

Ministerul Educației, 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

Chișinău 2020

The screenshot shows a Windows File Explorer window. The address bar displays the path: `IV > sem1 > TTGE > Laborator nr. 1 > OpenSSL > ca > root-ca`. The left sidebar shows the 'This PC' view with '3D Objects' selected. The main pane shows a list of folders:

Name	Date modified	Type
certs	9/29/2020 12:00 PM	File folder
clr	9/29/2020 9:05 AM	File folder
crl	9/29/2020 12:00 PM	File folder
db	9/29/2020 12:41 PM	File folder
private	9/29/2020 12:11 PM	File folder

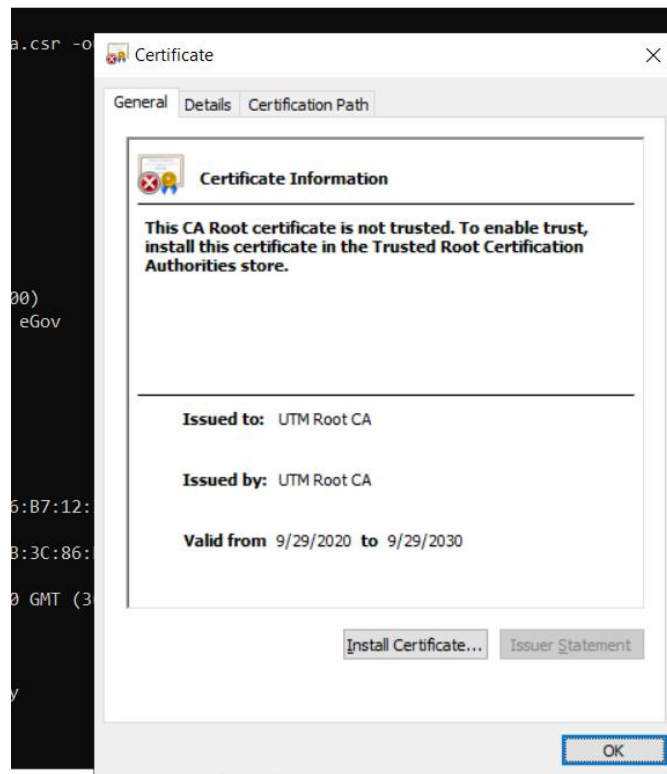
```
E:\univeristate\IV\sem1\TTGE\Laborator nr. 1\OpenSSL - Copy>openssl.exe
WARNING: can't open config file: C:/OpenSSL/openssl.cnf
OpenSSL> req -new -config root-ca.conf -out ca/root-ca.csr -keyout ca/root-ca/private/root-ca.key
Generating a 4096 bit RSA private key
.....++
.....++
unable to write 'random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

```
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 (00000000000000)
        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

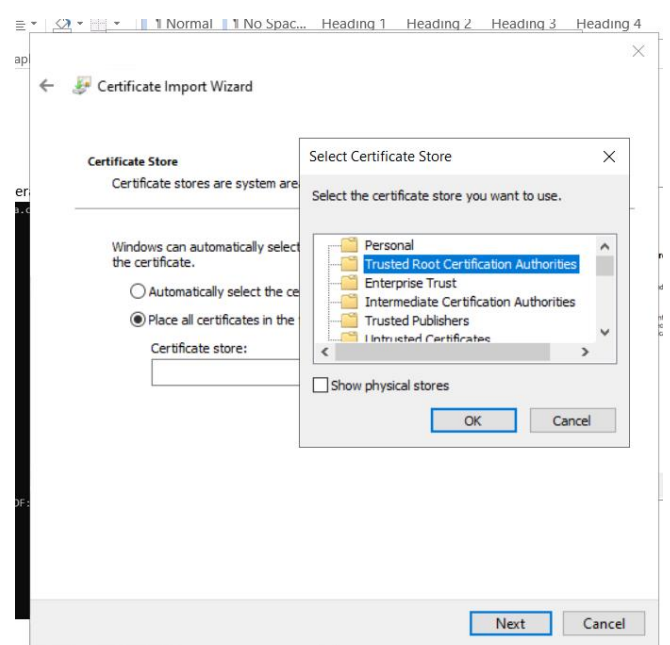
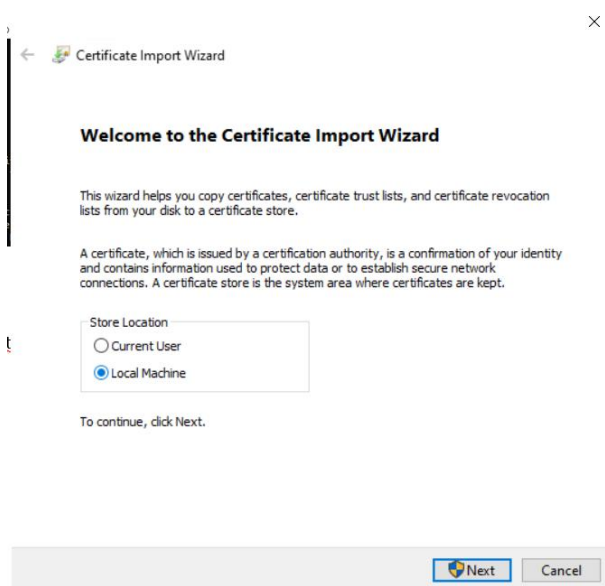
Certificate is to be certified until Sep 29 10:34:52 2030 GMT (3652 days)
Sign the certificate? [y/n]:y

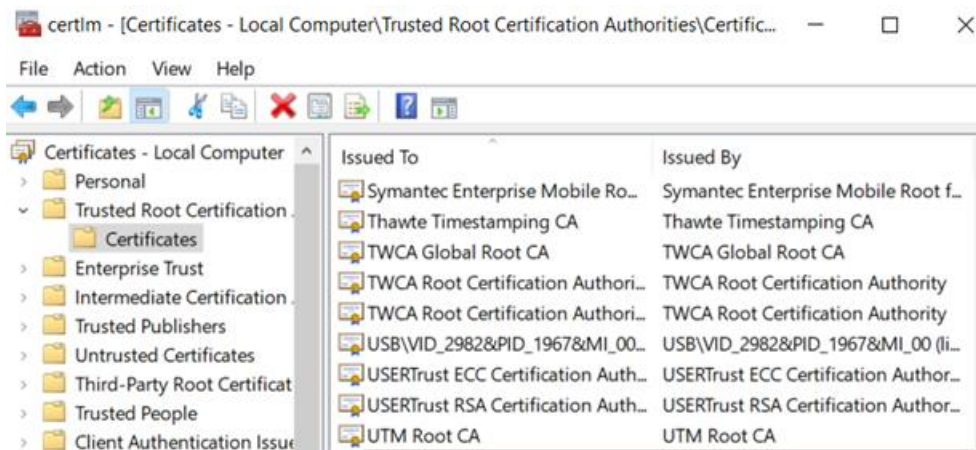
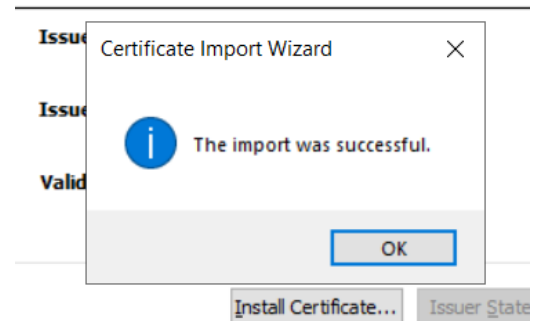
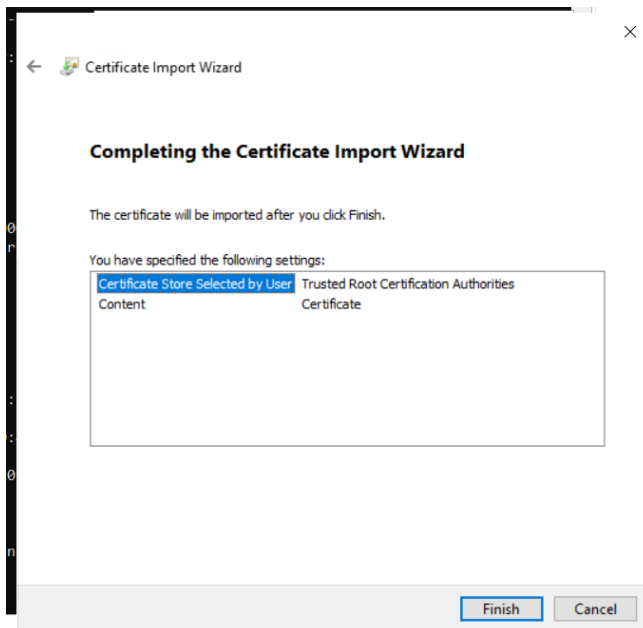
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Certificatul

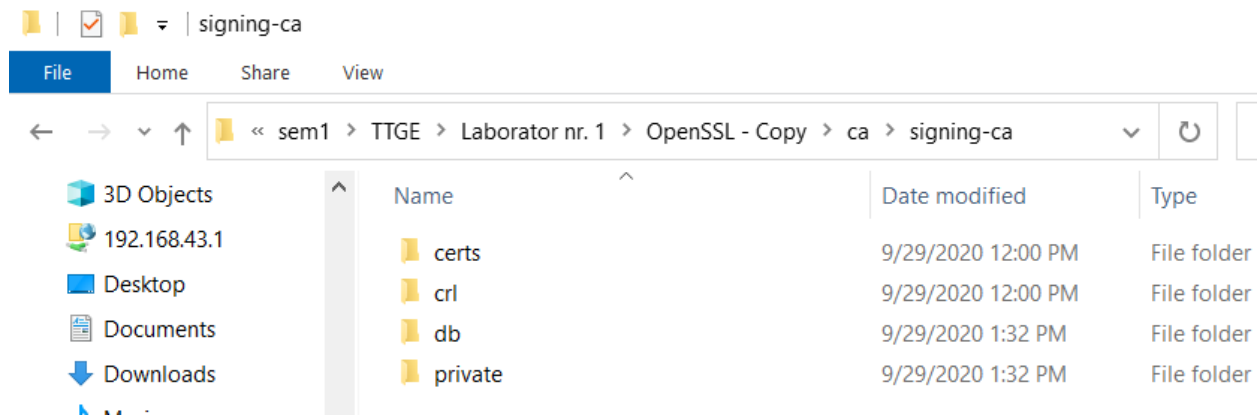


Instalarea certificatului

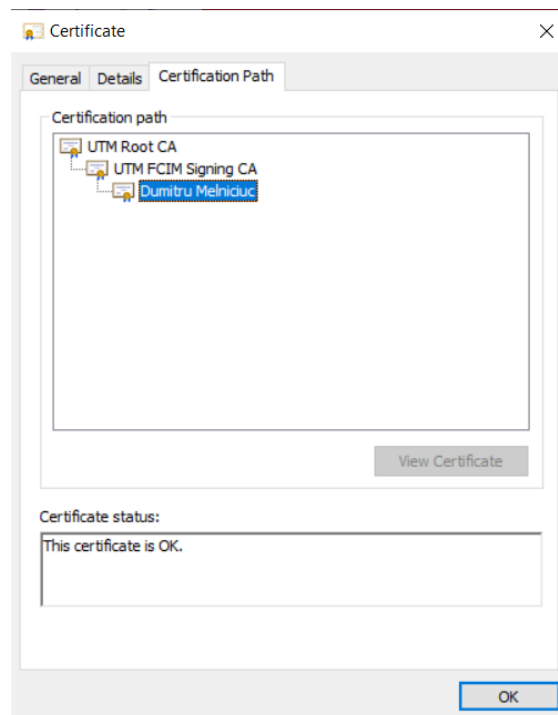




Structura OpenSSL\ca\signing-ca



Ierarhia certificatelor



Partea II

Crearea containerului PKCS12

iveristate > IV > sem1 > TTGE > Laborator nr. 2 > OpenSSL > certs					Search certs
Name	Date modified	Type	Size		
dumitrumelniciuc.crt	9/29/2020 1:02 PM	Security Certificate	7 KB		
dumitrumelniciuc.csr	9/29/2020 12:52 PM	CSR File	2 KB		
dumitrumelniciuc.key	9/29/2020 12:52 PM	Registration Entries	2 KB		
dumitrumelniciuc.pfx	10/16/2020 7:18 PM	Personal Informati...	5 KB		

Crearea semnaturii

Document **Signature** **Encryption** **Console** **About**

Signature appearance

Certificate E:\univeristate\IV\sem1\TTGE\Laborator nr. 2\OpenSS **Select**

Reason: Elaborare lucrare ☐ Visible signature

Contact: Melniciuc Dumitru

Location: utm

iSafePDF :: Signature done

The document has been succesfully processed

OK

iSafePDF

Document **Signature** **Encryption** **Console** **About**

```
*****Started (document = E:\univeristate\IV\sem1\TTGE\Laborator nr. 2\Lab 02 - Semnatura electronica.pdf => E:\univeristate\IV\sem1\TTGE\Laborator nr. 2\Lab 02 - Semnatura electronica_semnat.pdf)
Checking certificate ...
Certificate OK
Checking encryption options ...
Creating new MetaData object...
Processing document ...
Done :)
```

Deschideți fișierul PDF semnat cu Adobe Acrobat Reader

