Ministerul Educaţiei, al Culturii și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Departamentul Informatică și Ingineria Sistemelor

RAPORT

Lucrarea de laborator nr.1

TTGE

A efectuat:

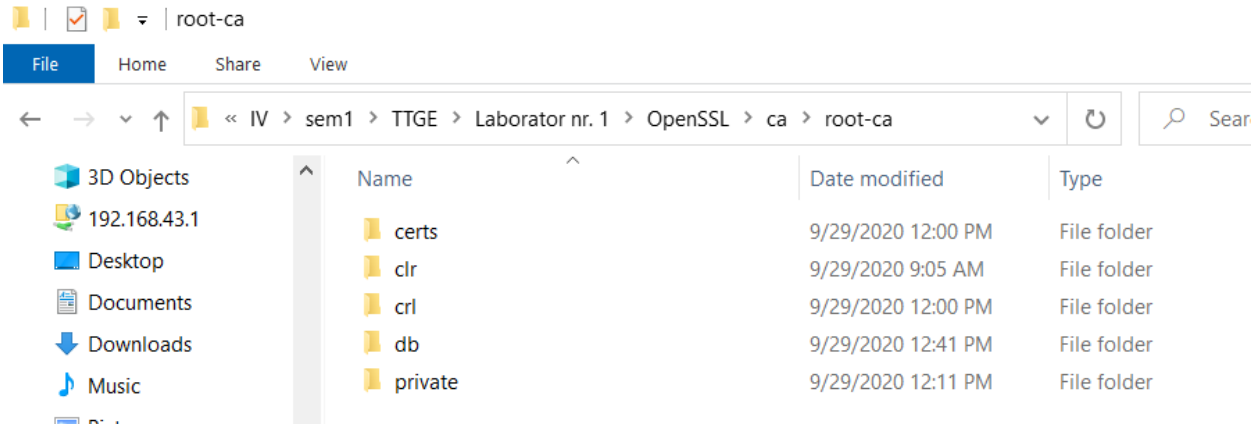
st. gr. C-171 D. Melniciuc

A verificat:

dr., conf.univ. O.Godonoga

Chişinău 2020

Structura OpenSSL\ca\root-ca



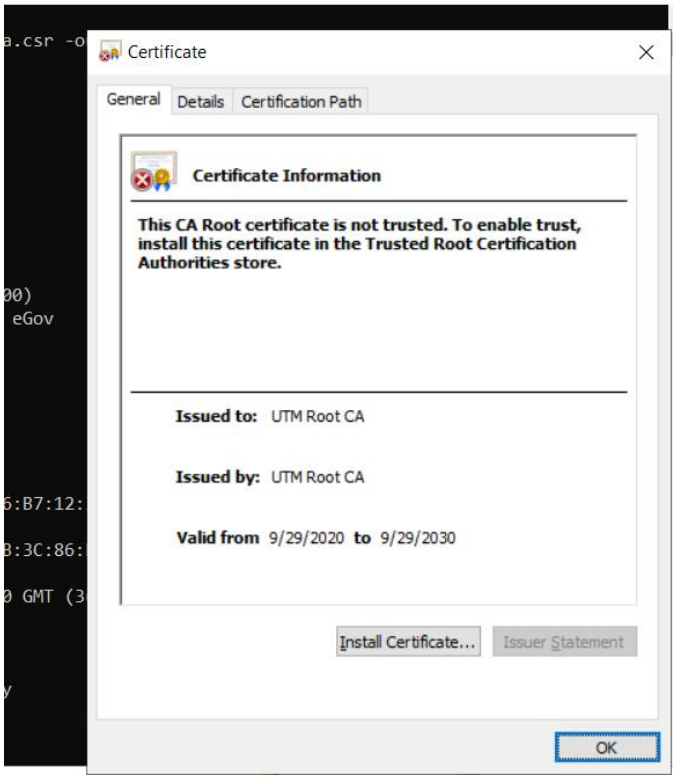
Crearea perechii de chei și cererea de semnare a certificatului cheii publice pentru autoritatea de certificare de nivel superior

```
E:\univeristate\IV\sem1\TTGE\Laborator nr. 1\OpenSSL - Copy>openssl.exe
WARNING: can't open config file: C:/OpenSSL/openssl.cnf
OpenSSL> req -new -config root-ca.conf -out ca/root-ca.csr -keyout ca/root-ca/private/root-ca.key
Generating a 4096 bit RSA private key
.....................................................................................................++
.....................................................................++
unable to write 'random state'
writing new private key to 'ca/root-ca/private/root-ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
Verify failure
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
```

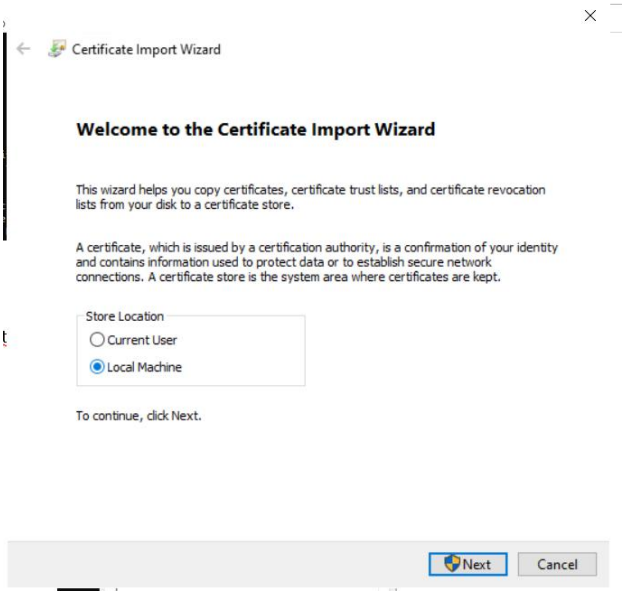
Semnarea certificatul cheii publice cu cheia privată generată la pasul precedent

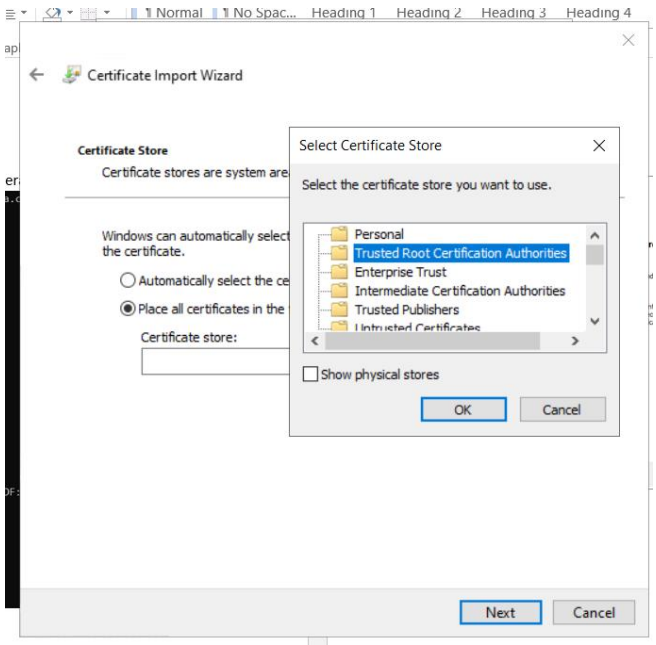
```
OpenSSL> ca -selfsign -config root-ca.conf -in ca/root-ca.csr -out ca/root-ca.crt -extensions root_ca_ext
Using configuration from root-ca.conf
Enter pass phrase for ./ca/root-ca/private/root-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 3 (0x3)
        Validity
            Not Before: Sep 29 10:34:52 2020 GMT
            Not After : Sep 29 10:34:52 2030 GMT
        Subject:
            organizationName          = UTM (0000000000000)
            organizationalUnitName    = UTM Root CA Curs eGov
            commonName                = UTM Root CA
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                BC:CA:CF:89:A9:AF:31:E2:7E:51:BD:4B:3C:86:B7:12:30:80:DF:8D
            X509v3 Authority Key Identifier:
                keyid:BC:CA:CF:89:A9:AF:31:E2:7E:51:BD:4B:3C:86:B7:12:30:80:DF:8D

Certificate is to be certified until Sep 29 10:34:52 2030 GMT (3652 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

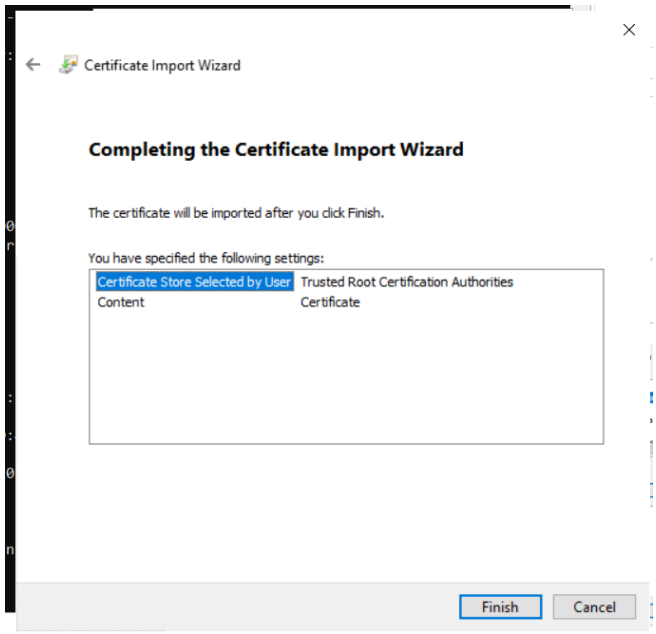
Certificatul

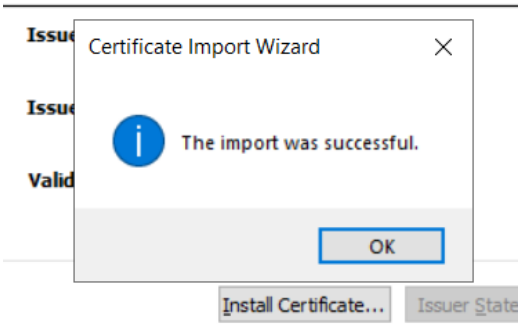


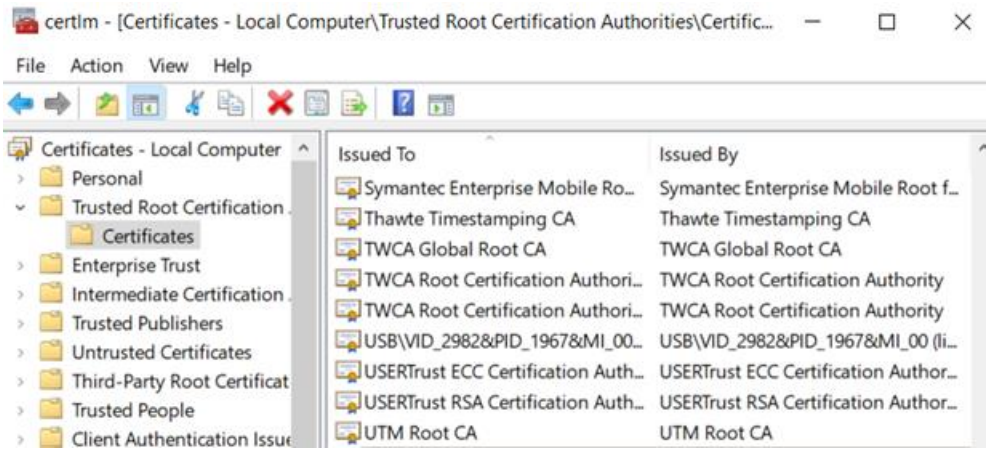
Instalarea certificatului



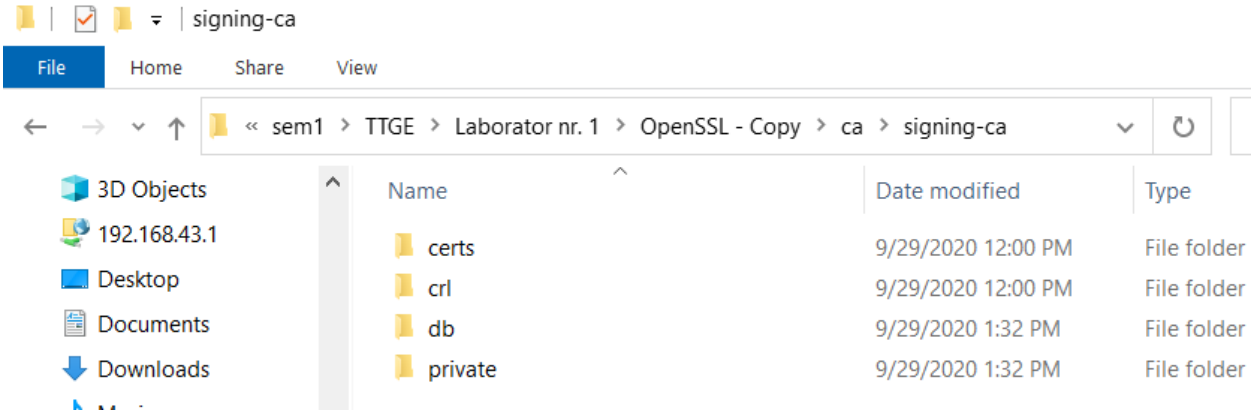



Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certification Authorities
Content
Certificate
Finish
Cancel

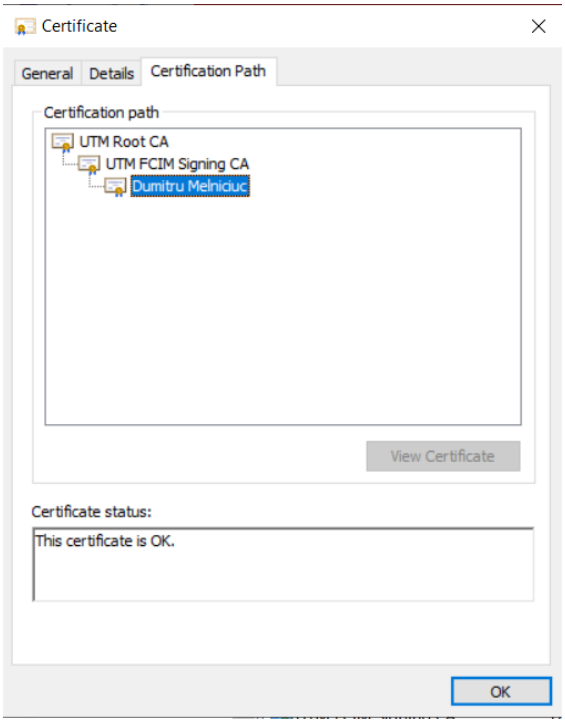

Issue
Issue
Valid
Certificate Import Wizard
The import was successful.
OK
Install Certificate...
Issuer State


certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certific...
File
Action
View
Help
Certificates - Local Computer
Personal
Trusted Root Certification
Certificates
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issue
Issued To
Issued By
Symantec Enterprise Mobile Ro...
Symantec Enterprise Mobile Root f...
Thawte Timestamping CA
Thawte Timestamping CA
TWCA Global Root CA
TWCA Global Root CA
TWCA Root Certification Authori...
TWCA Root Certification Authority
TWCA Root Certification Authori...
TWCA Root Certification Authority
USB\VID_2982&PID_1967&MI_00...
USB\VID_2982&PID_1967&MI_00 (li...
USERTrust ECC Certification Auth...
USERTrust ECC Certification Author...
USERTrust RSA Certification Auth...
USERTrust RSA Certification Author...
UTM Root CA
UTM Root CA

Structura OpenSSL\ca\signing-ca

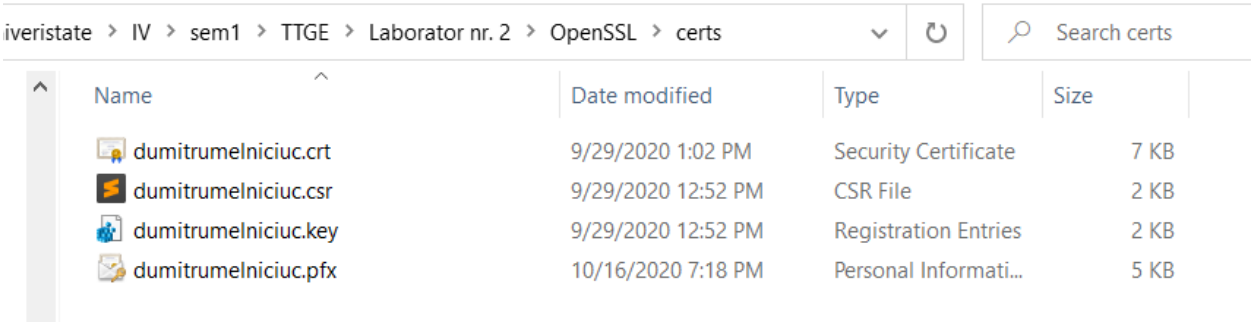


Ierarhia certificatelor

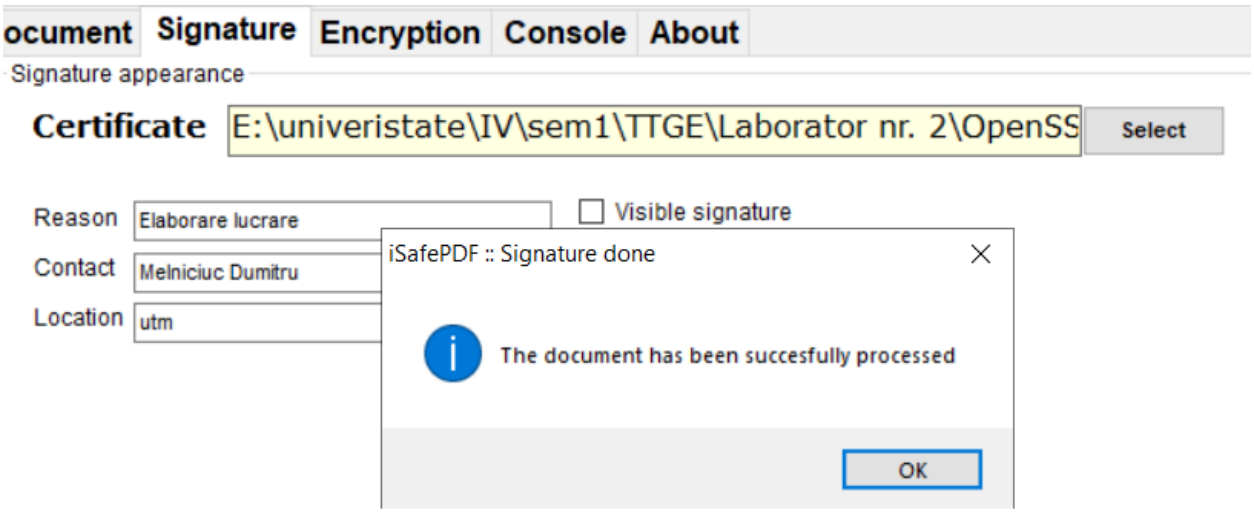


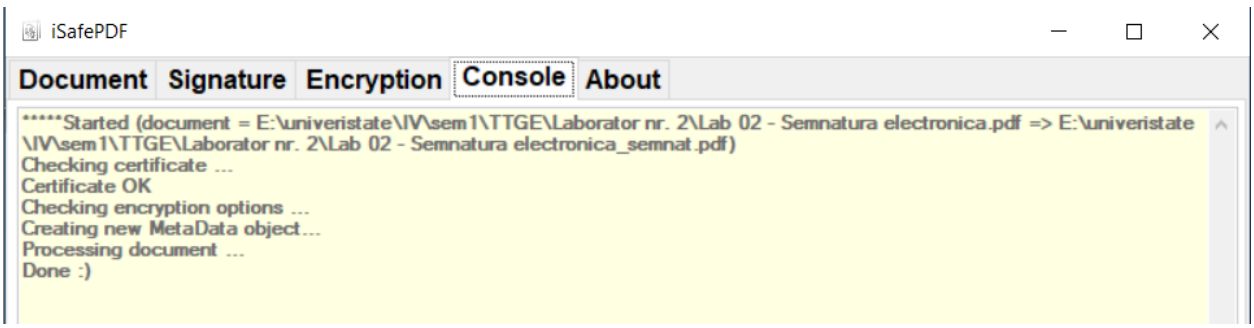
Partea II

Crearea containerului PKCS12



Crearea semnaturii





Deschideți fișierul PDF semnat cu Adobe Acrobat Reader