

WME - Obținere fișiere certificat pentru transmitere apeluri HTTPS prin RestServer

Pentru persoanele care doresc să folosească protocolul HTTPS și nu au un *certificat web* generat de o autoritate, pot să-și genereze un certificate *self-sign*, urmând pașii descriși aici.

1. Se downloadează OpenSSL de la adresa: <https://sourceforge.net/projects/openssl/files/>

Conținutul arhivei se mută în C:\OpenSSL, iar în Environment Variables se fac următoarele setări:

- a. la **User variables for ...** se adaugă în PATH C:\OpenSSL\bin

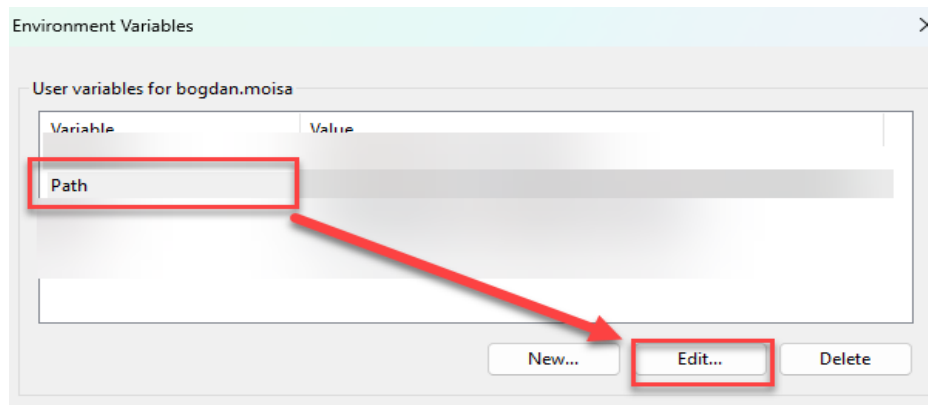


Figura 1

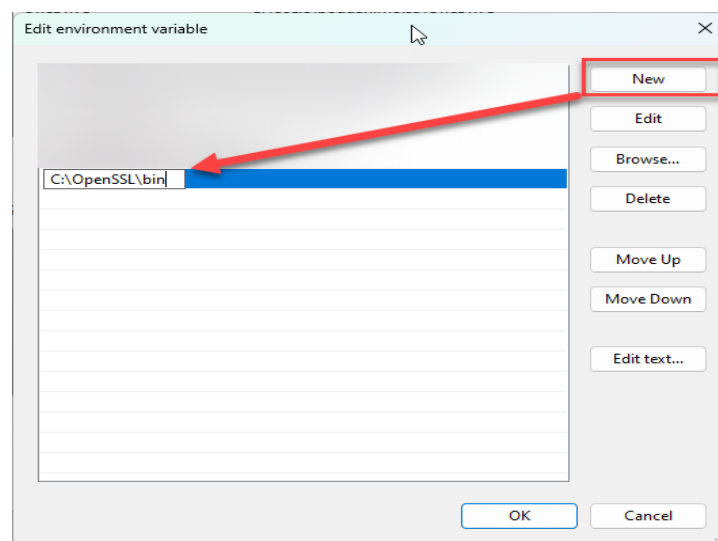


Figura 2

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

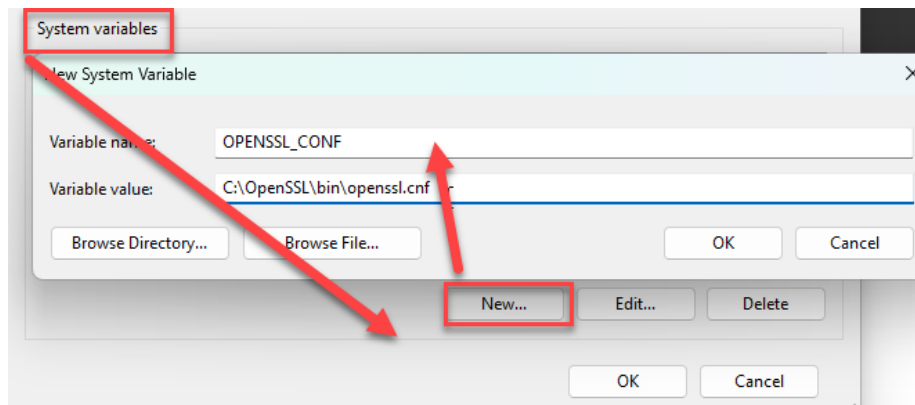


Figura 3

După aceste setări, se va da **restart la computer**.

2. După repornirea sistemului, pentru a verifica dacă avem instalat OpenSSL și nu avem probleme deschidem un **Command Prompt** cu drept de administrator și rulăm **openssl version**.

3. În procesul de generare a certificatului se vor genera 2 fișiere (.Cer și .key) care vor fi utilizate ulterior la configurarea RestServer.

a. Generare fișier **key**

Înainte de a rula comanda pentru a genera fișierul trebuie să setăm folderul în care se va salva acesta. Pentru a face acest lucru, înainte de a rula comanda pentru generarea fișierului, trebuie selectată calea în care va fi exportat fișierul (În cazul nostru, E:\OpenSSL):

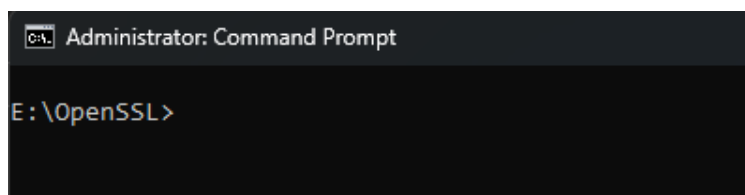


Figura 4

După ce am selectat calea în care dorim să fie exportat fișierul, se rulează comanda: **openssl genrsa -des3 -out firma.ro.key 2024**

!!! Atenție: firma.ro este denumirea pe care doriți să o acordați 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:
```

Figura 5

După executare, se vor primi mesajele **Enter pass phrase for firma.ro.key:** și **Verifying - Enter pass phrase for firma.ro.key:** în care trebuie introdusă și confirmată parola fișierului.

În urma acestui pas se va genera fișierul firma.ro.key în locația selectată.

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

Figura 6

b. Generare fișier csr

Pentru a genera fișierul csr se vor urma pașii de mai sus, rulând 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
130443:error:2400F079: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>
```

Figura 7

La final, va genera fișierul firma.ro.csr

c. Fișierul crt

Rulăm următoarea comandă pentru generarea fișierului 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:
```

Figura 8

După validarea parolei introdusă la fișierul .key se va genera fișierul .crt.

La final, se va genera fișierul firma.ro.crt care împreună cu firma.ro.key va fi configurat în RestServer.

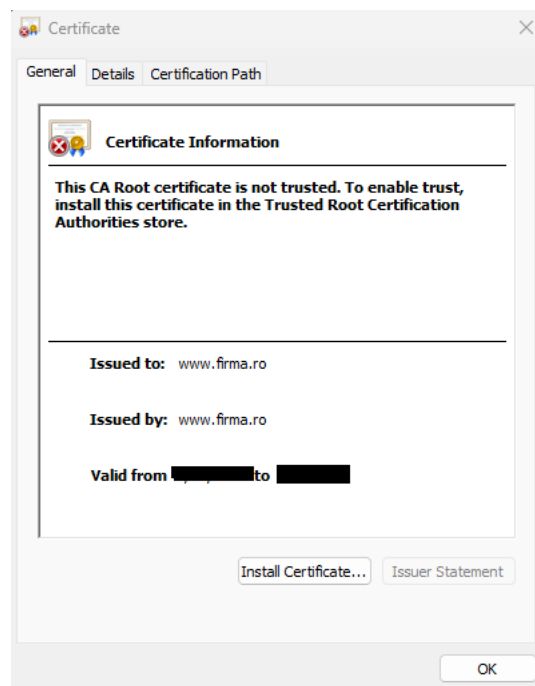


Figura 9

Review-uri document

Rev. 1.0	25.02.2025	Creare document
Rev. 1.1	06.05.2026	Actualizare template