LUCRAREA DE LABORATOR #2
Semnarea documentelor electronice

Scopul lucrării: Familiarizarea cu semnătura electronică.

Lucrarea de laborator constă în semnarea documentelor electronice utilizând perechea de chei, obținută ca rezultat a efectuării lucrării de laborator nr. 1. În lucrare fiecare student va transmite cererea de certificare profesorului pentru a obține certificatul cheii publice. Utilizând cheia privată și certificatul cheii publice studenții vor genera un container de formatul PCKS12 pentru a putea ulterior semna documente PDF.

În cadrul lucrării se vor utiliza următoarele instrumente, inclusiv structura de mape din lucrarea de laborator precedentă:

1. OpenSSL – se descarcă și se utilizează conform instrucțiunilor de laborator nr. 1;
2. Adobe Acrobat Reader – aplicație distribuită gratuit de compania Adobe; se descarcă de pe adresa https://get.adobe.com/reader/;
3. iSafePDF – aplicație de tip desktop cu surse deschise în .Net; poate fi descărcată de pe adresa http://isafepdf.eurekaa.org/download-isafepdf/.

Indicații de laborator

1. Certificarea cheii publice individuale
   1.1. Transmiteți profesorului cererea de certificare individuală, creată în cadrul lucrării de laborator nr. 1 – fișierul **dumitrumelniciuc.csr** pentru a certifica cheia publică.
   1.2. Obțineți de la profesor certificatul cheii publice – fișierul **dumitrumelniciuc.crt**. De asemenea obțineți de la profesor certificatul cheii publice al autorității de certificare de nivel superior (**root-ca.crt**) și al celei intermediare (**signing-ca.crt**). La necesitate, înlocuiți fișierele vechi **root-ca.crt** și **signing-ca.crt** cu cele obținute de la profesor.

2. Crearea containerului PKCS12
   2.1. Utilizând cheia privată individuală și certificatul cheii publice, creați containerul PKCS12 – fișierul **dumitrumelniciuc.pfx**. În acest scop utilizați instrumentul OpenSSL și următoarea instrucțiune:

```
openssl pkcs12 -export -out certs/dumitrumelniciuc.pfx -inkey
certs/dumitrumelniciuc.key -in certs/dumitrumelniciuc.crt -certfile
ca/signing-ca.crt
```

   În rezultat, în mapa **certs** va fi creat fișierul **dumitrumelniciuc.pfx**, care reprezintă un container PKCS12 ce conține cheia privată individuală, certificatul cheii publice individual, precum și certificatul cheii publice al autorității de certificare intermediare.
   Fișierul **dumitrumelniciuc.pfx** conține cheia privată individuală, respectiv acesta trebuie păstrat în mod securizat și nu poate fi distribuit public.
   Întrucât fișierul **dumitrumelniciuc.pfx** conține cheia privată, acesta poate fi filosit la semnarea documentelor electronice.

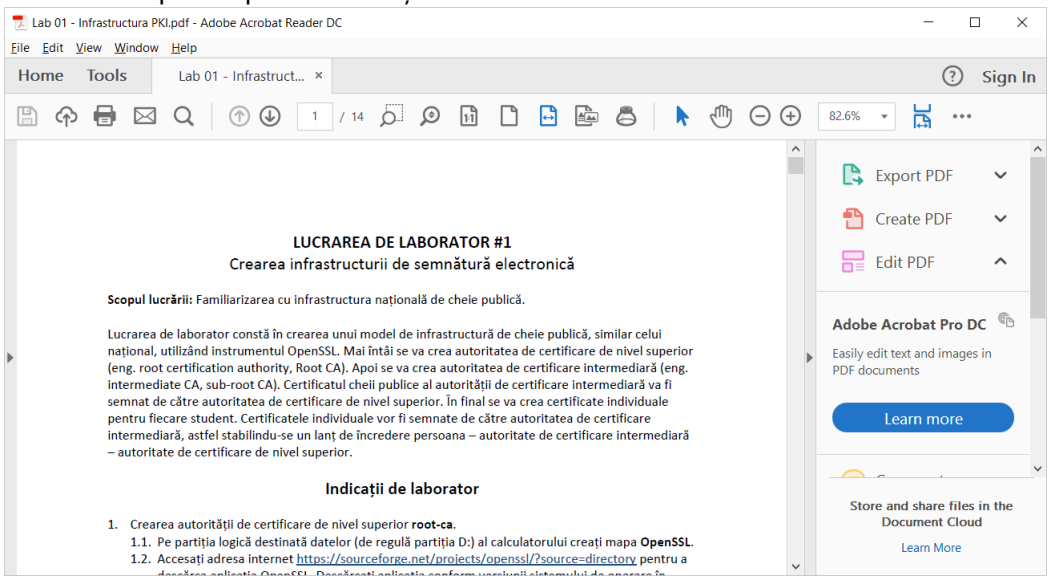
3. Aplicarea semnăturii electronice pe un document electronic de format PDF.

3.1. Descărcați și despachetați aplicația iSafePDF de pe adresa indicată mai sus. Se recomandă copierea aplicației în mapa lucrării de laborator.

3.2. Creați nota explicativă a lucrării de laborator nr. 1 și salvați fișierul în format PDF. Există mai multe procedee cum poate fi obținut fișierul PDF. Microsoft Word 2016 are opțiunea directă de a salva fișierele *.doc în format PDF.
Formatul PDF (Portable Document Format) este larg răspândit și este utilizat pentru a transporta documente finisate utilizatorilor finali ai acestora.

3.3. Verificați dacă pe calculator este instalată aplicația Adobe Acrobat Reader pentru a putea deschide fișiere de format PDF. Daca această aplicație nu există, descărcați-o de pe adresa indicată mai sus și instalați-o pe calculator.

3.4. Deschideți fișierul PDF creat în aplicația Adobe Acrobat Reader și observați lipsa de semnături electronice aplicate peste acest fișier.



3.5. Deschideți aplicația iSafePDF. Această aplicație are câteva pagini – **Document**, **Signature**, **Encryption**, **Console**, **About**.

3.6. Pe pagina **Document** în câmpul **Source file** selectați **Browse** pentru a indica la fișierul PDF pentru a fi semnat.

3.7. Copiați conținutul din câmpul **Source file** în câmpul **Target file** și modificați denumirea fișierului adăugând sufixul „**_semnat”**. Astfel, fișierul semnat se va genera în aceeași locație ca și fișierul PDF inițial.

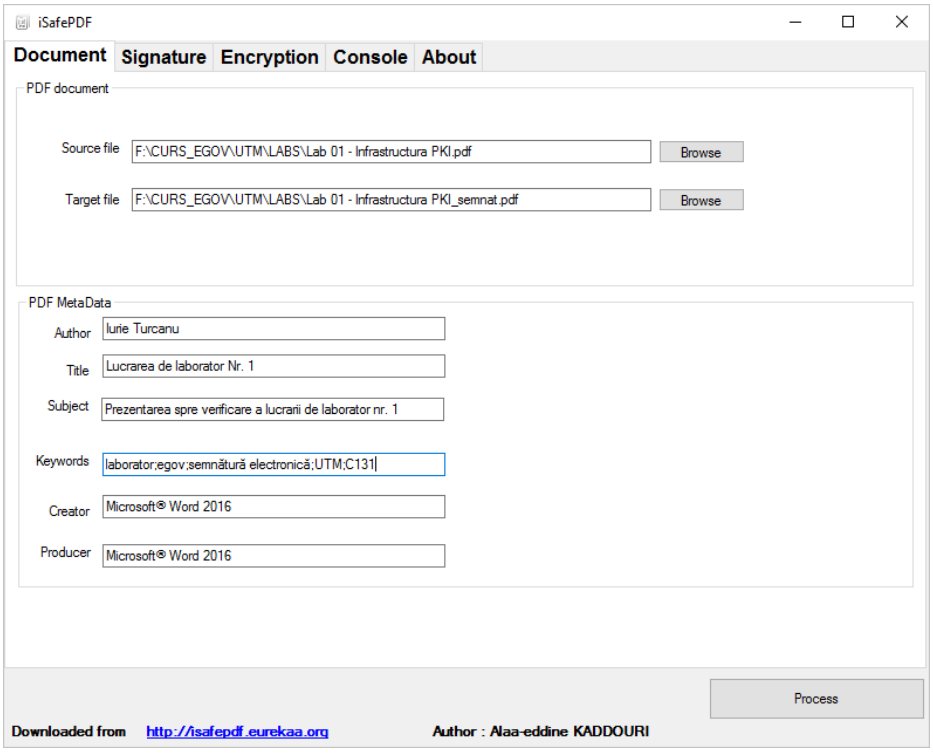
3.8. Completați grupul de câmpuri PDF MetaData după cum urmează:

3.8.1.**Author**: numele prenumele studentului

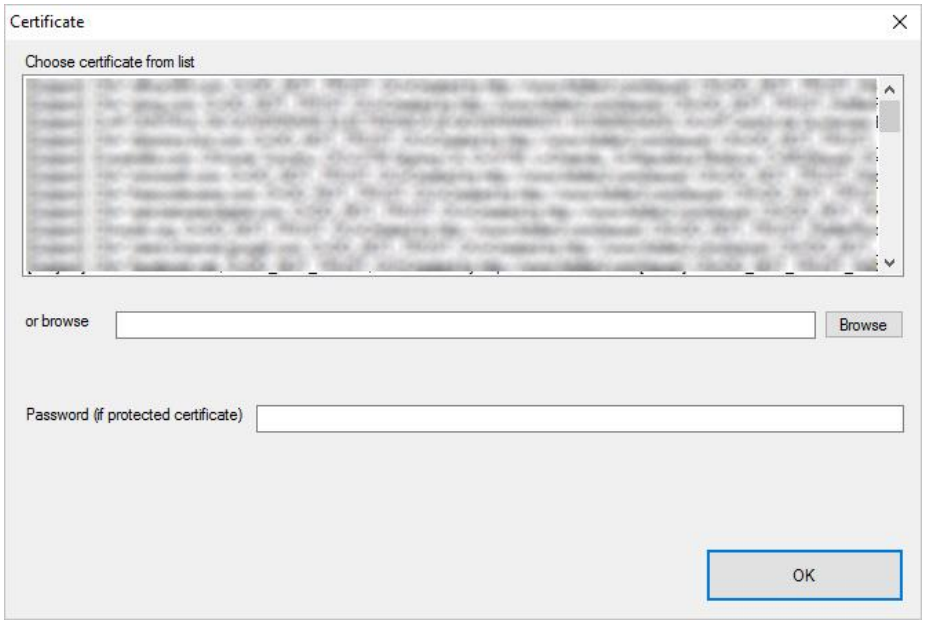
3.8.2.**Title**: Lucrarea de laborator nr. 1

3.8.3.**Subject**: Prezentarea spre verificare a lucrării de laborator nr. 1

3.8.4.**Keywords**: laborator; semnătură electronică;UTM;[grupa]

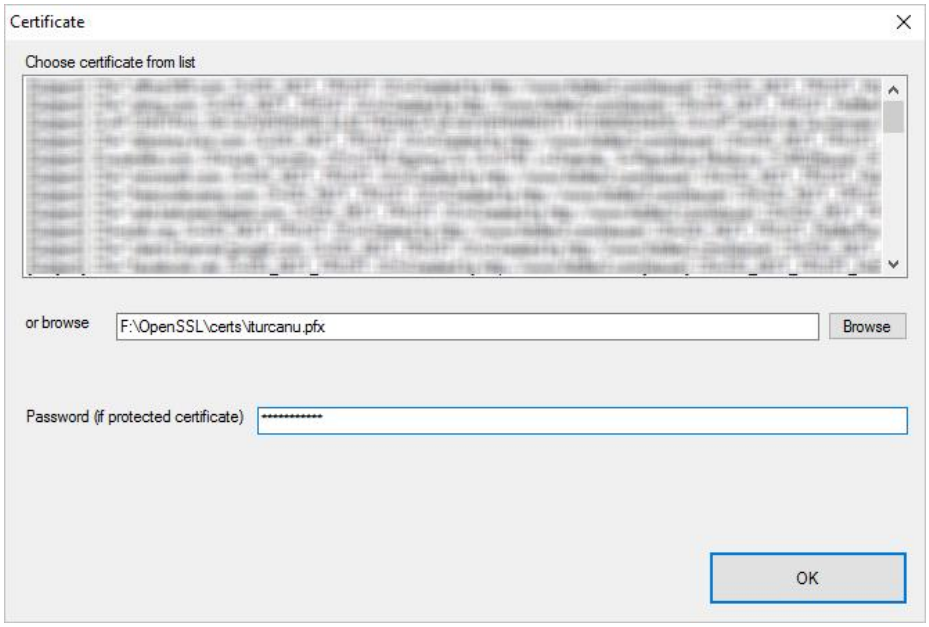


3.9. Pe pagina Signature În câmpul Certificate, prin apăsarea butonului Select selectați fișierul pfx cu care veți semna fișierul PDF selectat – **dumitrumelniciuc.pfx**. Va apărea un dialog pentru selectarea certificatului.



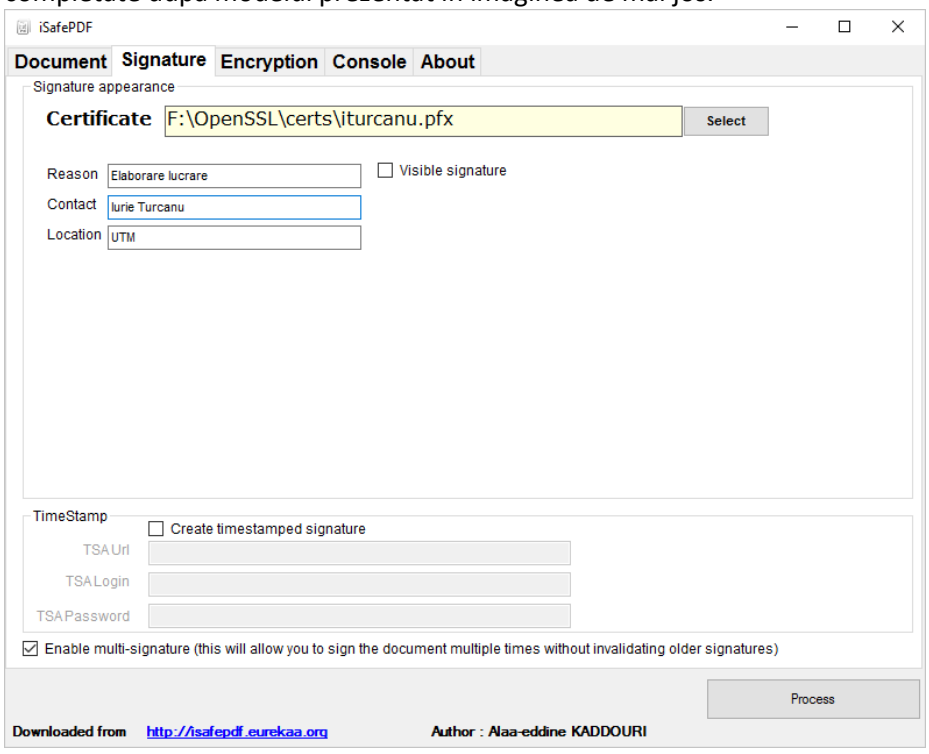
3.10. În acest dialog putem selecta un certificat dintr-o listă de certificate înregistrate în repozitoriu de certificate al sistemului de operare sau putem alege unul explicit, indicând la fișierul pfx. În această lucrare vom alege fișierul pfx individual. Apăsați butonul **Browse** pentru a alege fișierul **dumitrumelniciuc.pfx** individual.

3.11. În câmpul **Password** culegeți parola cheii private din fișierul pfx selectat.

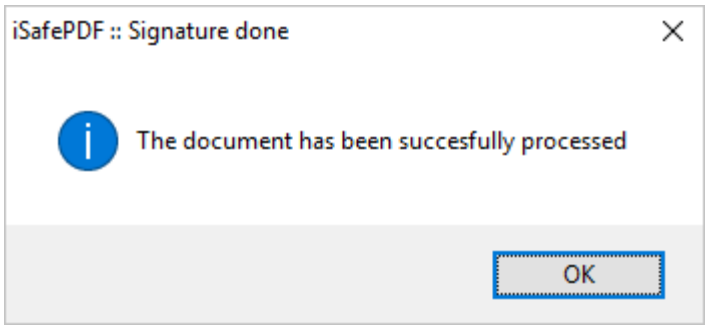


3.12. Apăsați **OK** pentru a continua.

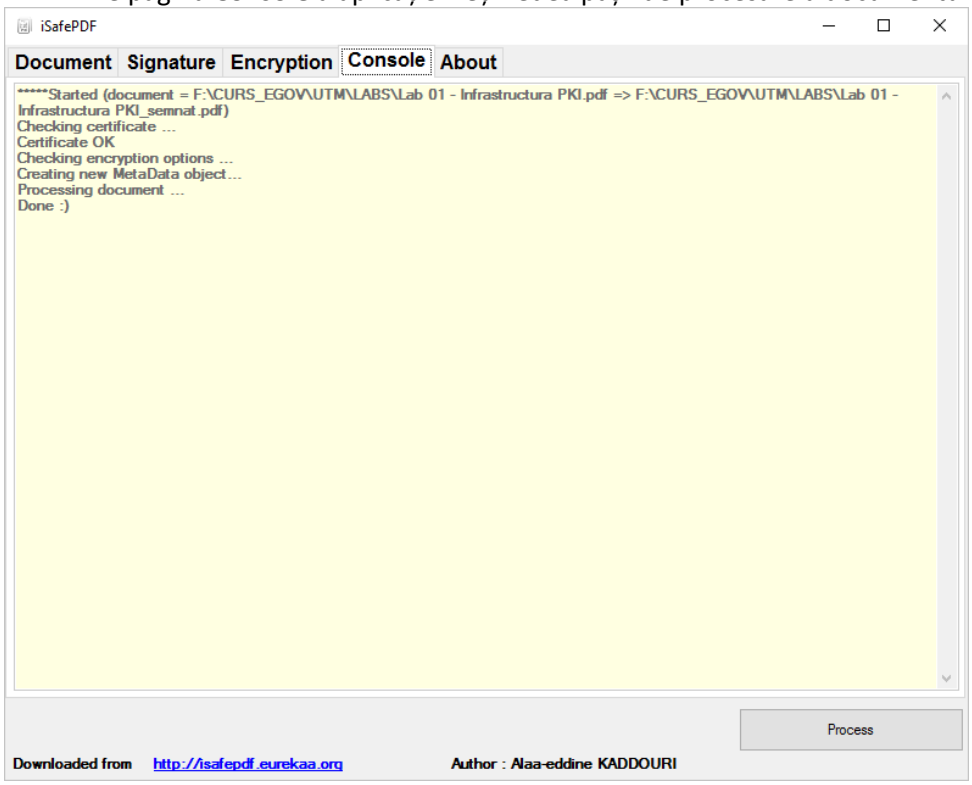
3.13. Odată selectat certificatul, pe pagina **Certificate** au apărut câteva câmpuri care trebuie completate după modelul prezentat în imaginea de mai jos.



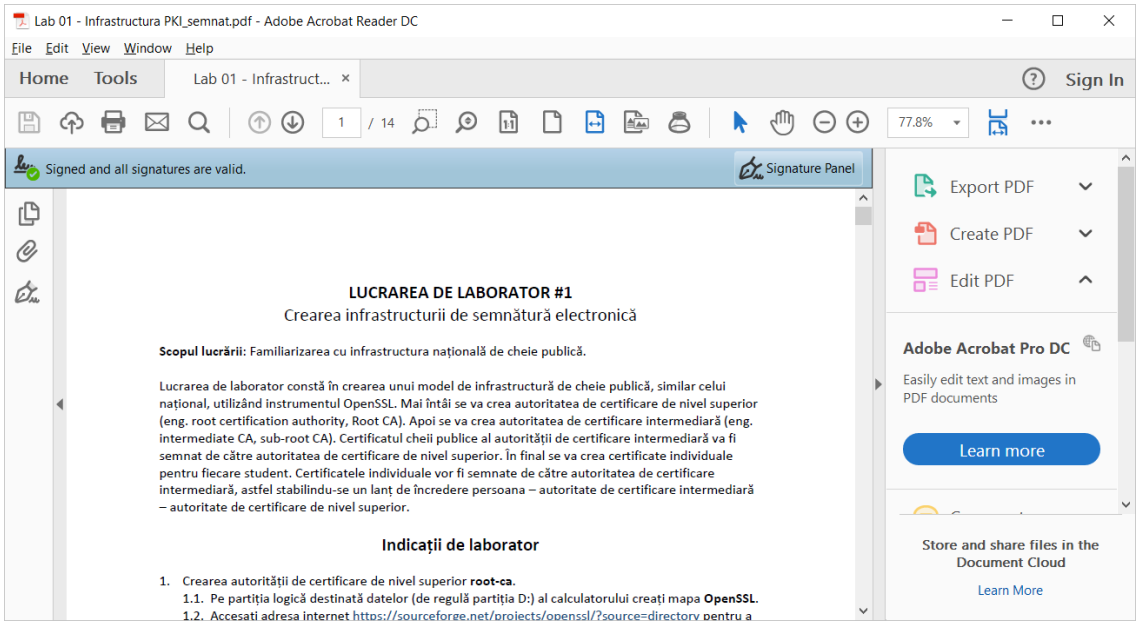
3.14. Apăsați butonul **Process** pentru a semna. Dacă semnarea a avut loc cu succes, va apărea un dialog de confirmare cu un mesaj confirmativ. Apăsați **OK**.



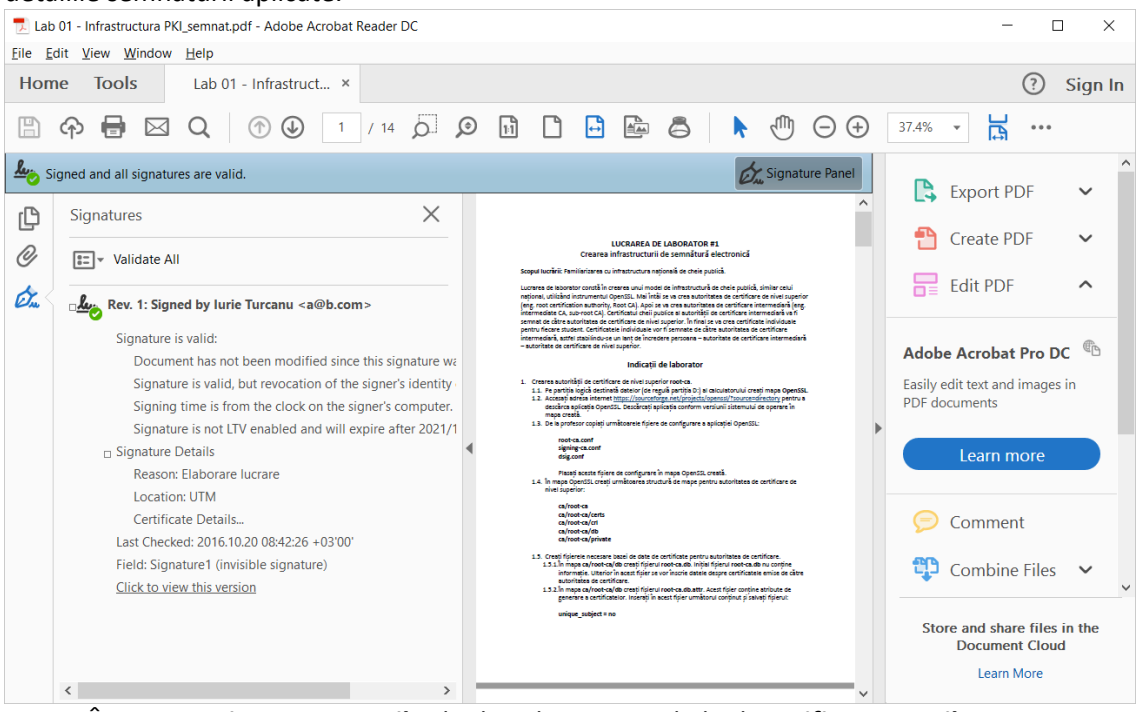
3.15. Pe pagina **Console** a aplicației veți vedea pașii de procesare a documentului.



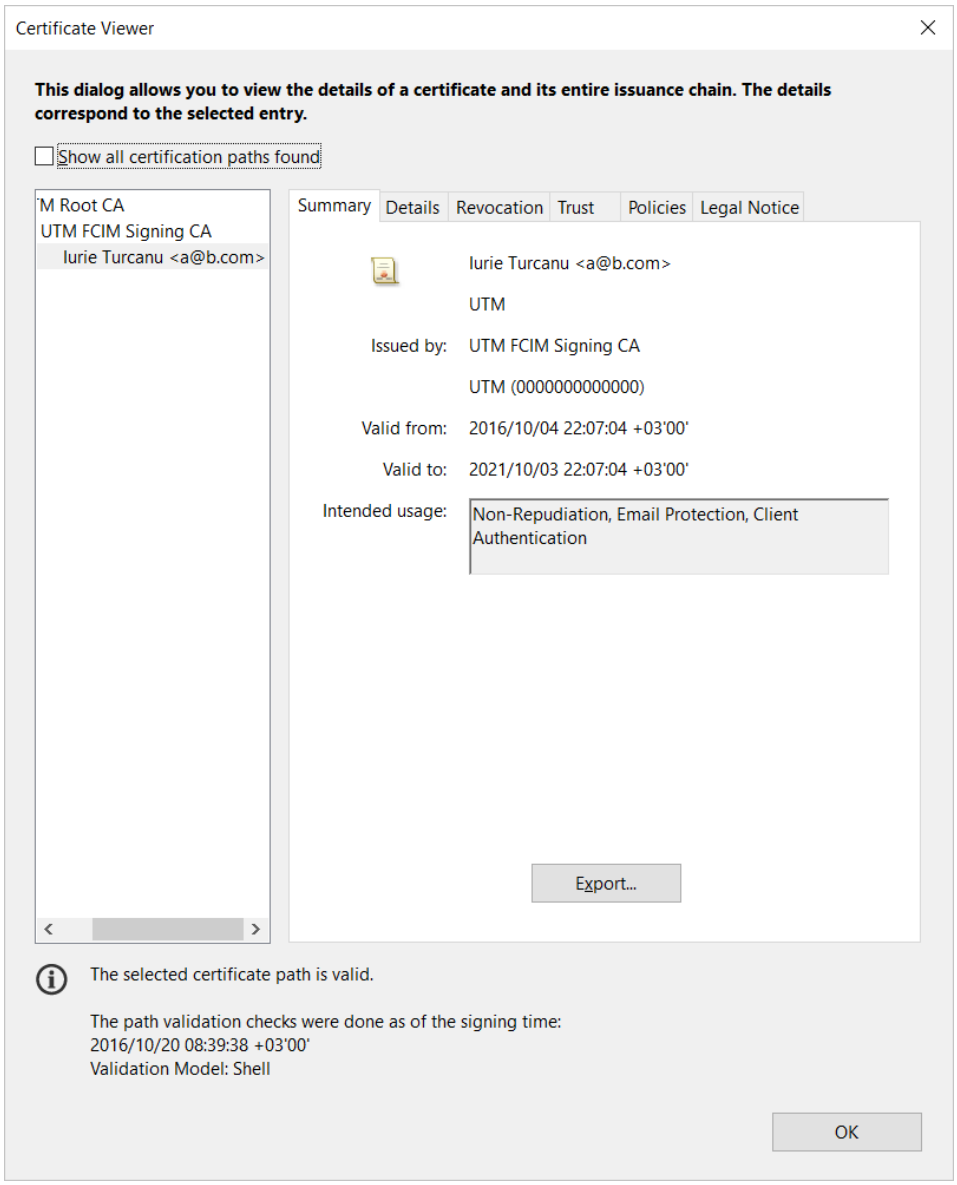
3.16. Deschideți fișierul PDF semnat cu Adobe Acrobat Reader. Observați indicația despre semnăturile electronice în partea de sus a documentului. Apăsați butonul **Signature Panel** pentru a vedea detalii privind documentul semnat.



3.17. În panoul **Signatures** expandați nodurile arborelui de semnături pentru a observa detaliile semnăturii aplicate.



3.18. În ramura **Signature Details** al arborelui accesați link-ul **Certificate Details** pentru a observa detaliile certificatului utilizat la semnare.



În rezultatul efectuării lucrării documentul PDF a fost semnat cu succes cu cheia privată individuală a studentului.

4. Transmiterea notei explicative semnate profesorului
   4.1. Transmiteți profesorului pentru verificare și aprobare nota explicativă a lucrării de laborator nr. 1 semnată electronic în conformitate cu instrucțiunile de laborator din prezenta lucrare.
5. Pregătiți nota explicativă a prezentei lucrări cu concluziile și constatările de rigoare. Semnați nota explicativă urmând pașii de mai sus și transiteți-o profesorului pentru verificare și aprobare.

RESURSE:

1. https://www.openssl.org/
2. https://www.sslshopper.com/article-most-common-openssl-commands.html
3. http://www.oid-info.com/cgi-bin/display?oid=1.2.498.3&action=display

4. http://isafepdf.eurekaa.org/download-isafepdf/
5. https://get.adobe.com/reader/