=vs.85%29.aspx>

# MS Windows certificate stores

System store	Physical store
MY	.Default
Root	.Default .LocalMachine .SmartCard
Trust	.Default .GroupPolicy .LocalMachine
CA	.Default .GroupPolicy .LocalMachine
UserDS	.UserCertificate

# Create MMC snap-in to manage certificate stores

- ▶ 1. Run "mmc.exe" from a command line window. A blank Console window shows up.
- ▶ 2. Click "Add/Remove Snap-in" from the "File" menu. The "Add/Remove Snap-in" dialog box shows up.
- ▶ 3. Click the "Add" button. A list of "Available standalone snap-ins" shows up.

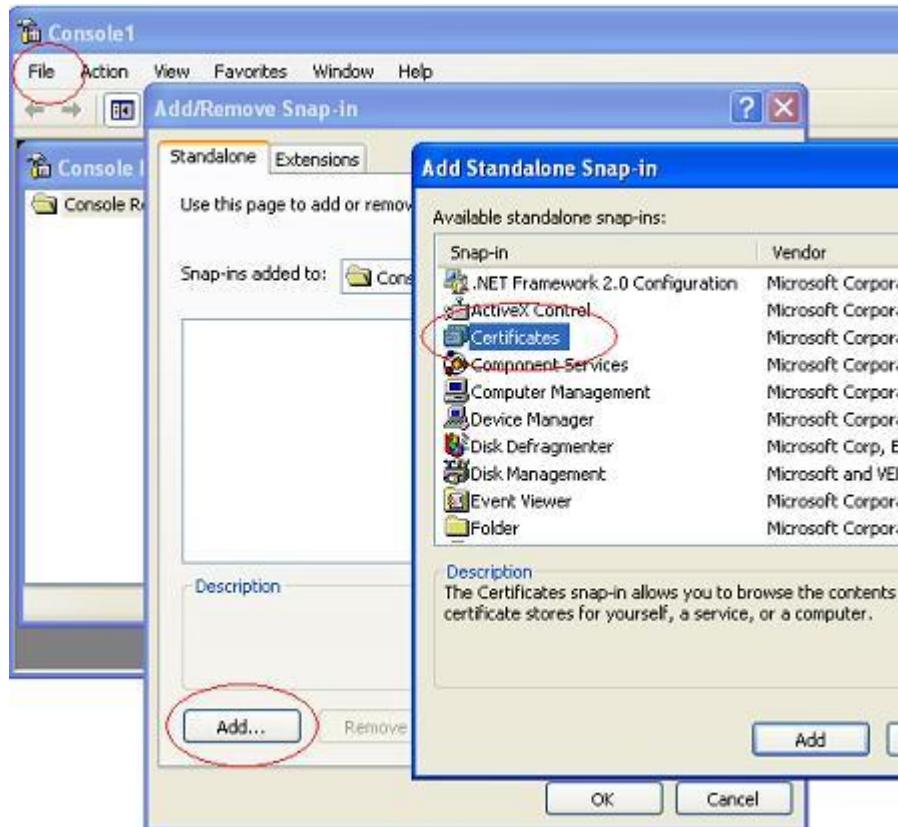
# Create MMC snap-in to manage certificate stores

- ▶ 4. Select "Certificates" and click "Add". The "Certificates snap-in" options dialog box shows up.
- ▶ 5. Select "Computer account" and click "Next". The "Select Computer" dialog box shows up.
- ▶ 6. Select "Local computer" and click "Finish". The "Certificates" snap-in is added.

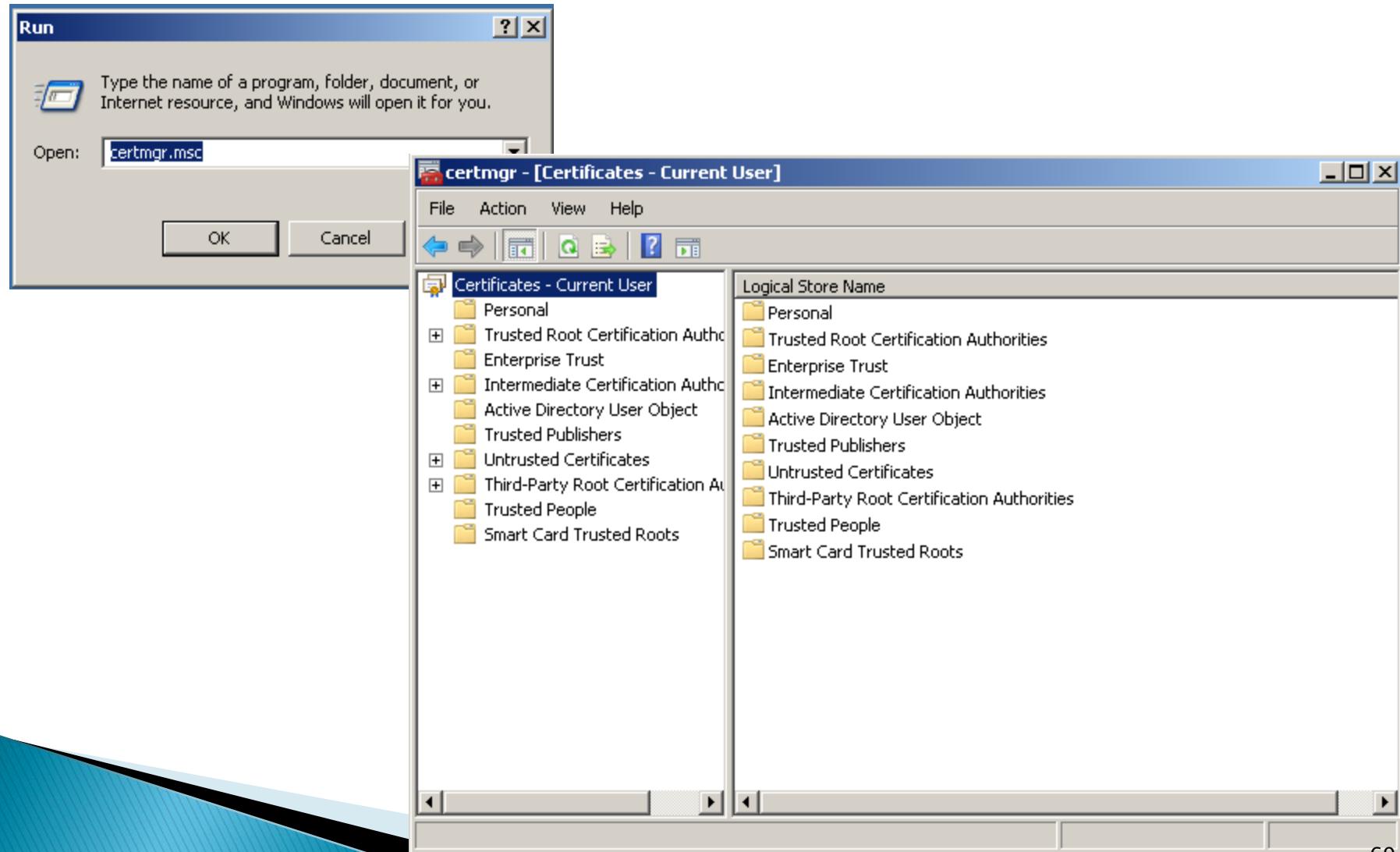
# Create MMC snap-in to manage certificate stores

- ▶ 7. Close the "Available standalone snap-ins" list dialog box.
- ▶ 8. Click "OK" on the "Add/Remove Snap-in" dialog box to accept the new snap-in.
- ▶ 9. Click "Save" from the "File" menu. The "Save As" dialog box shows up.
- ▶ 10. Enter "MyCertificatesConsole.msc" as the file name and click "Save".

# Create MMC snap-in to manage certificate stores



# MS Windows certificate stores



# MS Windows certificate stores

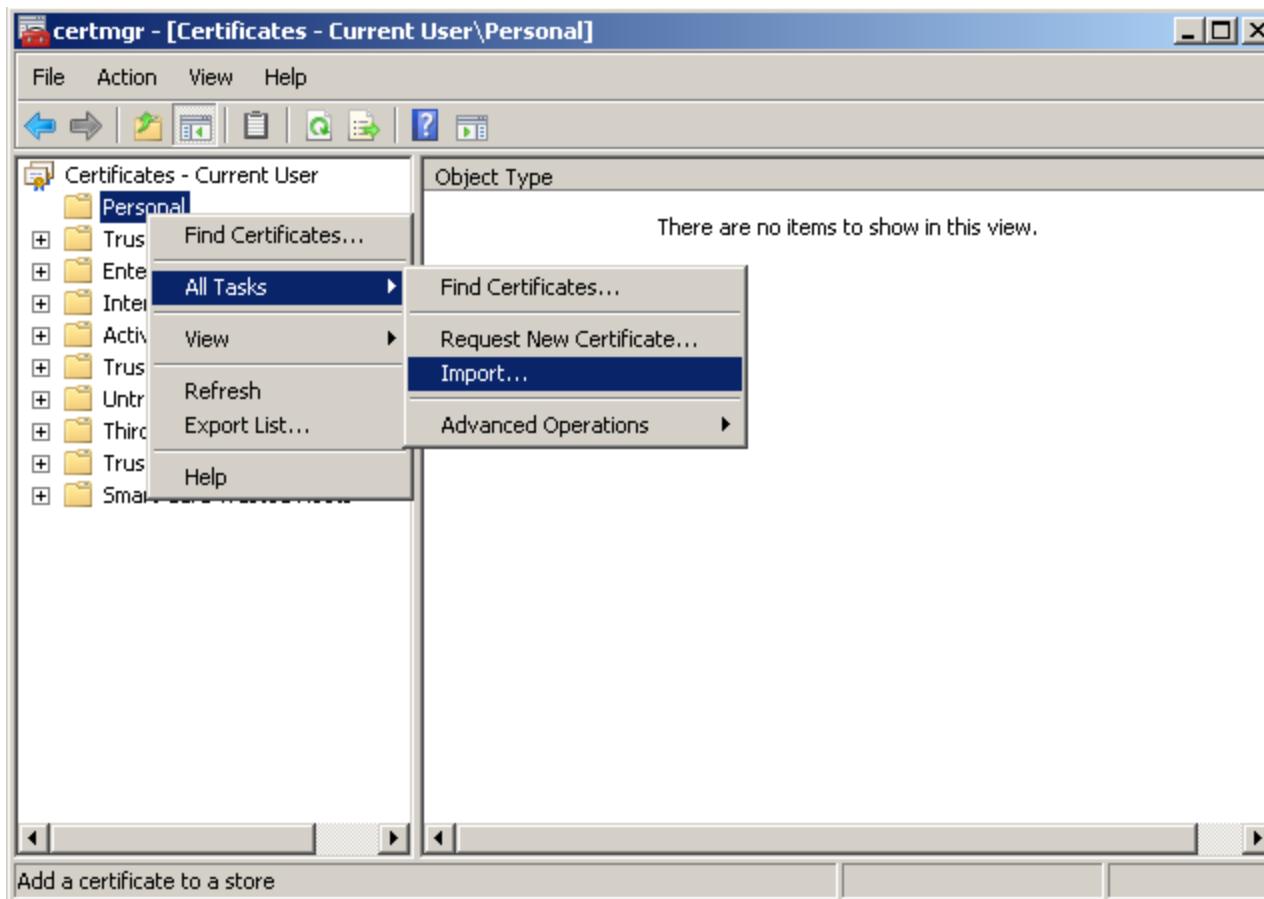
## ▶ Personal

- stores all the certificates for which the current user has the corresponding private keys:
  - certificates issued for the current user
  - for that computer
  - or for a service that runs on it

# MS Windows certificate stores

- ▶ **Trusted Root Certification Authorities**
  - stores the digital certificates of the CAs that are implicit trusted
- ▶ **Trusted People**
  - stores certificates issued for persons or entities that are trusted

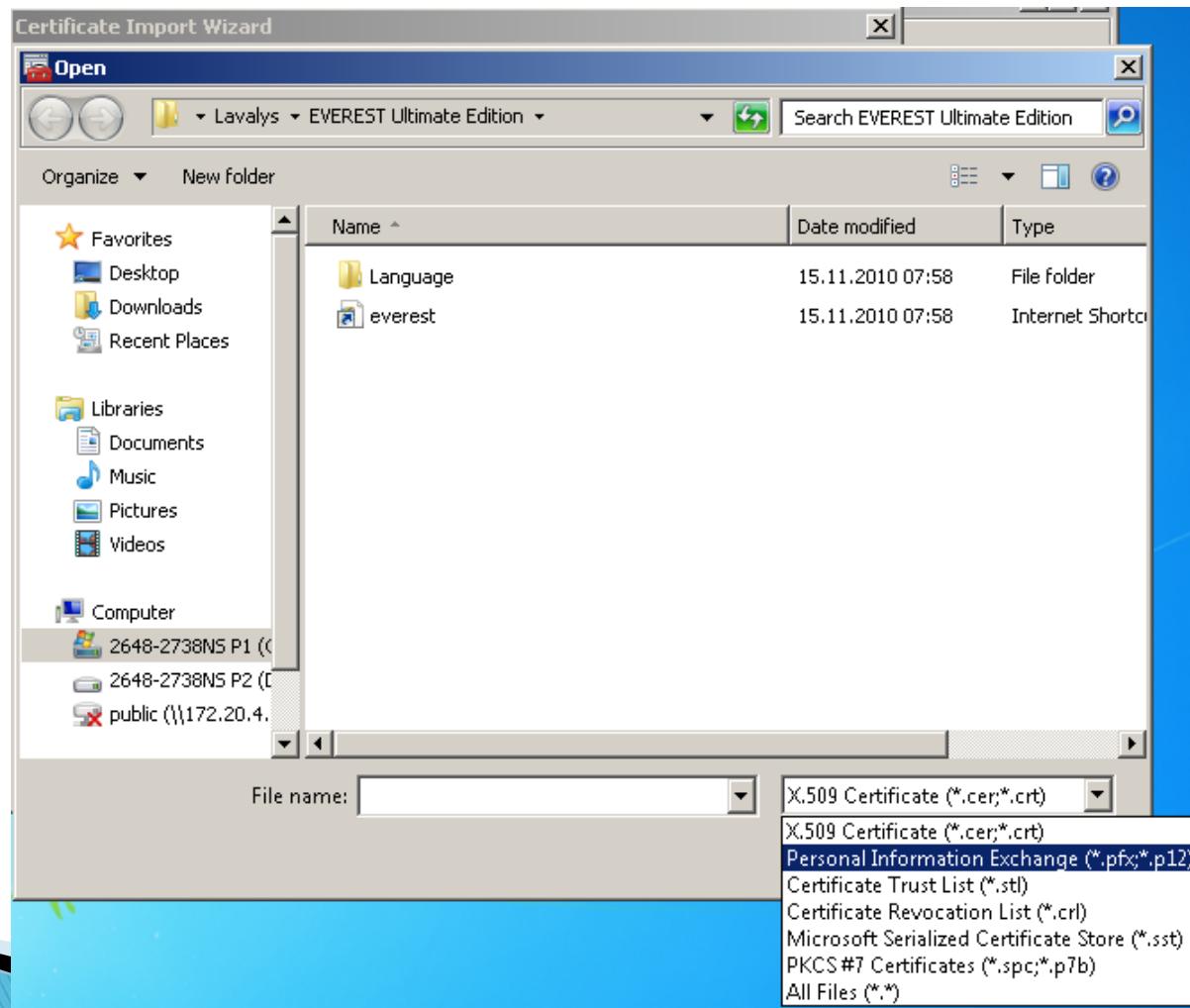
# Certificate import



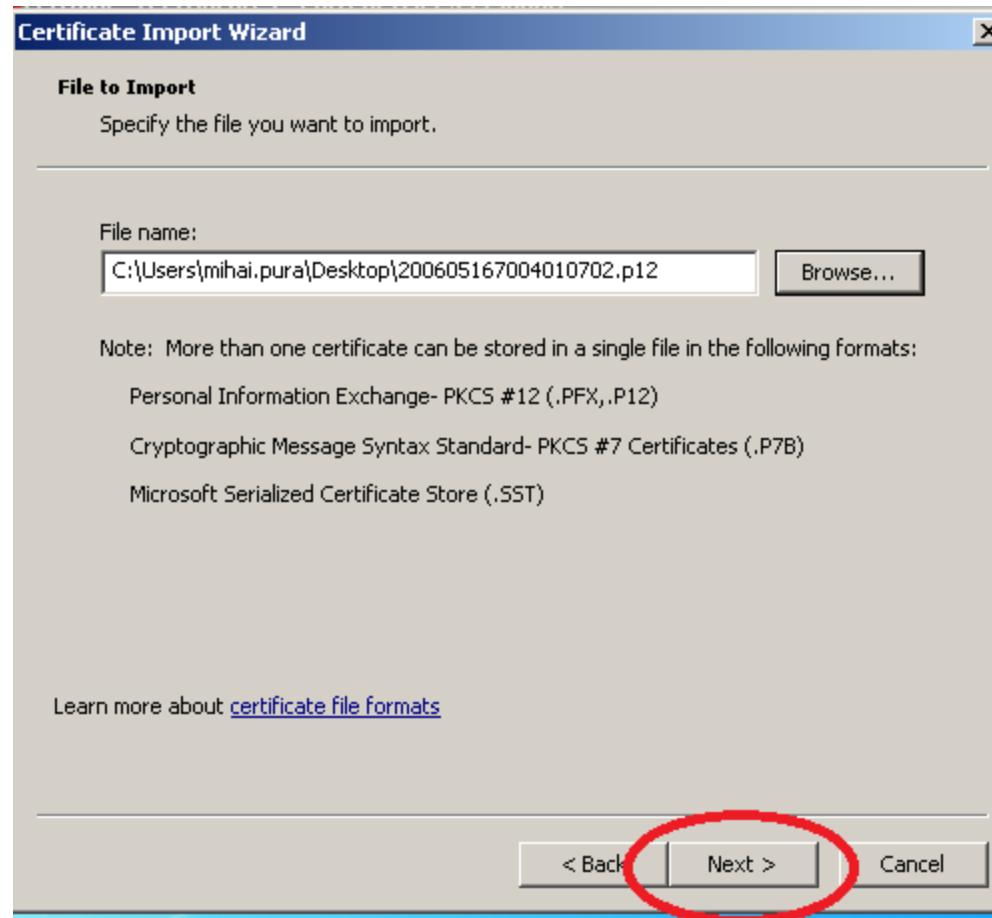
# Certificate import



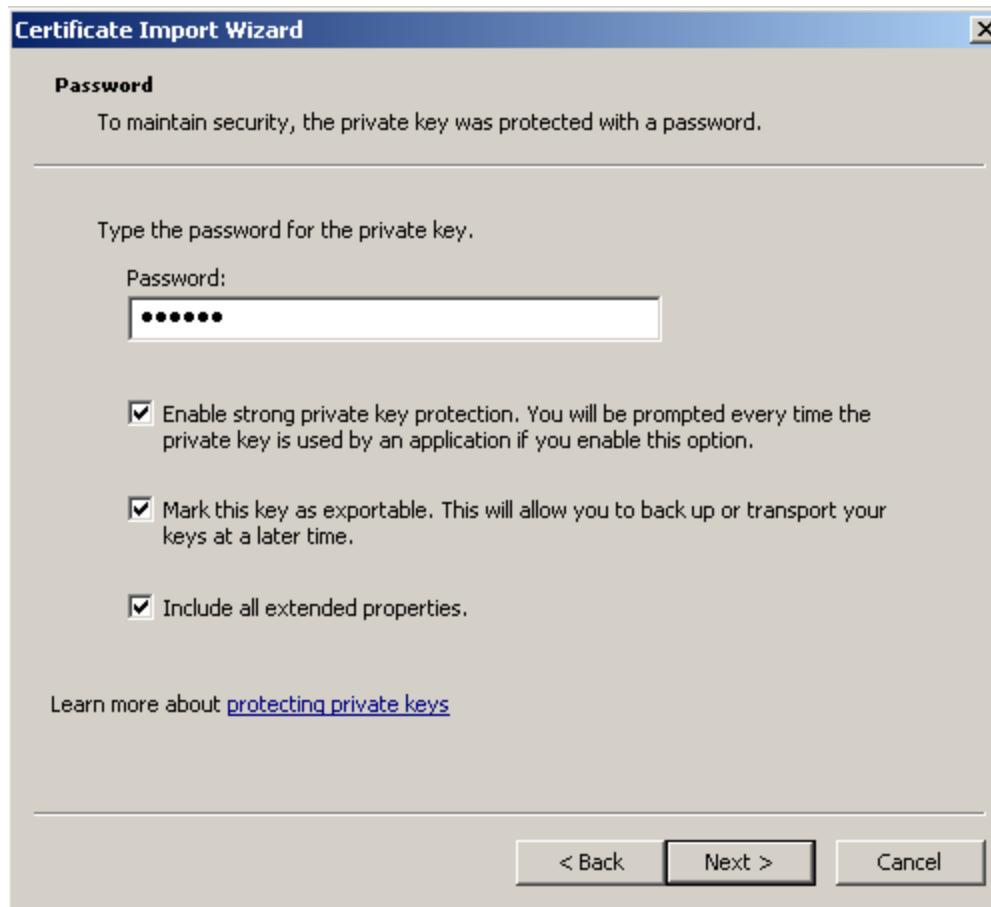
# Certificate import



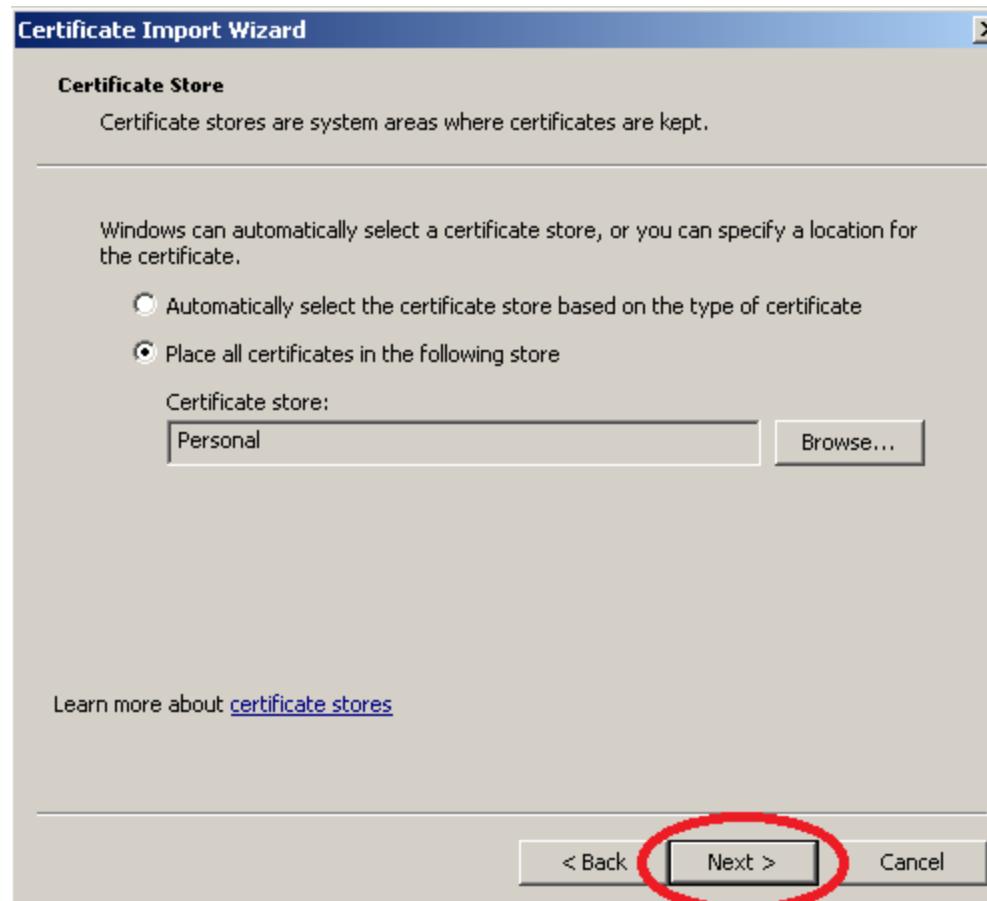
# Certificate import



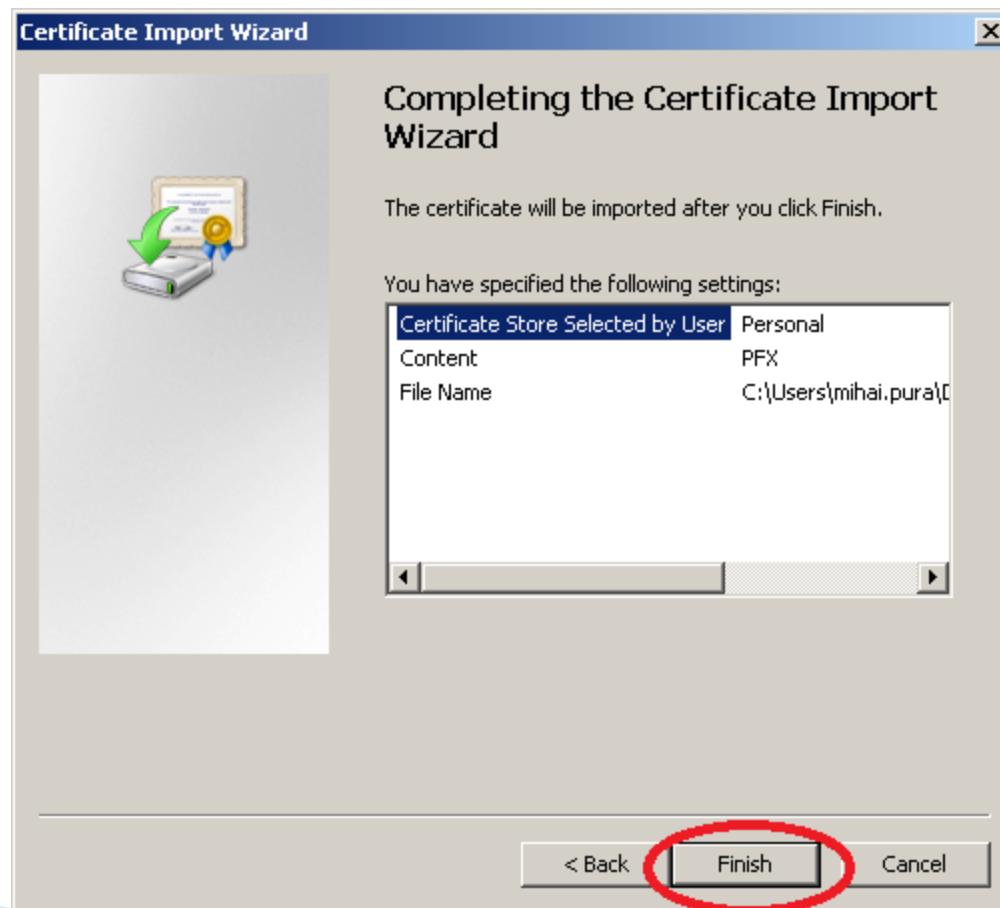
# Certificate import



# Certificate import



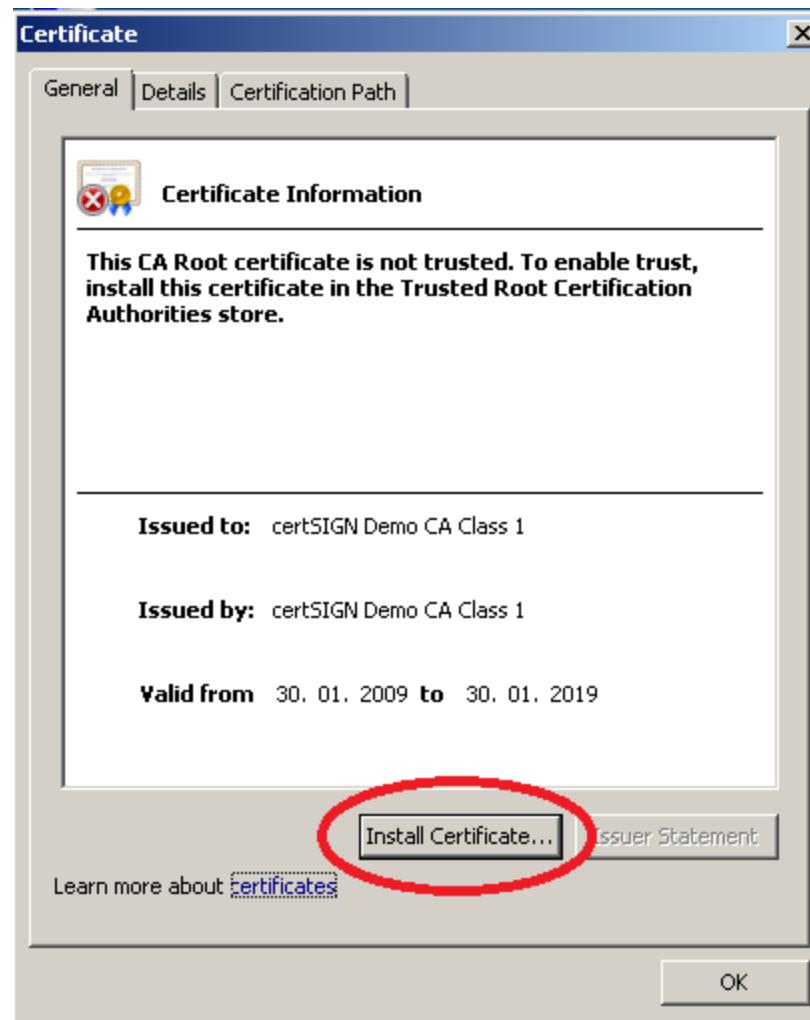
# Certificate import



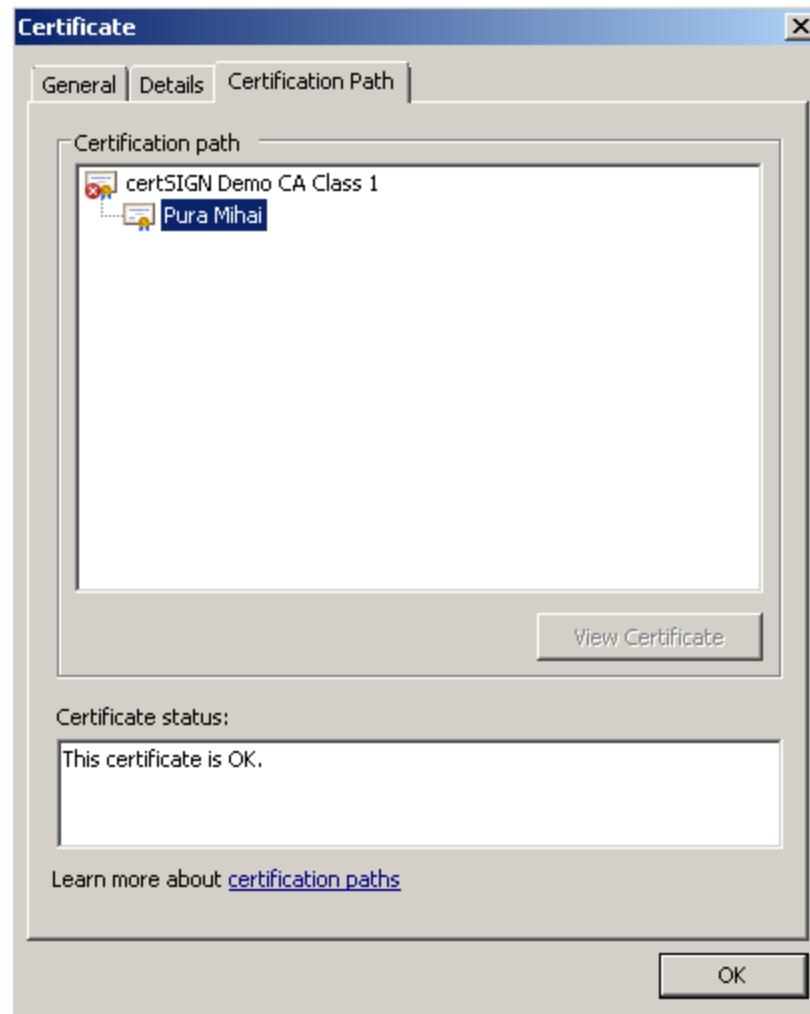
# Certificate import



# Certificate import for the CA



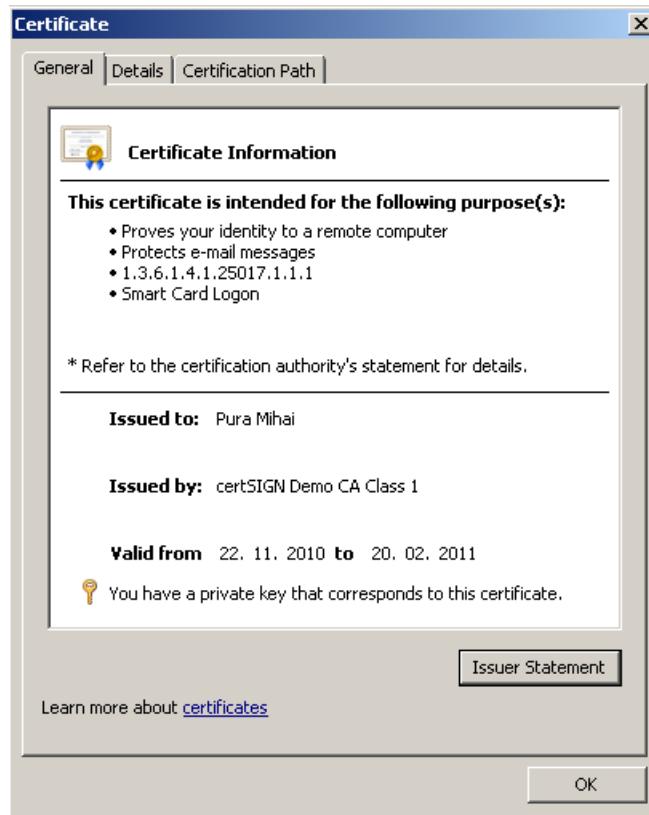
# Certification Path



# Certification Path

- ▶ To mark the CA as trusted
  - its digital certificates should be imported to the **Trusted Root Certification Authorities** store

# Certification Path



# Certificate search

**certSIGN.**  
Secure your on-line transactions

Despre noi   Produse   Servicii   Soluții de securitate   Resurse   Contact

**Testează**  
Certificate demo

**Certificate Demo**

Pentru a te familiariza cu procedurile de obținere a diferitelor tipuri de certificate, precum și cu certificatele însele, îți oferim posibilitatea de a obține imediat un certificat de test din categoriile prezentate mai jos. Certificatele sunt perfect funcționale și pot fi folosite timp de 3 luni, după care expiră.

În plus, poți cunoaște mai bine și alte etape din ciclul de viață al unui certificat : obținerea lui de către o entitate parteneră - acea persoană care dorește să beneficieze de serviciile infrastructurii noastre de chei publice, prin verificarea unei semnături sau prin criptarea unui document/e-mail -, revocarea sau consultarea listei de certificate revocate – CRL.

**Ghid**

▶ Pași pentru obținerea unui certificat digital

**Căutare**



Copyright 2007 certSIGN. Toate drepturile rezervate. [Codul de practici și proceduri \(doc\)](#) | [Politica de certificare \(pdf\)](#) | [Termeni utilizare site](#) | [Sitemap](#)

**Uni**  
GRUP

# Certificate search

**certSIGN.**  
Secure your on-line transactions

Despre noi   Produse   Servicii   Soluții de securitate   Resurse   Contact

**Căutare**

**Testează**  
Certificate demo



**Obține certificat Demo!**

Pentru a obține un certificat trebuie să completezi Numele și Prenumele persoanei care deține certificatul sau adresa de e-mail și să apeși butonul **Caută**.

Nume:  Numele de familie (Ex: Popescu)

Prenume:  Prenumele (Ex: Marian)

Email:

**Caută**

Copyright 2007 certSIGN. Toate drepturile rezervate. [Codul de practici și proceduri \(doc\)](#) | [Politica de certificare \(pdf\)](#) | [Termeni utilizare site](#) | [Sitemap](#)

**UNI**  
GRUP

# Certificate search

**certSIGN.**

Secure your on-line transactions

Despre noi   Produse   Servicii   Soluții de securitate   Resurse   Contact

**Căutare**

**Testează**  
Certificate demo



**Obține certificat Demo!**

S-au găsit următoarele certificate care corespund criteriilor introduse:

Nume	Serial	Tip certificat	Autoritate	Email
Mihai Pura	200605167004019A	Demo semnare	certSIGN Demo CA Class 1	puramihai@yahoo.com
Mihai Pura	2006051670040103C6	Demo semnare	certSIGN Demo CA Class 1	puramihai@yahoo.com
Mihai Pura	2006051670040103C7	Demo semnare	certSIGN Demo CA Class 1	puramihai@yahoo.com
Mihai Pura	200605167004010702	Demo semnare	certSIGN Demo CA Class 1	puramihai@yahoo.com

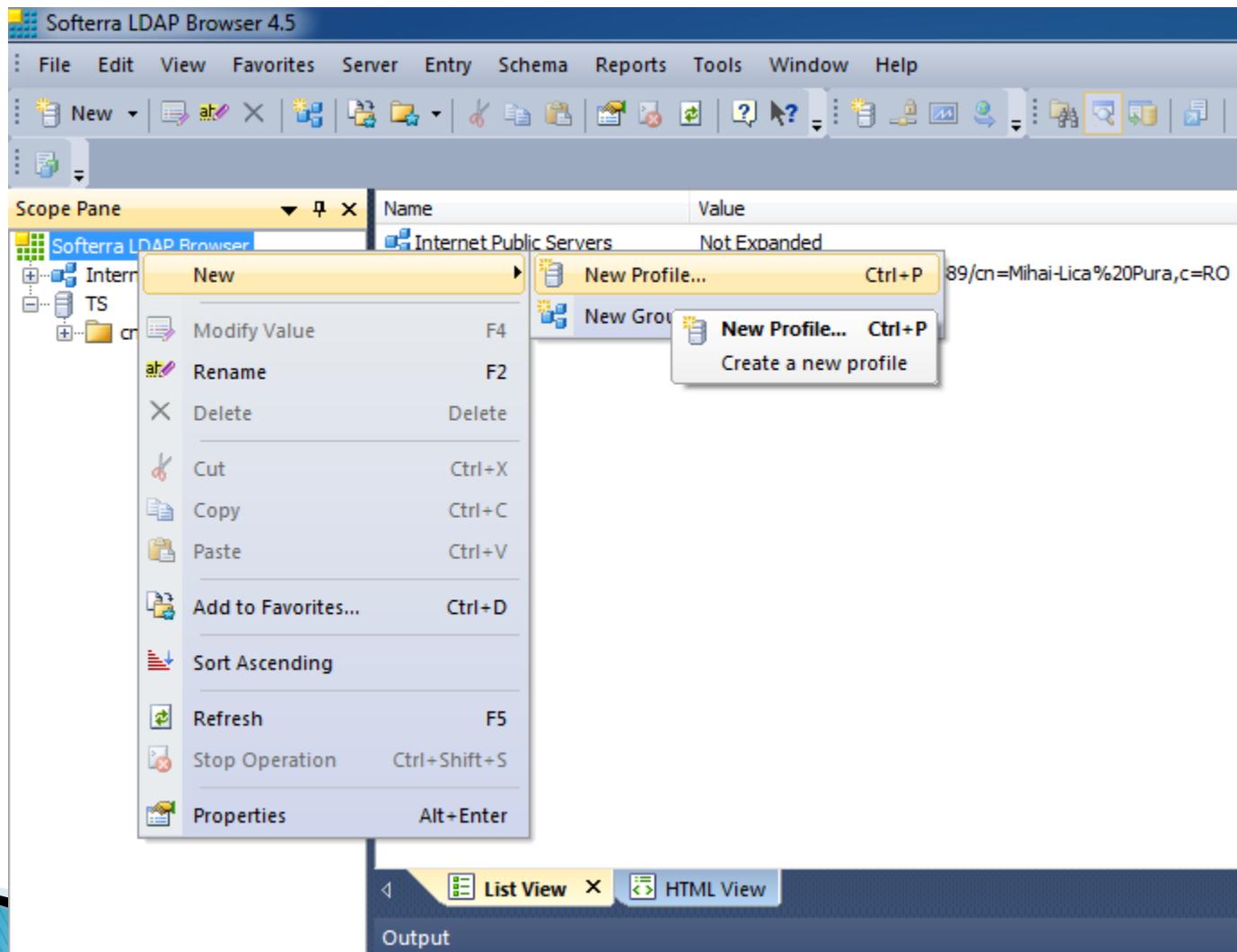
# Certificate search – LDAP

- ▶ LDAP – Lightweight Directory Access Protocol
  - application protocol for querying and modifying data of directory services implemented in Internet Protocol networks
- ▶ A directory is a set of objects with attributes organized logically in a hierarchical manner
- ▶ Exemplificare
  - **Softerra LDAP Browser**
  - <http://www.ldapbrowser.com/download.htm>

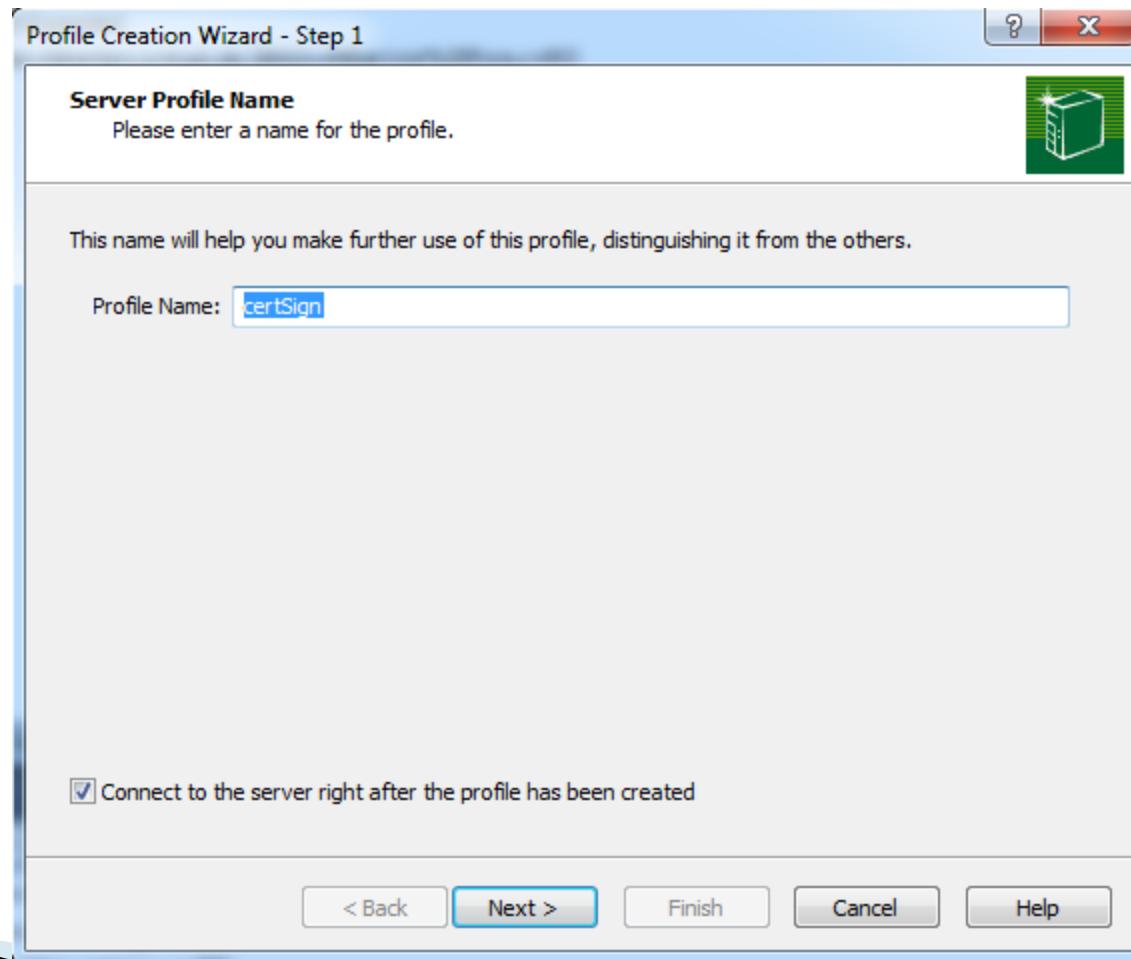
# LDAP

- ▶ RFC 2587 – Internet X.509 Public Key Infrastructure LDAPv2 Schema
  - <https://www.ietf.org/rfc/rfc2587.txt>
  - defines the attributes and object classes to be supported by an LDAP CR server
- ▶ RFC 2559 – Internet X.509 Public Key Infrastructure Operational Protocols – LDAPv2
  - <https://tools.ietf.org/html/rfc2559>
  - defines the access method to a repository with which an End-Entity or a CA can retrieve or modify the certificate and CRL information stored in a CR

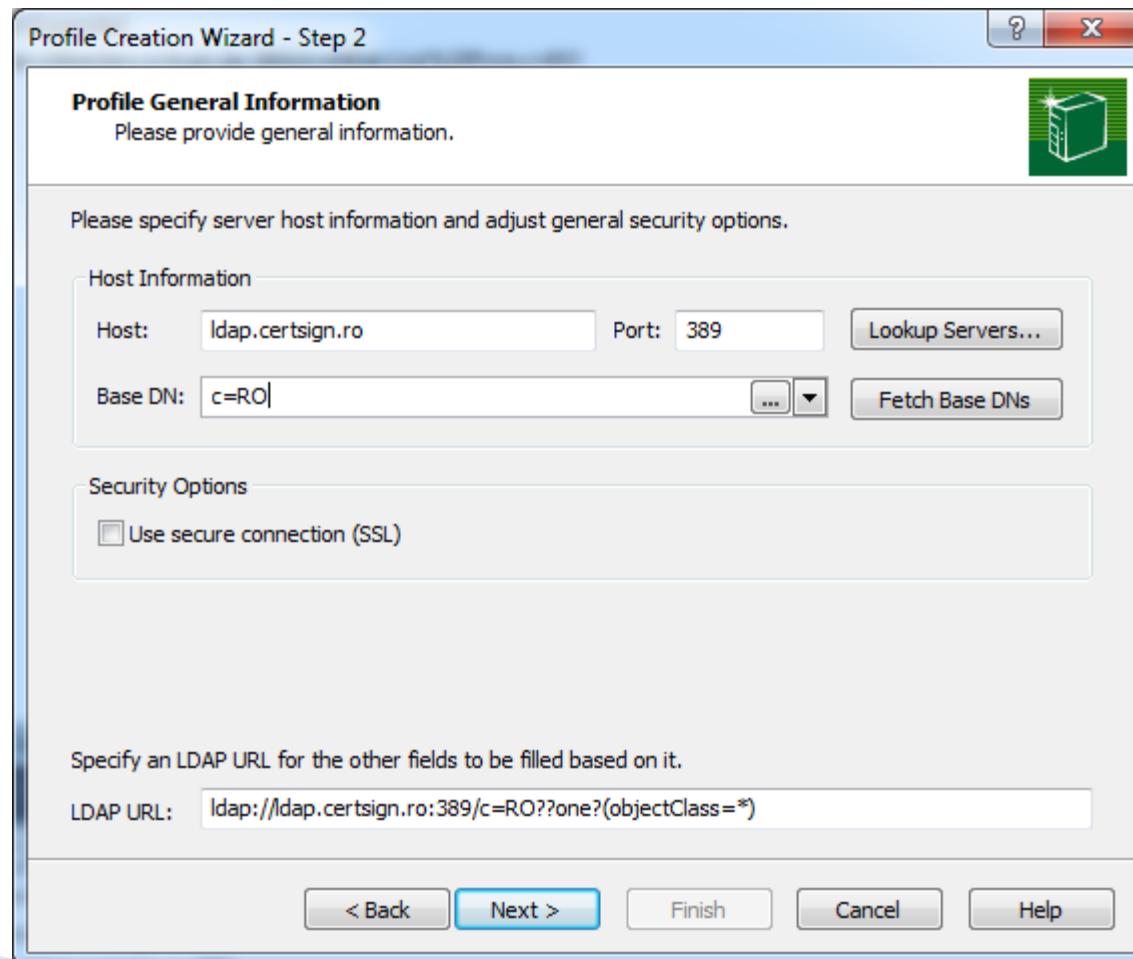
# Softerra LDAP Browser



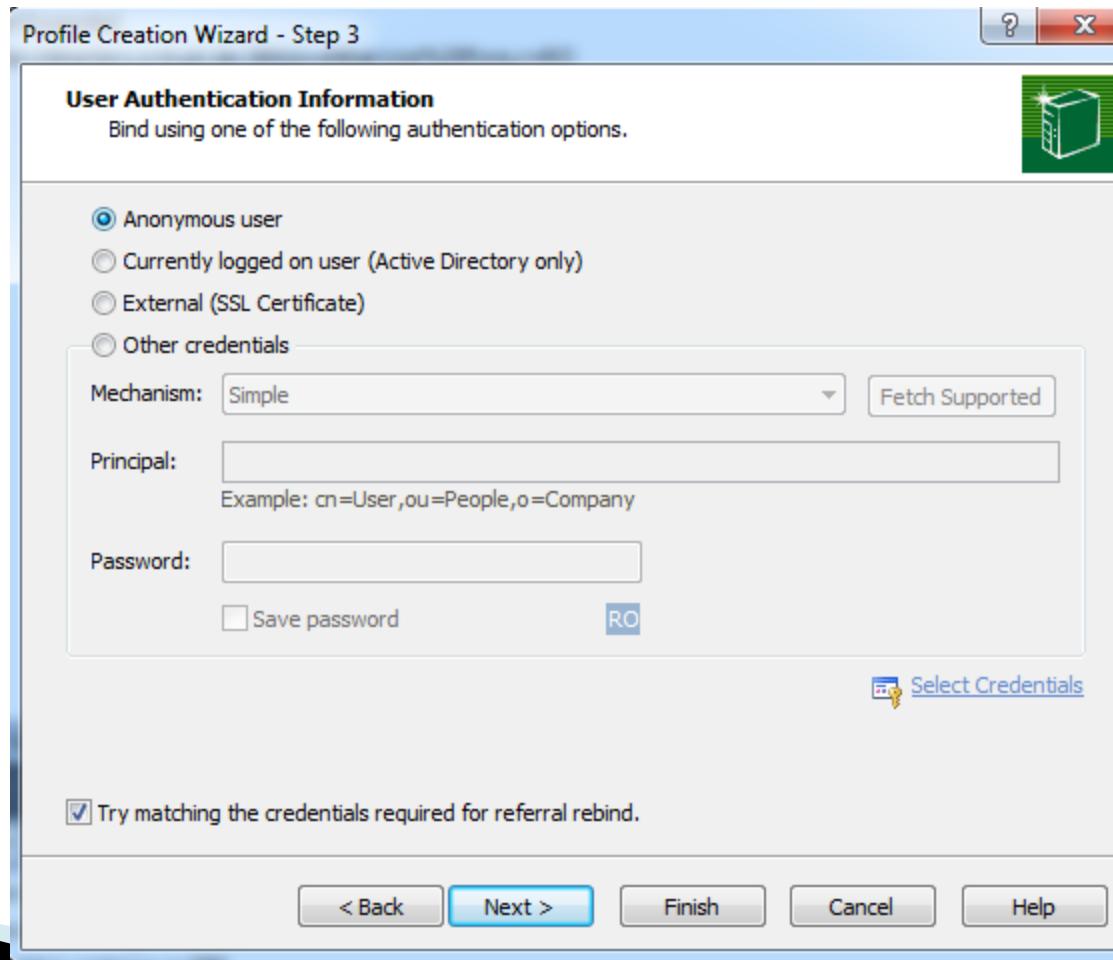
# Softerra LDAP Browser



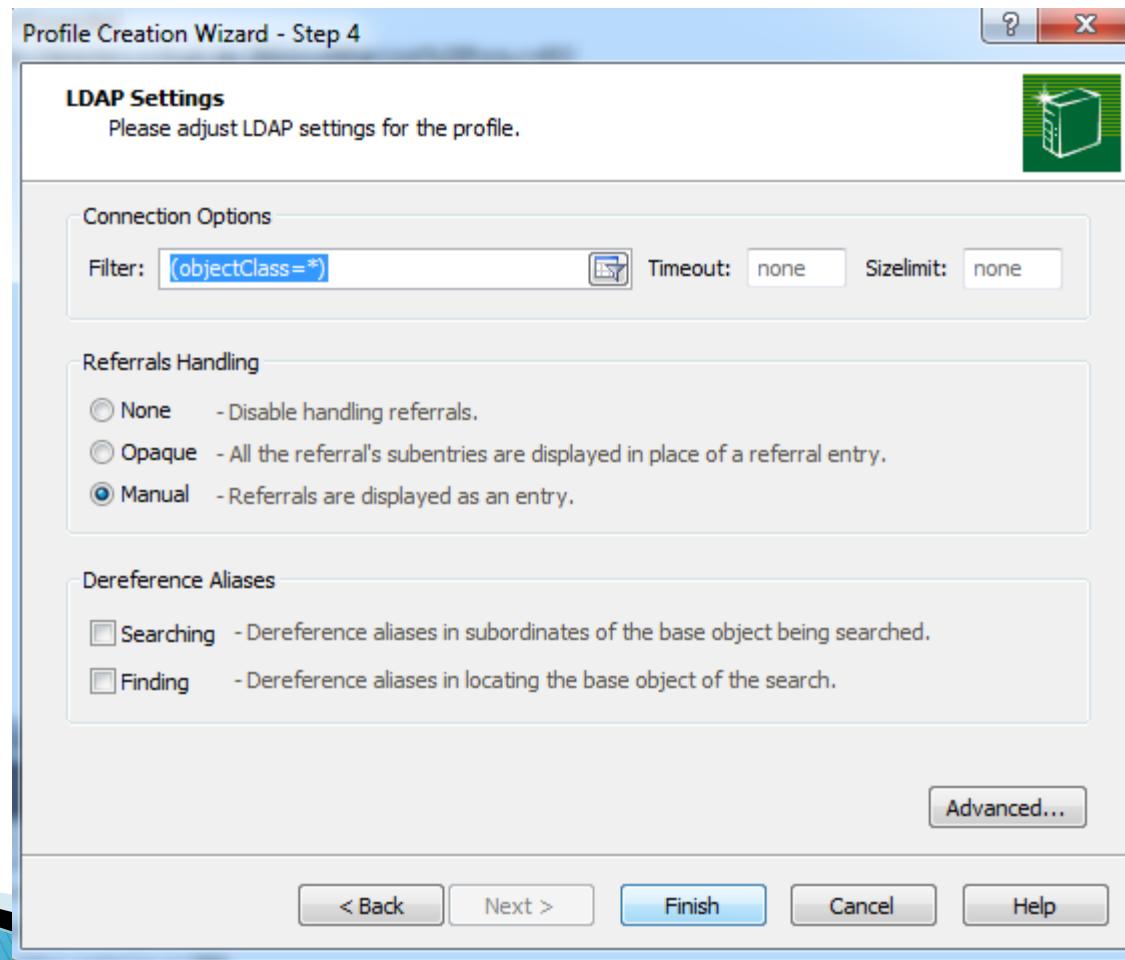
# Softerra LDAP Browser



# LDAP – search for and save a digital certificate



# LDAP – search for and save a digital certificate



# LDAP – search for and save a digital certificate

The screenshot shows the Softerra LDAP Browser 4.5 interface. The title bar indicates the search results for "ou=certSIGN Demo CA Class 1, o=certSIGN, c=RO". The main window displays a table of attributes for this object, with a tooltip showing the details for the "cn" attribute.

Name	Value	Type
ou	certSIGN Demo CA Class 1	Attribute
objectClass	top	Attribute
objectClass	organizationalRole	Attribute
objectClass	certificationAuthority	Attribute
description	Autitate de certificare	Attribute
cn	certSIGN Demo CA Class 1 Size: 22	Attribute
certificateRevocationList	ldap://www.certsign.ro/certSIGN, certSIGN Demo CA Class 1	Attribute
cACertificate;binary	certSIGN Demo CA Class 1	Attribute

The left pane shows the LDAP tree structure, with the selected node being "ou=certSIGN Demo CA Class 1". The bottom pane shows the "Output" section with error messages related to loading RootDSE entries from ldap.certsign.ro:389.

```
Output
Show all items | View Details
Error loading RootDSE entry from ldap.certsign.ro:389.
```

# LDAP – search for and save a digital certificate

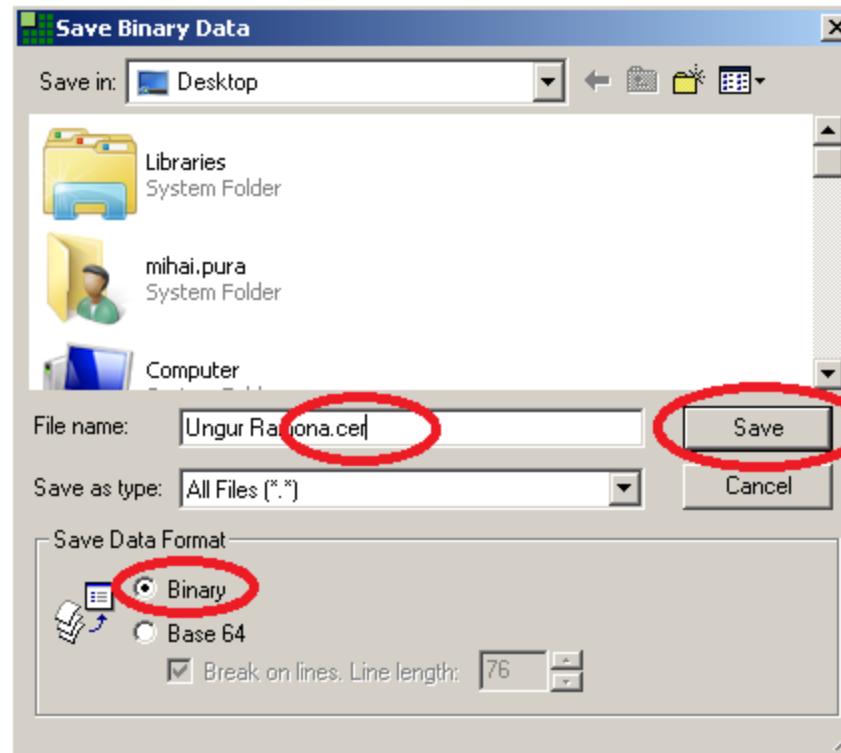
The screenshot shows an LDAP browser window with the title bar "cn=Ungur Ramona,ou=Credits Administration Department,o=FINANSBANK(ROMANIA) S.A.,l=Bucuresti,c=RO". The menu bar includes File, Edit, View, Tools, and Help. The toolbar contains icons for back, forward, search, and file operations. The left pane displays a tree view of the LDAP structure under "Browser root", including "certSIGN", "Sibiu", "Bucuresti", and various organizational units like "Cabinetul Calin Tatomir" and "ITREX CONSULTING SRL". The right pane lists attributes for the selected entry:

Name	Value	Type	Size
objectClass	top	text ...	3
objectClass	person	text ...	6
objectClass	organizationalPerson	text ...	20
cn	Ungur Ramona	text ...	12
telephoneNumber	-	text ...	1
mail	-	text ...	1
sn	-	text ...	1
userCertificate;binary	30 82 05 DD 30 [REDACTED]	Show X.509 Certificate(s) Information...	1505
creatorsName	cn=Manager	...er...	10
createTimestamp	20060714154607	...er...	15
modifiersName	cn=Manager	...er...	10
modifyTimestamp	20060714154607	...er...	15
subschemaSubentry	cn=Subschema	...er...	12

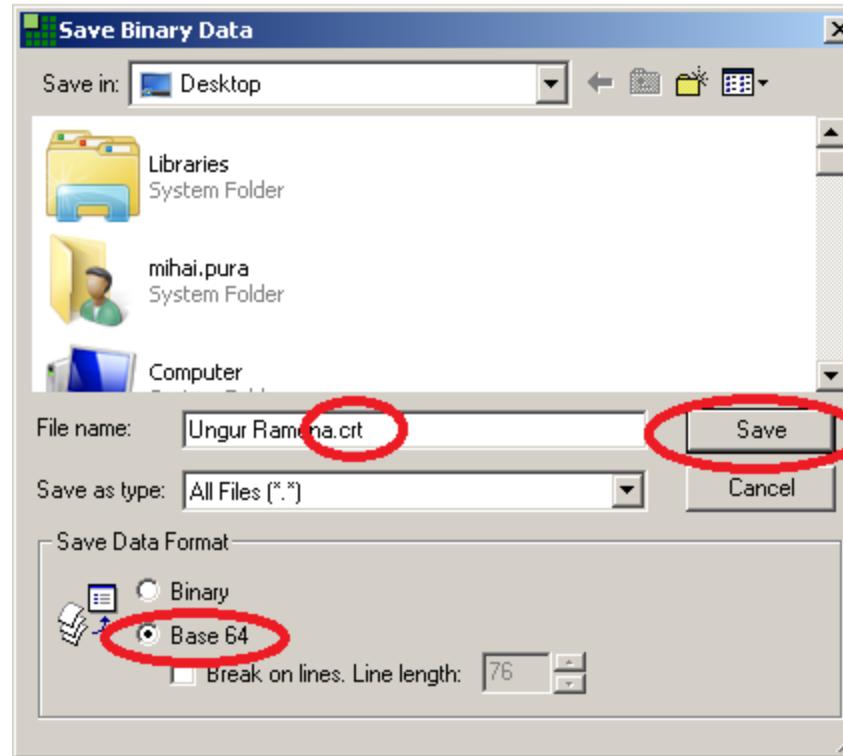
A context menu is open over the "userCertificate;binary" entry, listing options: Refresh (F5), Cut (Ctrl+X), Copy (Ctrl+C), Paste (Ctrl+V), Save Data (selected), and Properties (Alt+Enter). The bottom pane shows a "Messages" log with several error messages related to size limits:

- [ERROR 81] Can't contact LDAP server
- Successfully connected to ldap.certsign.ro
- [ERROR 4] Sizelimit exceeded
- [ERROR 4] Sizelimit exceeded
- Successfully connected to ldap.certsign.ro
- Successfully connected to ldap.certsign.ro
- [ERROR 4] Sizelimit exceeded
- [ERROR 4] Sizelimit exceeded

# LDAP – search for and save a digital certificate

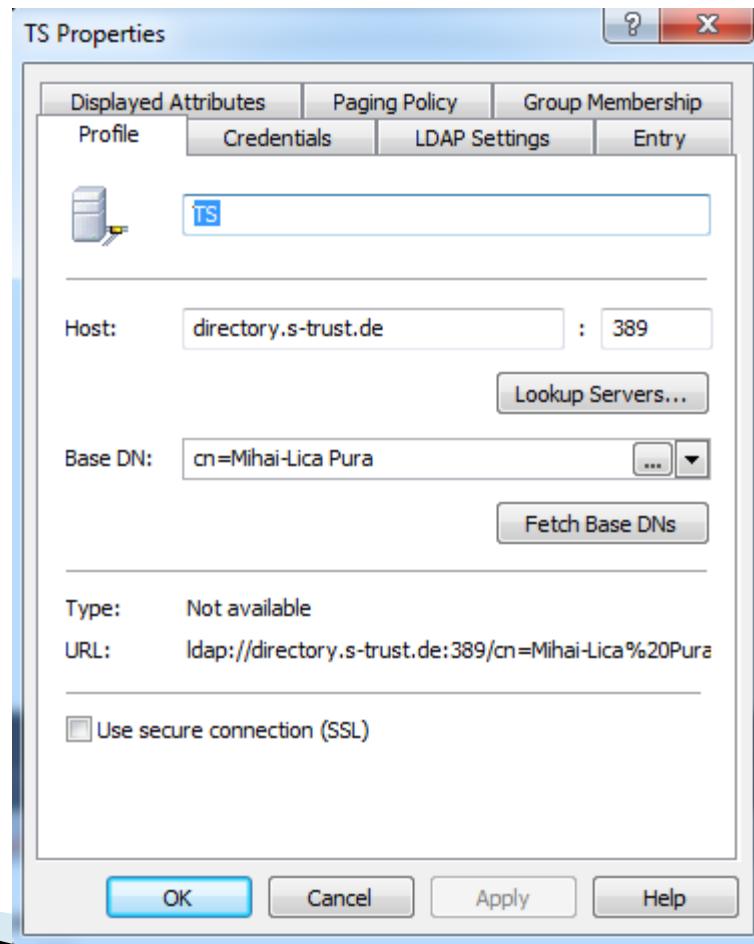


# LDAP – search for and save a digital certificate

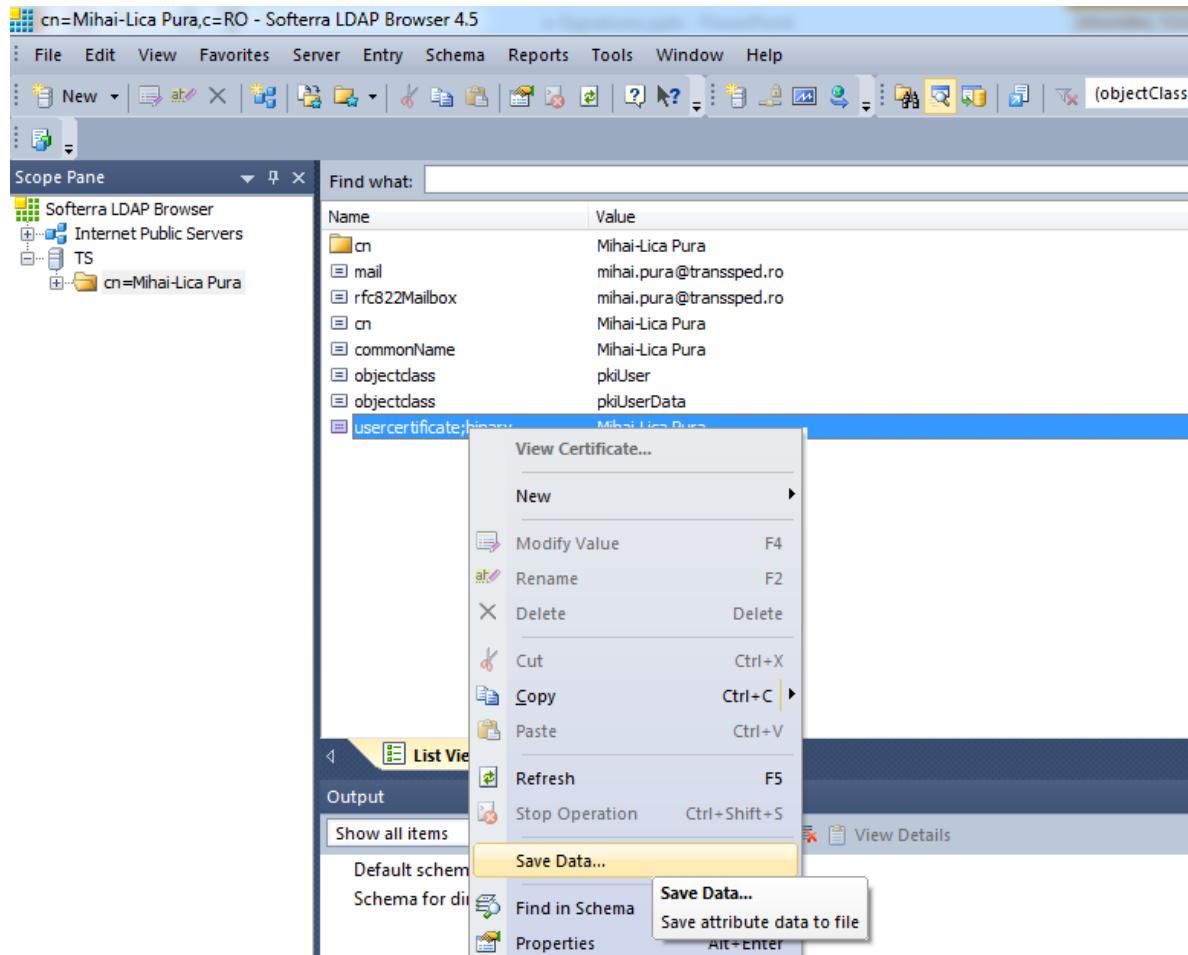


# Trans Sped LDAP Server

- ▶ `ldap://directory.s-trust.de`



# Trans Sped LDAP Server



# Certificate revocation

- ▶ A certificate must be revoked when
  - the private key pair is compromised
  - the private key pair is lost
  - the person leaves the company
- ▶ All users know to no longer trust in the revoked certificates
- ▶ The CA makes available the revocation information for the certificates it has issued
  - CRL – Certificate Revocation List
  - OCSP – Online Certificate Status Protocol

# Certificate revocation

**certSIGN.**  
Secure your on-line transactions

Despre noi   Produse   Servicii   Soluții de securitate   Resurse   Contact

**Căutare**

**Testează**  
Certificate demo



**Testează**  
Certificate demo

Testează certificat  
Caută un certificat  
**Revocă un certificat** (This option is circled in red)  
Lista certificate revocate

**Ghid**

- ▶ Pași pentru obținerea unui certificat digital

Pentru a te familiariza cu procedurile de obținere a diferitelor tipuri de certificate, precum și cu certificatele însele, îți oferim posibilitatea de a obține imediat un certificat de test din categoriile prezentate mai jos. Certificatele sunt perfect funcționale și pot fi folosite timp de 3 luni, după care expiră.

În plus, poți cunoaște mai bine și alte etape din ciclul de viață al unui certificat : obținerea lui de către o entitate parteneră - acea persoană care dorește să beneficieze de serviciile infrastructurii noastre de chei publice, prin verificarea unei semnături sau prin criptarea unui document/e-mail -, revocarea sau consultarea listei de certificate revocate – CRL.

Copyright 2007 certSIGN. Toate drepturile rezervate. | [Codul de practici și proceduri \(doc\)](#) | [Politica de certificare \(pdf\)](#) | [Termeni utilizare site](#) | [Sitemap](#)

**UNI**  
GRUP

10  
1

# Certificate revocation

 certSIGN.  
Secure your on-line transactions

Despre noi   Produse   Servicii   Soluții de securitate   Resurse   Contact  

**Testează**  
Certificate demo



## Revocare certificat Demo!

Pentru a căuta certificatul pe care dorești să îl revoci, completează numele, prenumele și e-mailul persoanei care detine certificatul și apasă butonul **Căută**.

Nume:  Numele de familie (Ex: Popescu)

Prenume:  Prenumele (Ex: Marian)

Email:

# Certificate revocation

 certSIGN.  
Secure your on-line transactions

Despre noi   Produse   Servicii   Soluții de securitate   Resurse   Contact   Căutare

**Testează**  
Certificate demo



## Revocare certificat Demo!

Pentru a putea revoca un certificat trebuie să cunoști serialul acestuia și să fiți autorizați.

Serial certificat:  Serialul certificatului pe care dorești să îl revoci.

Pin:  Parola de management a certificatului (parola pe care ai introdus-o la emisie)

**Continuă**

**Numărul serial al certificatului:**  
**– trebuie să fie exact în forma în care a fost scris în fereastra de la emiterea certificatului din care am descărcat fișierul P12**

**– trebuie scris cu majuscule (pentru cifrele hexazecimale A, B, C, D, E, F) și fără spații**

Copyright 2007 certSIGN. Toate drepturile rezervate.

[Codul de practici și proceduri \(pdf\)](#) | [Sfaturi de securitate \(pdf\)](#) | [Documente legale și politici](#)



# Certificate Revocation List

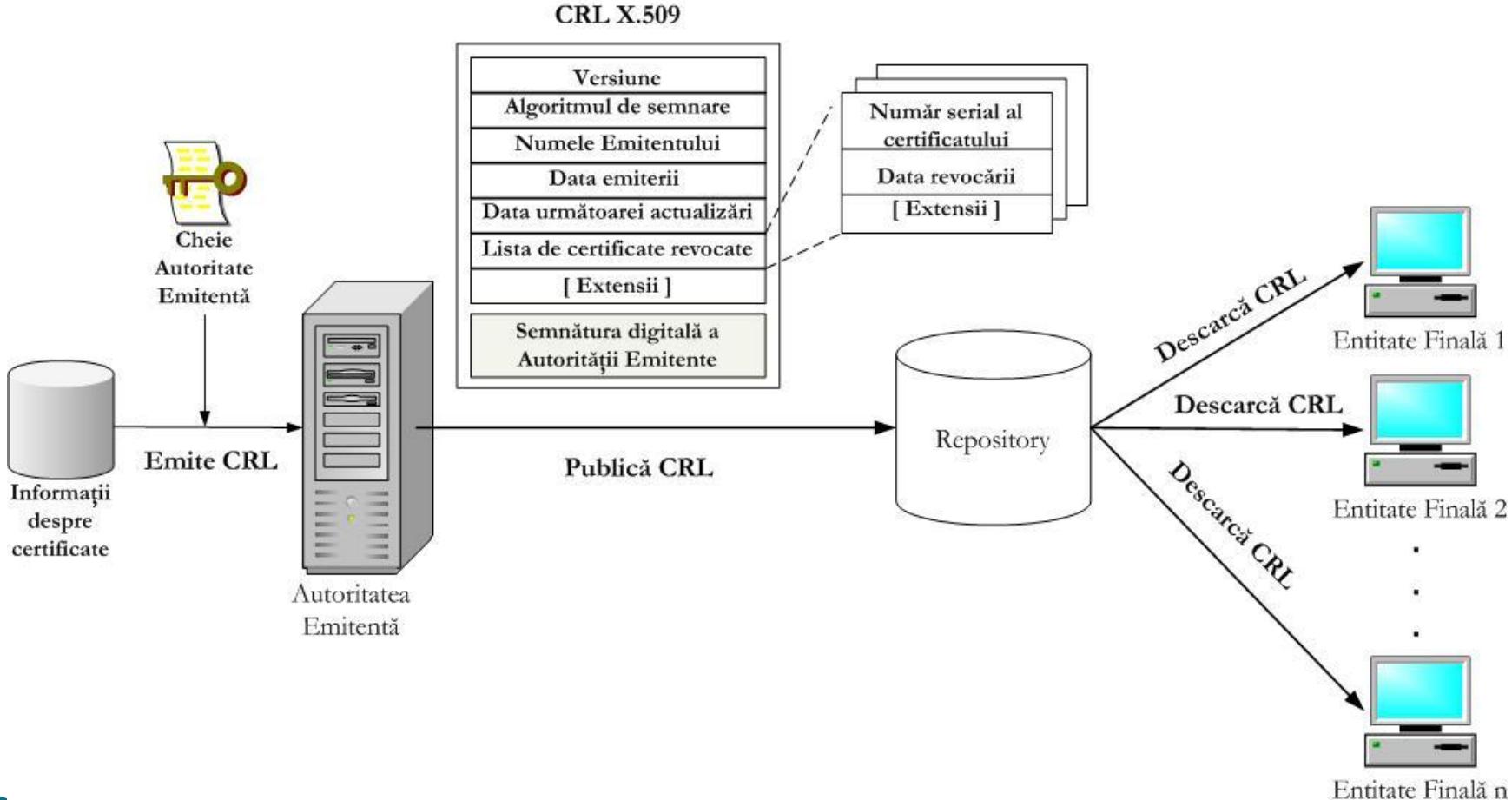
- ▶ contains a list of serial numbers for the certificates that were revoked by the CA
- ▶ the information contained in the CRL is digitally signed by the issuing CA
- ▶ the CRLs are made public by the CA and can be downloaded usually from a web site

# Certificate Revocation List

<b>CRL Version</b>
<b>Issuer's signature alg.ID</b>
<b>Issuer's X.500 name</b>
<b>Date &amp; time of this update</b>
<b>Cert.serial number</b>
<b>Revocation date</b>
<b>Cert.serial number</b>
<b>Revocation date</b>
<b>Cert.serial number</b>
<b>Revocation date</b>
<b>ISSUER SIGNATURE OF CRL</b>

Revoked certificates

# Certificate Revocation List



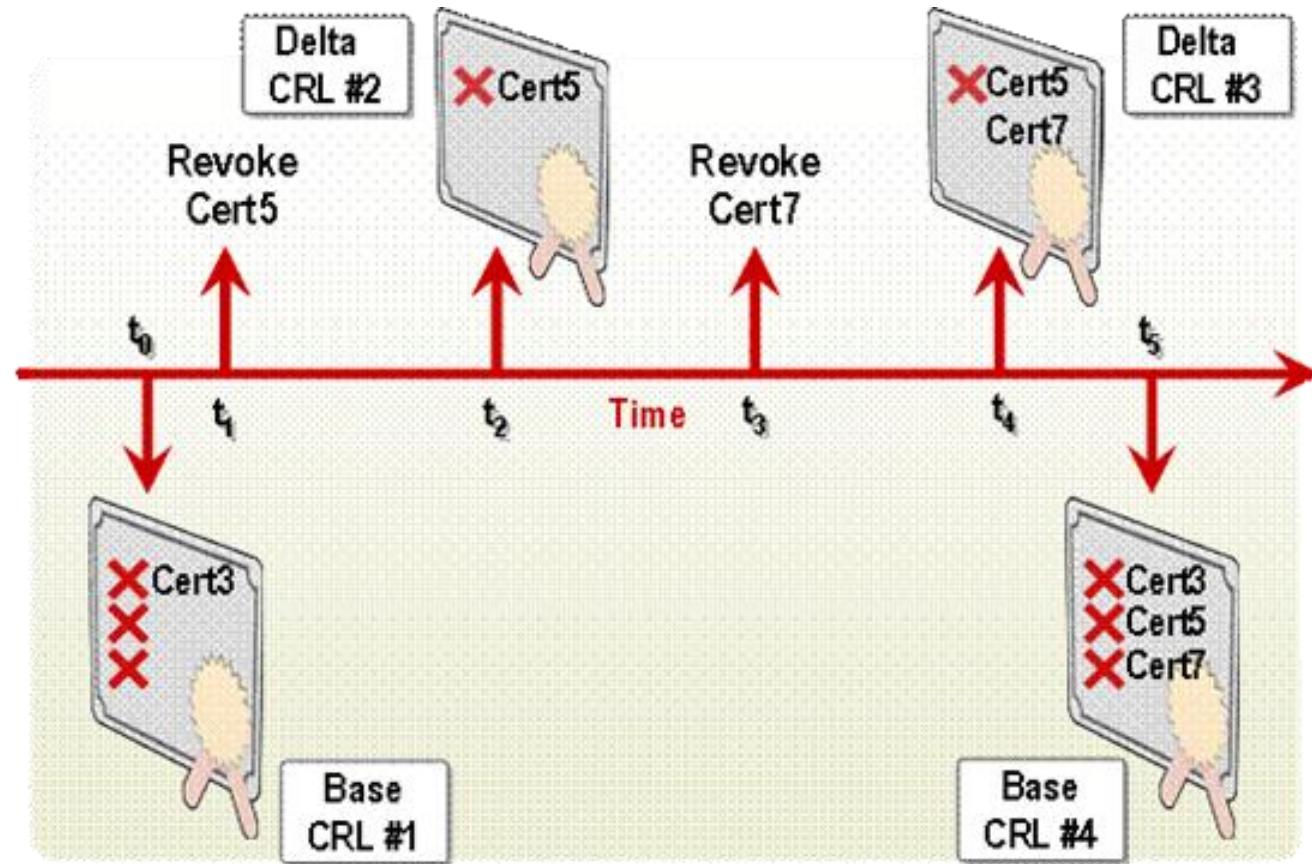
# Certificate Revocation List

- ▶ To check if a certificate has been revoked
  - look for its serial number in the list from the CRL
  - if the serial number is found in the CRL, than the certificate has been revoked
  - otherwise, the certificate has not been revoked

# Certificate Revocation List

- ▶ Relaying parties check CRL before using a certificate
- ▶ Caching a CRL in a local cache
- ▶ Rather than one long CRL, keep multiple shorter CRLs

# Certificate Revocation List



# Certificate Revocation List

- ▶ Distribute the CRL to multiple places and spread the load using the certificate extension field cRLDistributionPoints
- ▶ Use a sufficiently scalable and powerful CR server

# Certificate Revocation List

 certSIGN®  
Secure your on-line transactions

Despre noi   Produse   Servicii   Soluții de securitate   Resurse   Contact

**Testează**  
Certificate demo



**Testează**

**Certificate demo**

---

Testează certificat  
Caută un certificat  
Revocă un certificat  
[Listă certificate revocate](#)

**Ghid**

- Pași pentru obținerea unui certificat digital

**Certificate Demo**

Pentru a te familiariza cu procedurile de obținere a diferitelor tipuri de certificate, precum și cu certificatele însele, îți oferim posibilitatea de a obține imediat un certificat de test din categoriile prezentate mai jos. Certificatele sunt perfect funcționale și pot fi folosite timp de 3 luni, după care expiră.

În plus, poți cunoaște mai bine și alte etape din ciclul de viață al unui certificat : obținerea lui de către o entitate parteneră - acea persoană care dorește să beneficieze de serviciile infrastructurii noastre de chei publice, prin verificarea unei semnături sau prin criptarea unui document/e-mail -, revocarea sau consultarea listei de certificate revocate – CRL.

Copyright 2007 certSIGN. Toate drepturile rezervate. [Codul de practici și proceduri \(doc\)](#) | [Politica de certificare \(pdf\)](#) | [Termeni utilizare site](#) | [Sitemap](#)

**UTI**  
GRUP

11

# Certificate Revocation List

 certSIGN®

Secure your on-line transactions

[Despre noi](#) [Produse](#) [Servicii](#) [Soluții de securitate](#) [Resurse](#) [Contact](#)

[Căutare](#)

**Testează**  
Certificate demo

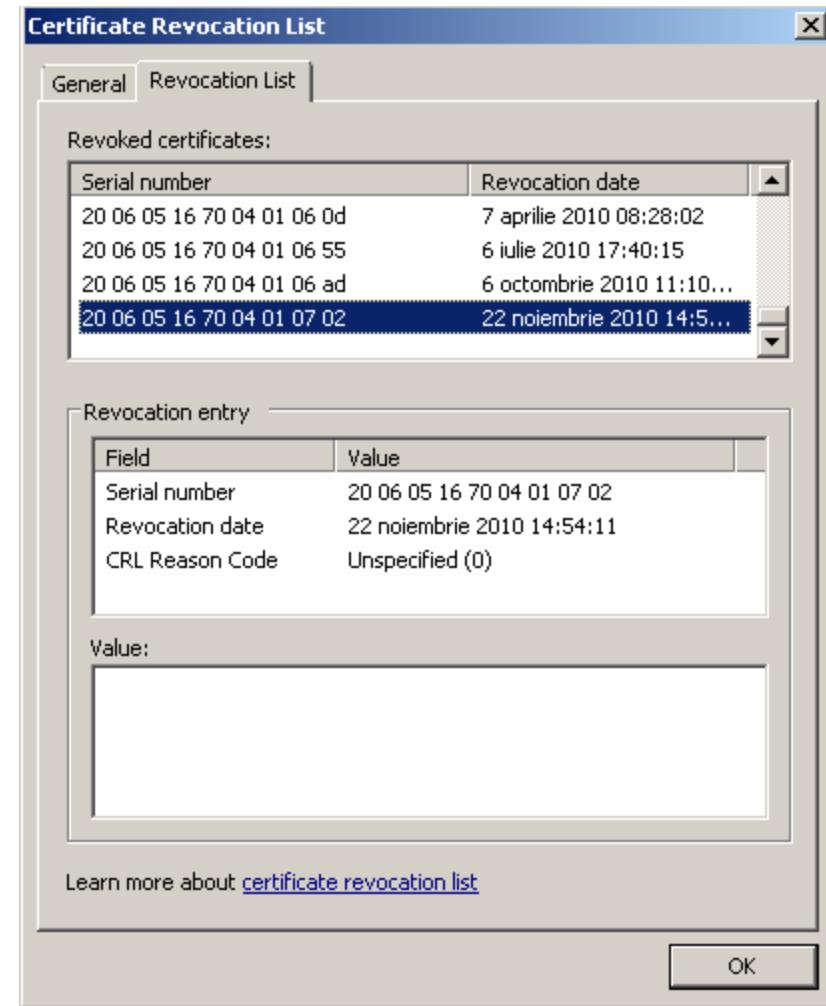
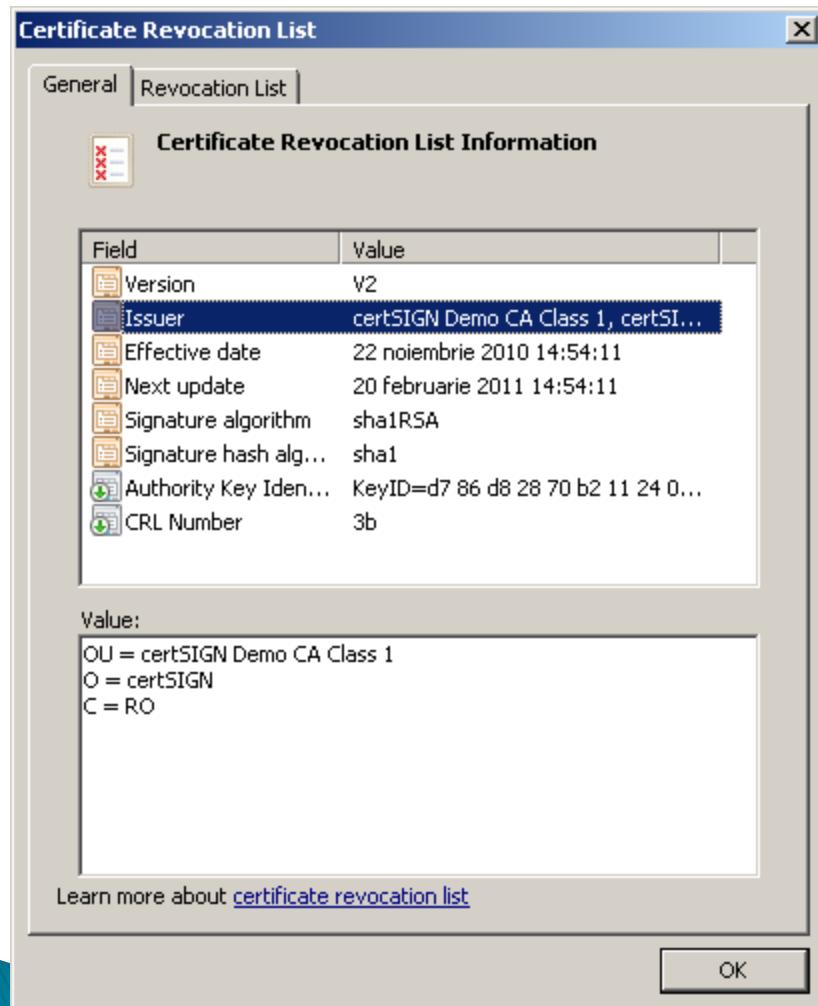


## Certificate/Crl-uri clase Demo!

Lista cu autoritățile care emit certificate Demo. Poți descărca CRL-ul sau certificatul autorității facând clic pe link-ul corespunzător.

Autoritate	Serial	Stare	Acțiuni
certSIGN Demo CA Class 1	049a	Activ	<a href="#">Download CRL</a> <a href="#">Certificat</a>

# Certificate Revocation List



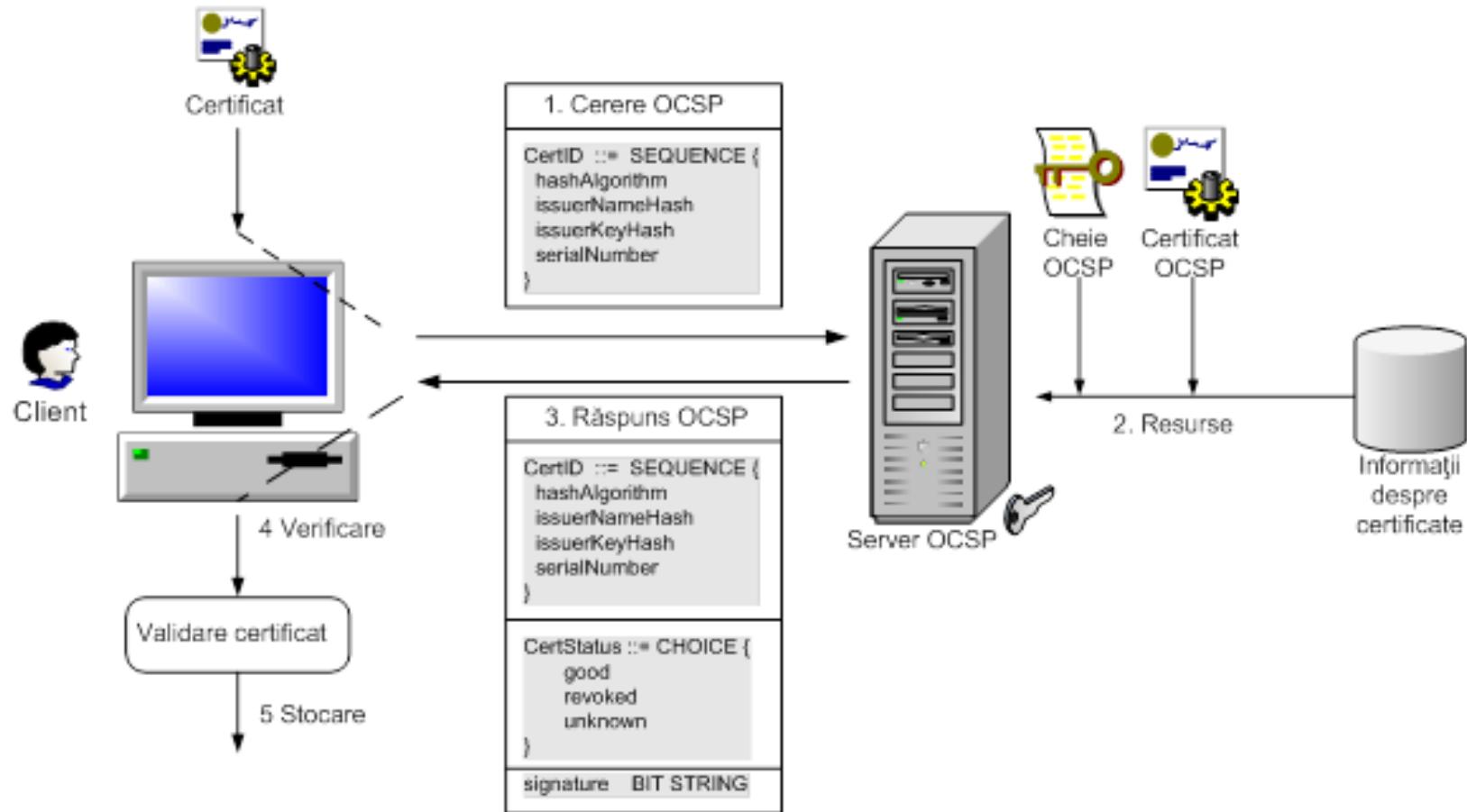
# Import CRL into certificate store

- ▶ The same way a digital certificate is imported

# OCSP

- ▶ RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
  - <https://tools.ietf.org/html/rfc6960>
  - Inquires issuing CA whether a certificate is still valid
  - Response: YES/NO
- ▶ <http://www.openssl.org/docs/apps/ocsp.html>

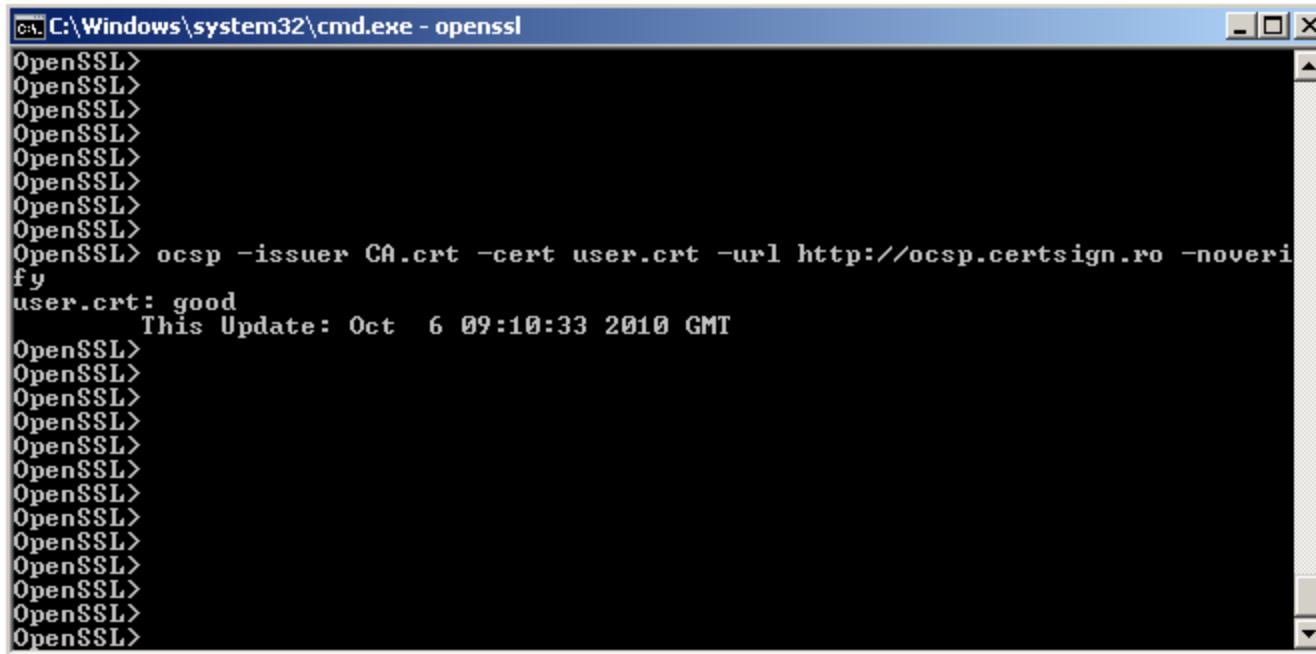
# OCSP



# Verify revocation status with openssl

- ▶ openssl can be downloaded from  
<http://gnuwin32.sourceforge.net/packages/openssl.htm>
- ▶ The command for OCSP validation of a certificate stored in user.crt is:
- ▶ `openssl ocsp -issuer CA.crt -cert user.crt -url http://ocsp.certsign.ro -noverify -text`
- ▶ CA certificate and the certificate that needs to be validated must be in **PEM (BASE64)** format.

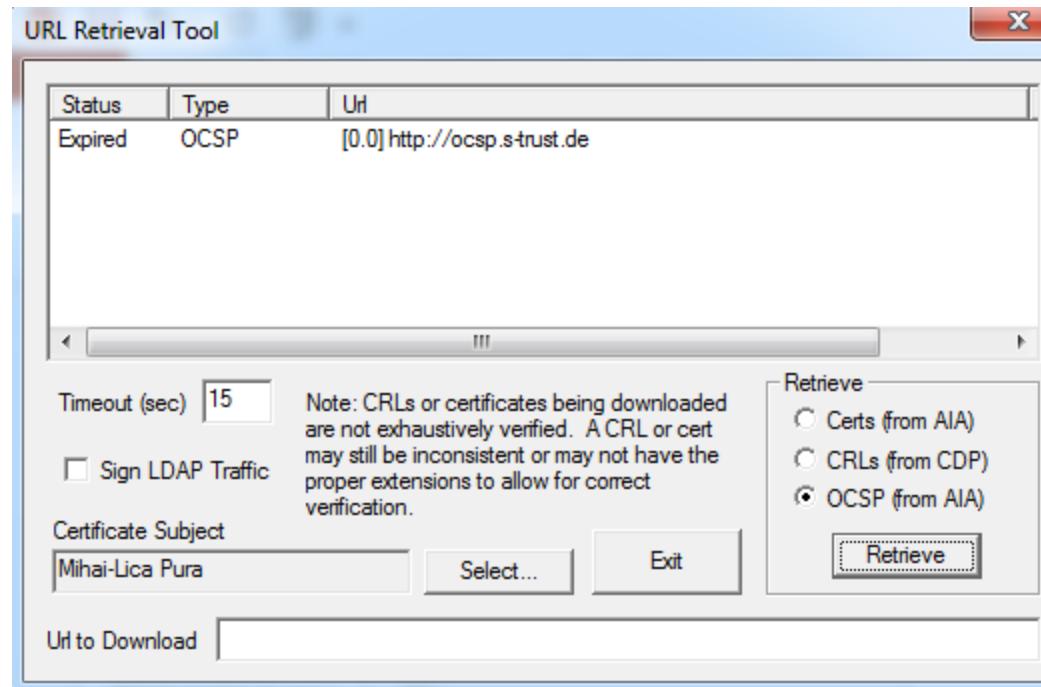
# Verify revocation status with openssl



```
C:\Windows\system32\cmd.exe -openssl
OpenSSL>
OpenSSL>
OpenSSL>
OpenSSL>
OpenSSL>
OpenSSL>
OpenSSL>
OpenSSL>
OpenSSL>
OpenSSL> ocsp -issuer CA.crt -cert user.crt -url http://ocsp.certsign.ro -noverify
user.crt: good
      This Update: Oct  6 09:10:33 2010 GMT
OpenSSL>
```

# Verify revocation status with CertUtil

- ▶ certutil –url path\user.cer

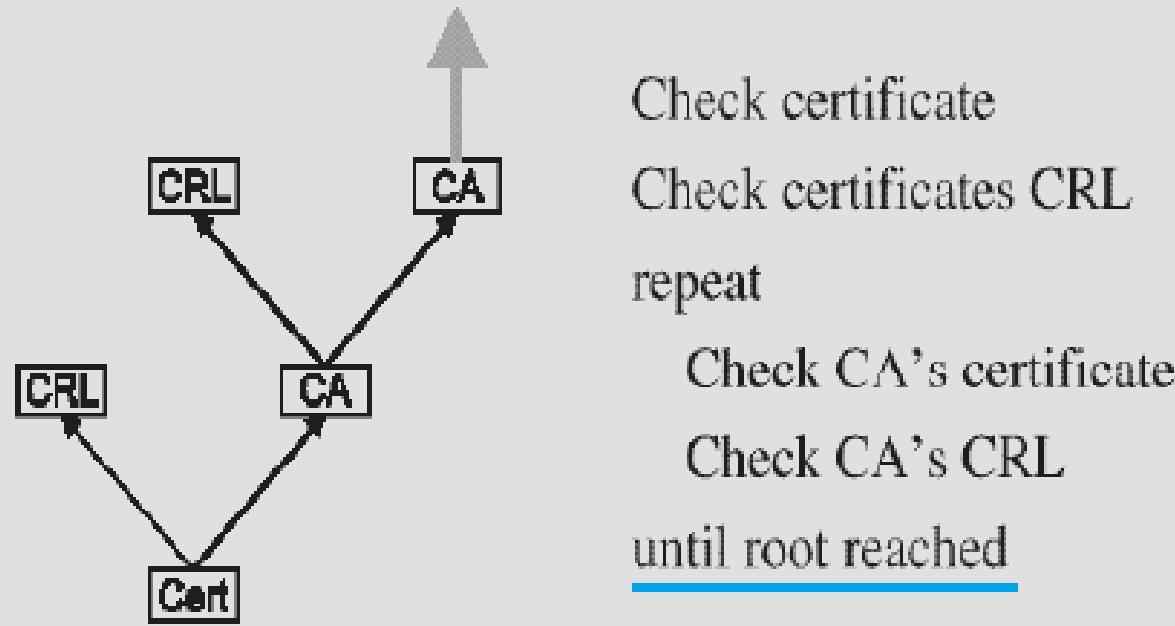


# Certificate validation

- ▶ Certificate validation
  - verify certificate information (**expiration**, scope, policies, etc.)
- ▶ Path validation
  - verify certificate's signature using issuer CA public-key (from CA's certificate)
- ▶ Status validation
  - verify **revocation** status using issuer CA's CRL/OCSP

# Certificate validation

Checking works in reverse order to normal lookup



# Free/Open source CA

- ▶ <https://www.ejbca.org/>
- ▶ <https://www.dogtagpki.org/>
- ▶ <http://simpleauthority.com/>
- ▶ <http://www.cacert.org/>
  - the URL for source code download can be found at About CACert.org
- ▶ <https://letsencrypt.org/>

# PKI in the real world

- ▶ Document signing
  - Signatures with legal value
- ▶ Email encryption & signing (S/MIME)
- ▶ Transport-layer VPNs (using SSL)
- ▶ Network-layer VPNs (using IPSec)
- ▶ Web servers authentication (HTTPS)

# PKI in the real world

- ▶ Web servers & Client mutual authentication (HTTPS)
- ▶ TCP servers & Clients authentication (SSL)
- ▶ User authentication to services (databases, etc.)
- ▶ Network/IT Infrastructure services access (smartcard logon)
- ▶ ...

# Electronic signature vs. digital signature

- ▶ **Electronic signatures:**
  - legal concept that captures
    - intent
    - and consent
  - can be anything, from a scripted text, click-to-sign, image or voice image that illustrates an action of consent
- ▶ **Digital signatures:** It's the mechanism that secures documents with cryptography

<https://security.stackexchange.com/questions/17554/what-is-the-difference-between-an-electronic-signature-and-a-digital-signature>

# Electronic signature vs. digital signature

- ▶ Are electronic signatures (according to the above definition) **legally binding**?
- ▶ There is no absolute answer, because it depends of the national regulations
- ▶ e.g. U.S.A.  
<https://www.globalsign.com/en/blog/electronic-signatures-vs-digital-signatures/>

# E-signature vs. e-seal

- ▶ According to eIDAS (EU regulation 2014/910)

<https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>

- **e-seal**
  - Created by a legal person (e.g. an organization)
  - Without any human interaction (automatically)
- **e-signature**
  - Created by a natural person (e.g. a human person)
  - The person adding the signature performs some action for this operation
  - The person is authenticated

# The use of digital signatures

- ▶ **1. Signing digital documents**
  - PDF
  - XML
  - Any other kind of files (PKCS#7)
- ▶ **2. Certificate login**
- ▶ **3. Code signing**
  - Java Web Start applications
  - Microsoft Office macros
  - Microsoft software installation packages

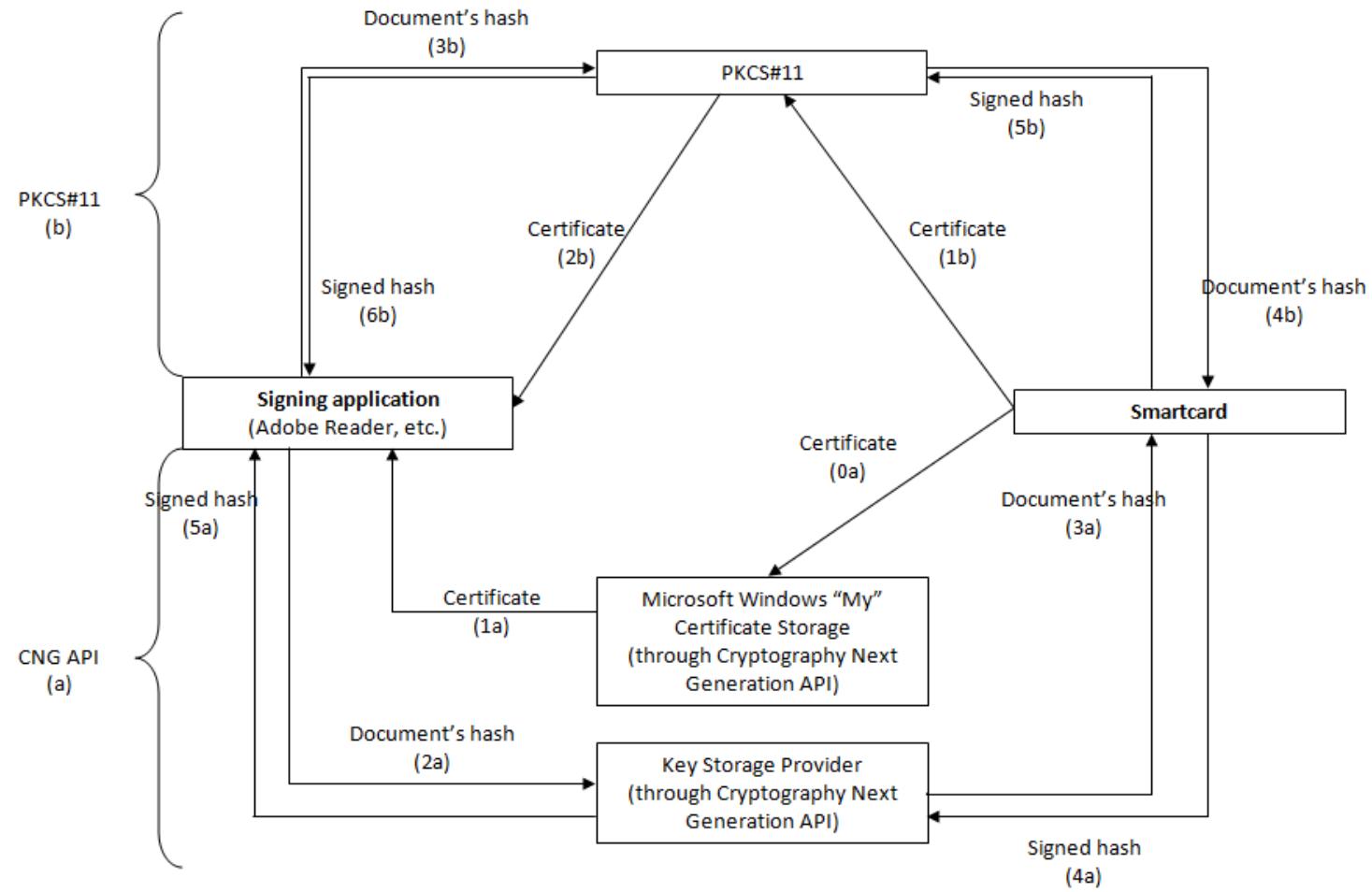
# The use of digital signatures

- ▶ **ANAF**
  - Annual financial reports
  - [https://static.anaf.ro/static/10/Anaf/Declaratii\\_R/instructiuni/etape\\_depunere.htm](https://static.anaf.ro/static/10/Anaf/Declaratii_R/instructiuni/etape_depunere.htm)
  - [https://static.anaf.ro/static/10/Anaf/Declaratii\\_R/instructiuni/Instructiuni\\_D200.htm](https://static.anaf.ro/static/10/Anaf/Declaratii_R/instructiuni/Instructiuni_D200.htm)
- ▶ **CNAS**
  - Reports of medics and pharmacists
  - <http://www.cnas.ro/casmb/page/procedura-de-inregistrare-a-certificatelor-digitale.html>
- ▶ **UNNPR**

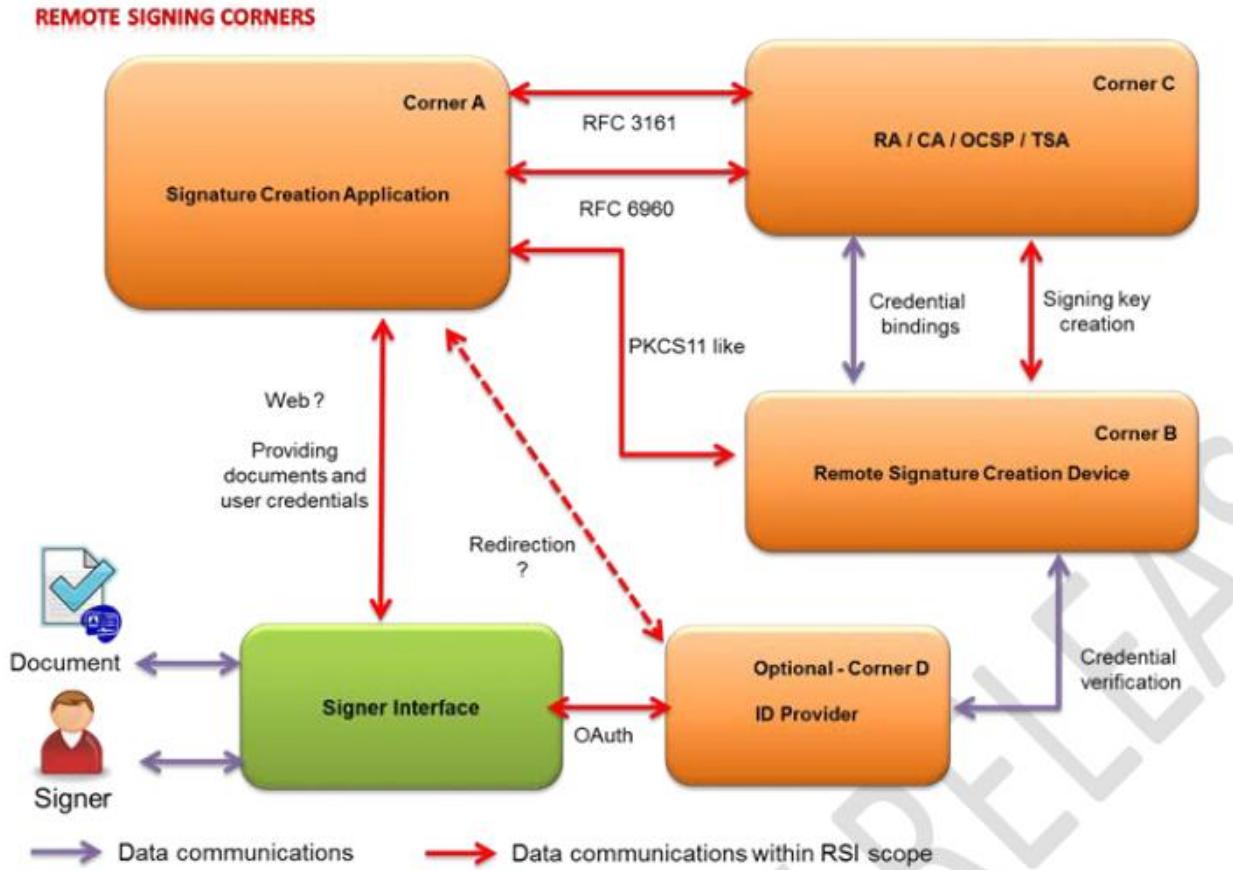
# The use of digital signatures

- ▶ **MySMIS 2014**
  - Access EU funds – Ministry of European Funds
  - <https://2014.mysmis.ro/>
  - <http://www.fonduri-ue.ro/mysmis>
- ▶ **SEAP (Sistemul Electronic de Achiziții Publice)**
  - <http://licitatiiseap.ro/seap/>
  - <https://www.e-licitatie.ro/>
- ▶ **ITM (Inspectoratul Teritorial al Muncii)**
- ▶ **Monitorul Oficial**
- ▶ **ONRC (Oficiul Național al Registrului Comerțului)**
- ▶ **etc.**

# Performing a digital signature (local)



# Performing a digital signature (cloud/remote/mobile/server)



<http://www.cloudsignatureconsortium.org/>

# Digital signatures and PDF files

- ▶ Adobe Acrobat Reader DC
- ▶ [http://get.adobe.com/reader/?promoid=KLX  
ME](http://get.adobe.com/reader/?promoid=KLXME)
- ▶ Previously, a PDF document could be signed only with Adobe Acrobat Professional
- ▶ Starting with Adobe Acrobat Reader X, signing can now be done from the reader

# Sign a PDF file

test.pdf - Adobe Acrobat Reader DC

File Edit View Plug-Ins Window Help

Home Tools test.pdf

Q sign

 Fill and sign documents and forms electronically

Fill & Sign

Open ▾

 Sign

 Sign

 Text

 Digitally sign or certify documents and validate authenticity

Certificates

Open ▾

 Digitally Sign

 Digitally sign document

 Validate All Signatures

 Add stamps such as 'approved' or 'draft'

Stamp

 Stamp

 Add comments with highlights, sticky notes, and mark-up tools

Comment

 Stamps

134

# Sign a PDF file

The screenshot shows the Adobe Acrobat Reader DC interface for a file named "test.pdf". The toolbar includes standard options like File, Edit, View, Plug-Ins, Window, Help, Home, and Tools. The Home tab is selected. The main window displays the PDF content with the text "Test file.". A floating dialog box titled "Acrobat Reader" provides instructions for drawing a signature area. It contains an information icon, a message about dragging to draw a signature, a "Do not show this message again" checkbox, and an "OK" button.

test.pdf - Adobe Acrobat Reader DC

File Edit View Plug-Ins Window Help

Home Tools test.pdf x

1 / 1 147% 147%

Certificates Digitally Sign Validate All Signatures

Test file.

Acrobat Reader

Using your mouse, click and drag to draw the area where you would like the signature to appear. Once you finish dragging out the desired area, you will be taken to the next step of the signing process.

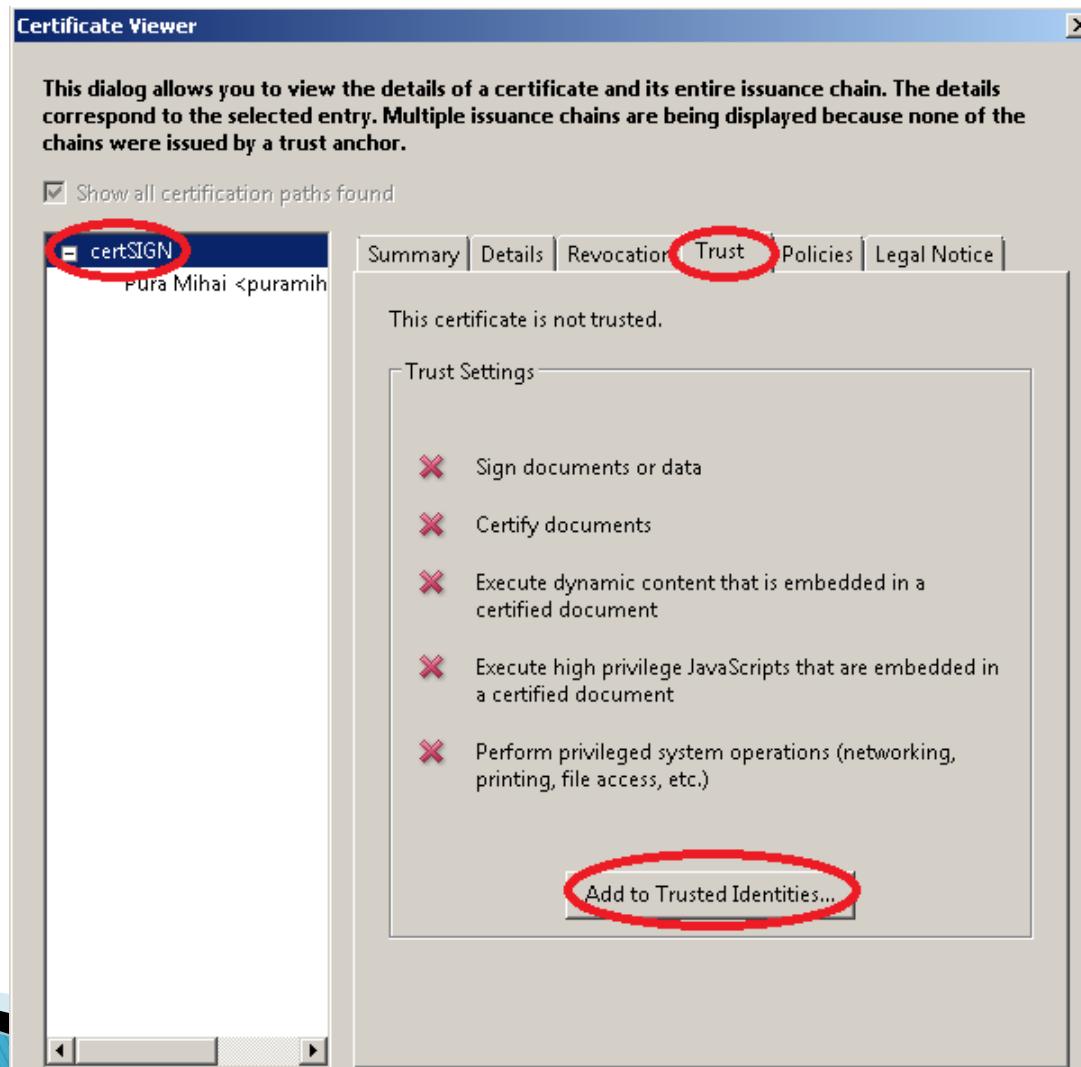
Do not show this message again

OK

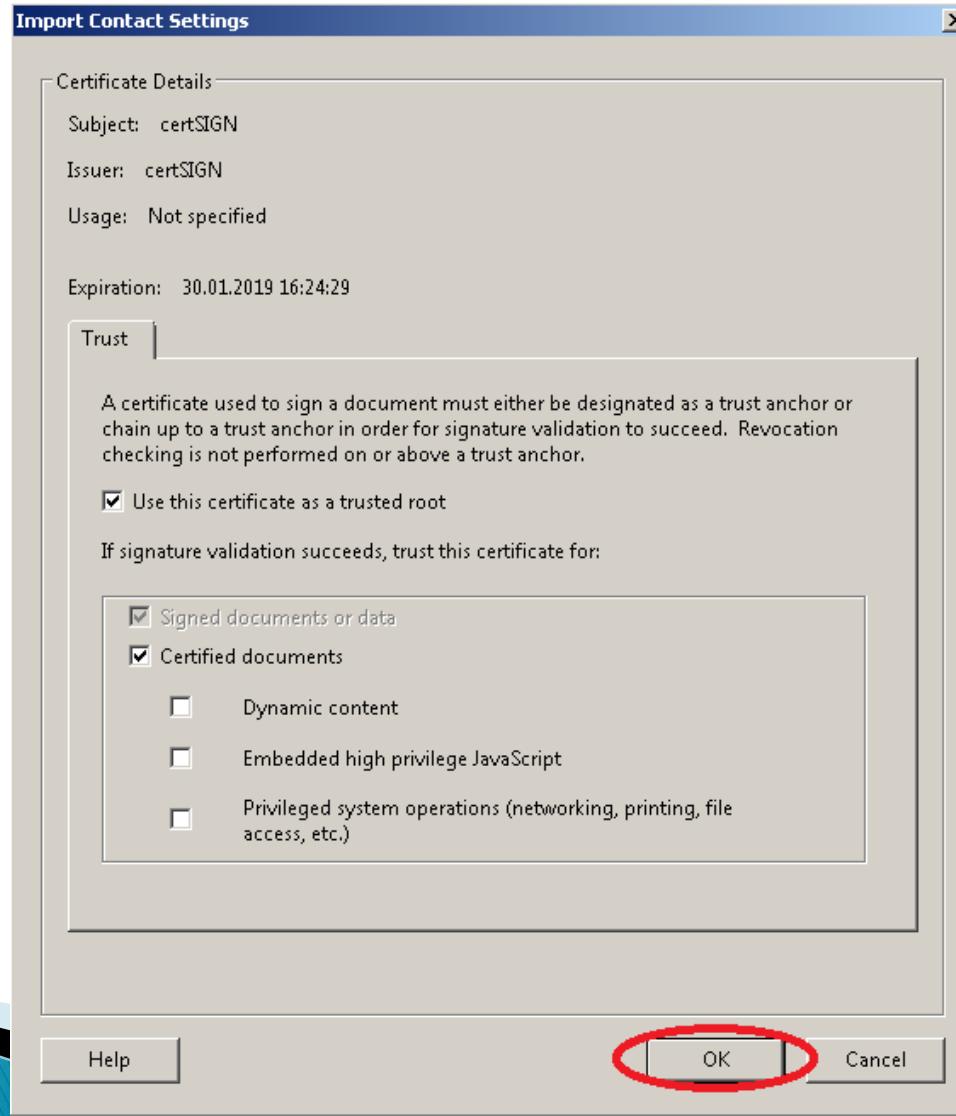
# Sign a PDF file



# Sign a PDF file

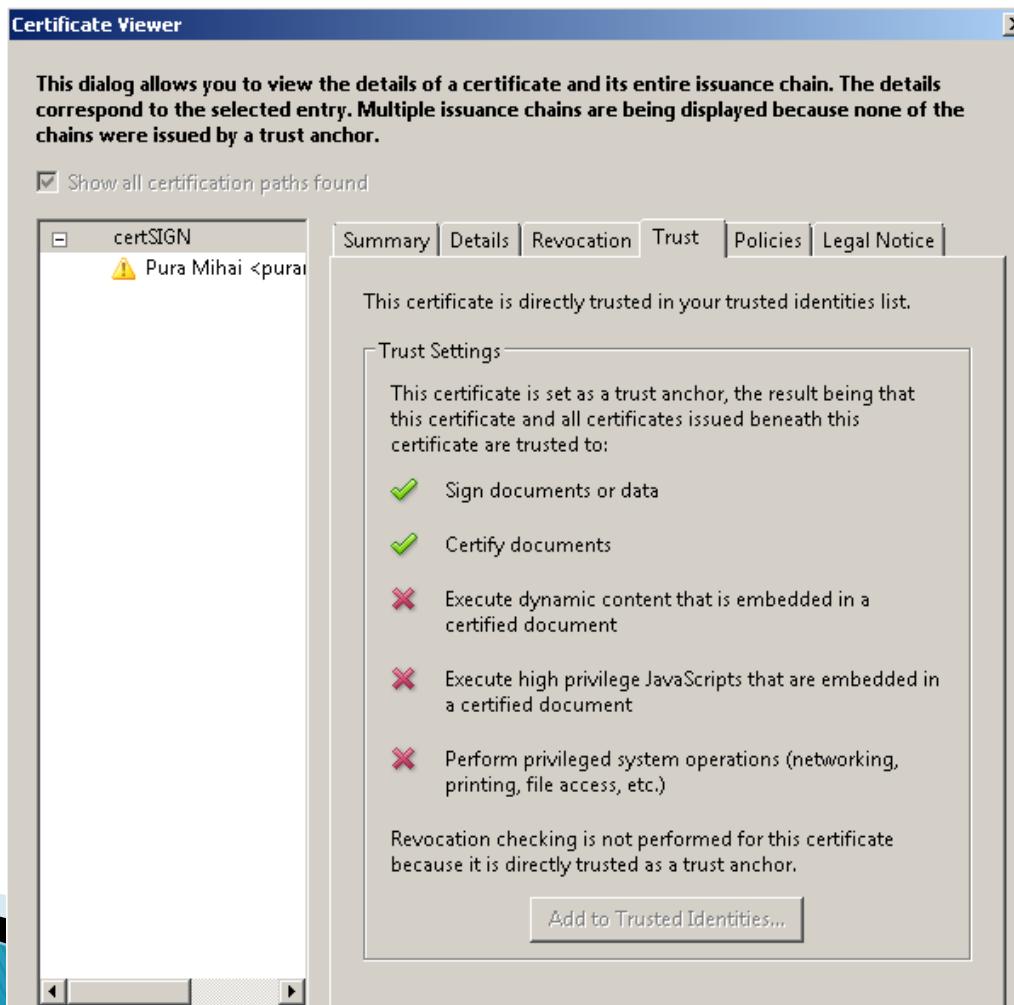


# Sign a PDF file

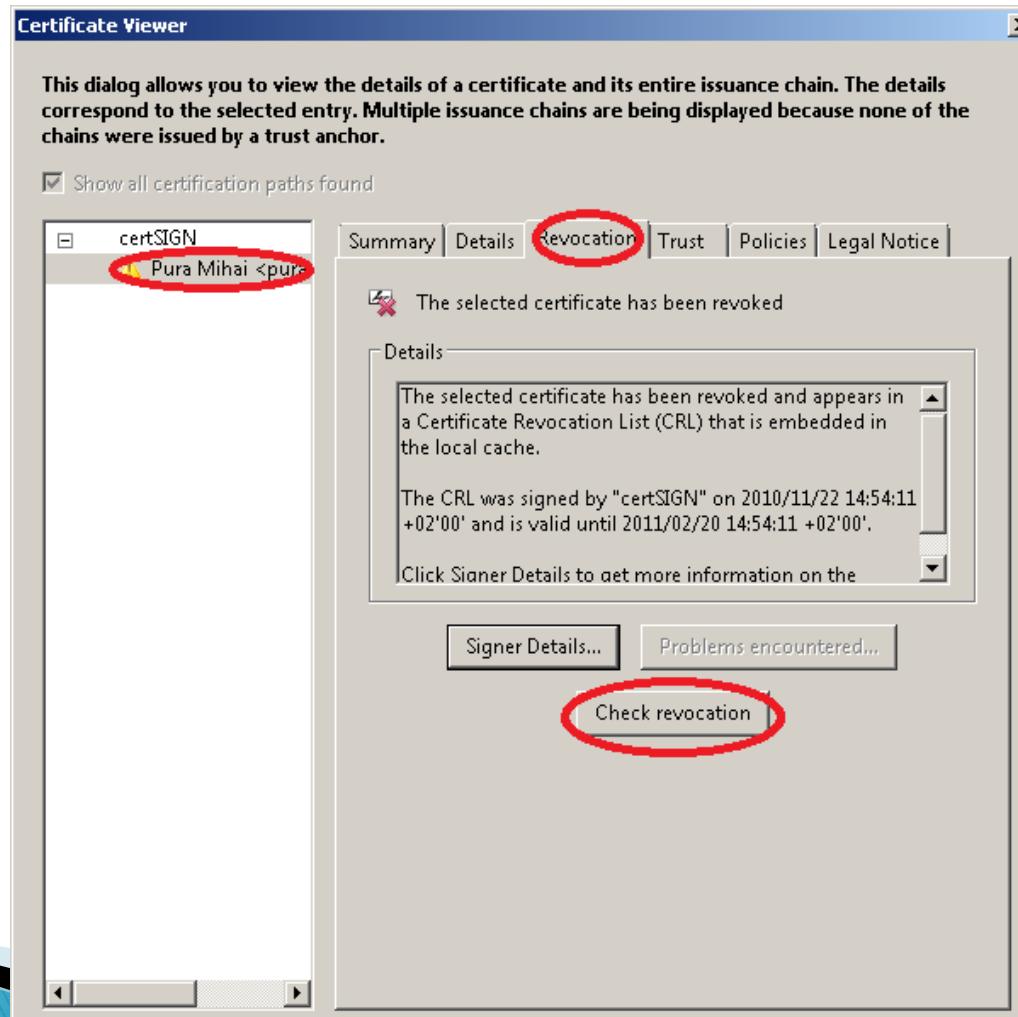


# Sign a PDF file

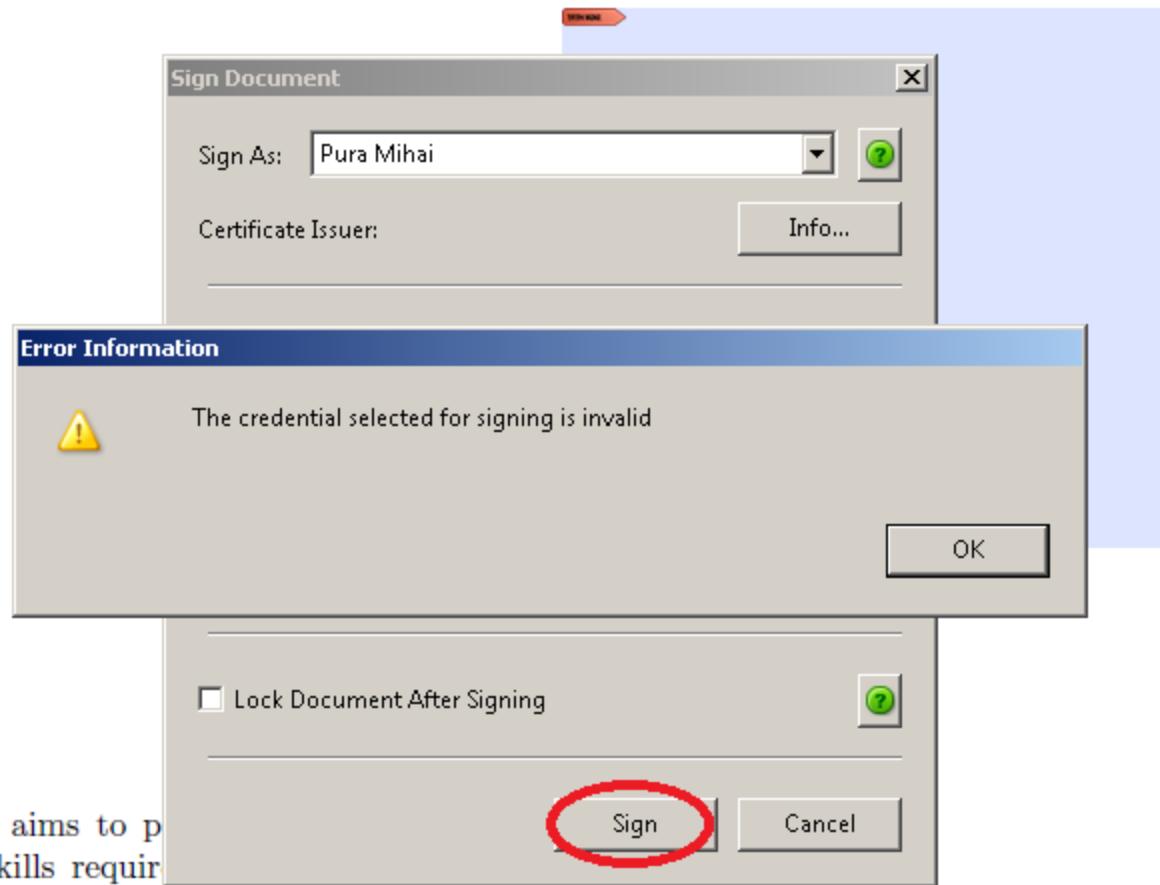
- ▶ Close and then reopen Certificate Viewer



# Sign a PDF file



# Sign a PDF file



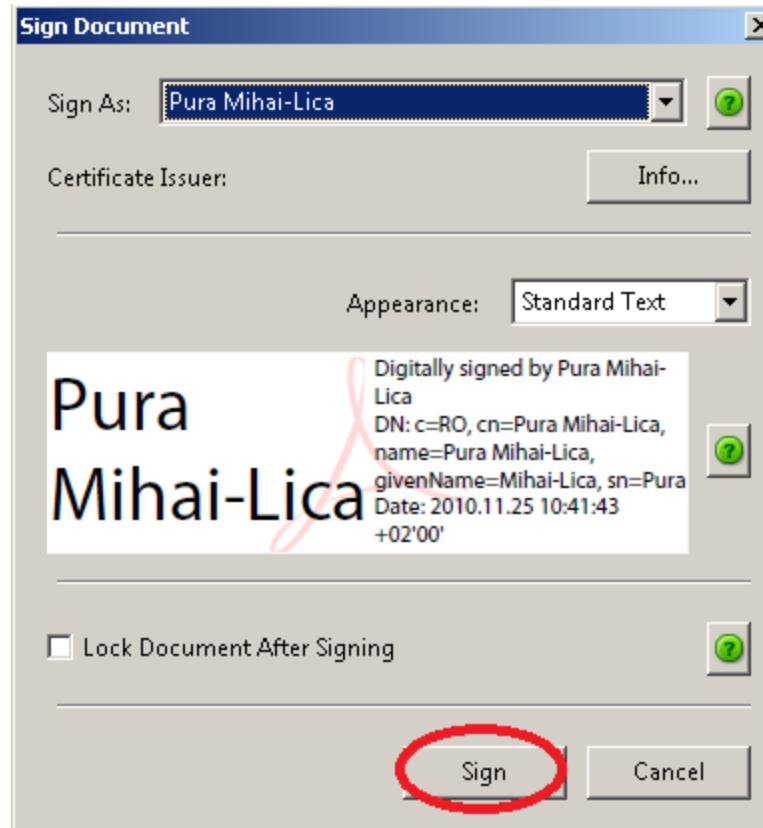
Document aims to p  
se the skills requir

<http://www-h.eng.cam.ac.uk/help/tpl/languages/C%2B%2B/doc/doc.html><sup>1</sup>

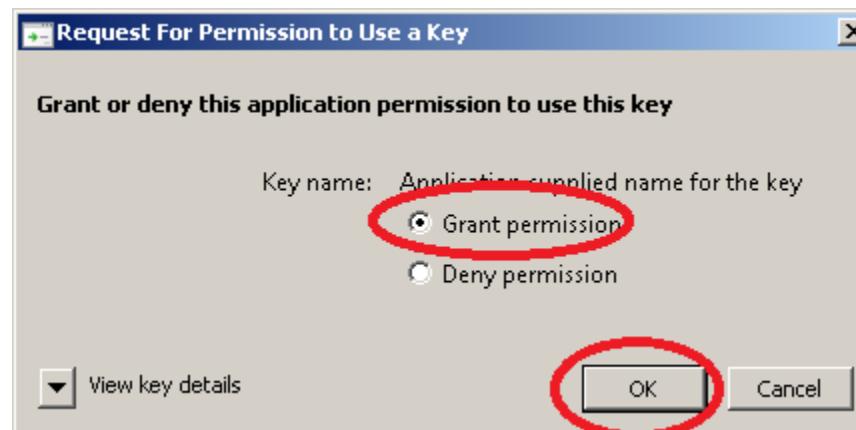
<http://www-h.eng.cam.ac.uk/help/tpl/languages/C%2B%2B/doc/doc.pdf><sup>2</sup>

<http://www-h.eng.cam.ac.uk/help/documentation/docsource/index.html><sup>3</sup>

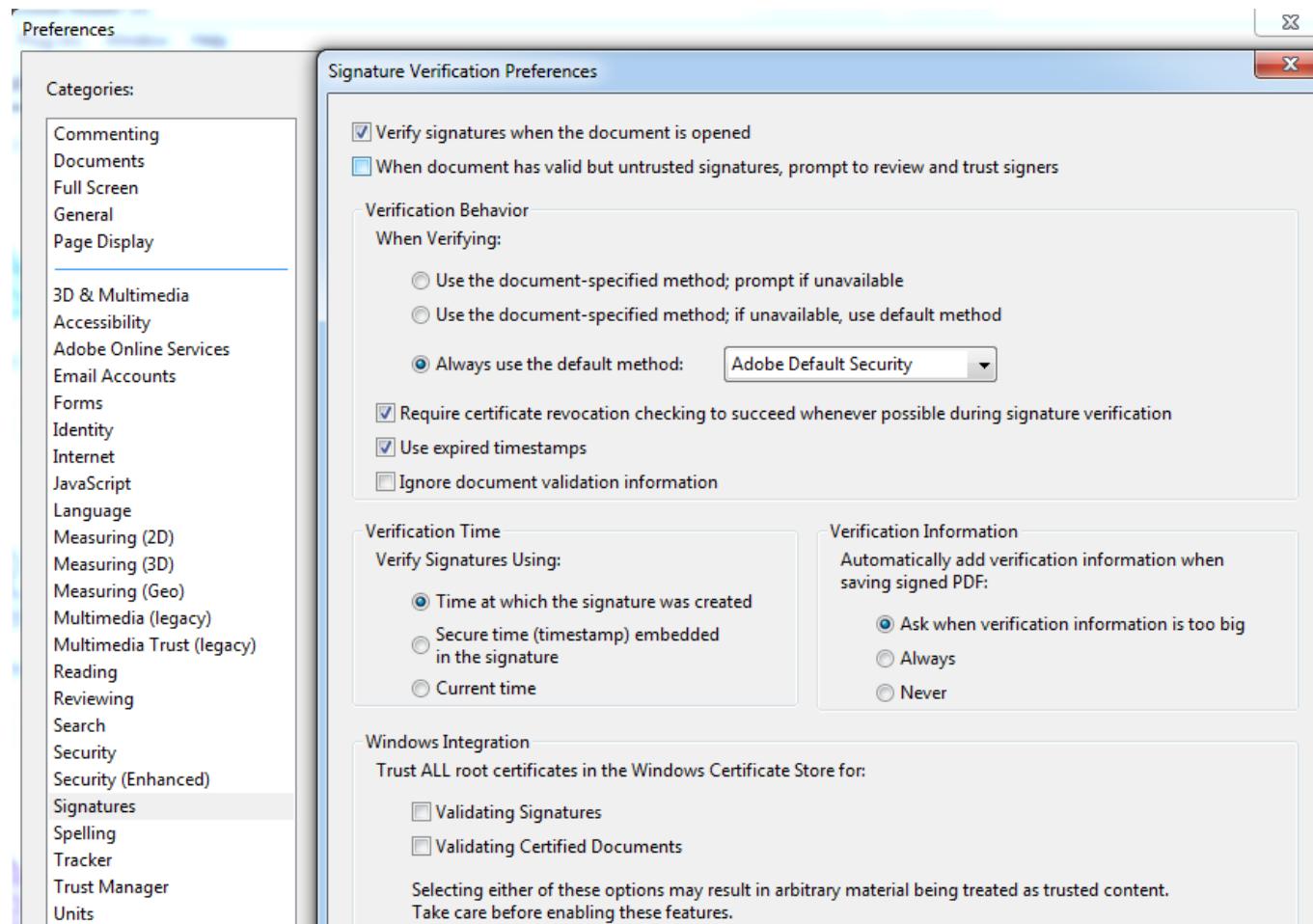
# Sign a PDF file



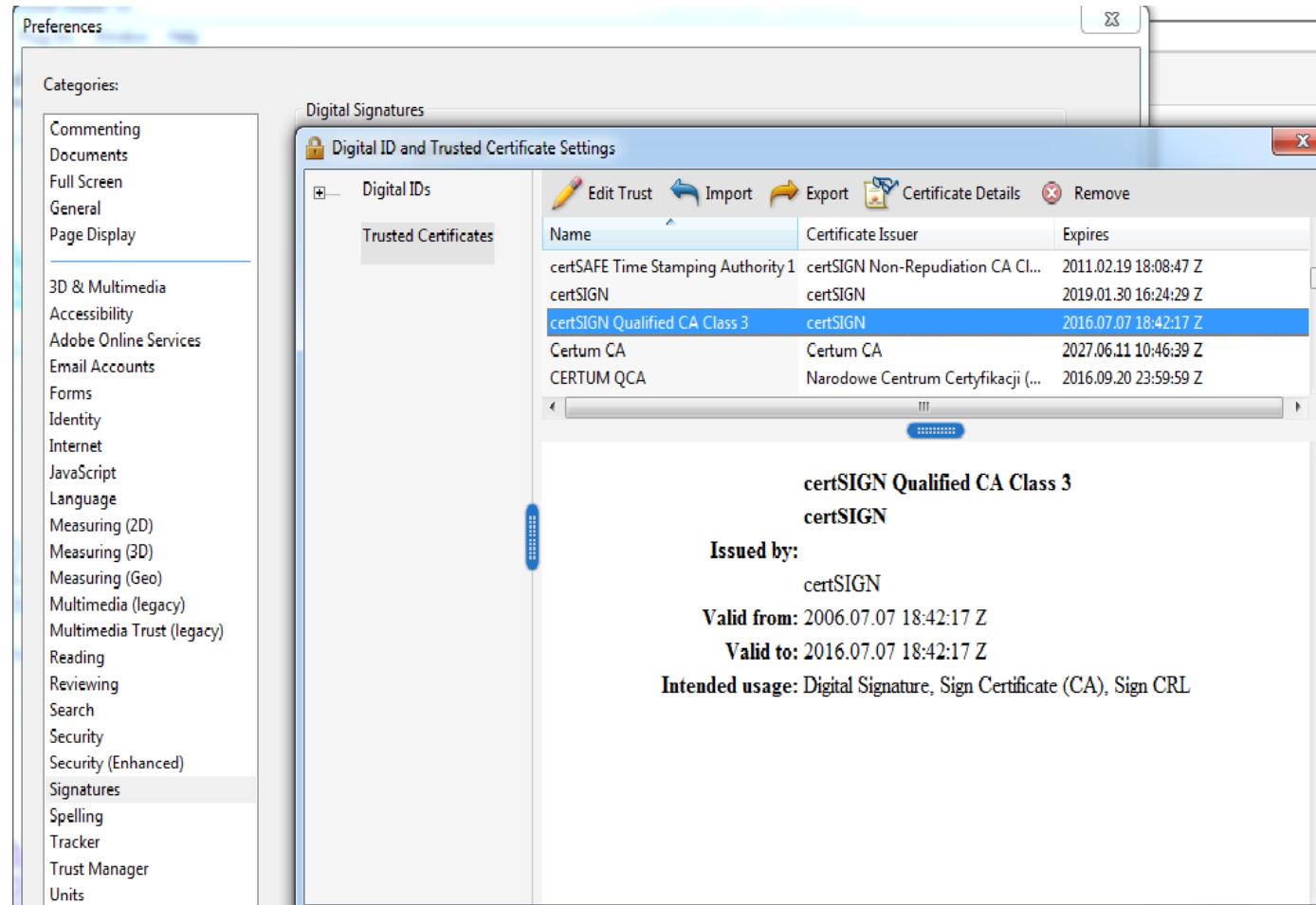
# Sign a PDF file



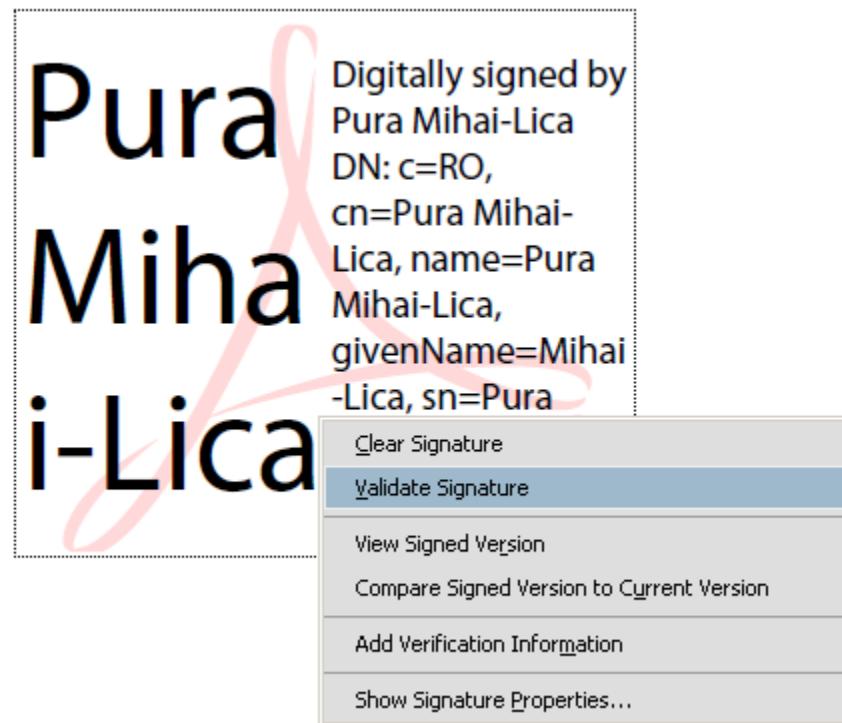
# Verify signatures from a PDF file



# Verify signatures from a PDF file



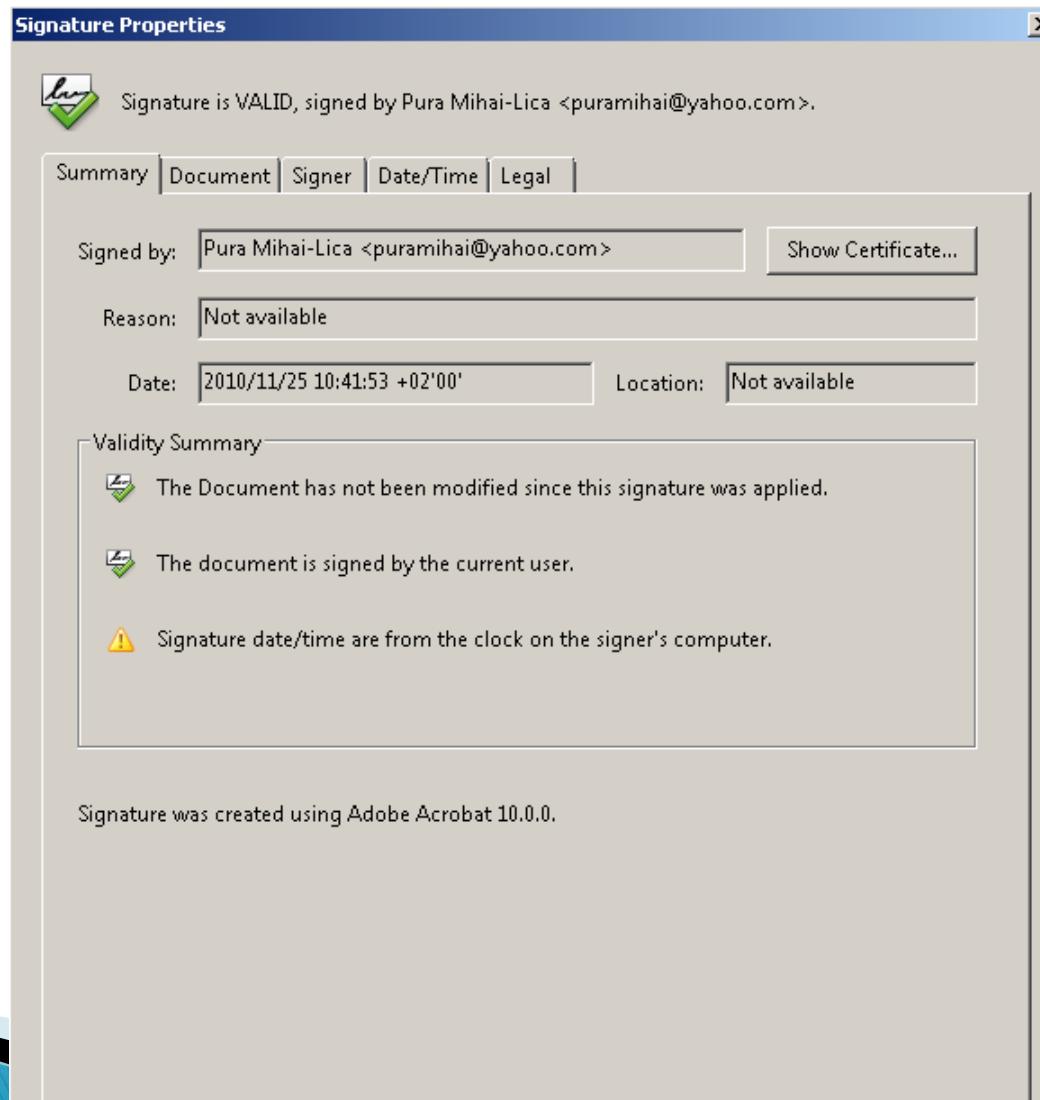
# Verify signatures from a PDF file



# Verify signatures from a PDF file



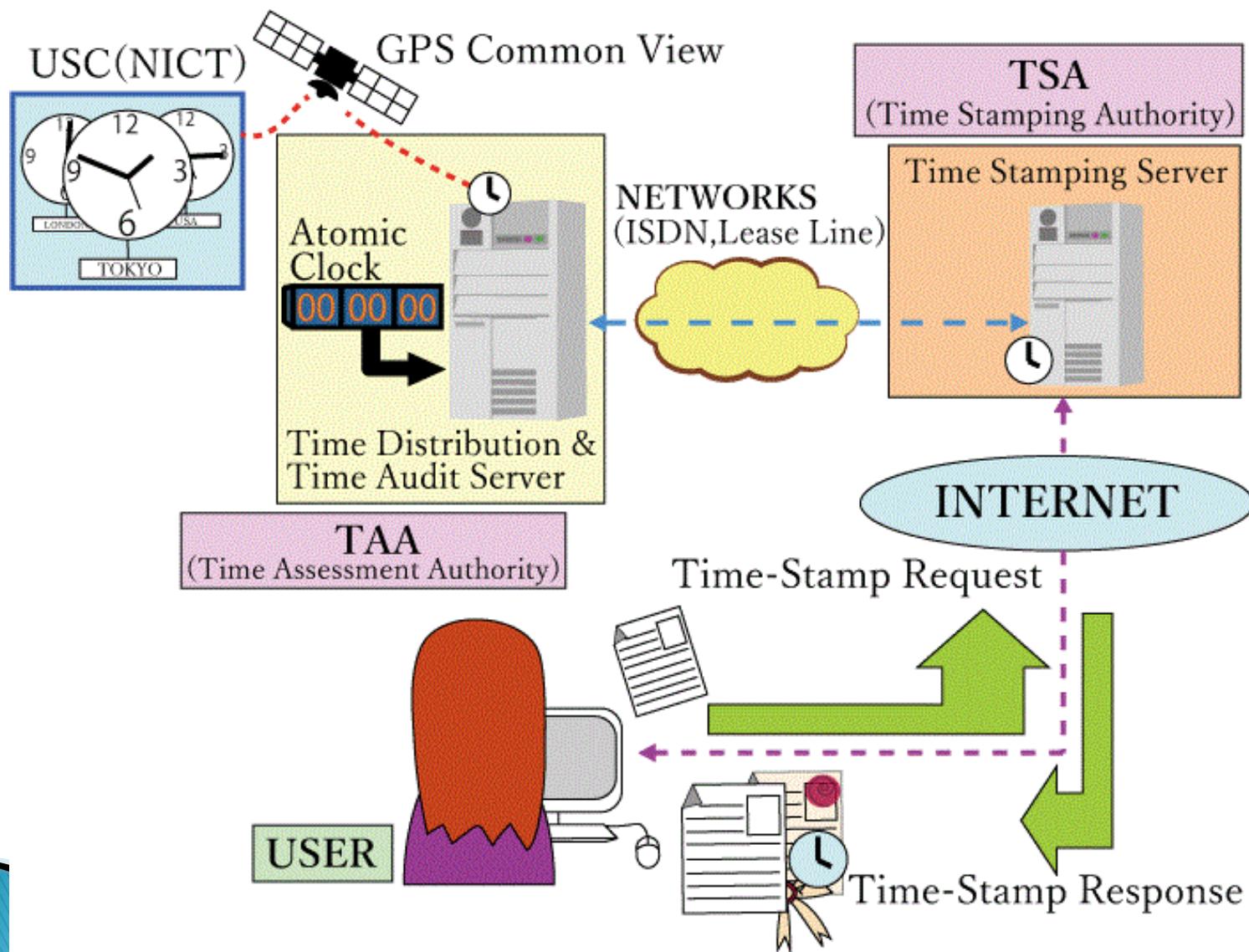
# Verify signatures from a PDF file



# Timestamps

- ▶ TSA – Timestamp Authority (trusted party)
  - applies timestamps to documents
  - Allows a client to prove at a later date that some datum existed before a particular time
    - e.g. an electronic signature on a document existed before a particular time
  - Usually used to add a timestamp-attribute to a digital signature

# Timestamps



# Timestamps

- ▶ Free timestamp test servers:
- ▶ <http://clepsydre.edelweb.fr/dvcs/service-tsp>
- ▶ <http://time.certum.pl/>
- ▶ <http://timestamping.edelweb.fr/service/tsp>
- ▶ <http://www.edelweb.fr/cgi-bin/service-tsp>
- ▶ <http://tsa.safecreative.org/>
- ▶ <https://freetsa.org/tsr>
- ▶ <https://opentimestamps.org/>

# Timestamps

- ▶ Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
- ▶ RFC 3161
- ▶ <https://www.ietf.org/rfc/rfc3161.txt>
  
- ▶ Policy Requirements for Time-Stamping Authorities (TSAs)
- ▶ RFC 3628
- ▶ <https://tools.ietf.org/html/rfc3628>

# Timestamps

- ▶ RFC 3628
- ▶ <https://tools.ietf.org/html/rfc3628#section-5.1>
- ▶ NOTE 1:
- ▶ Without additional measures the relying party may not be able to ensure the validity of a time-stamp token beyond the end of the validity period of the supporting certificate.
- ▶ See Annex C on verification of the validity of a time-stamp token beyond the validity period of the TSU's certificate.

# Time stamp a PDF file

test.pdf - Adobe Acrobat Reader DC

File Edit View Plug-Ins Window Help

Home Tools test.pdf

Q time



Certificates

Open ▾

Digitally sign or certify  
documents and validate  
authenticity

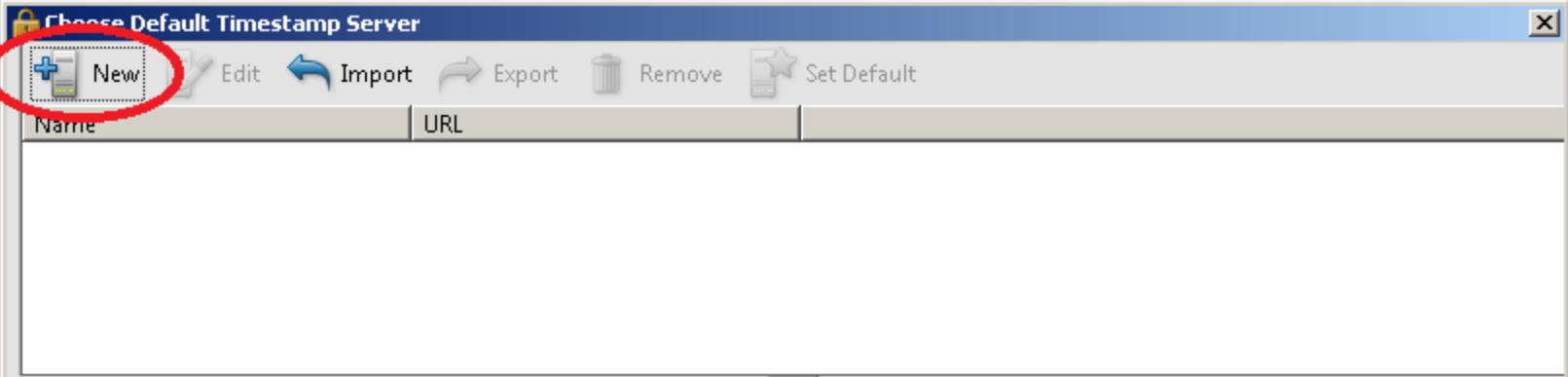


Time Stamp



Time stamp document

# Time stamp a PDF file



The screenshot shows a Windows-style dialog box titled "Choose Default Timestamp Server". At the top, there is a toolbar with several icons: a yellow folder (New), a pencil (Edit), a left arrow (Import), a right arrow (Export), a trash can (Remove), and a star (Set Default). The "New" icon is circled in red. Below the toolbar is a table with two columns: "Name" and "URL". The table is currently empty. At the bottom of the dialog box, there is a section titled "Configure Time Stamp Servers" with the following text:

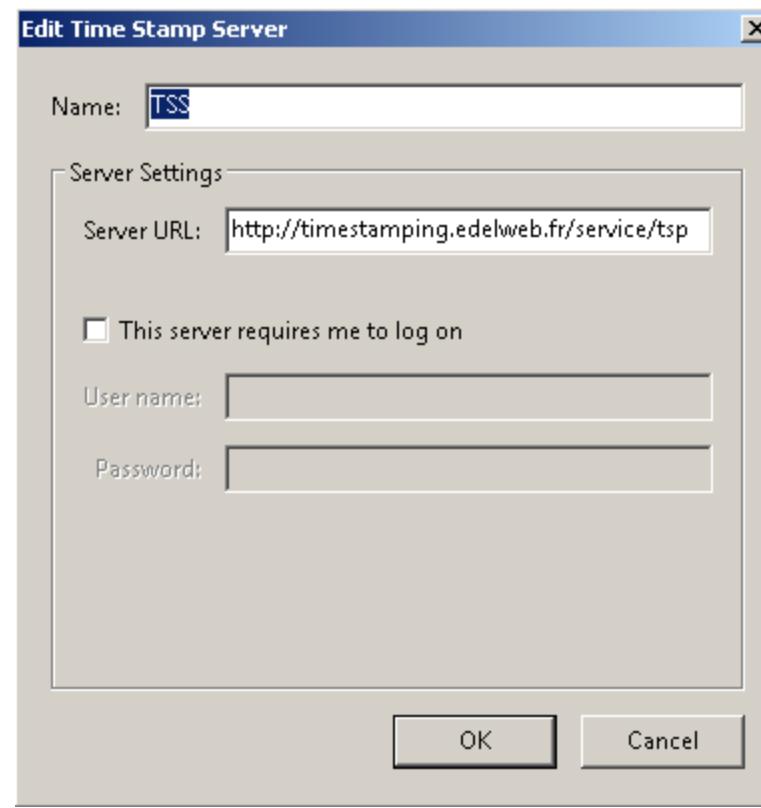
In order to timestamp a document, you need to configure a default *Time Stamp Server*. If you are in a workgroup, your computer administrator may provide you with Time Stamp Server configuration information.

Select one of the entries above and click *Edit* to view or change settings, or click *New* to add and configure a Time Stamp Server. Select a default server using *Set Default*. If you have selected a default server then this server will be used to timestamp documents and a time stamp will be embedded with every signature that you create.

Click *Export* to share your Time Stamp Server settings with others.

At the very bottom of the dialog box, there are two buttons: "Cancel" and "Next".

# Time stamp a PDF file



# Time stamp a PDF file

**Choose Default Timestamp Server**

Name	URL
TSS	<a href="http://timestamping.edelweb.fr/s...">http://timestamping.edelweb.fr/s...</a>

**Configure Time Stamp Servers**

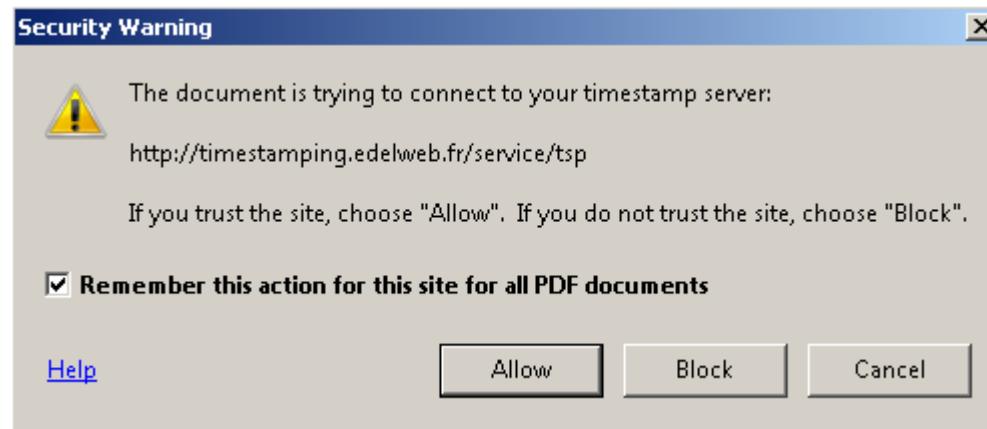
In order to timestamp a document, you need to configure a default *Time Stamp Server*. If you are in a workgroup, your computer administrator may provide you with Time Stamp Server configuration information.

Select one of the entries above and click *Edit* to view or change settings, or click *New* to add and configure a Time Stamp Server. Select a default server using *Set Default*. If you have selected a default server then this server will be used to timestamp documents and a time stamp will be embedded with every signature that you create.

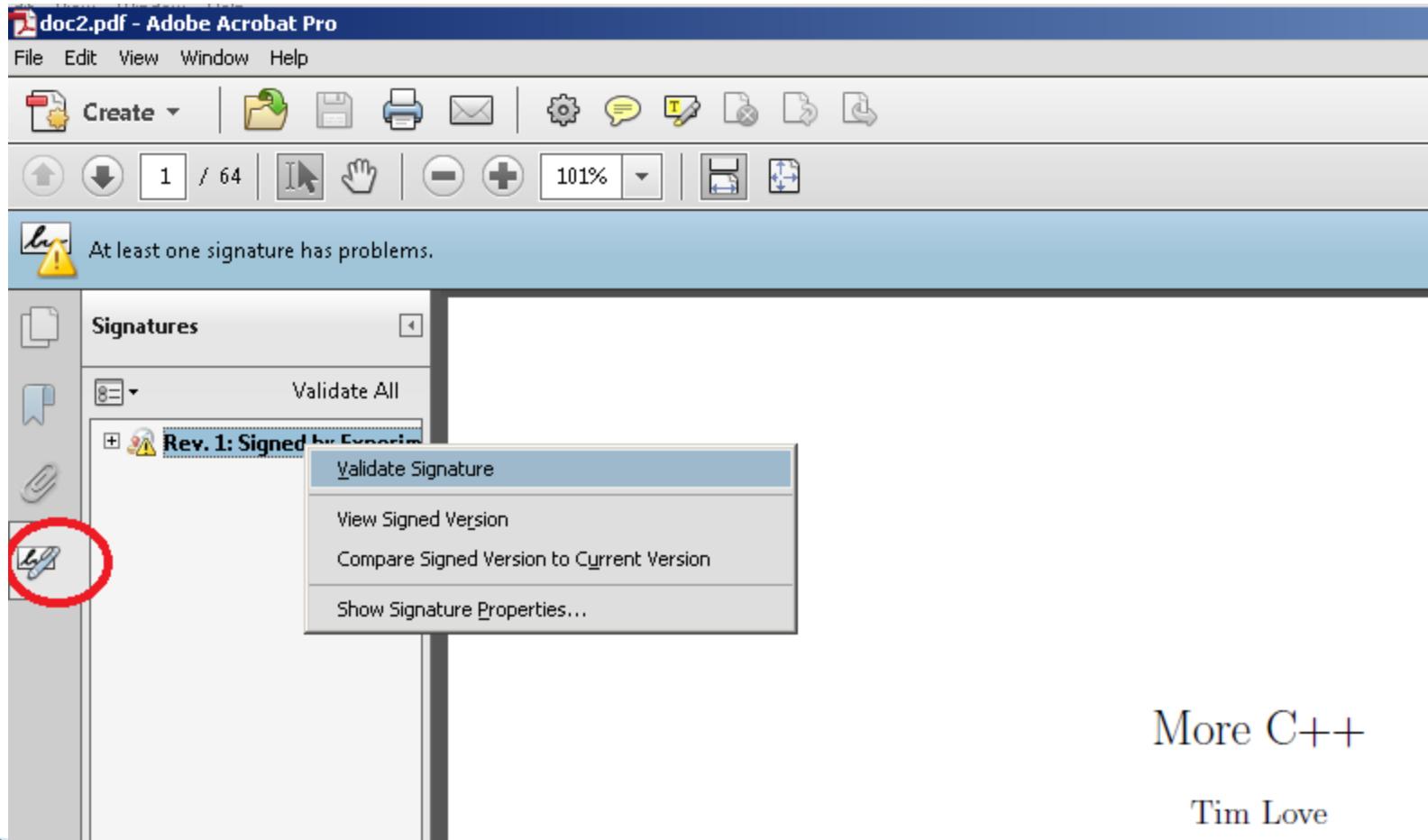
Click *Export* to share your Time Stamp Server settings with others.

**Cancel** **Next**

# Time stamp a PDF file



# Verify a timestamp from a PDF file



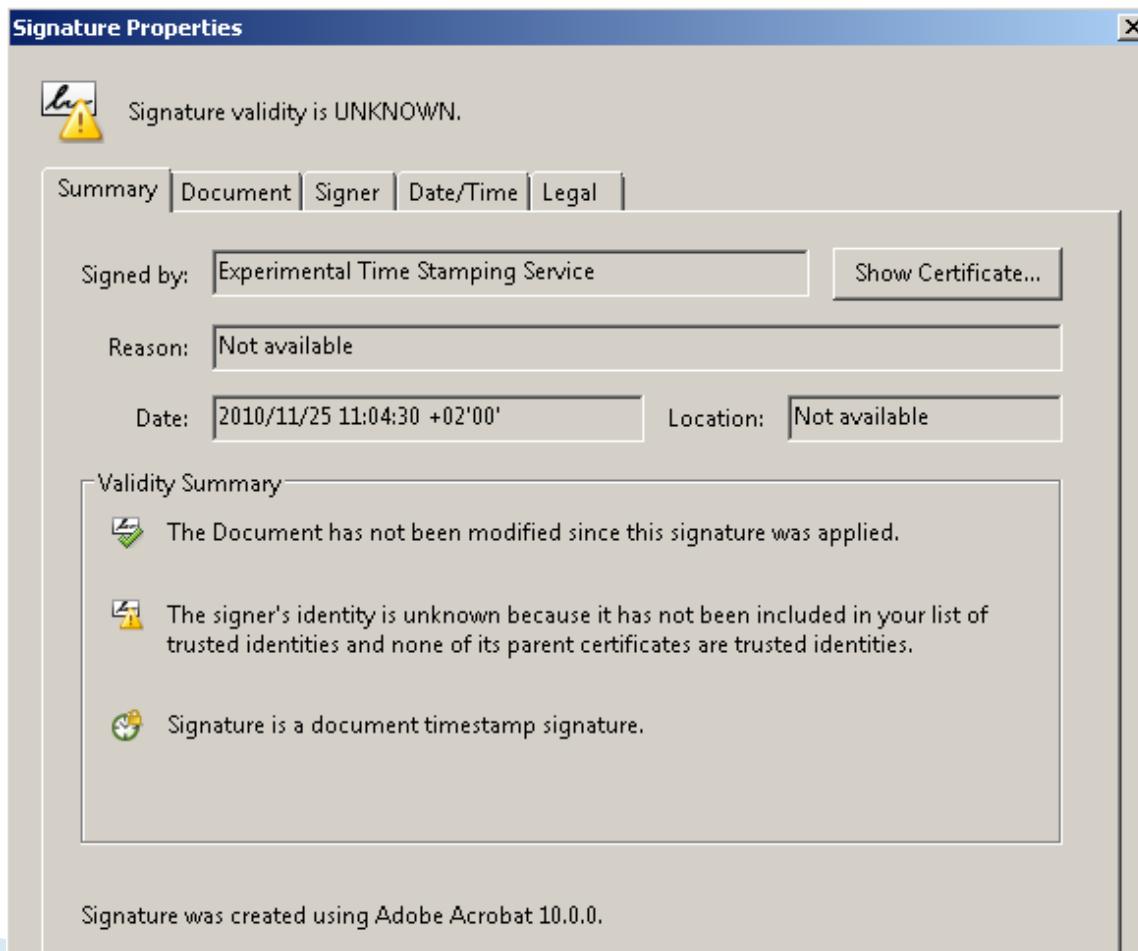
More C++

Tim Love

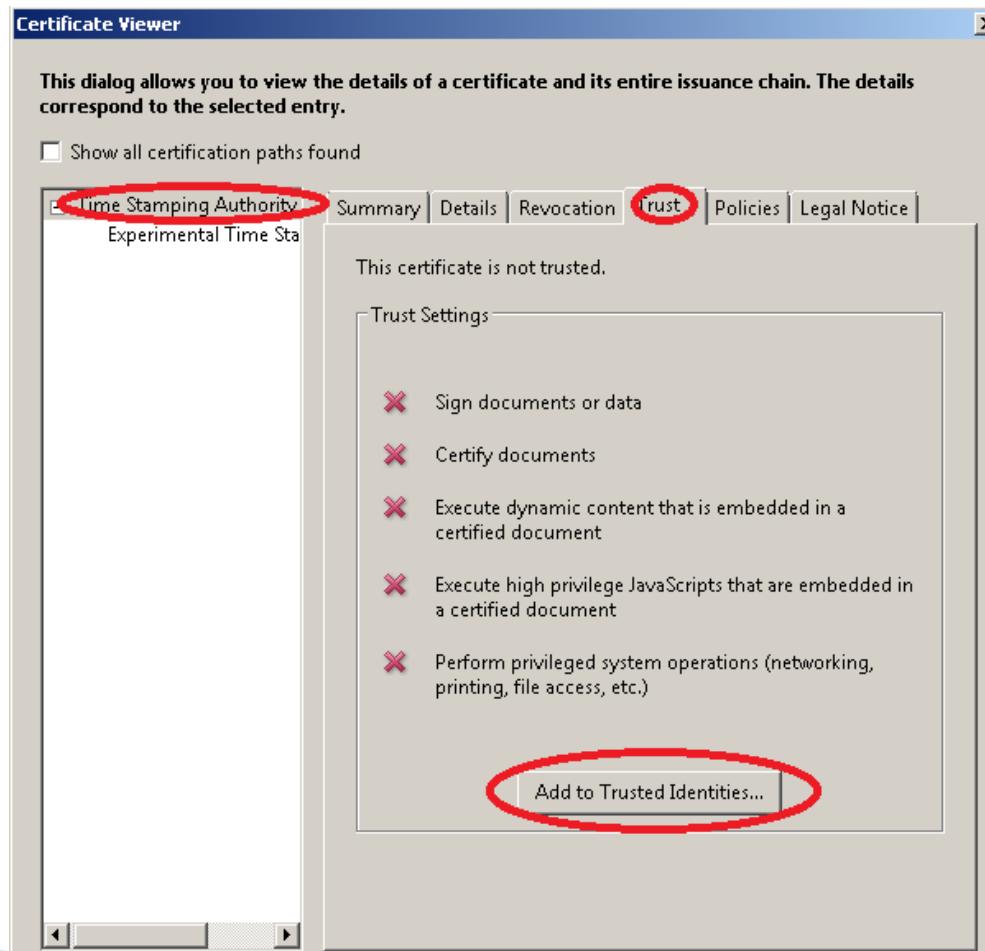
# Verify a timestamp from a PDF file



# Verify a timestamp from a PDF file

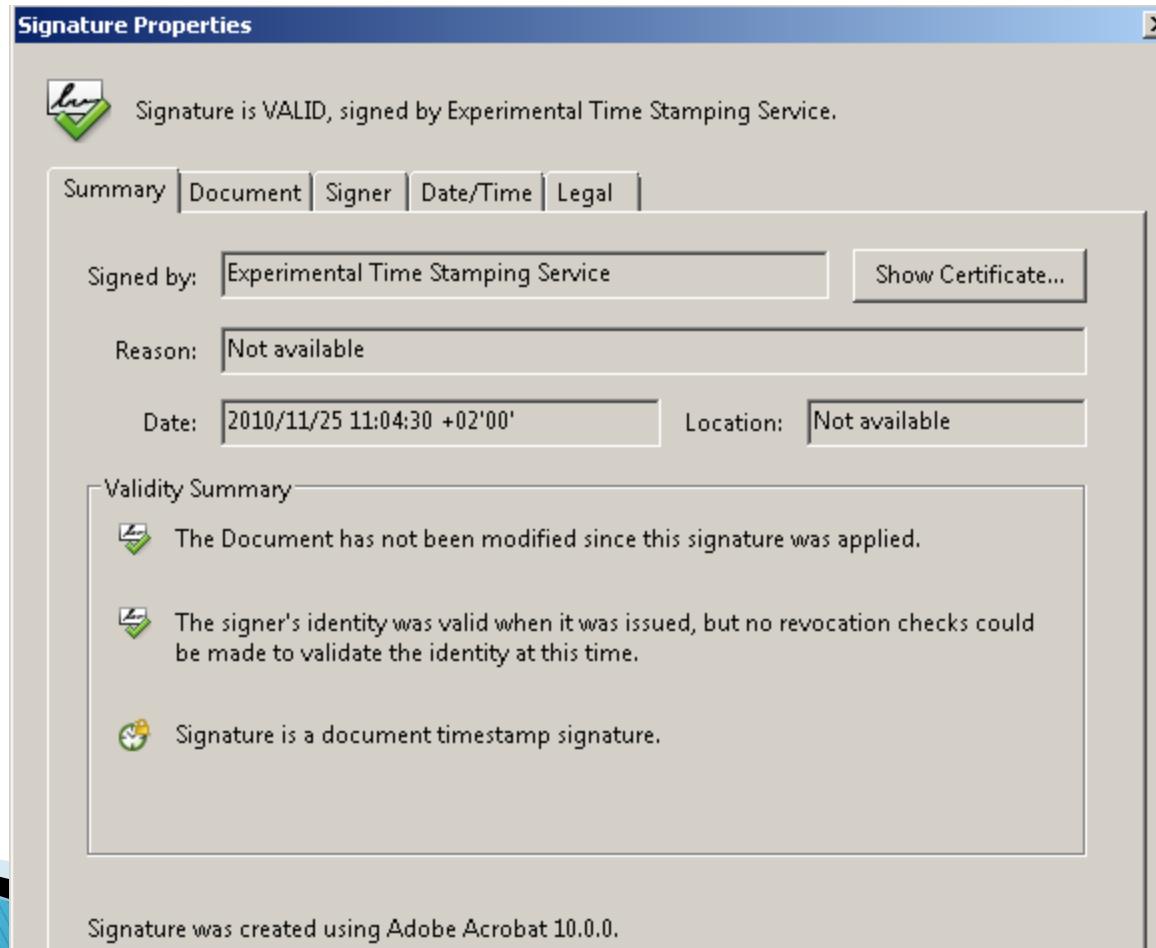


# Verify a timestamp from a PDF file



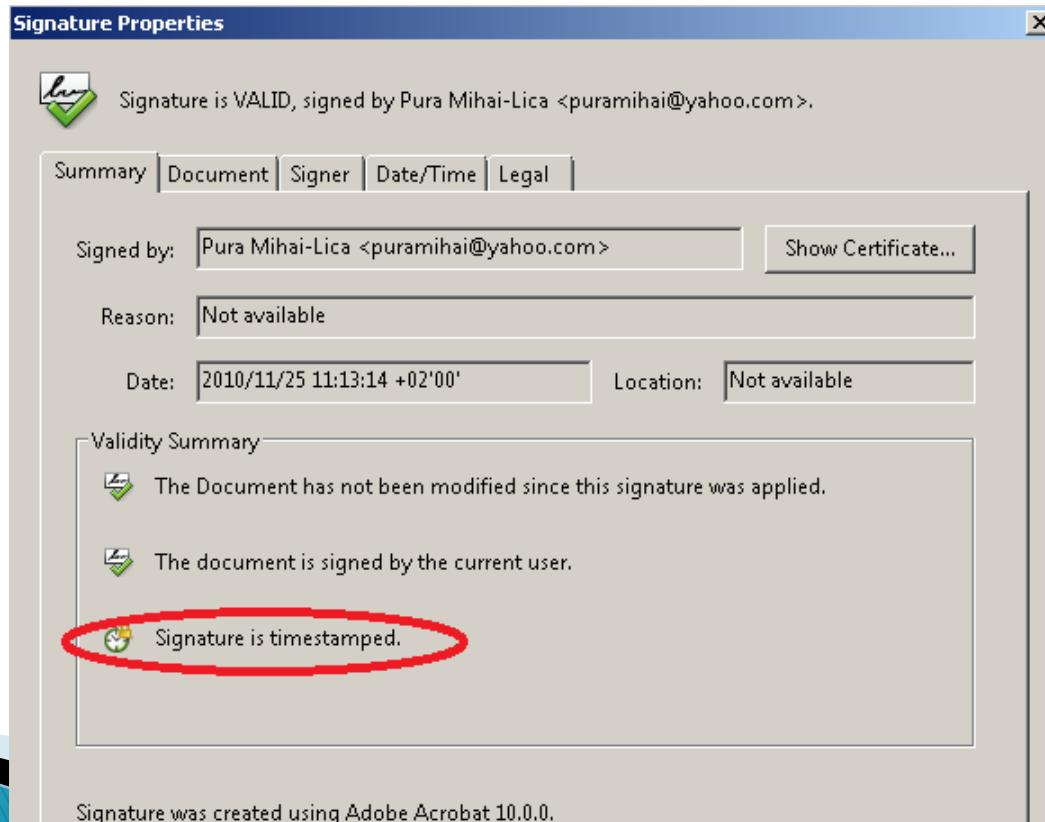
# Verify a timestamp from a PDF file

- ▶ Close dialog box and revalidate signature



# Sign and timestamp a PDF file

- After configuring a time stamp server, every digital signature that will be created will be time stamped.



# Timestamped URL screenshot

- ▶ [https://freetsa.org/index\\_en.php](https://freetsa.org/index_en.php)

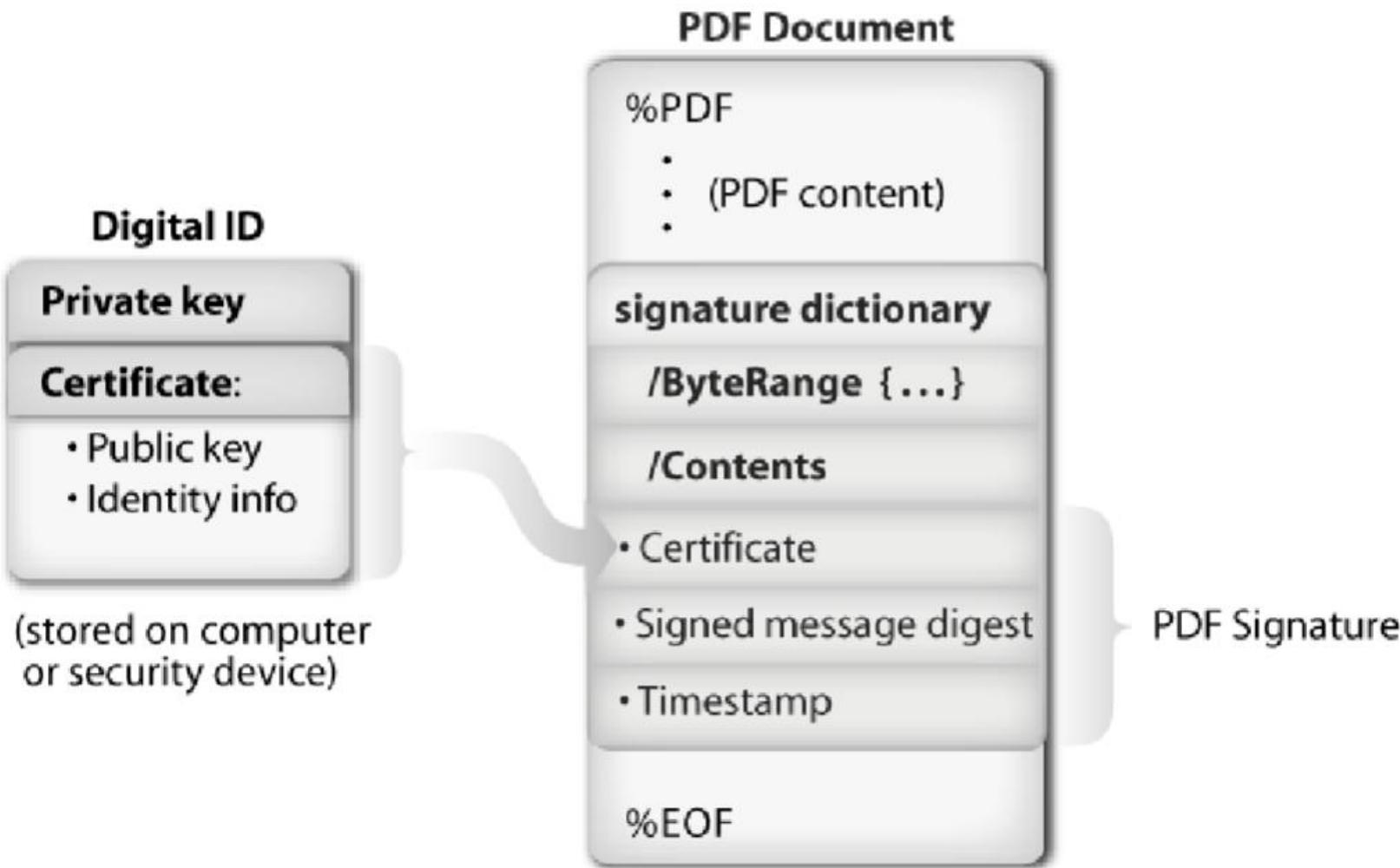
**URL screenshot online**

Web content and links in PDF / PNG format (attachment) + Signature with Timestamping (SHA-512). Aprox wait time 25 secons.

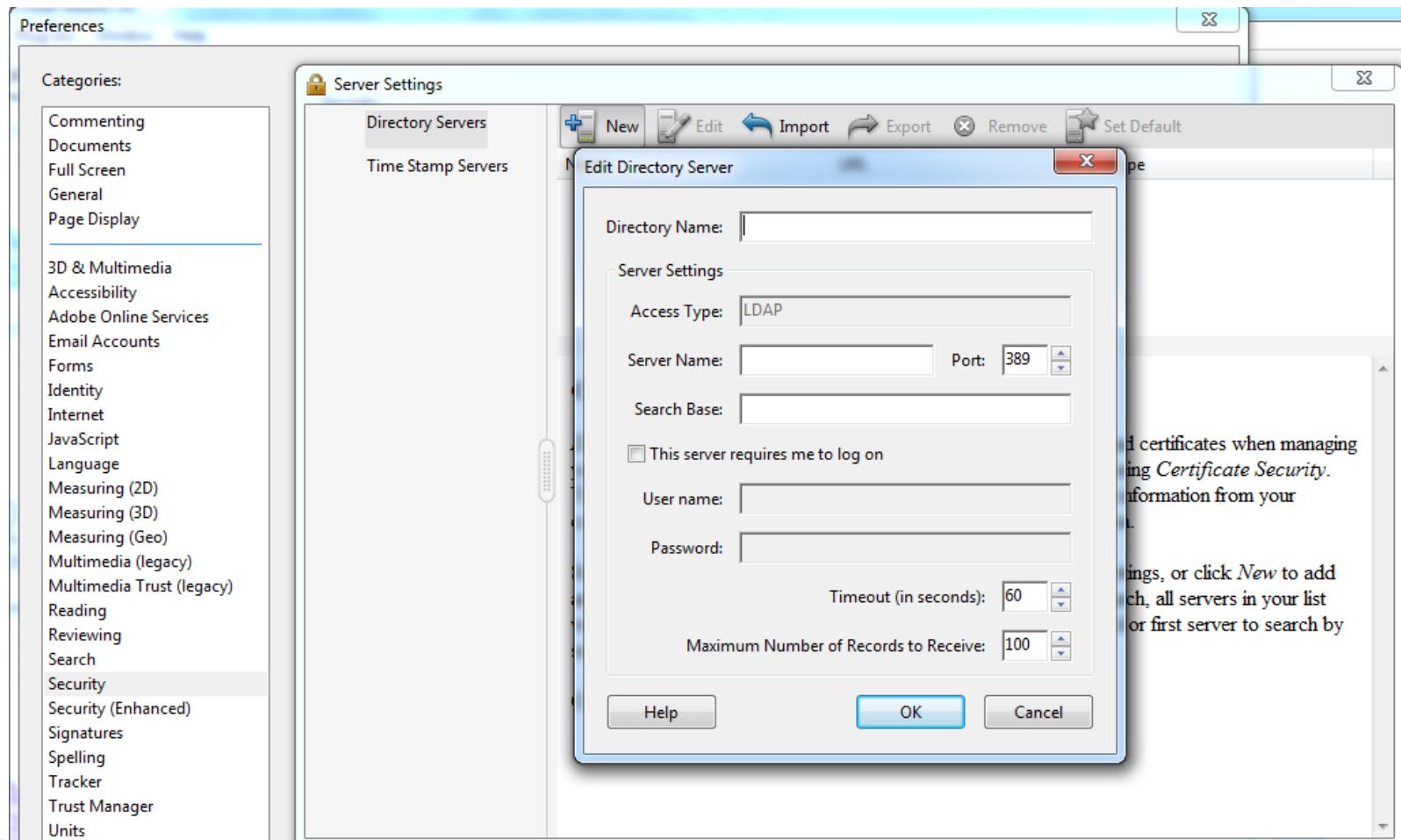
Normal.     I'm Feeling Lucky (slower).     TOR ".onion" domain / Web visited through the Tor-network

Browser agent: 'Mozilla/5.0 (X11; Linux x86\_64; rv:47.0) Gecko/20100101 Firefox/47.0'

# PDF signatures



# Using LDAP for searching certificates



# Sign Microsoft Office Documents

Info

New

Open

Save

Save As

Print

Share

Export

Close

---

Account

Options

Protect Document

Control what types of changes people can make to this document.

**Mark as Final**  
Let readers know the document is final and make it read-only

**Encrypt with Password**  
Password-protect this document

**Restrict Editing**  
Control the types of changes others can make

**Restrict Access**  
Grant people access while removing their ability to edit, copy, or print.

**Add a Digital Signature**  
Ensure the integrity of the document by adding an invisible digital signature

Properties

Size 11,0KB

Pages 1

Words 2

Total Editing Time 0 Minutes

Title Add a title

Tags Add a tag

Comments Add comments

Related Dates

Last Modified Today, 11:31

Created Today, 11:31

Last Printed

Related People

Author  mihai-lica.pura

16  
8

# Sign Microsoft Office Documents

Info

New

Open

Save

Save As

Print

Share

Export

Close

---

Account

Options

Info

New Microsoft Word Document

Desktop

Protect Document

Control what types of changes people can make to this document.

Inspect Document

Before publishing this file, be aware of the following:

- Document properties and author information

Versions

There are no previous versions.

Sign

See additional information about what you are signing...

You are about to add a digital signature to this document. This signature will not be visible within the content of this document.

Commitment Type:

Created this document

Purpose for signing this document:

To include information about the signer, click the details button. [Details...](#)

Signing as: Mihai-Lica Pura

Issued by: Trans Sped QCA

Change...

Sign Cancel

Properties

11,0KB

1

2

0 Minutes

Add a title

Add a tag

Add comments

Today, 11:31

Today, 11:31

mihai-lica.pura

# Sign Microsoft Office Documents

Info

New

Open

Save

Save As

Print

Share

Export

Close

---

Account

Options

## Info

New Microsoft Word Document

Desktop

Signed Document

This document has been signed and marked as final. It should not be edited. If anyone tampers with this document, the signatures will become invalid.

 View Signatures

Protect Document

This document has been marked as final to discourage editing.

 Protect Document ▾

Inspect Document

Before publishing this file, be aware that it contains:

- Document properties and author's name

 Check for Issues ▾

Properties ▾

Size	11,0KB
Pages	1
Words	2
Total Editing Time	0 Minutes
Title	None
Tags	None
Comments	None

Related Dates

Last Modified	Today, 11:31
Created	Today, 11:31
Last Printed	

Related People

Author	 mihai-lica.pura
--------	---

# Sign Microsoft Office Documents

New Microsoft Word Document.docx - Word

MARKED AS FINAL An author has marked this document as final to discourage editing.

SIGNATURES This document contains valid signatures. View Signatures...

Signature Details

Valid Signature - The signed content has not changed and the signer's certificate is valid.

Signature type: XAdES-EPES

Commitment Type: Created this document

Purpose for signing this document:

Signing as: Mihai-Lica Pura

Issued by: Trans Sped QCA

View...

See the additional information about the signer... was collected...

Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Protects e-mail messages
- 1.3.6.1.4.1.39965.1.1.1
- 0.4.0.1456.1.1

\* Refer to the certification authority's statement for details.

Issued to: Mihai-Lica Pura

Issued by: Trans Sped QCA

Valid from 12. 03. 2015 to 12. 03. 2016

Signatures

Valid signatures:

Mihai... 23.11.2015

# Sign Microsoft Office Documents

- ▶ The same steps apply for:
  - Microsoft PowerPoint
  - Microsoft Excel

# Sign/Verify any kind of file

- ▶ Exercise scenarios:
  - ▶ 1. Signing with an expired certificate
  - ▶ 2. Signing with a revoked certificate
  - ▶ 3. Signing with a valid certificate
  - ▶ 4. Verifying signatures obtained from 1, 2 and 3

# Sign/Verify any kind of file

- ▶ Exercise scenarios:
- ▶ 5. Verifying a signature after the certificate has expired
  - certificate was valid at the moment of signing
- ▶ 6. Verifying a signature after the certificate was revoked
  - certificate was valid at the moment of signing

# Sign/Verify any kind of file

- ▶ 7. Signing with a timestamp for the document
- ▶ 8. Signing with a timestamp for the signature
- ▶ 9. Cosigning a signed file
- ▶ 10. Signing with a detached signature
- ▶ 11. Signing a PDF file (ProSigner)
- ▶ 12. Signing Microsoft Office files: docx, xlsx, pptx (ProSigner)

# Sign/Verify any kind of file

- ▶ 13. Encrypting a file for a recipient
- ▶ 14. Encrypting a file for multiple recipients
- ▶ 15. Decrypting a file
- ▶ 16. Sign a file, then encrypt it for one or more recipients
- ▶ 17. Decrypt an encrypted file, then verify signature

# Sign/Verify any kind of file

- ▶ PKCS #7: Cryptographic Message Syntax Standard
- ▶ <http://www.rsa.com/rsalabs/node.asp?id=2129>
- ▶ ASN.1 compiler
  - <https://holtstrom.com/michael/tools/asn1decoder.php>
  - <http://phpseclib.sourceforge.net/x509/asn1parse.php>
  - <http://lionet.info/asn1c/asn1c.cgi>

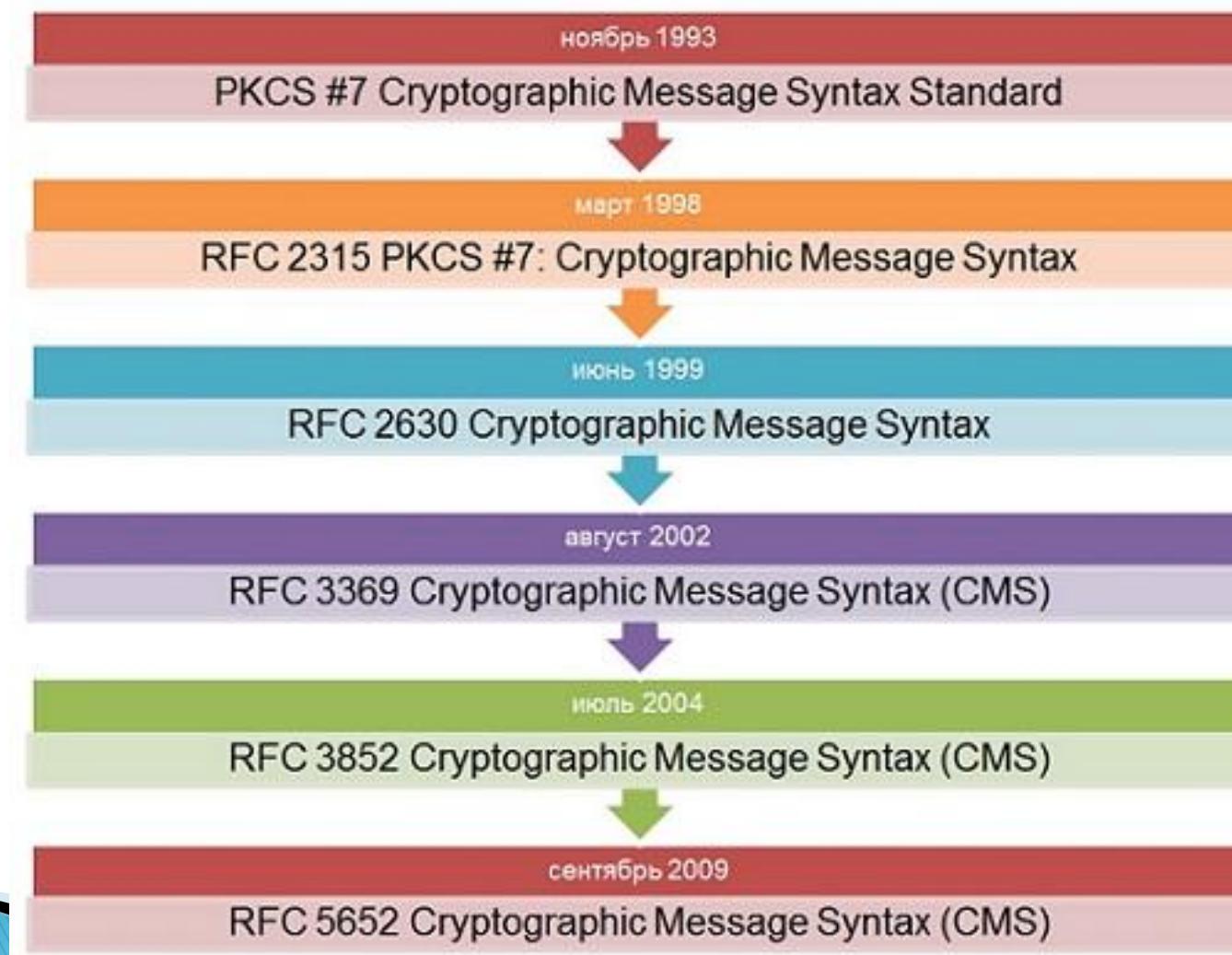
# Sign/Verify any kind of file

- ▶ DeskSeal
- ▶ Attached/Detached Signatures
- ▶ Time stamp signature
- ▶ Co signatures

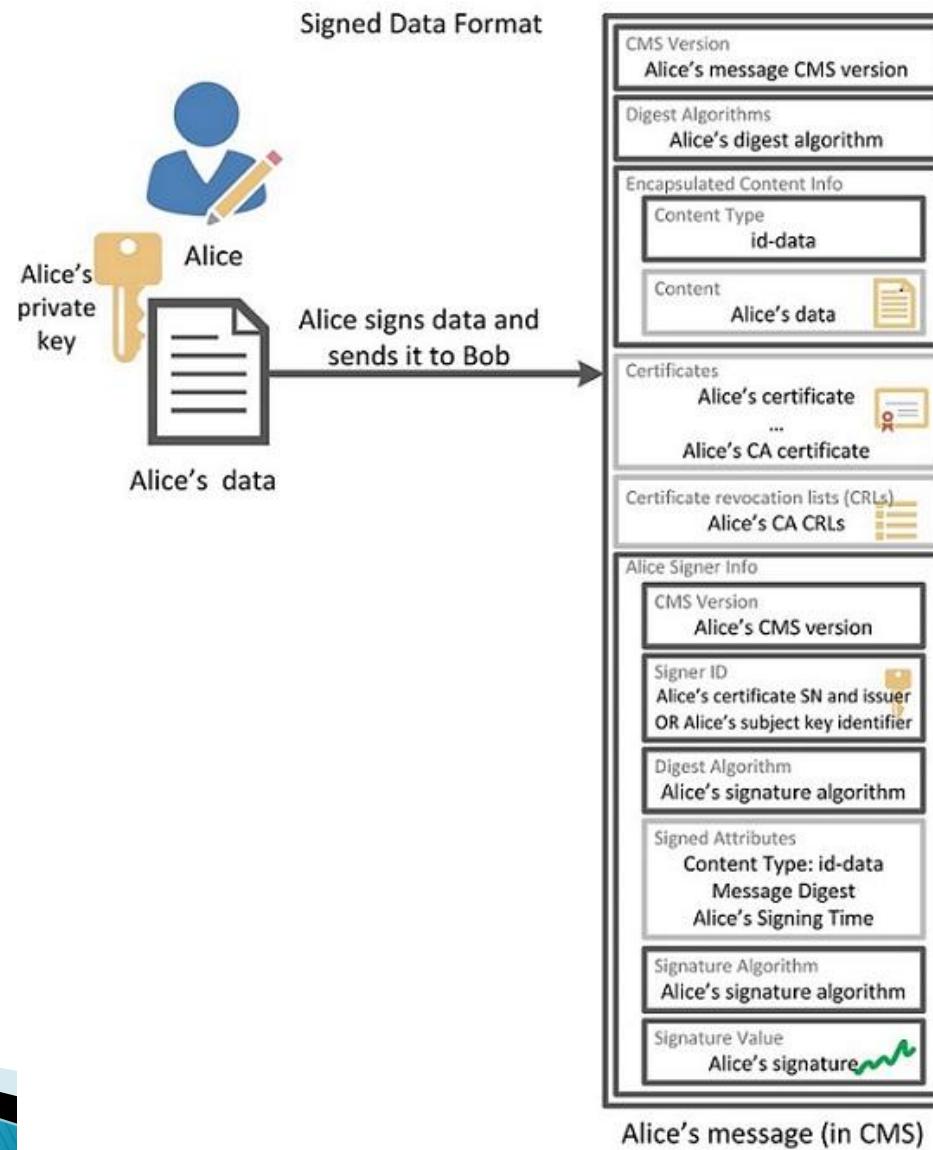
# Sign/Verify any kind of file

- ▶ **ProSigner**
- ▶ **LDAP configuration**
  - LDAP over SSL
- ▶ **OCSP configuration**
  - Signing validation request
  - Verify OCSP server response
- ▶ **PDF signing configuration**
  - Add a background image to the signature

# PKCS#7 signatures



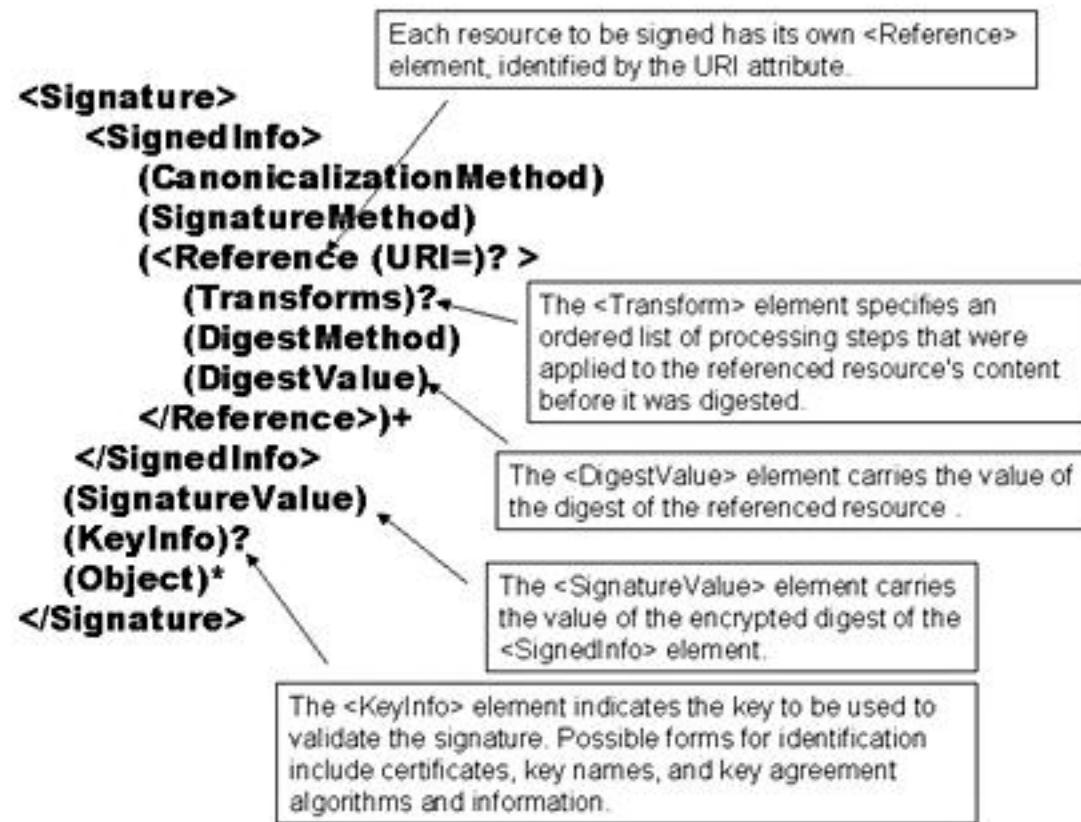
# PKCS#7 signatures



# Sign/verify XML files (XMLDSig)

- ▶ **XMLDSig specification**
  - <http://www.w3.org/TR/xmldsig-core/>
- ▶ **XML Signer**
  - <https://www.signfiles.com/xml-signer/>
  - Signs XML files (XML Signer)
  - And verifies XML signatures (XML Signer Viewer)
- ▶ **Sample XML file to sign**
  - <https://www.w3schools.com/xml/note.xml>

# Sign/verify XML files (XMLDSig)



<https://www.xml.com/pub/a/2001/08/08/xmldsig.html>

# Sign/verify XML files (XMLDSig)

- ▶ **Determine which resources are to be signed**
  - will take the form of identifying the resources through a Uniform Resource Identifier (URI)

# Sign/verify XML files (XMLDSig)

- ▶ **Calculate the digest of each resource**
  - each referenced resource is specified through
    - a **<Reference>** element
    - and its digest
      - (calculated on the identified resource and not the **<Reference>** element itself)
      - placed in a **<DigestValue>** child element like
  - If reference URI is “” it refers the content of the current XML document
  - The **<DigestMethod>** element identifies the algorithm used to calculate the digest

# Sign/verify XML files (XMLDSig)

- ▶ **Collect the Reference elements**
  - Collect the **<Reference>** elements (with their associated digests) within a **<SignedInfo>** element like
  - The **<CanonicalizationMethod>** element indicates the algorithm was used to canonize the **<SignedInfo>** element
  - Different data streams with the same XML information set may have different textual representations, e.g. differing as to whitespace

# Sign/verify XML files (XMLDSig)

- ▶ **Collect the Reference elements**
  - To help prevent inaccurate verification results, XML information sets **must first be canonized** before extracting their bit representation for signature processing
  - The **<SignatureMethod>** element identifies the algorithm used to produce the signature value

# Sign/verify XML files (XMLDSig)

## ▶ Signing

- Calculate the digest of the `<SignedInfo>` element, sign that digest and put the signature value in a `<SignatureValue>` element

## ▶ Add key information

- If keying information is to be included, it will be placed in a `<KeyInfo>` element
- Here the keying information contains the X.509 certificate for the sender, which would include the public key needed for signature verification

# Sign/verify XML files (XMLDSig)

- ▶ Enclose in a **Signature** element
  - Place the
    - <SignedInfo>
    - <SignatureValue>,
    - <KeyInfo>
  - into a <**Signature**> element
- The <**Signature**> element comprises the XML signature

# Signature expiration

- ▶ What is the problem?
- ▶ Exercises using Adobe Acrobat Reader DC

# Signature expiration

- ▶ *User A*
  - signs his document using a signature scheme
  - applies to a TSA to get a timestamp on the signature
- ▶ *User B* can do the *User A*'s signature validation
  - this involves validation of the *User A*'s certificate
- ▶ many years later when the certificate of *User A* can be already expired or revoked

# Signature expiration

- ▶ The validation decision are based on the timestamp applied on the signature
  - The signature was made before the timestamp
  - The applied timestamp is considered the signing-time
- ▶ Without the timestamp, the *User B* can not be sure about the status of the User A's certificate at the *signing-time*

# Advanced Electronic Signatures

- ▶ CAdES
- ▶ [http://www.etsi.org/deliver/etsi\\_ts/101700\\_101799/101733/](http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/)
- ▶ PAdES
- ▶ [http://www.etsi.org/deliver/etsi\\_ts/102700\\_102799/10277801/01.01.01\\_60/ts\\_10277801v010101p.pdf](http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf)
- ▶ XAdES
- ▶ [https://portal.etsi.org/webapp/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=28064](https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=28064)

# Signatures with Long-Term Validation Material

- ▶ Validation material
  - is needed to validate the signature
    - certificates
    - and revocation information
      - OCSP responses
      - and/or CRLs
  - is included in the signature
- ▶ This signature allows the validation as long as there are no technology changes (e.g. algorithms becomes weak)

# Signatures with Long-Term Validation Material

- ▶ Examples:
  - CAdES-B-LT [i.11],
  - XAdES-B-LT [i.14],
  - PAdES-B-LT [i.16]

# Signatures providing Long Term Availability and Integrity of Validation Material

- ▶ Re-compute
  - the hash of the originally signed document
  - and the signed attributes
- ▶ with a specific hash algorithm
  
- ▶ Protect
  - re-computed values
  - and previously added validation material and timestamps
- ▶ with a new timestamp

# Signatures providing Long Term Availability and Integrity of Validation Material

- ▶ The original signature can be validated as long as:
  - the latest added timestamp can be validated
  - and the latest used hash-algorithm is still trustworthy
- ▶ Examples:
  - CAdES-B-LTA [i.11], CAdES-E-A [i.12],
  - XAdES-B-LTA [i.14], XAdES-E-A [i.15],
  - PAdES-B-LTA [i.16], PAdES-E-LTV [i.17]

# Signatures providing Long Term Availability and Integrity of Validation Material

- ▶ A Signature providing
  - Long Term Availability
  - and Integrity of Validation Material
- ▶ is suitable for **long-term preservation**

# Signatures providing Long Term Availability and Integrity of Validation Material

- ▶ Mechanism (similar for the different formats):
  - All the missing validation material is added
  - a hash is computed over the existing signature including the originally signed document
  - and a time-stamp is computed over the final hash computation
  - The time-stamp is added into the signature

# Signatures providing Long Term Availability and Integrity of Validation Material

## ► Mechanism (similar for the different formats):

- Once a signature is already in this form, the preservation service
  - only considers the validity of the last archival time-stamp
  - e.g.
    - the expiration of the signing certificate of the TSU
    - and the trustworthiness of the cryptographic algorithms used within the time-stamp

# Signatures providing Long Term Availability and Integrity of Validation Material

- ▶ Each of the AdES formats provides levels suitable for long-term preservation
- ▶ In part one of CAdES [i.11], PAdES [i.16] and XAdES [i.14] baseline levels are defined:
  - CAdES-B-LTA,
  - PAdES-B-LTA and
  - XAdES-B-LTA

# Signatures providing Long Term Availability and Integrity of Validation Material

- ▶ The baseline levels were designed for high interoperability.
- ▶ In addition, part two of CAdES [i.12], PAdES [i.17] and XAdES [i.15] provide more general extended levels:
  - CAdES-E-A,
  - PAdES-E-LTV and
  - XAdES-E-A

# Timestamp expiration

- ▶ Timestamps (RFC 3161) are also signatures
  - they rely on certificates (the TSA certificate)
  - and thus they expire
  - also, timestamp becomes useless in the same moment as the TSA ceases operation or is compromised

# Timestamp expiration

- ▶ Solutions (PKI)
  - ▶ I. Use just **one timestamp**, but whenever the latest time stamp is about to expire
    - but *before* expiration
    - one needs to obtain a new timestamp computed over the previous timestamp
  - ▶ II. get **several timestamps** on one file
    - regularly timestamp it before any of the TSA certificates is about to expire

# Timestamp expiration

- ▶ If the TSA's private key is compromised (and thus revoked)
  - the time stamp signature cannot be trusted
  - as whoever compromised it could sign documents with old time stamps
  - users would want to be warned before accepting a time stamp signature from a compromised certificate

# Timestamp expiration

## ► Solutions

- Get a signed time stamp from **multiple TSAs**
  - if any one is not revoked, that signature can still be trusted
- Use **threshold signing**
  - an attacker would have to compromise a number of parties in order to forge signatures
  - which is much less likely than compromise of a single party

# Timestamp expiration

- ▶ <https://crypto.stackexchange.com/questions/3291/signature-and-timestamp-for-long-term-document-archival-question>
- ▶ [https://en.wikipedia.org/wiki/Trusted\\_timestamping](https://en.wikipedia.org/wiki/Trusted_timestamping)

# Advanced Electronic Signatures

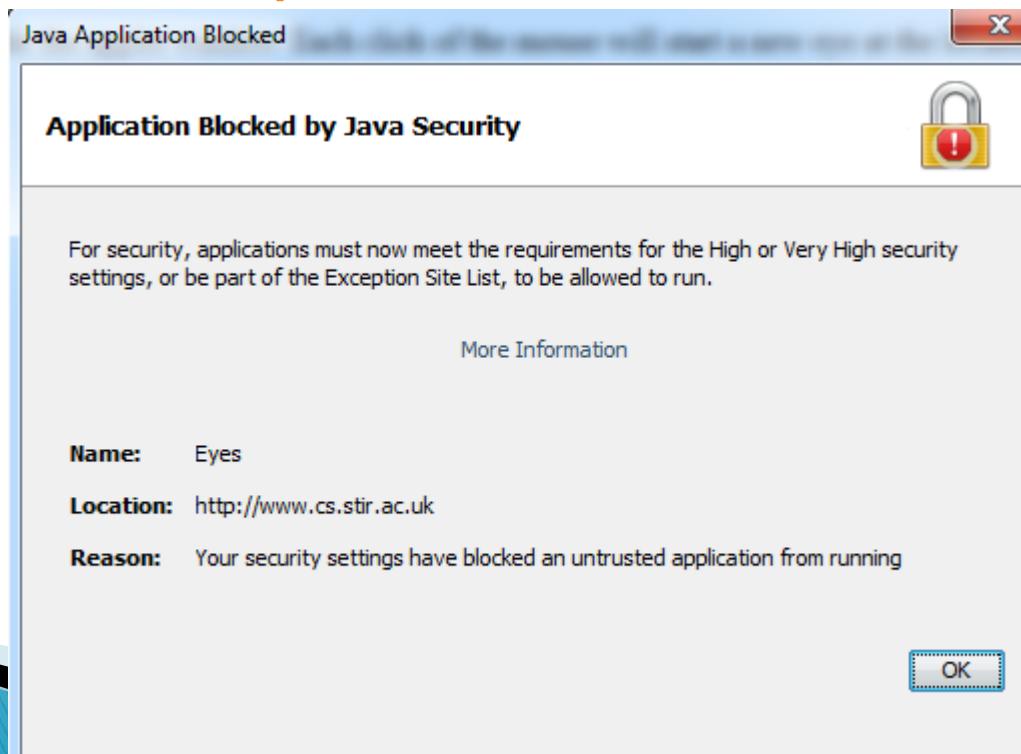
- ▶ Signing tools
- ▶ A. web:
  - ▶ <https://ec.europa.eu/cefdigital/DSS/webapp-demo/home>
- ▶ B. desktop:
  - ▶ <http://xolidosign.en.softonic.com/>
- ▶ C. others:
  - ▶ <https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/software-verifica>

# Certificate login

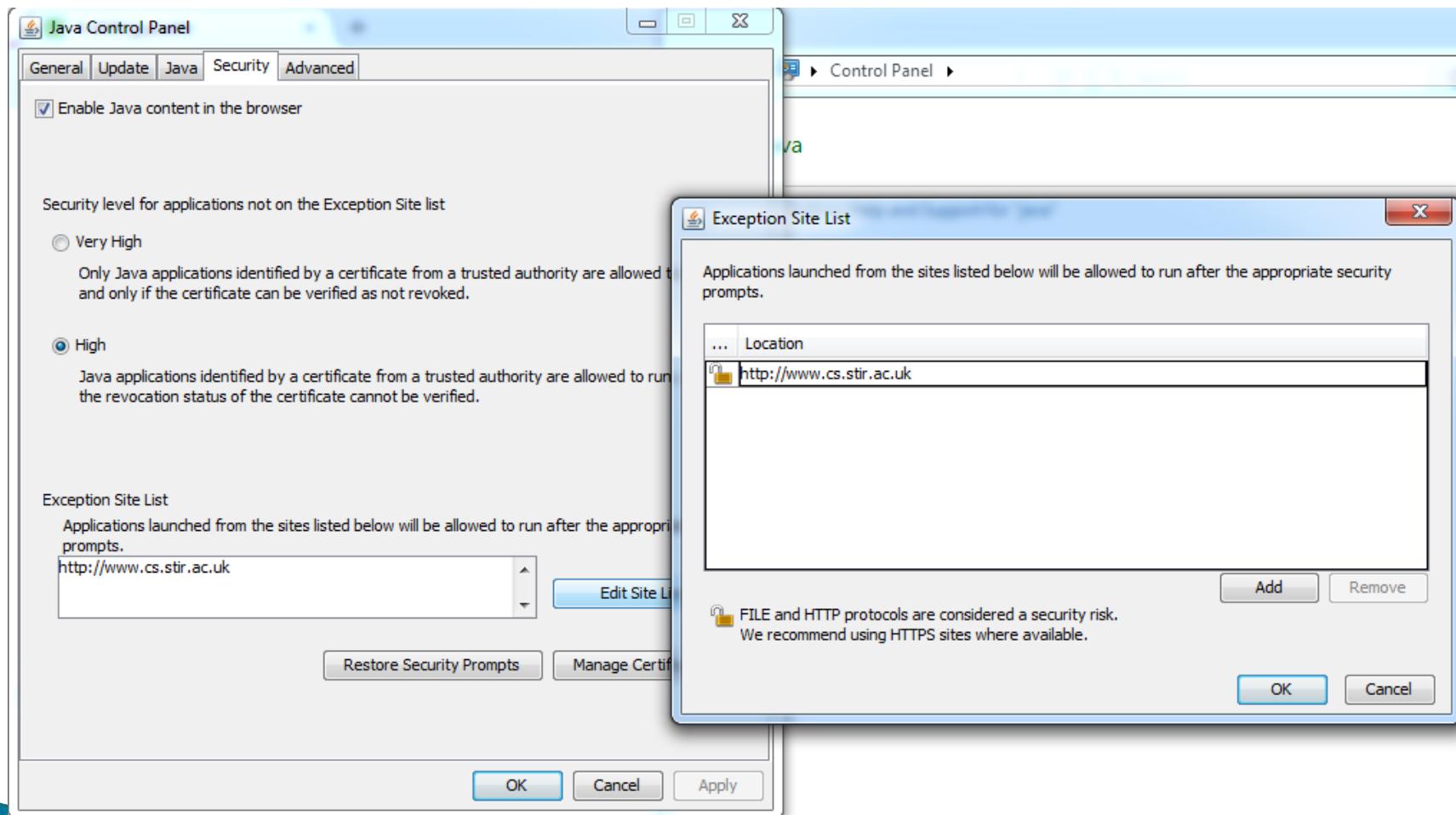
- ▶ **Centrul Național de Administrare a Registrelor Naționale Notariale**
  - <https://eguvernare.stsisp.ro/>
  - <https://www.infonot.eu/>
- ▶ <https://www.cacert.org/>
  - First install cacert CA certificate
    - in Trusted Root Certification Authorities (for Microsoft Edge, Microsoft Internet Explorer and Google Chrome)
    - or the corresponding certificate store in Mozilla Firefox
  - If using Google Chrome, enable certificate request generation in the browser settings

# Code signing – Unsigned Java applets (obsolete)

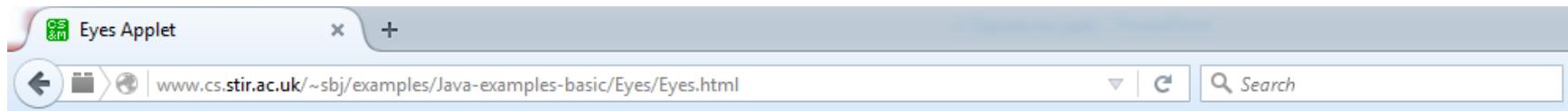
- ▶ <http://www.cs.stir.ac.uk/~sbj/examples/Java-examples-basic/>
- ▶ <http://www.sitepoint.com/java-applets-obsolete-still-part-web/>



# Code signing – Unsigned Java applets (obsolete)

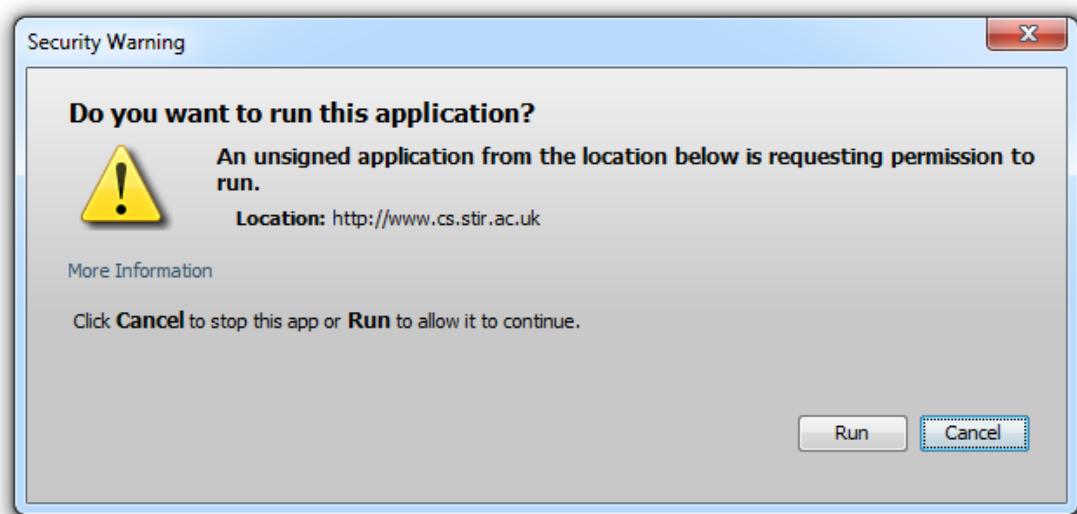


# Code signing – Unsigned Java applets (obsolete)



## Eyes that Follow the Mouse

This applet draws eyes that follow the mouse cursor around inside the applet window. Each click of the mouse will start a new eye at the location you clic



# Code signing – Signed Java applets (obsolete)

The screenshot shows a web browser window with the URL [dss.digitpa.gov.it/signature](http://dss.digitpa.gov.it/signature). The page title is "DSS WebApp". On the left, there's a sidebar with "Signature applet" (selected), "Extend a signature", "Validate a signature", "Useful links" (with "Joinup", "Source code", "Report a bug", and "TL Manager"), and a logo for "Digital Signature". A central modal dialog box titled "Signature applet" asks "Do you want to run this application?". It displays the following information:

- Name:** SD-DSS Demo Applet
- Publisher:** ESSI AP
- Location:** <http://dss.digitpa.gov.it>

The dialog also contains a warning message: "This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above." There is a checkbox for "Do not show this again for apps from the publisher and location above". At the bottom are "Run" and "Cancel" buttons, along with "More Information" and a shield icon.

# Code signing – Signed Java applets (obsolete)

The screenshot shows a Java security dialog box over a web browser window. The browser address bar shows 'dss.digitpa.gov.it/signature'. The dialog box asks 'Do you want to run this application?' with details about the applet: Name: SD-DSS Demo Applet, Publisher: ESSI AP, Location: http://dss.digitpa.gov.it. It includes a warning about unrestricted access and a checkbox to remember the choice. A 'More Information' button is present. A 'Run' and 'Cancel' button are at the bottom. A 'More Information' window is open, providing details about running vs canceling, publisher verification, and digital signatures, with a 'View Certificate Details' link and a 'Close' button.

Do you want to run this application?

Name: SD-DSS Demo Applet

Publisher: ESSI AP

Location: http://dss.digitpa.gov.it

This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.

Do not show this again for apps from the publisher and location above

 More Information

Run Cancel

Joinup

Source code

Report a bug

TL Manager

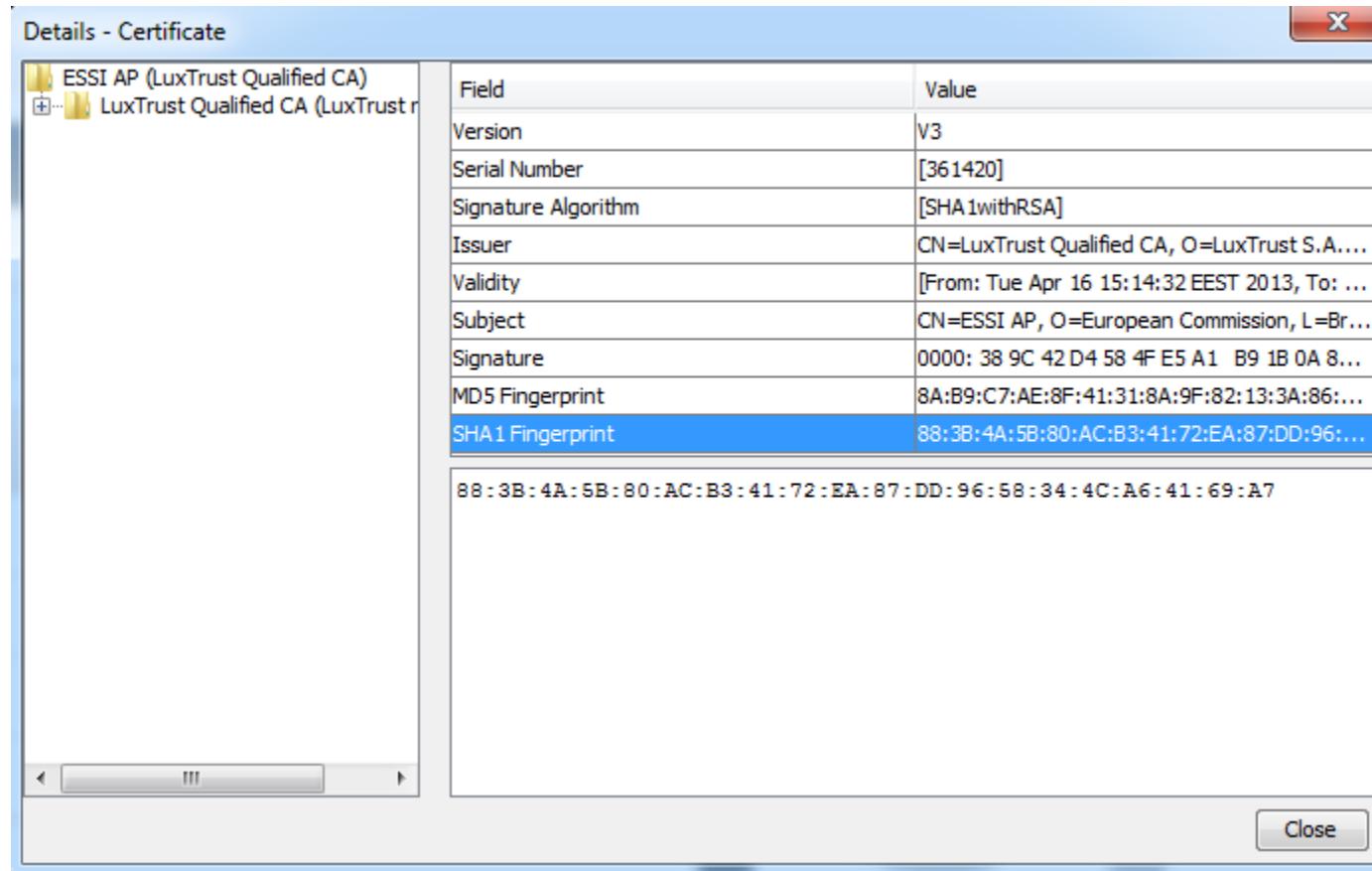
More Information

Clicking Run allows the application to run with unrestricted access to your personal files and other resources on your computer (for example, the web cam and microphone).  
Clicking Cancel prevents the application from running.  
The publisher name is verified by a trusted certificate authority. Run this application only if you trust the source (i.e. the website) that this application is from.  
The digital signature for this application was generated with a certificate from a trusted certificate authority.

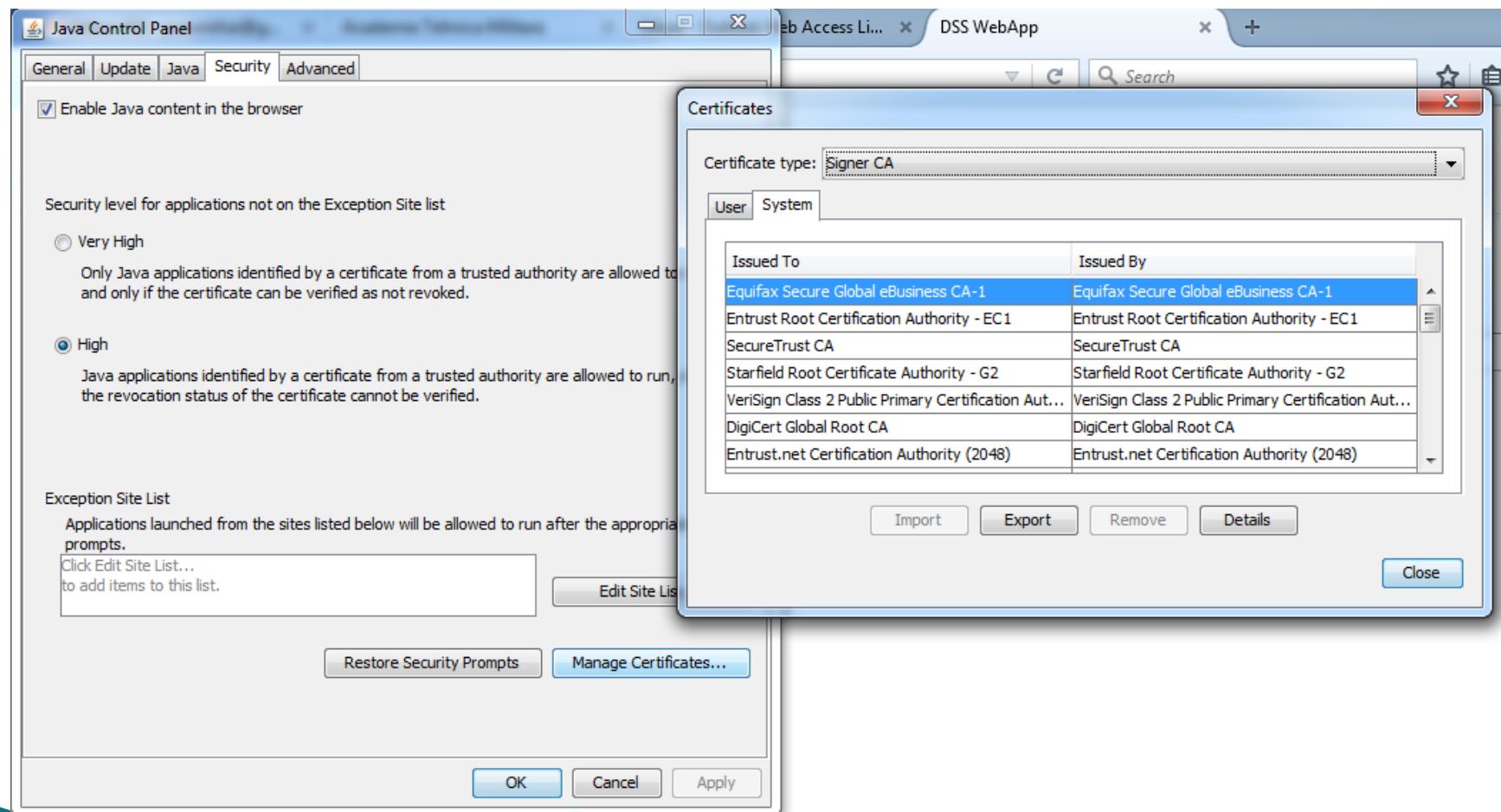
[View Certificate Details](#)

Close

# Code signing – Signed Java applets (obsolete)



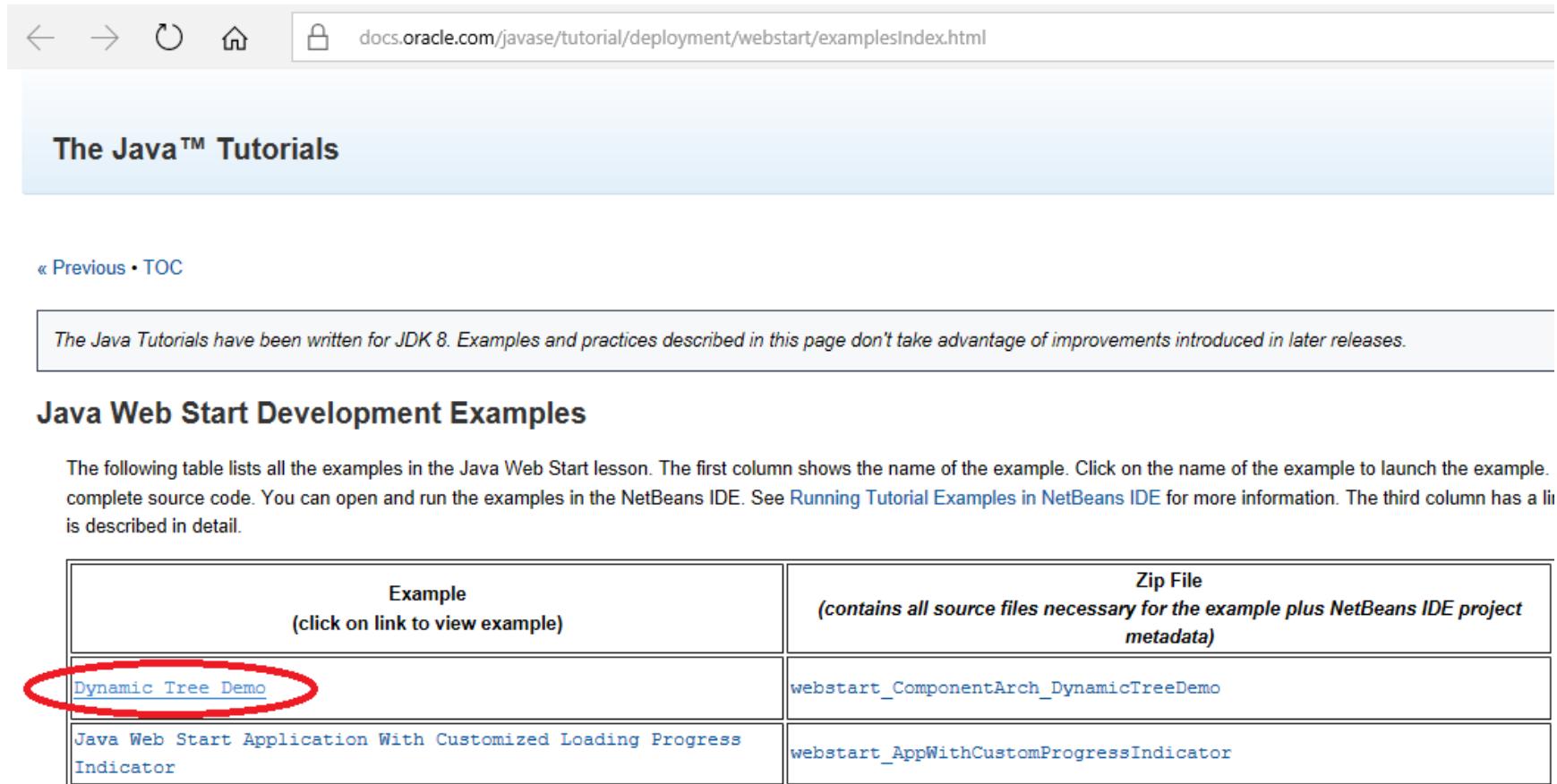
# Code signing – Signed Java applets (obsolete)



# Code signing – Java Web Start

- ▶ Java Web Start sample applications
  - <https://docs.oracle.com/javase/tutorial/deployment/webstart/examplesIndex.html>
- ▶ Java certificate stores
  - Control Panel –> Java –> Security tab –> Manage certificates

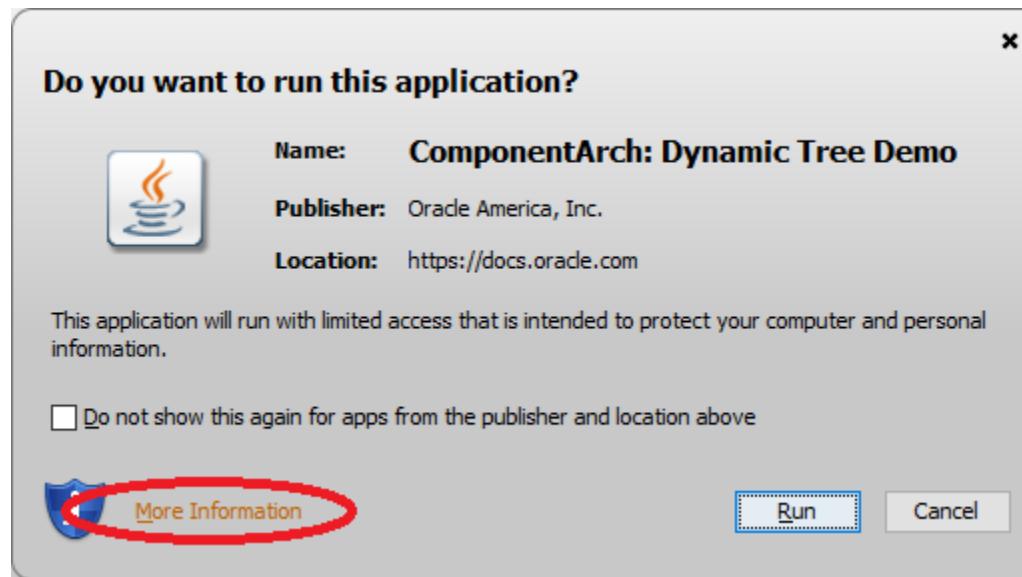
# Code signing – Java Web Start



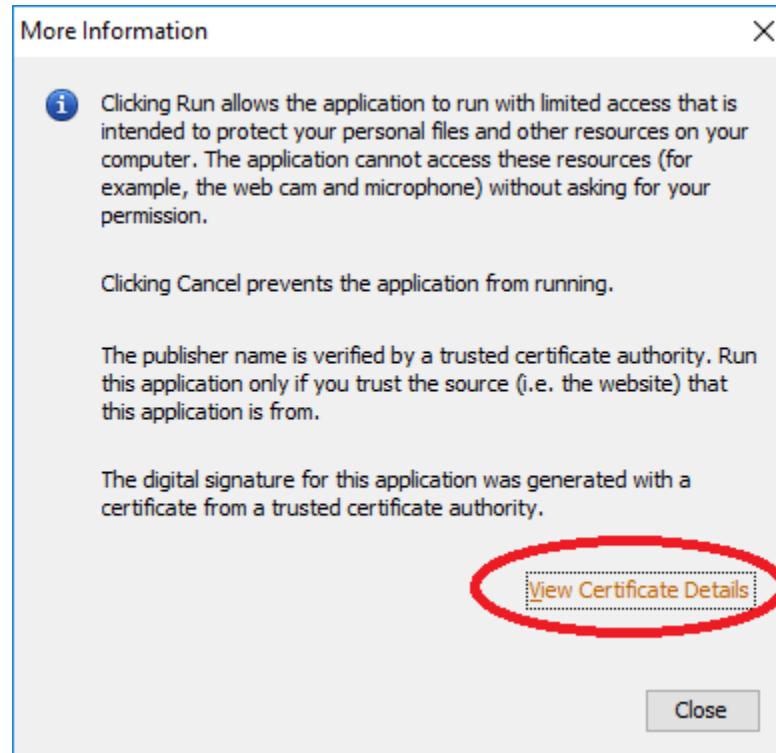
The screenshot shows a web browser window with the URL [docs.oracle.com/javase/tutorial/deployment/webstart/examplesIndex.html](https://docs.oracle.com/javase/tutorial/deployment/webstart/examplesIndex.html). The page title is "The Java™ Tutorials". Below the title, there is a navigation bar with links for "« Previous" and "TOC". A note at the top states: "The Java Tutorials have been written for JDK 8. Examples and practices described in this page don't take advantage of improvements introduced in later releases." The main content section is titled "Java Web Start Development Examples". It contains a table with two columns: "Example" (with a sub-instruction "(click on link to view example)") and "Zip File" (with a sub-instruction "(contains all source files necessary for the example plus NetBeans IDE project metadata)"). There are two rows in the table. The first row has a red oval around the link "Dynamic Tree Demo" in the "Example" column. The second row contains the links "webstart\_ComponentArch\_DynamicTreeDemo" and "webstart\_AppWithCustomProgressIndicator" respectively.

Example (click on link to view example)	Zip File (contains all source files necessary for the example plus NetBeans IDE project metadata)
<a href="#">Dynamic Tree Demo</a>	<a href="#">webstart_ComponentArch_DynamicTreeDemo</a>
<a href="#">Java Web Start Application With Customized Loading Progress Indicator</a>	<a href="#">webstart_AppWithCustomProgressIndicator</a>

# Code signing - Java Web Start



# Code signing – Java Web Start



# Code signing - Java Web Start

Details - Certificate

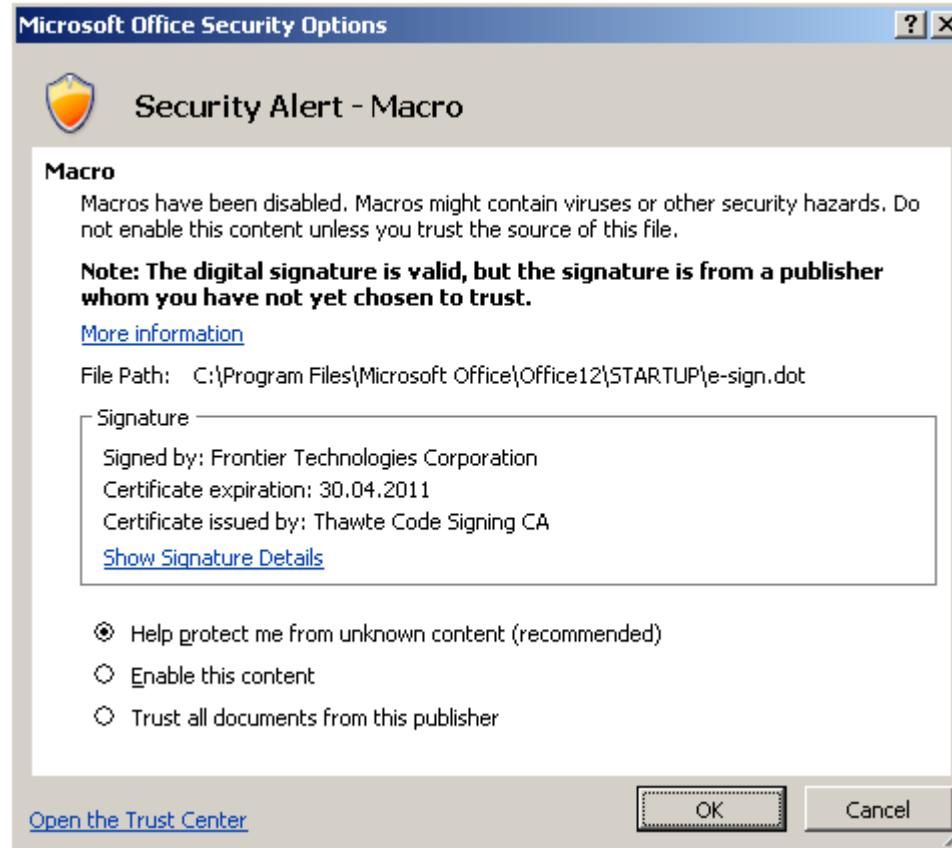
Field	Value
Version	V3
Serial Number	[33037644167568058970164719475676101...]
Signature Algorithm	[SHA1withRSA]
Issuer	CN=VeriSign Class 3 Public Primary Certificati...
Validity	[From: Wed Nov 08 02:00:00 EET 2006, To: ...]
Subject	CN=VeriSign Class 3 Public Primary Certificati...
Signature	0000: 93 24 4A 30 5F 62 CF D8 1A 98 2F 3...
MD5 Fingerprint	CB:17:E4:31:67:3E:E2:09:FE:45:57:93:F3:0...
SHA1 Fingerprint	4E:B6:D5:78:49:9B:1C:CF:5F:58:1E:AD:56:...

CN=VeriSign Class 3 Public Primary Certification Authority - G5,  
OU="(c) 2006 VeriSign, Inc. - For authorized use only",  
OU=VeriSign Trust Network,  
O="VeriSign, Inc.",  
C=US

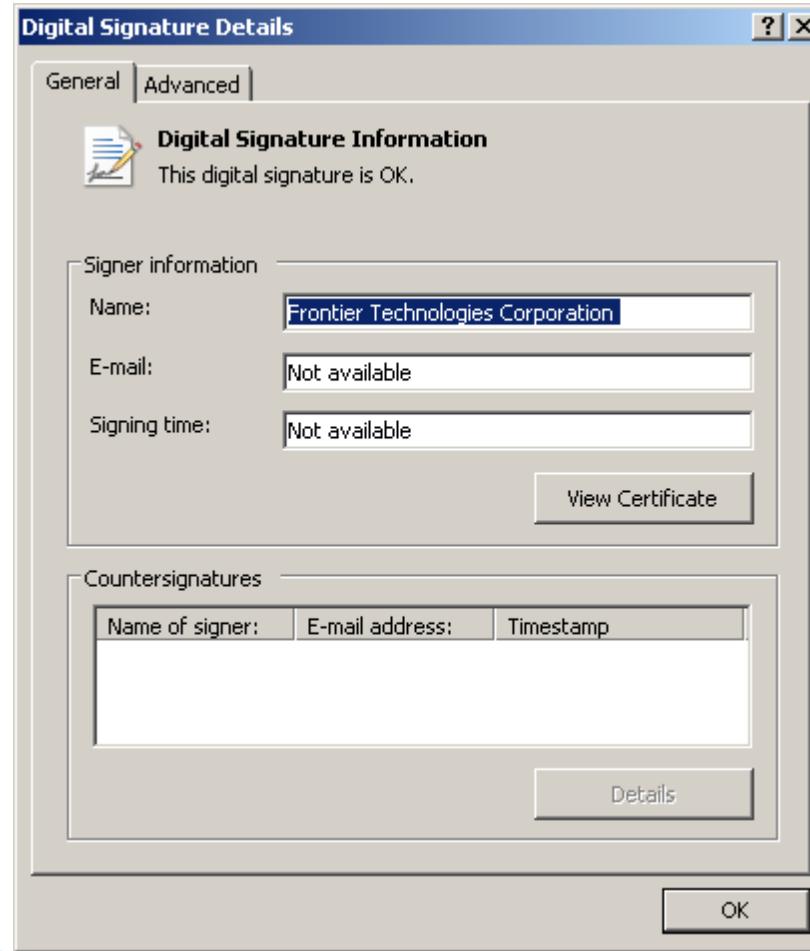
< >

[Close](#)

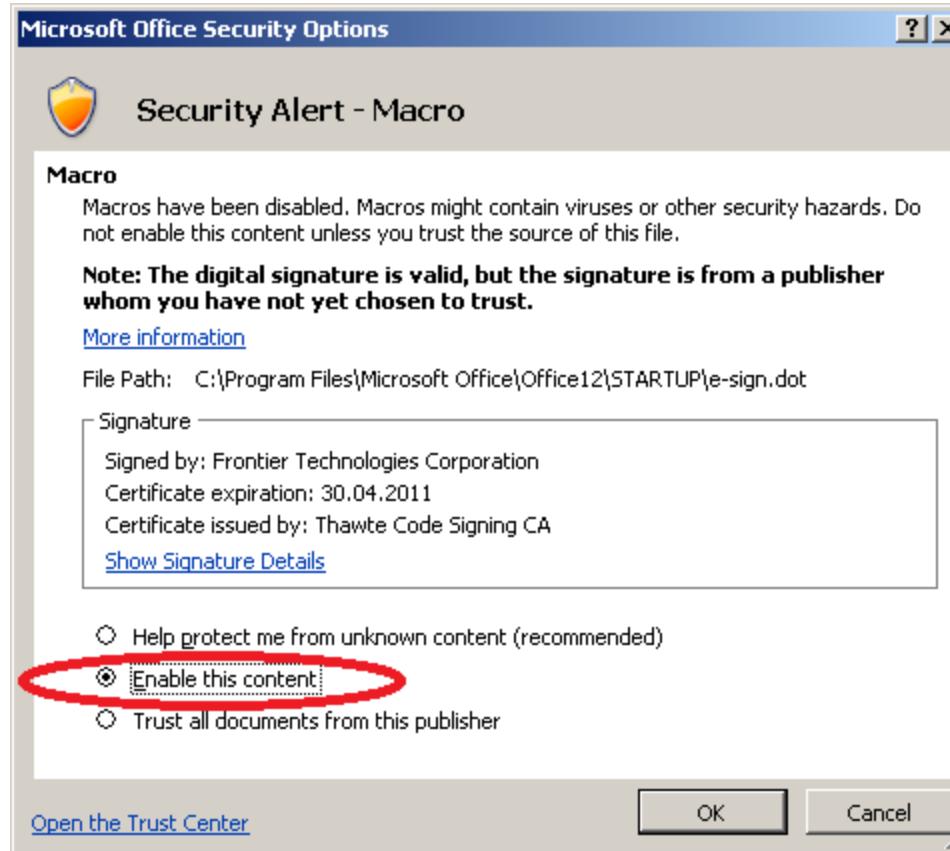
# Code signing – Macros



# Code signing – Macros



# Code signing – Macros



# Code signing – Executables

- ▶ User Account Control on Microsoft Windows 7 and greater

# Cryptography libraries – High Level

- ▶ **Digital Signature Services**

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Start+using+Digital+Signature+Services+%28DSS%29++Releases+and+Bitbucket>

- ▶ **Bouncy Castle**

<https://www.bouncycastle.org/>

- ▶ **SecureBlackbox**

<http://www.secureblackbox.com/#>

# Cryptography libraries – Low Level

- ▶ **OpenSSL**

<https://www.openssl.org/>

- ▶ **MIRACL**

<https://github.com/miracl/MIRACL>

<https://libraries.docs.miracl.com/miracl-explained/what-is-miracl>

- ▶ **libecc**

<https://github.com/ANSSI-FR/libecc>

# Microsoft Trusted Root Certificate Program

- ▶ <https://technet.microsoft.com/en-us/library/cc751157.aspx>
- ▶ Provides to clients a list of all the certificates of the certificate authorities that are trusted by Microsoft

# Microsoft Trusted Root Certificate Program

- ▶ Trusted Root Certification Authorities logical certificate store
  - is populated with all these certificates from the moment that a Windows operating system is installed
- ▶ The list of the certificate authorities that Microsoft trusts is permanently updated

# Microsoft Trusted Root Certificate Program

- ▶ The update of the contents of Trusted Root Certification Authorities (**automatic update**):
  - By Internet Explorer:
  - every time a user
    - access a HTTPS site,
    - or opens a S/MIME e-mail message,
    - or downloads a signed ActiveX control,
  - and the operating system, in its verifications, encounters a certificate that is not present in the Trusted store
    - it will verify online if this certificate is on the trusted CAs list of Microsoft
    - and if yes, it will be downloaded in the store

# Microsoft Trusted Root Certificate Program

- ▶ For a CA to have its certificate included on the Microsoft trusted CAs list, it must:
  - Obtain a preliminary approval for the participation, which is granted based on some information requested by Microsoft
  - The CA must send a test certificate issued by its root certificate authority
  - The CA must then sign an agreement with Microsoft

# Microsoft Trusted Root Certificate Program

- ▶ The root certificate of the CA must have
  - a minimum 2048 bit length RSA key
  - the validity period must be at least 8 years
  - but it should expire before 2030
  
- ▶ The certificates issued by the CA must
  - support the CRL Distribution Point extension
  - and the CRL distribution point must be publically accessible

# Microsoft Trusted Root Certificate Program

- ▶ The CA
  - must have a written certificate revocation policy
  - must be able to revoke any of the issued certificates
  - must be the subject of an annual security audit
  - and it must sent the results to Microsoft

# Microsoft Trusted Root Certificate Program

- ▶ Using Internet Explorer
  - access a HTTPS web site for which the certificate is issued by a certificate authority that has its root certificate on the Microsoft trusted CAs list
  - E.g.
  - <https://ca.transped.ro>
- ▶ The page will be automatically opened, like a regular HTTP web page

# Microsoft Trusted Root Certificate Program



ca.transsped.ro - Windows Internet Explorer

https://ca.transsped.ro/

File Edit View Favorites Tools Help

Favorites Suggested Sites Free Hotmail Web Slice Gallery

ca.transsped.ro

pagina principala

Telefon: 0212108700, 0212120439,  
Email: supportqca@transsped.ro [>>]

| emitere c.c. | reemitere c.c. | revocare c.c. | depozitar c.a. | www.transsped.ro |

\* Pentru emiterea unui certificat calificat apasati AICI si urmati instructiunile.

Completarea documentului de confirmare pentru ANAF

Dupa ce ati instalat certificatul si ati verificat daca este instalat corect, trebuie sa completati documentul de confirmare. Documentul de confirmare il puteti gasi pe site-ul [www.anaf.ro](http://www.anaf.ro) > Asistenta Contribuabili > Toate formularurile cu explicatii > Formularul 150 , aici la sfarsitul paragrafului veti gasi documentul de confirmare in format pdf.

Cautare Certificat Calificat

Pentru cautarea unui certificat calificat emis de Trans Sped QCA puteti folosi serviciul on-line de cautare a certificatelor.

Trans Sped este Autoritate de Certificare (AC), emitenta de certificate electronice.

# Microsoft Trusted Root Certificate Program

ca.transsped.ro - Windows Internet Explorer

https://ca.transsped.ro/

File Edit View Favorites Tools Help

Favorites Suggested Sites Free Hotmail Web

ca.transsped.ro

**Trans Sped**  
Join us in e-Society

| emitere c.c. | reemitere c.c. | revocare c.c. | depozitar c.a. | www.transsped.ro |

\* Pentru emiterea unui certificat calificat apasati AICI si urmati instructiunile.

Completarea documentului de confirmare pentru ANAF

Website Identification

TC TrustCenter Class 2 CA II has identified this site as:  
ca.transsped.ro

This connection to the server is encrypted.  
Should I trust this site?

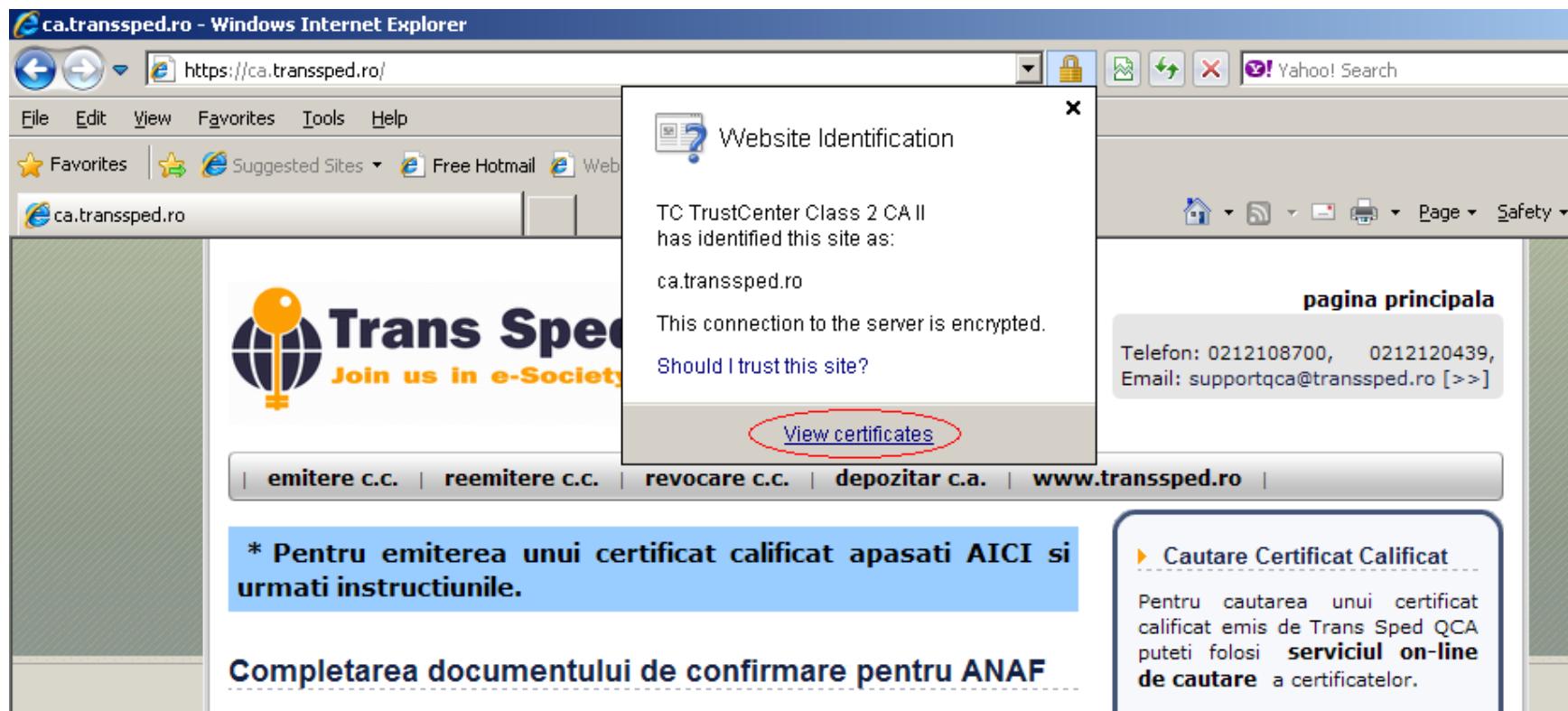
[View certificates](#)

pagina principala

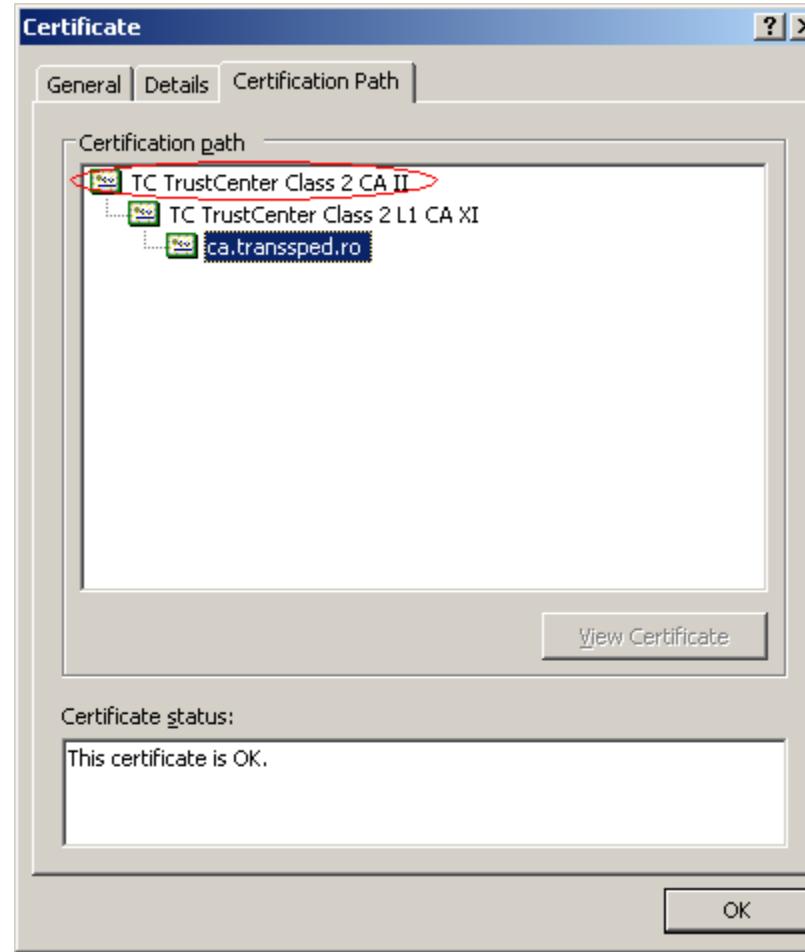
Telefon: 0212108700, 0212120439,  
Email: supportqca@transsped.ro [>>]

► Cautare Certificat Calificat

Pentru cautaarea unui certificat calificat emis de Trans Sped QCA puteti folosi **serviciul on-line de cauta** a certificatelor.



# Microsoft Trusted Root Certificate Program

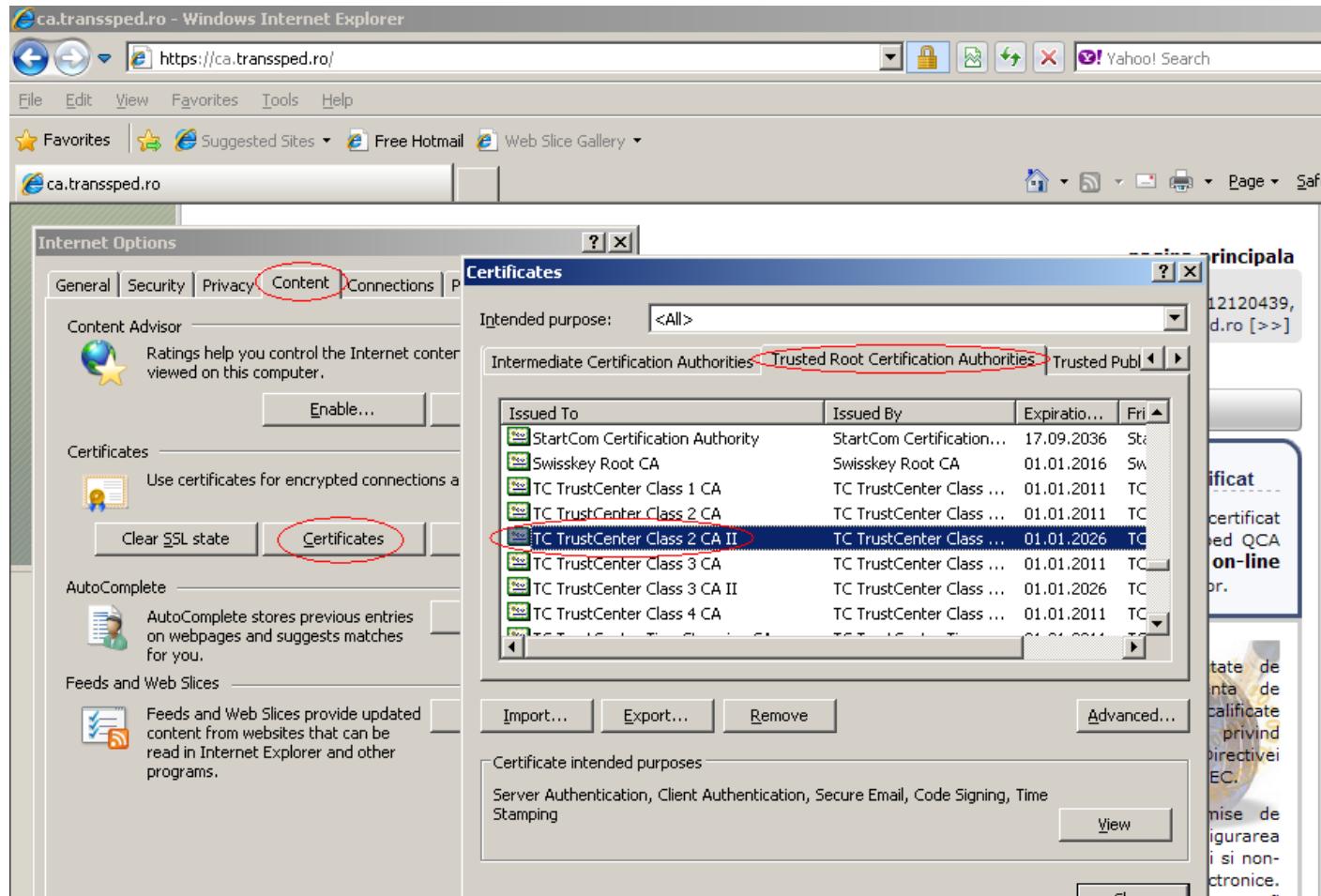


# Microsoft Trusted Root Certificate Program

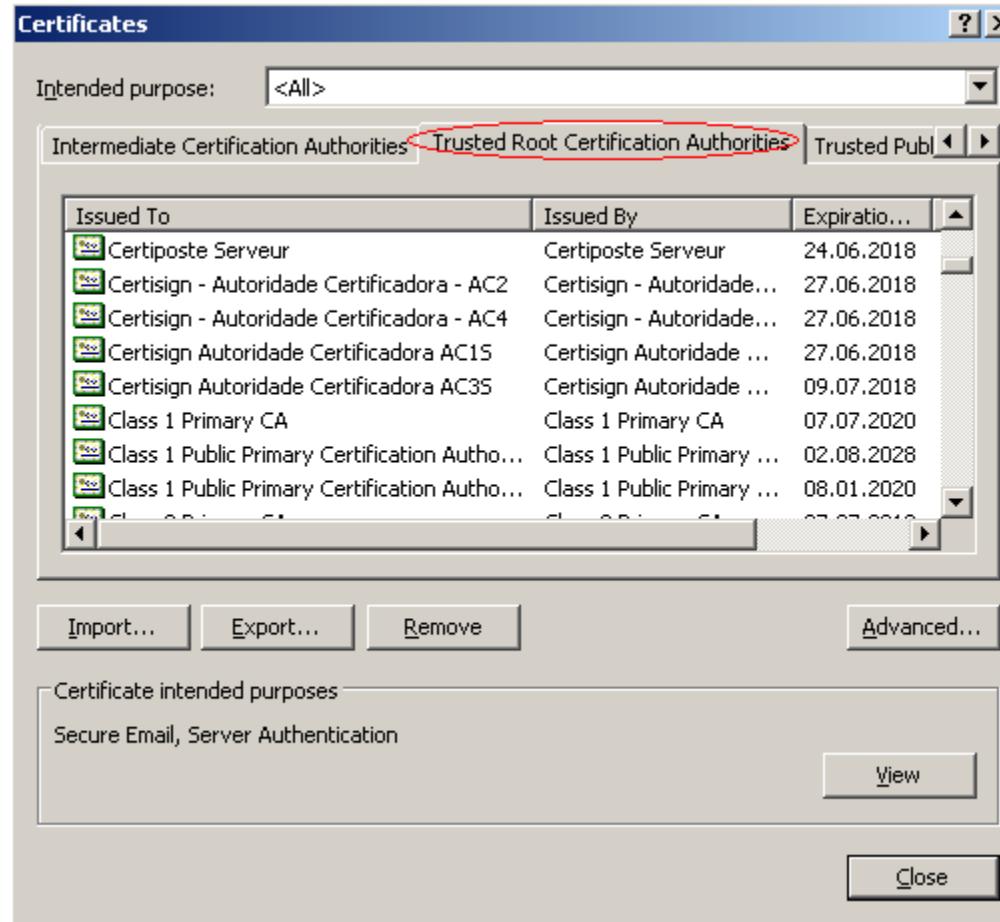
The screenshot shows a Microsoft Internet Explorer window with the following details:

- Title Bar:** "ro - Windows Internet Explorer"
- Address Bar:** "https://ca.transped.ro/"
- Toolbar:** Includes icons for Favorites, Tools, Help, Suggested Sites, Free Hotmail, and Web Slice Gallery.
- Menu Bar:** Includes icons for Home, Refresh, Stop, Page, Safety, Tools, and Help.
- Content Area:**
  - Trans Sped Logo:** "Join us in e-Society!"
  - Navigation Links:** "emitere c.c.", "reemitere c.c.", "revocare c.c.", "depozitar c.a.", "www.transped.ro".
  - Text Box:** "Pentru emiterea unui certificat calificat apasati AICI si urmati instructiunile."
  - Section Header:** "Completarea documentului de confirmare pentru ANAF"
  - Description:** "Dupa ce ati instalat certificatul si ati verificat daca este instalat corect, trebuie sa completati documentul de confirmare. Documentul de confirmare il puteti gasi pe site-
- Tools Menu (open):** Shows options like Reopen Last Browsing Session, Pop-up Blocker, Manage Add-ons, Work Offline, Compatibility View, Full Screen, Toolbars, Explorer Bars, Developer Tools, Suggested Sites, Send to OneNote, and Internet Options.

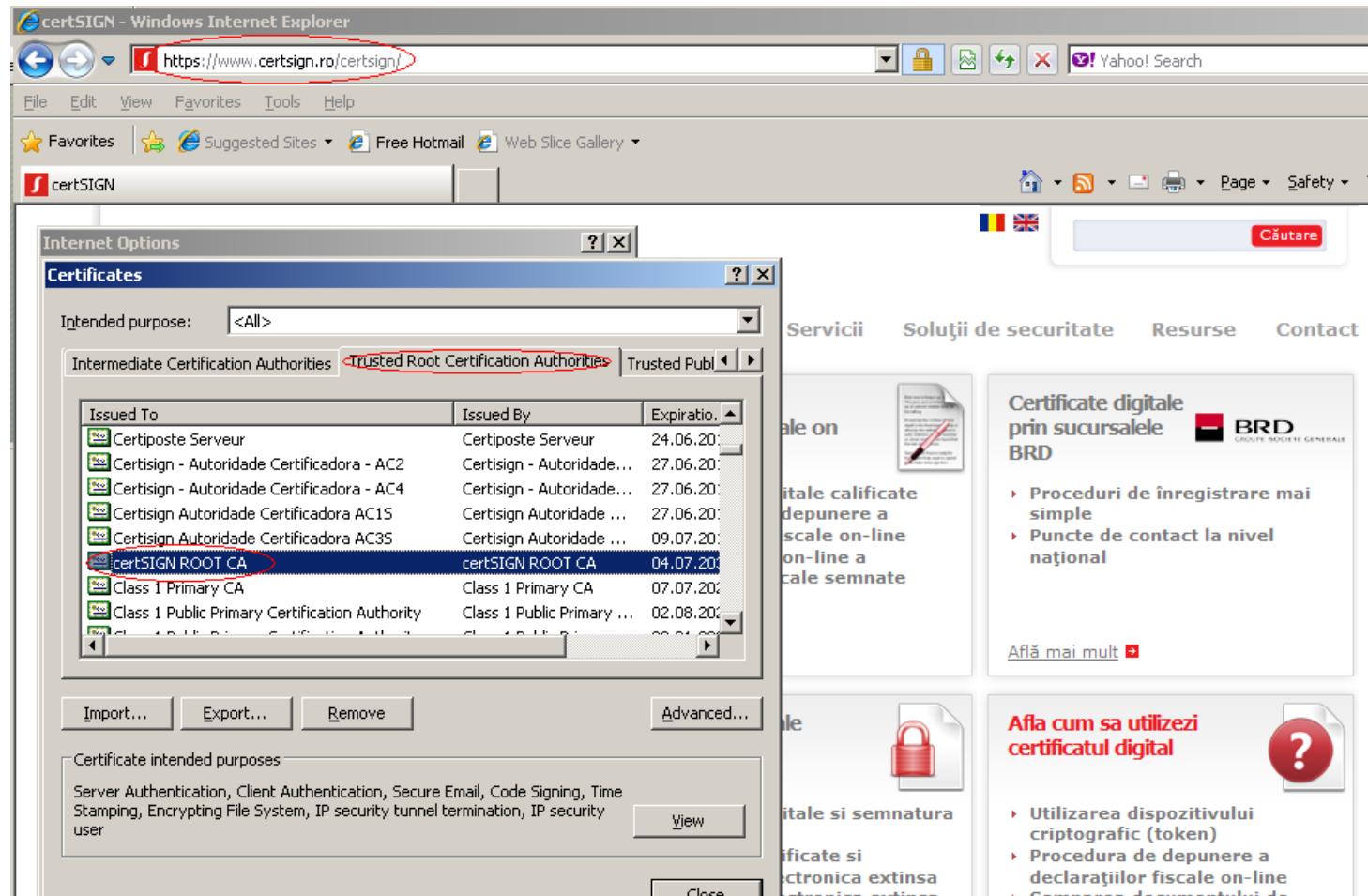
# Microsoft Trusted Root Certificate Program



# Microsoft Trusted Root Certificate Program



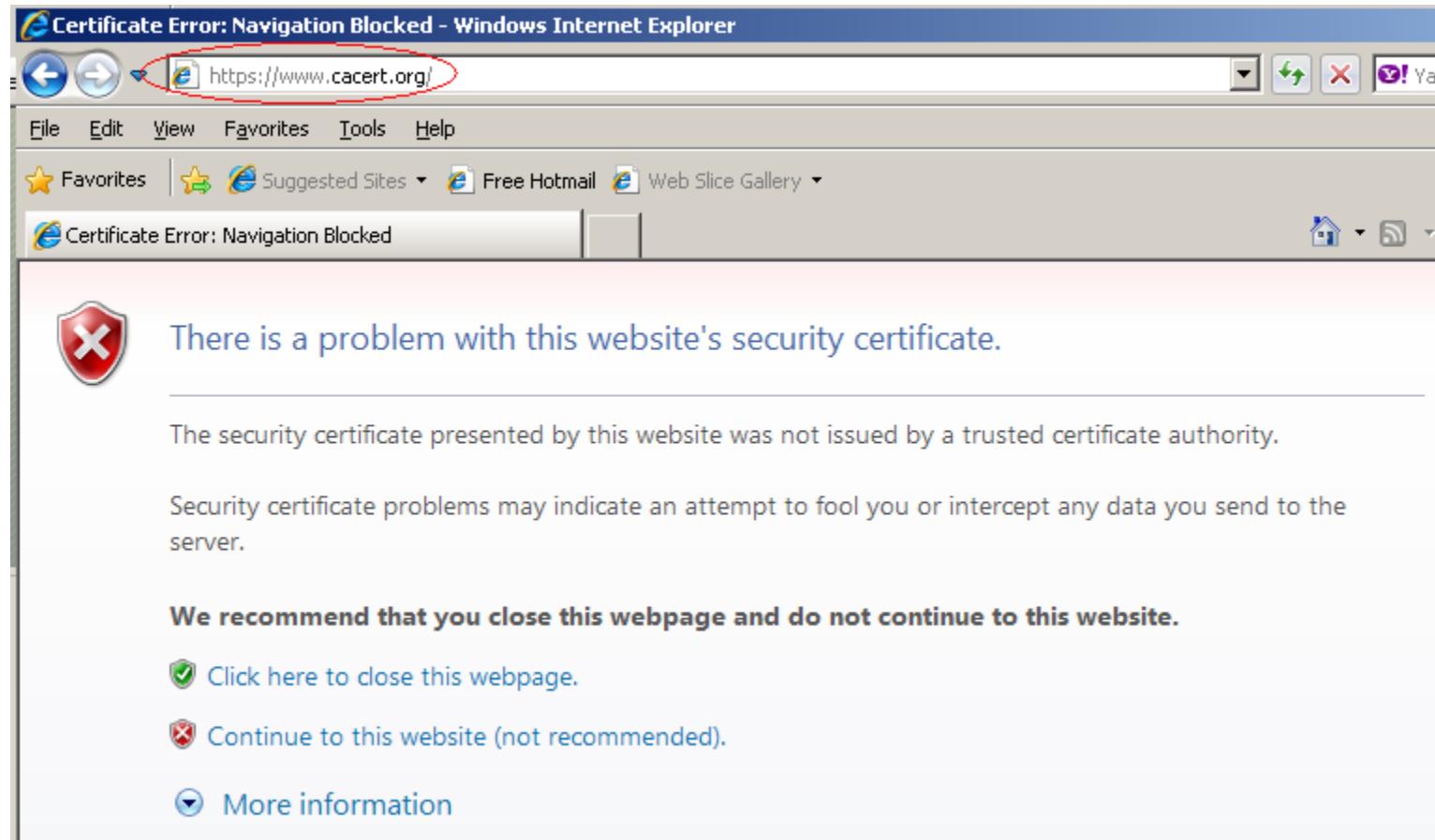
# Microsoft Trusted Root Certificate Program



# Microsoft Trusted Root Certificate Program

- ▶ Using Internet Explorer
  - access a HTTPS web site for which the certificate is NOT issued by a certificate authority that has its root certificate on the Microsoft trusted CAs list
  - E.g.
  - <https://www.cacert.org>
- ▶ The page will NOT be automatically opened

# Microsoft Trusted Root Certificate Program



# Microsoft Trusted Root Certificate Program

The screenshot shows a Microsoft Internet Explorer window with the title "Welcome to CAcert.org - Windows Internet Explorer". The address bar displays "CA https://www.cacert.org/" and shows a red "Certificate Error" icon. A tooltip window titled "Untrusted Certificate" is overlaid on the page. It contains the following text:

The security certificate presented by this website was not issued by a trusted certificate authority.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

[About certificate errors](#)

[View certificates](#)

The main content of the page includes the CAcert logo, a "Are you new to CAcert?" section, and an "ATE-Melbourne" event announcement.

# Microsoft Trusted Root Certificate Program



# Microsoft Trusted Root Certificate Program

Welcome to CAcert.org - Windows Internet Explorer  
CA https://www.cacert.org/index.php?id=3 Certificate Error Yahoo! Search

File Edit View Favorites Tools Help

Favorites Suggested Sites Free Hotmail Web Slice Gallery

CA Welcome to CAcert.org

Join CAcert.org  
Join Community Agree Root Certificate

My Account  
Password Login  
Lost Password  
Net Cafe Login  
Certificate Login

+ About CAcert.org  
+ Translations

CAcert

You are bound by the Root Distribution Licence for any re-distributions of CAcert's roots.

Class 1 PKI Key  
Click here if you want to import the root certificate into Microsoft Internet Explorer 5.x/6.x  
[Root Certificate \(PEM Format\)](#) (highlighted with a red box)  
[Root Certificate \(DER Format\)](#)  
[Root Certificate \(Text Format\)](#)  
CRL  
Fingerprint SHA1: 13:5C:EC:36:F4:9C:B8:E9:3B:1A:B2:70:CD:80:88:46:76:CE:8F:33  
Fingerprint MD5: A6:1B:37:5E:39:0D:9C:36:54:EE:BD:20:31:46:1F:6B

Class 3 PKI Key  
[Intermediate Certificate \(PEM Format\)](#)  
[Intermediate Certificate \(DER Format\)](#)  
[Intermediate Certificate \(Text Format\)](#)  
CRL

# Microsoft Trusted Root Certificate Program

The screenshot shows a Microsoft Internet Explorer window with the title bar "Welcome to CAcert.org - Windows Internet Explorer". The address bar displays "CA https://www.cacert.org/". A context menu is open over the address bar, with the "Copy Address" option highlighted.

The main content area shows the CAcert.org homepage. On the left, there's a large logo with the word "CACert" and a green circular graphic. Below it is a section titled "Are you new to CAcert?". It contains text about joining the community and using certificates, along with links to the "Root Distribution License" and "ATE-Melbourne".

A "Website Identification" dialog box is overlaid on the page. It contains the following text:

CA Cert Signing Authority  
has identified this site as:  
www.cacert.org

This connection to the server is encrypted.

Should I trust this site?

[View certificates](#)

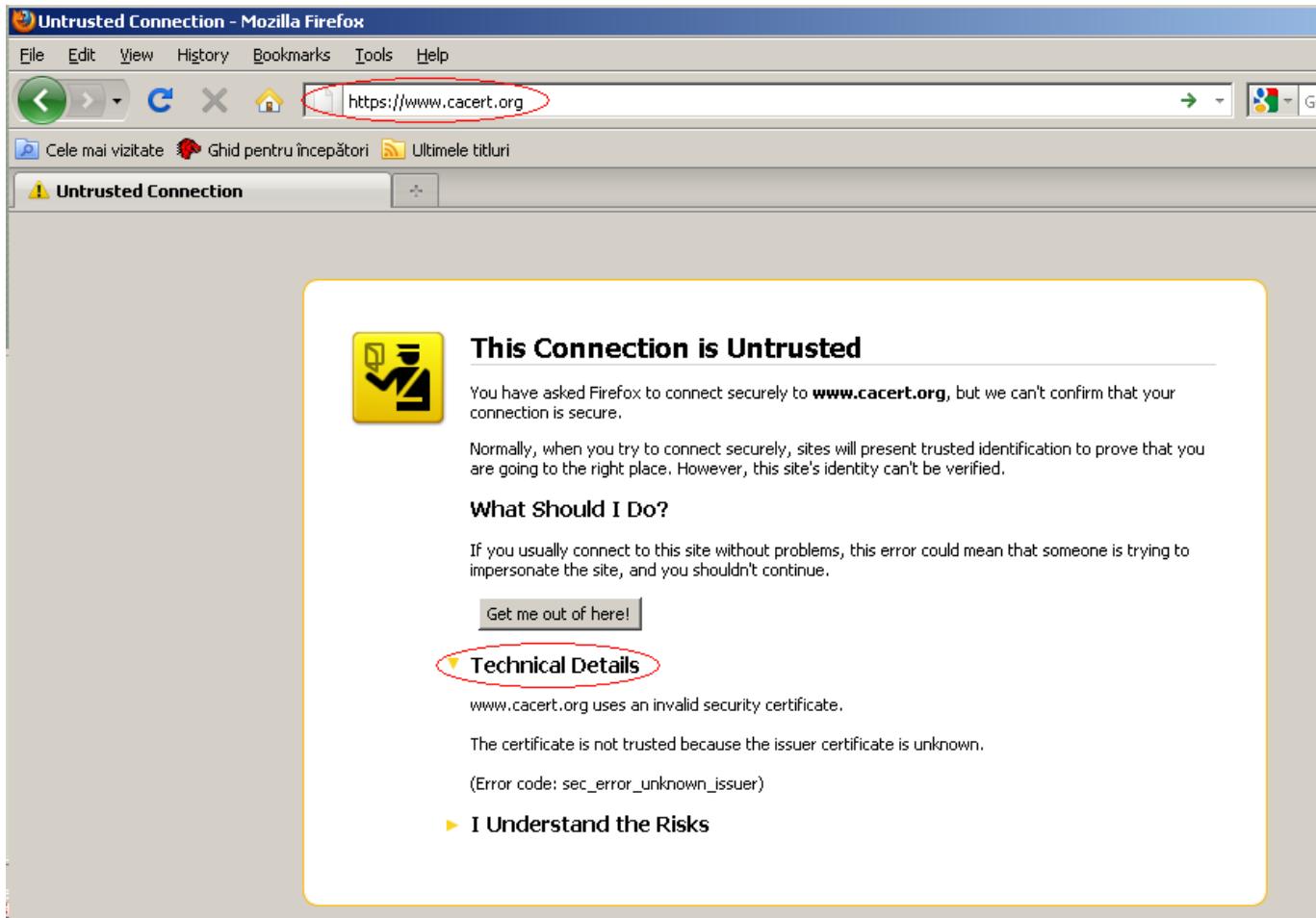
# Mozilla CA Certificate Policy

- ▶ <https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/>
- ▶ When downloading and installing
  - Firefox,
  - Thunderbird
  - or other Mozilla applications
- ▶ their certificate store it is populated will a list of certificates
- ▶ All these certificates are marked as trusted so Firefox and Thunderbird, for example, will use them for digital signatures validation without displaying any message to the user

# Mozilla CA Certificate Policy

- ▶ As for the Microsoft Program, a CA will be included on this list after a request and a special verification process
- ▶ The major differences from the Microsoft verification process are that no fees are requested, and the verification is public

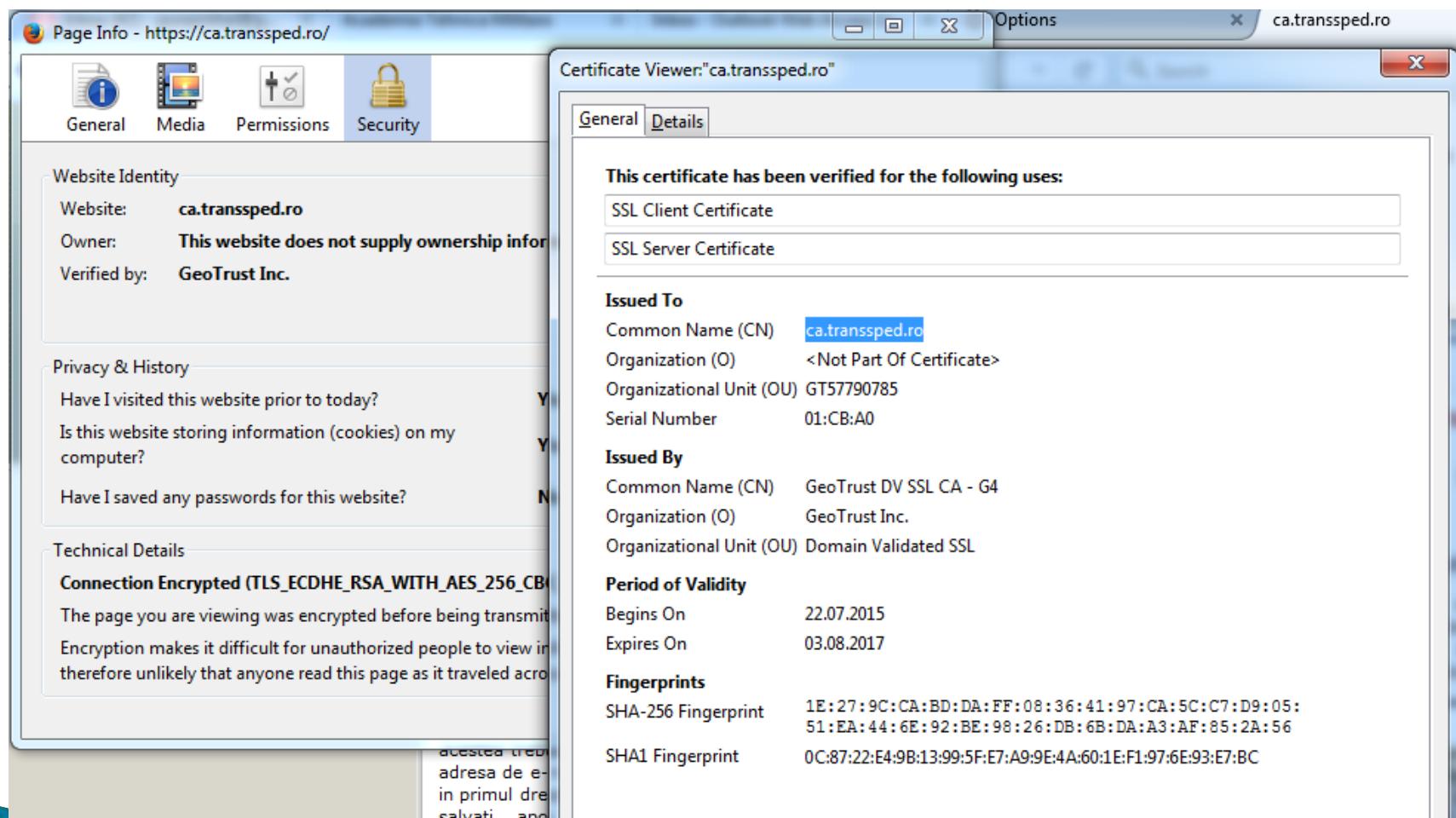
# Mozilla CA Certificate Policy



# Mozilla CA Certificate Policy

The screenshot shows a Mozilla browser window with the URL <https://ca.transped.ro>. The address bar includes a lock icon and the URL. The main content area displays a secure connection message from **transsped.ro**, verified by GeoTrust Inc. A blue button labeled "More Information" is visible. To the right, the website header features the text "ans Sped" and "us in e-Society!". Below the header, there are two blue buttons labeled "reemitere/reinnoire c.c.(standard)" and "reemitere/reinnoire". A prominent blue callout box contains the text: "**\* Pentru emiterea unui certificat calificat apasati AICI si urmati instructiunile.**". Further down, a section titled "**Completarea documentului de confirmare pentru ANAF**" provides instructions: "Dupa ce ati instalat certificatul si ati verificat daca este instalat corect, trebuie sa completati documentul de confirmare. Documentul de confirmare il puteti gasi pe site-ul [www.anaf.ro](http://www.anaf.ro) > Servicii on-line> Declaratii electronice > Descarcare declaratii >Document de confirmare > Formularul 150 , aici la sfarsitul paragrafului veti gasi link-ul catre documentul de confirmare in format pdf." A red warning message at the bottom states: "**ATENTIE ! Pentru completarea documentului folositi numai Adobe Reader 8.2 pe care il puteti descarca de [AICI](#).**".

# Mozilla CA Certificate Policy



The screenshot shows two overlapping windows from Mozilla Firefox. The main window is titled "Page Info - https://ca.transsped.ro/" and displays the "Security" tab. It shows the website identity as "ca.transsped.ro", ownership information as "This website does not supply ownership information", and verification by "GeoTrust Inc.". The "Privacy & History" section shows no history or saved passwords. The "Technical Details" section indicates the connection is encrypted with TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384. The second window, titled "Certificate Viewer: ca.transsped.ro", displays the certificate details. It lists the following verified uses: "SSL Client Certificate" and "SSL Server Certificate". The "Issued To" section shows the common name as "ca.transsped.ro", organization as "<Not Part Of Certificate>", organizational unit as "GT57790785", and serial number as "01:CB:A0". The "Issued By" section shows the common name as "GeoTrust DV SSL CA - G4", organization as "GeoTrust Inc.", and organizational unit as "Domain Validated SSL". The "Period of Validity" section shows the certificate begins on 22.07.2015 and expires on 03.08.2017. The "Fingerprints" section provides SHA-256 and SHA1 fingerprints.

Page Info - https://ca.transsped.ro/

General Media Permissions Security

Website Identity

Website: **ca.transsped.ro**

Owner: **This website does not supply ownership information**

Verified by: **GeoTrust Inc.**

Privacy & History

Have I visited this website prior to today? **Yes**

Is this website storing information (cookies) on my computer? **Yes**

Have I saved any passwords for this website? **No**

Technical Details

**Connection Encrypted (TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384)**

The page you are viewing was encrypted before being transmitted.

Encryption makes it difficult for unauthorized people to view it, therefore unlikely that anyone read this page as it traveled across the Internet.

Accessed through address bar  
in primul drept salvati and

Certificate Viewer: "ca.transsped.ro"

General Details

This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN) **ca.transsped.ro**

Organization (O) **<Not Part Of Certificate>**

Organizational Unit (OU) **GT57790785**

Serial Number **01:CB:A0**

Issued By

Common Name (CN) **GeoTrust DV SSL CA - G4**

Organization (O) **GeoTrust Inc.**

Organizational Unit (OU) **Domain Validated SSL**

Period of Validity

Begins On **22.07.2015**

Expires On **03.08.2017**

Fingerprints

SHA-256 Fingerprint **1E:27:9C:CA:BD:DA:FF:08:36:41:97:CA:5C:C7:D9:05:51:EA:44:6E:92:BE:98:26:DB:6B:DA:A3:AF:85:2A:56**

SHA1 Fingerprint **0C:87:22:E4:9B:13:99:5F:E7:A9:9E:4A:60:1E:F1:97:6E:93:E7:BC**

# Mozilla CA Certificate Policy

The screenshot shows the Mozilla Firefox Advanced preferences interface. The left sidebar lists various categories: General, Search, Content, Applications, Privacy, Security, Sync, and Advanced. The Advanced category is currently selected, indicated by an orange border around its icon.

The main content area displays the "Advanced" settings page. At the top, there are tabs for General, Data Choices, Network, Update, and Certificates. The Certificates tab is active, highlighted with an orange bar.

**Requests**

When a server requests my personal certificate:

- Select one automatically
- Ask me every time

Query OCSP responder servers to confirm the current status of my certificates

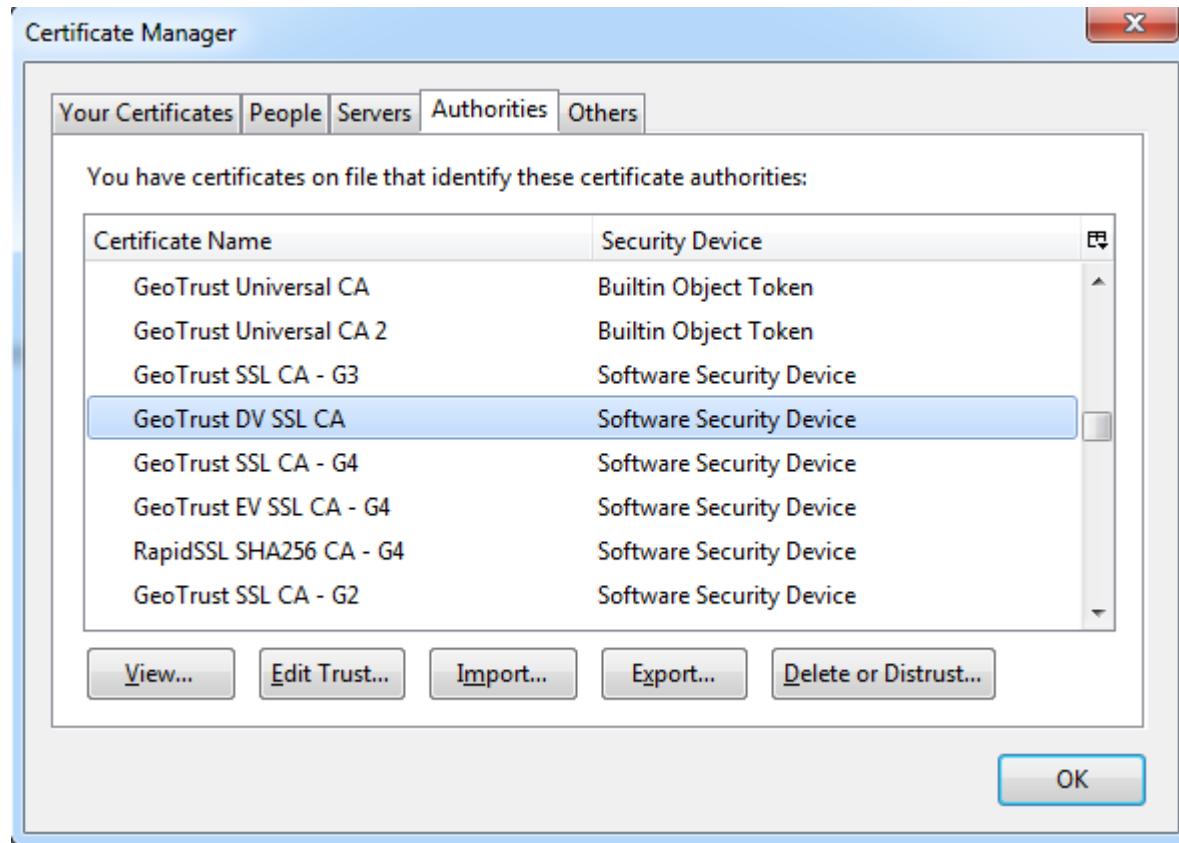
[View Certificates](#) [Security Devices](#)

A modal dialog box titled "Certificate Manager" is displayed over the preferences window. It lists "Your Certificates" and includes tabs for People, Servers, Authorities, and Others. The Authorities tab is selected, showing a list of certificate authorities:

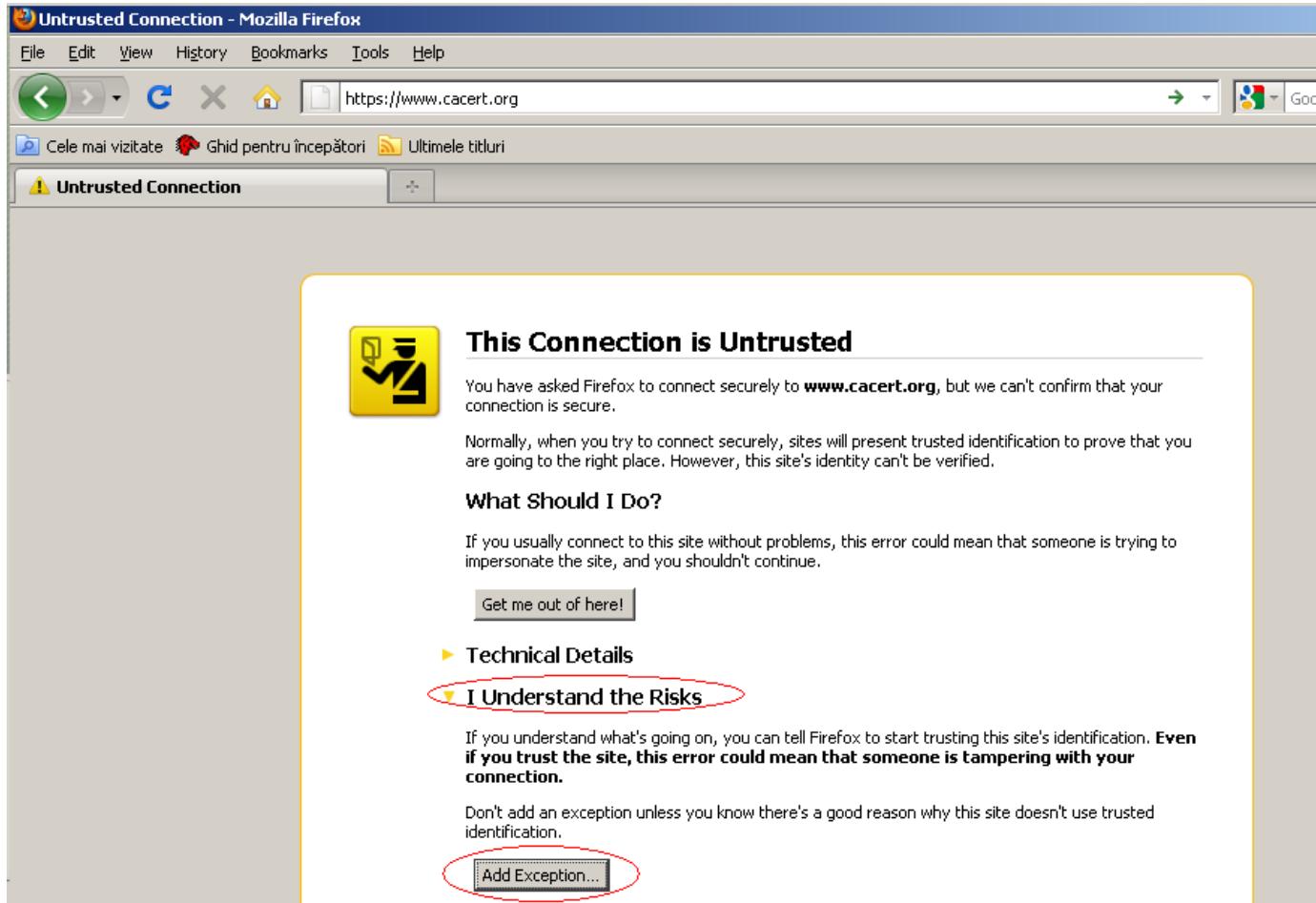
Certificate Name	Security Device
A-Trust Ges. f. Sicherheitssysteme im elektr....	Builtin Object Token
A-Trust-nQual-03	Builtin Object Token
AC Camerfirma S.A.	Builtin Object Token
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	Builtin Object Token
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token

Buttons at the bottom of the dialog include View..., Edit Trust..., Import..., Export..., Delete or Distrust..., and OK.

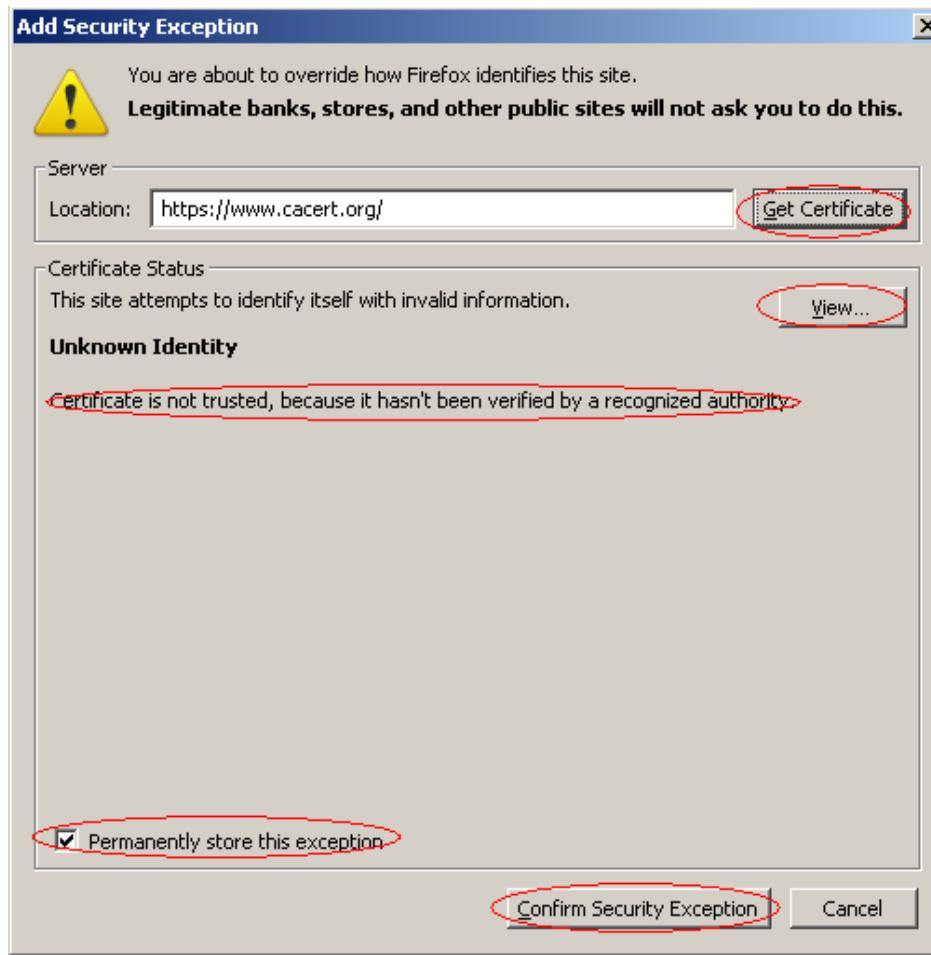
# Mozilla CA Certificate Policy



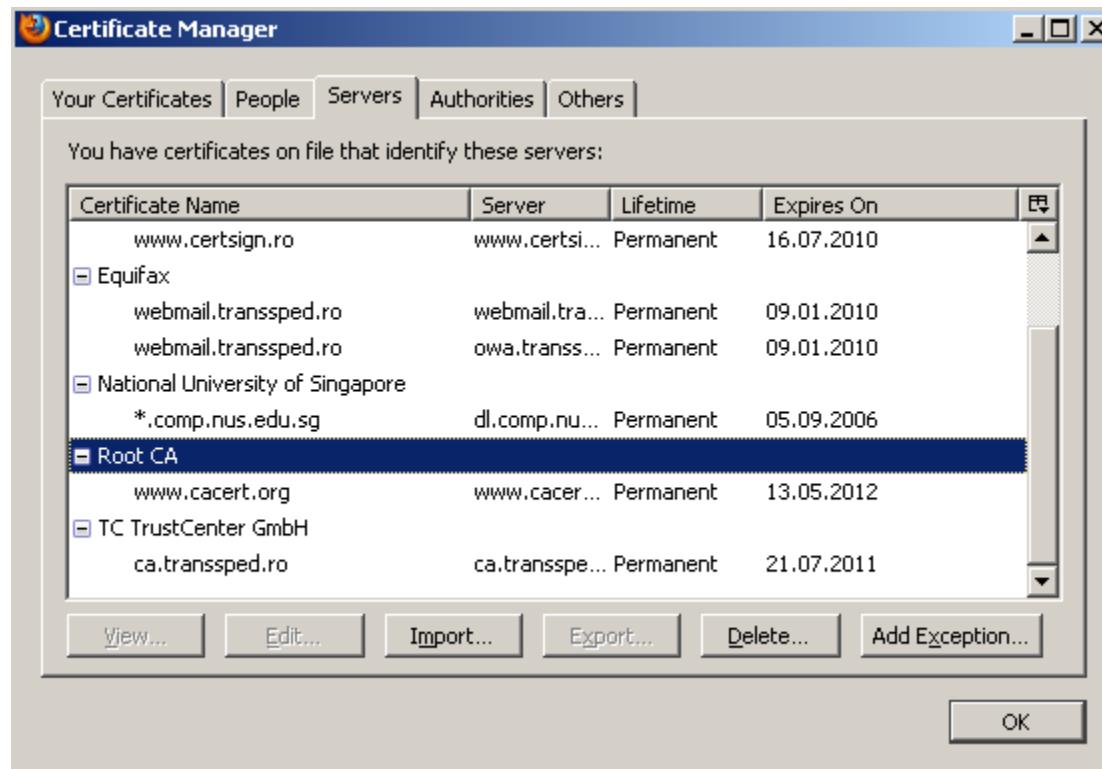
# Mozilla CA Certificate Policy



# Mozilla CA Certificate Policy



# Mozilla CA Certificate Policy



# Mozilla CA Certificate Policy

Firefox | about:preferences#advanced

Search

General

Search

Content

Applications

Privacy

Security

Sync

Advanced

## Advanced

General Data Choices Network Update Certificates

### Requests

When a server requests my personal certificate:

Select one automatically

Ask me every time

Query OCSP responder servers to confirm the current validity of certificates

[View Certificates](#) [Security Devices](#)

# Legislation

- ▶ Legea nr. 455/2001 privind **semnătura electronică**
  - [http://www.transsped.ro/content/L\\_2001\\_07\\_18\\_455.pdf](http://www.transsped.ro/content/L_2001_07_18_455.pdf)
- ▶ HG 1259/2001 privind Normele tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnatura electronică
  - [http://www.transsped.ro/content/HG\\_2001\\_12\\_13\\_1259.pdf](http://www.transsped.ro/content/HG_2001_12_13_1259.pdf)
- ▶ eIDAS Regulation no. 910/2014
  - <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32014R0910&from=EN>

# Legislation

- ▶ Legea nr. 451 din 1 noiembrie 2004 privind **marca temporală**
  - <https://www.certsign.ro/ro/documentatie/legislatie/legea-451-2004-privind-marca-temporală>
- ▶ Legea nr. 589 din 15 decembrie 2004 privind regimul juridic al **activității electronice notariale**
  - <https://www.certsign.ro/ro/documentatie/legislatie/legea-589-2004-activitate-electronica-notariala>
- ▶ Normele tehnice și metodologice pentru aplicarea legii 589/2004 privind regimul juridic al activității electronice notariale
  - <https://www.certsign.ro/ro/documentatie/legislatie/norme-aplicare-lege-activitate-electronica-notariala>

# Legislation

- ▶ Legea 135/2007 a arhivării electronice
  - <https://www.certsign.ro/ro/documentatie/legislatie/legea-135-2007-arhivare-electronica>
- ▶ Ordin MEF 858/2008 privind depunerea **declarațiilor fiscale prin mijloace electronice de transmitere la distanță**
  - <https://www.certsign.ro/ro/documentatie/legislatie/ordin-declaratii-fiscale-online>

# Romanian CAs

- ▶ AlfaSign
  - ▶ <https://www.alfasign.ro/>
- ▶ certSIGN
  - ▶ <https://www.certsign.ro/>
- ▶ CERT DIGITAL
  - ▶ <https://www.certdigital.ro/>
- ▶ DigiSign
  - ▶ <https://www.digisign.ro/>
- ▶ Trans Sped
  - ▶ <http://www.transped.ro/>

# References

- ▶ The Value of Certificate Revocation Lists (CRLs) in a PKI
  - <https://blogs.technet.microsoft.com/staysafe/2012/02/09/the-value-of-certificate-revocation-lists-crls-in-a-pki/>
- ▶ Formats of a digital signature
  - <http://developers-club.com/posts/191866/>
- ▶ Introduction to XML Digital Signatures
  - <https://flylib.com/books/en/2.329.1.75/1/>

# References

- ▶ Certificate Trust
  - <https://piv.idmanagement.gov/pivcertchains/>
- ▶ Windows XP: Certificate Status and Revocation Checking
  - <https://social.technet.microsoft.com/wiki/contents/articles/4954.windows-xp-certificate-status-and-revocation-checking.aspx>
- ▶ Digital Signatures in a PDF
  - [https://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat\\_DigitalSignatures\\_in\\_PDF.pdf](https://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf)