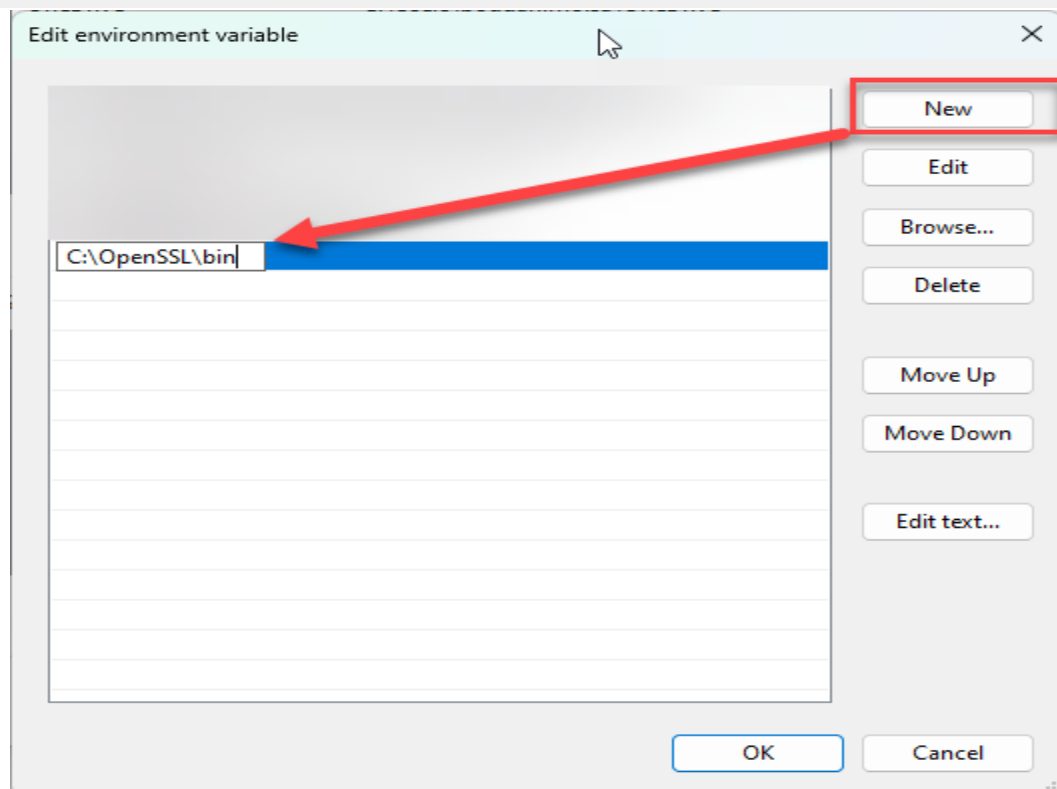
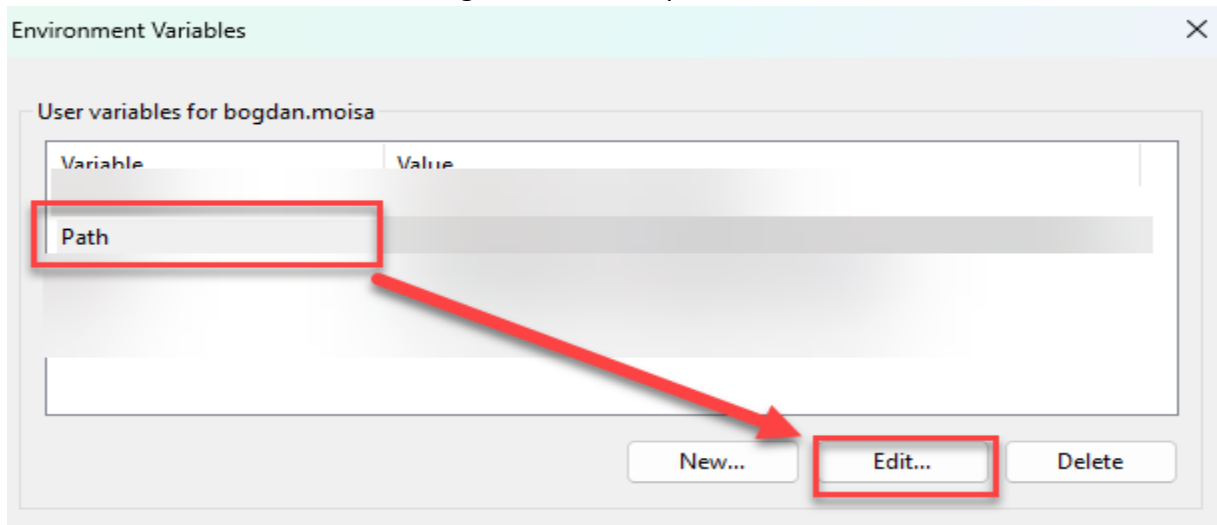


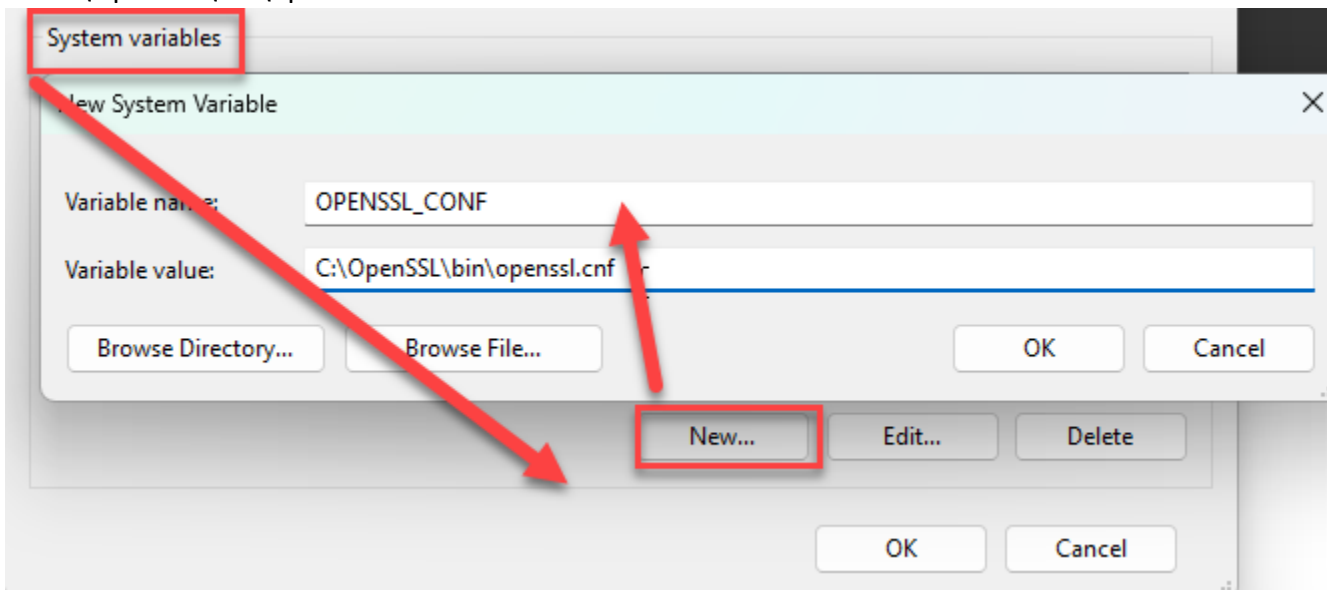
Obtinere fisier certificat pentru transmitere apeluri HTTPS prin RestServer

Pentru persoanele care doresc sa foloseasca protocolul HTTPS si nu au un certificat web generat de o autoritate, pot sa-si genereze un certificate self-sign urmand pasii descrisi aici.

1. Se downloadeza OpenSSL de la adresa: <https://sourceforge.net/projects/openssl/files/>
Continutul arhivei se muta in C:\OpenSSL, iar in Enviroment Variables se fac urmatoarele setari:
 - a. la **User variables for ...** se adauga in PATH C:\OpenSSL\bin



- b. In **System variables** se adauga variabila **OPENSSL_CONF** cu calea **C:\OpenSSL\bin\openssl.cnf**

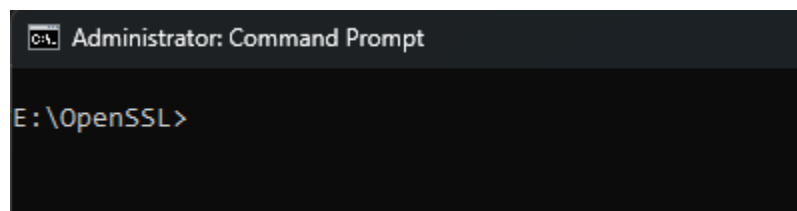


Dupa aceste setari se va da **restart la computer**.

2. Dupa repornirea sistemului, pentru a verifica daca avem instalat OpenSSL si nu avem probleme deschidem un **Command Prompt** cu drept de administrator si rulam:
openssl version
3. In procesul de generare a certificatului se vor genera 2 fisiere (.Cer si .key) care vor fi utilizate ulterior la configurarea RestServer.

a. Generare fisier **key**

Inainte de a rula comanda pentru a genera fisierul trebuie sa setam folderul in care se va salva acesta. Pentru a face acest lucru, inainte de a rula comanda pentru generarea fisierului, trebuie selectata calea in care va fi exportat fisierul (In cazul meu E:\OpenSSL):



Dupa ce am selectat calea in care dorim sa fie exportat fisierul se ruleaza comanda:

openssl genrsa -des3 -out firma.ro.key 2024

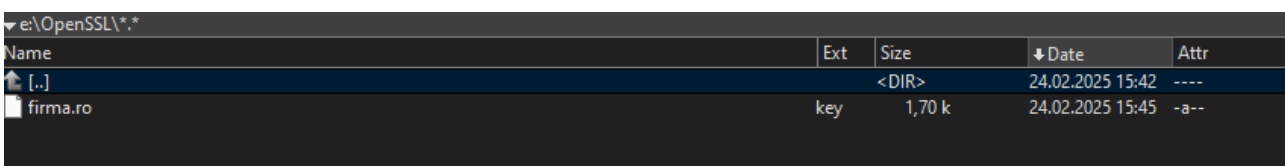
!!! Atentie: firma.ro este denumirea pe care doriti sa o acordati certificatului.

```
Administrator: Command Prompt - openssl genrsa -des3 -out firma.ro.key 2024

E:\OpenSSL>openssl genrsa -des3 -out firma.ro.key 2024
Generating RSA private key, 2024 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for firma.ro.key:
```

Dupa executare se vor primi mesaje **Enter pass phrase for firma.ro.key:** si **Verifying - Enter pass phrase for firma.ro.key:** in care trebuie introdusa si confirmata parola fisierului.

In urma acestui pas se va genera fisierul firma.ro.key in locatia selectata.



Name	Ext	Size	Date	Attr
[..]	<DIR>		24.02.2025 15:42	----
firma.ro	key	1,70 k	24.02.2025 15:45	-a--

b. Generare fisier csr

Pentru a genera fisierul csr se vor urma pasii de mai sus, ruland comanda: **openssl req -key firma.ro.key -new -out firma.ro.csr**

```
Administrator: Command Prompt

E:\OpenSSL>openssl genrsa -des3 -out firma.ro.key 2024
Generating RSA private key, 2024 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for firma.ro.key:
Verifying - Enter pass phrase for firma.ro.key:

E:\OpenSSL>openssl req -key firma.ro.key -new -out firma.ro.csr
Enter pass phrase for firma.ro.key:
Can't load ./rnd into RNG
18448:error:2406F079:random number generator:RAND_load_file:Cannot open file:crypto/rand/randfile.c:98:Filename=./rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RO
State or Province Name (full name) [Some-State]:Iasi
Locality Name (eg, city) []:Iasi
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

E:\OpenSSL>
```

La final va genera fisierul firma.ro.csr

c. Fisierele crt

Rulam urmatoarea comanda pentru generarea fisierului crt: ***openssl x509 -signkey firma.ro.key -in firma.ro.csr -req -days 3650 -out firma.ro.crt***

```
E:\OpenSSL>openssl x509 -signkey firma.ro.key -in firma.ro.csr -req -days 3650 -out firma.ro.crt
Signature ok
subject=C = RO, ST = Iasi, L = Iasi, O = XXX
Getting Private key
Enter pass phrase for firma.ro.key:
```

Dupa validarea parolei introdusa la fisierul .key se va genera fisierul .crt.

La final va genera fisierul firma.ro.crt care impreuna cu firma.ro.key va fi configurat in RestServer.

