Instruction —

CSR Generation

Generating CSR file using the OpenSSL tool

version 1.2

Table of contents

1. Contents of the instructions manual

This instructions manual is designed to help generate the CSR file (certificate request file) needed to purchase and issue certificates:

- SSL,
- E-mail ID,
- Code Signing,
- Krajowy Węzeł (Eng. National Node).

This instructions manual presents the process of generating a CSR using OpenSSL tool, which is the world's most widely used implementation of the Transport Layer Security (TLS) protocol. Users around the world use this tool to carry out tasks such as creating Certificate Signing Requests (CSRs). This step will be discussed in this manual.

Recommendation: Remember to never delete the generated certificate files and try to keep them all in one folder.

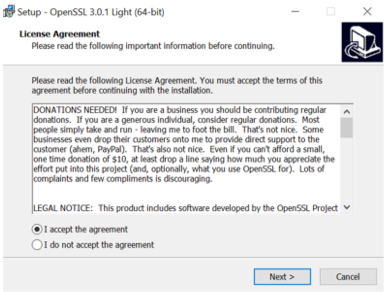
2. Installing the OpenSSL tool

a) Download the OpenSSL tool from https://slproweb.com/products/Win32OpenSSL.html. Select the appropriate installation file that is compatible with the operating system on which you are planning to carry out the process.

Note: We suggest using the recommended files by the OpenSSL team. Products recommended and created by OpenSSL developers feature the following comment in their description: (Recommended for users by the creators of OpenSSL)

b) Install the software according to the steps below:

- Accept the terms and conditions
- Select the storage location (We recommend that you keep the default value)
- Select a folder name (We recommend to keep the default value)



Setup - OpenSSL 3.0.1 Light (64-bit)

License Agreement

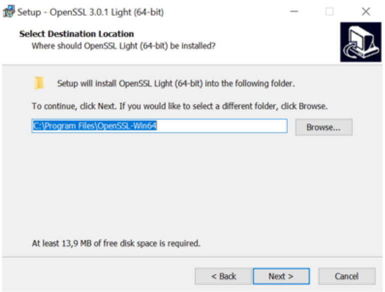
Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

DONATIONS NEEDED! If you are a business you should be contributing regular donations. If you are a generous individual, consider regular donations. Most people simply take and run - leaving me to foot the bill. That's not nice. Some businesses even drop their customers onto me to provide direct support to the customer (ahem, PayPal). That's also not nice. Even if you can't afford a small, one time donation of $10, at least drop a line saying how much you appreciate the effort put into this project (and, optionally, what you use OpenSSL for). Lots of complaints and few compliments is discouraging.

LEGAL NOTICE: This product includes software developed by the OpenSSL Project

● I accept the agreement
○ I do not accept the agreement



Setup - OpenSSL 3.0.1 Light (64-bit)

Select Destination Location

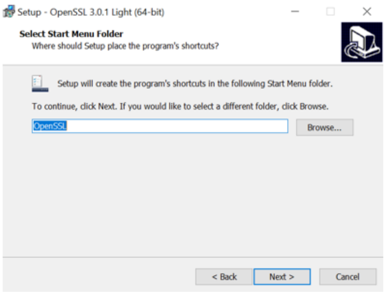
Where should OpenSSL Light (64-bit) be installed?

Setup will install OpenSSL Light (64-bit) into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\OpenSSL-Win64

At least 13,9 MB of free disk space is required.



Setup - OpenSSL 3.0.1 Light (64-bit)

Select Start Menu Folder

Where should Setup place the program's shortcuts?

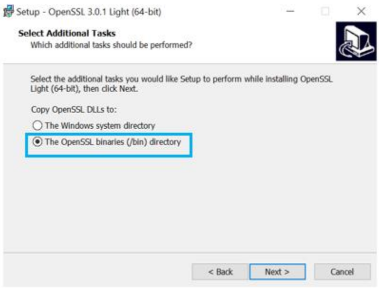
Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

OpenSSL

- Choose the method of running the program (We recommend the OpenSSL binaries)
- Install the program by clicking Install

- If you wish to make donations, please select the option you want. Click Finish to complete the installation.



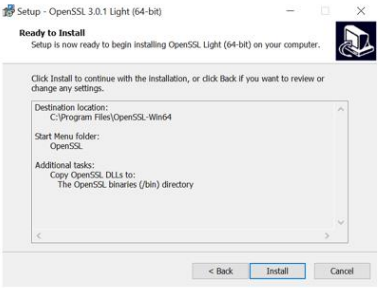
Setup - OpenSSL 3.0.1 Light (64-bit)

Select Additional Tasks
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing OpenSSL Light (64-bit), then click Next.

Copy OpenSSL DLLs to:

○ The Windows system directory
● The OpenSSL binaries (/bin) directory



Setup - OpenSSL 3.0.1 Light (64-bit)

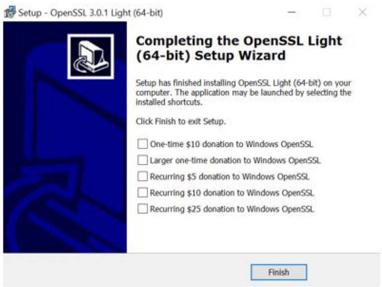
Ready to Install
Setup is now ready to begin installing OpenSSL Light (64-bit) on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files\OpenSSL-Win64

Start Menu folder:
OpenSSL

Additional tasks:
Copy OpenSSL DLLs to:
The OpenSSL binaries (/bin) directory



Setup - OpenSSL 3.0.1 Light (64-bit)

Completing the OpenSSL Light (64-bit) Setup Wizard

Setup has finished installing OpenSSL Light (64-bit) on your computer. The application may be launched by selecting the installed shortcuts.

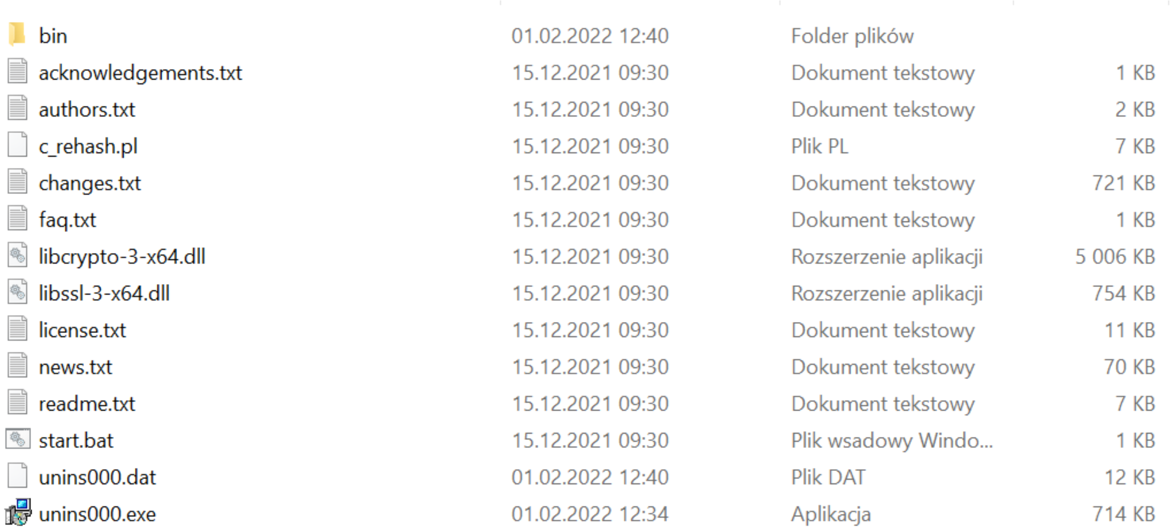
Click Finish to exit Setup.

□ One-time $10 donation to Windows OpenSSL
□ Larger one-time donation to Windows OpenSSL
□ Recurring $5 donation to Windows OpenSSL
□ Recurring $10 donation to Windows OpenSSL
□ Recurring $25 donation to Windows OpenSSL

3. Running OpenSSL

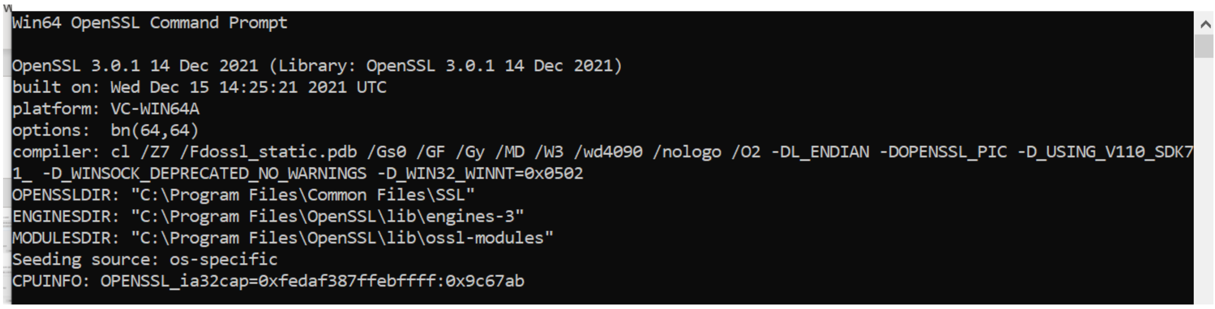
a) Navigate to the folder where the program was installed. The default value is: C:\Program Files\OpenSSL

b) Run the start.bat file



bin	01.02.2022 12:40	Folder plików	
acknowledgements.txt	15.12.2021 09:30	Dokument tekstowy	1 KB
authors.txt	15.12.2021 09:30	Dokument tekstowy	2 KB
c_rehash.pl	15.12.2021 09:30	Plik PL	7 KB
changes.txt	15.12.2021 09:30	Dokument tekstowy	721 KB
faq.txt	15.12.2021 09:30	Dokument tekstowy	1 KB
libcrypto-3-x64.dll	15.12.2021 09:30	Rozszerzenie aplikacji	5 006 KB
libssl-3-x64.dll	15.12.2021 09:30	Rozszerzenie aplikacji	754 KB
license.txt	15.12.2021 09:30	Dokument tekstowy	11 KB
news.txt	15.12.2021 09:30	Dokument tekstowy	70 KB
readme.txt	15.12.2021 09:30	Dokument tekstowy	7 KB
start.bat	15.12.2021 09:30	Plik wsadowy Windo...	1 KB
unins000.dat	01.02.2022 12:40	Plik DAT	12 KB
unins000.exe	01.02.2022 12:34	Aplikacja	714 KB

After running the file, the console will appear on screen allowing you to start generating your CSR file. The CSR file will be generated using the commands.



```
Win64 OpenSSL Command Prompt

OpenSSL 3.0.1 14 Dec 2021 (Library: OpenSSL 3.0.1 14 Dec 2021)
built on: Wed Dec 15 14:25:21 2021 UTC
platform: VC-WIN64A
options:  bn(64,64)
compiler: cl /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK7
1_ -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3"
MODULESDIR: "C:\Program Files\OpenSSL\lib\ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0xfedaf387ffebffff:0x9c67ab
```

4. Creating a CSR file

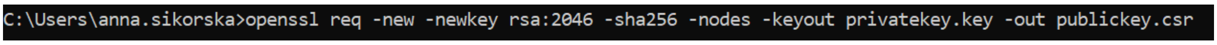
4.1 Creating files on RSA

Once the console opens, you will need to type the appropriate commands. Commands vary depending on the type of certificate or certificate key. (Commands can be pasted by pressing the CTRL+V key combination). If you make a mistake, the console will notify you of the type of error and you can re-enter the correct command)

a) Generating an SSL certificate with RSA keys

Type the following command and press Enter

openssl req -new -newkey rsa:***2048*** –sha256 -nodes -keyout ***privatekey***.key -out ***publickey***.csr



```
C:\Users\anna.sikorska>openssl req -new -newkey rsa:2046 -sha256 -nodes -keyout privatekey.key -out publickey.csr
```

Note: values in bold and blue can be modified as needed.

2048 – key length, instead of 2048 you can use: 3072, 4096

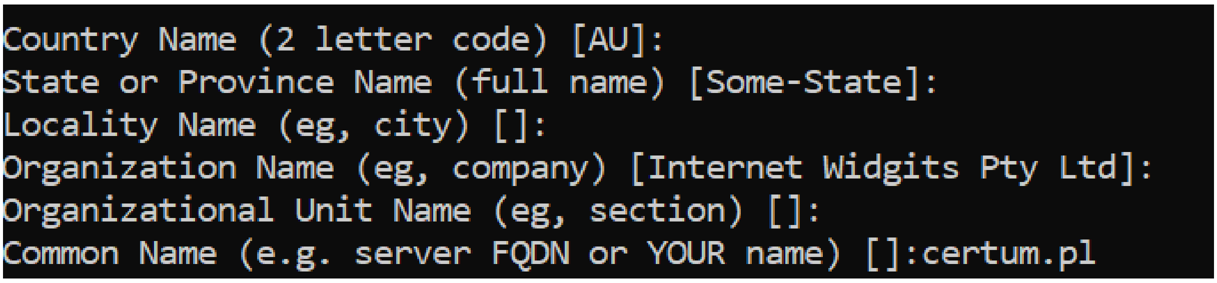
privatekey – name of .key files that will be created (name as you want to)

publickey – name of .csr file that will be created (name as you want to)

b) After entering the command, you will be prompted for more details to fill in depending on the type of certificate.

NOTE: For a Commercial DV certificate, fill in only the CN field by entering the domain you want to protect, e.g., www.certum.pl. For a Wildcard certificate, enter *certum.pl before the domain

Skip the fields that precede the CN by clicking Enter



```
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:certum.pl
```

Description of other fields.

NOTE: These fields are required in case of OV and EV certificates

Country name: Use a two-letter code without punctuation for the country, for example: PL.

State or province: List the full name of the voivodeship, state or province, for example: Zachodniopomorskie, Brandenburg, Texas, etc.

City or Town: Enter the city, e.g., Szczecin, New York, Berlin. Don't shorten the name of the city.

Company: Enter the full and correct company name.

Organizational unit: Enter the organizational unit

CN: domain name, e.g., certum.pl

Note: do not enter an email address, security password, or optional company name when generating the CSR. Skip these steps by pressing ENTER.

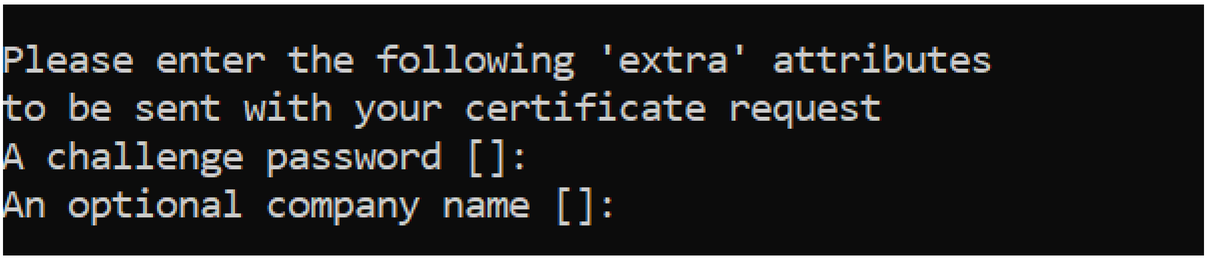
c) After entering data into additional fields, you will be prompted for additional attributes related to your password. Leave them blank by pressing enter.

Please enter the following 'extra' attributes

to be sent with your certificate request

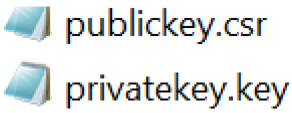
A challenge password []:

An optional company name []:



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

d) You will know that you have finished generating the CSR when your user name appears on the screen. When you enter the command, a public/private key pair will be created. Both keys will be saved locally on your computer, in your folder. To issue a certificate, you will need the certificate's public key file .csr.



publickey.csr

privatekey.key

NOTE: never delete .key files, you will need it to make .pfx certficate

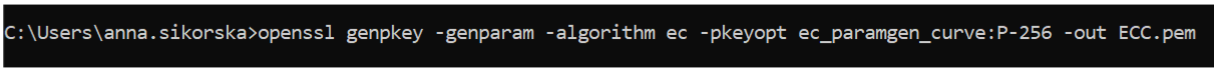
4.1 Creating files on ECC

If you want to generate certificate files on ECC keys, e.g., necessary for a Krajowy Węzęł (Eng. National Node) certificate, follow these steps:

a) start the generation of the pem file, from which the .CRT and .KEY files will be exported

openssl genpkey -genparam -algorithm ec -pkeyopt ec_paramgen_curve:P-256 -out **ECC**.pem

The value marked in blue and bold can be edited. This name will be used to create the .pem file and is needed for the second request.



```
C:\Users\anna.sikorska>openssl genpkey -genparam -algorithm ec -pkeyopt ec_paramgen_curve:P-256 -out ECC.pem
```

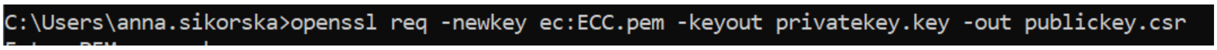
b) run second command that creates two certificate files from .pem files

NOTE: remember to use the same .pem file name as you used to generate the first request

openssl req -newkey ec:**ECC**.pem -keyout **privatekey**.key -out **publickey**.csr

The value marked in bold and blue can be edited. Files will be created under this name, and the content of the .CSR file should be submitted to Certum using the certificate ordering form.

ECC – the name of .pem file, created with first request.



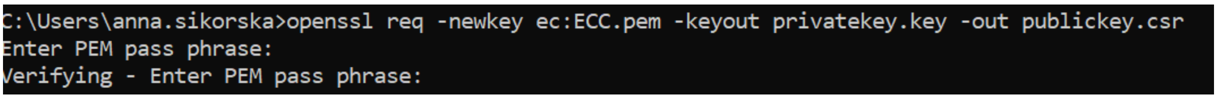
```
C:\Users\anna.sikorska>openssl req -newkey ec:ECC.pem -keyout privatekey.key -out publickey.csr
```

c) You will be asked to enter a password

Enter PEM pass phrase:

Enter a password that you will remember.

NOTE: the password you enter will not be visible!!! Don't worry if you don't see anything. When you press Enter, the password will be processed and overwritten.



```
C:\Users\anna.sikorska>openssl req -newkey ec:ECC.pem -keyout privatekey.key -out publickey.csr
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

d) Next Fill the rest of the fields by entering the necessary data for the certificate according to the table.

NOTE: For a Commercial DV certificate, fill in only the CN field by entering the domain you want to protect, e.g., www.certum.pl. For a Wildcard certificate, enter *certum.pl before the domain.

Country name: Use a two-letter code without punctuation for the country, for example: PL.

State or province: List the full name of the voivodeship, state or province, for example: Zachodniopomorskie, Brandenburg, Texas, etc.

City or Town: Enter the city, e.g., Szczecin, New York, Berlin. Don't shorten the name of the city.

Company: Enter the full and correct company name.

Organizational unit: Enter the organizational unit

CN: domain name, e.g., certum.pl

Note: do not enter an email address, security password, or optional company name when generating the CSR. Skip these steps by pressing ENTER.

e) Once these steps are completed, three files will be created:

ECC.pem

privatekey.key

publickey.csr

Provide Certum with the content of the .csr file

5. Providing the CSR file to Certum

When the process is complete, regardless of the key generation method (ECC or RSA), the files are automatically created in the User’s folder: C:\Users\anna.sikorska>

You will need the public part of the certificate to issue the certificate.

The file should be opened in Notepad.

To do this, click on the file. You will be asked to select the program in which you want to open the file. Select the Notepad. Once you have made your selection, open the file again. Copy the content and paste it into the order form.

6. Creating a .pfx file

The .pfx file is needed to install the certificate. You can create the .pfx file after issuing the certificate.

a) After issuing the certificate download the certificate file (in the binary or text form) , from the Certificate Management Certum Store

6.1 Create from .cer file

a) Use the following command:

```
openssl pkcs12 -export -out certificate.pfx -inkey privatekey.key -in 1f1da808028adaae5d5ced0679e04657.cer
```

Bold values mean:
certificate - the name under which the .pfx file will be created
privatekey - name of the private key, generated together with the public key (must be exactly the same)
1f1da808028adaae5d5ced0679e04657 - the name of the .cer file downloaded from Certum's store

After entering the command you will be asked to enter the password if you use a certificate with ECC keys. This is not required for RSA certificates.

After executing the request a .pfx file will be created under the specified name in the same folder.

certificate.pfx

6.2 Create file from .pem file

a) Use the following command:

```
openssl pkcs12 -export -inkey private-privatekey.key -in nameofpemfiles.pem -certfile intermediateca.pem -out pfxname.pfx
```

privatekey – name of .key file created during CSR generation.
nameofpemfiles – name of .pem downloaded from Certum Store (use exactly the same name)
Intermediateca – name of intermediate CA downloaded from Certum Store (use exactly the same name)

Pfxname – name of pfx file that you will created

NOTE: you need an intermediate file which you can also download from the Certum store. Use exactly the same file’s name.

NOTE: If you want to encrypt the .pfx file add the attribute -aes256 to the request

Additionally, if you want to decode your CSR, use the following command:

```
openssl req -newkey ec:ECC.pem -keyout keyprivate.key -out keypublic.csr -nodes
```