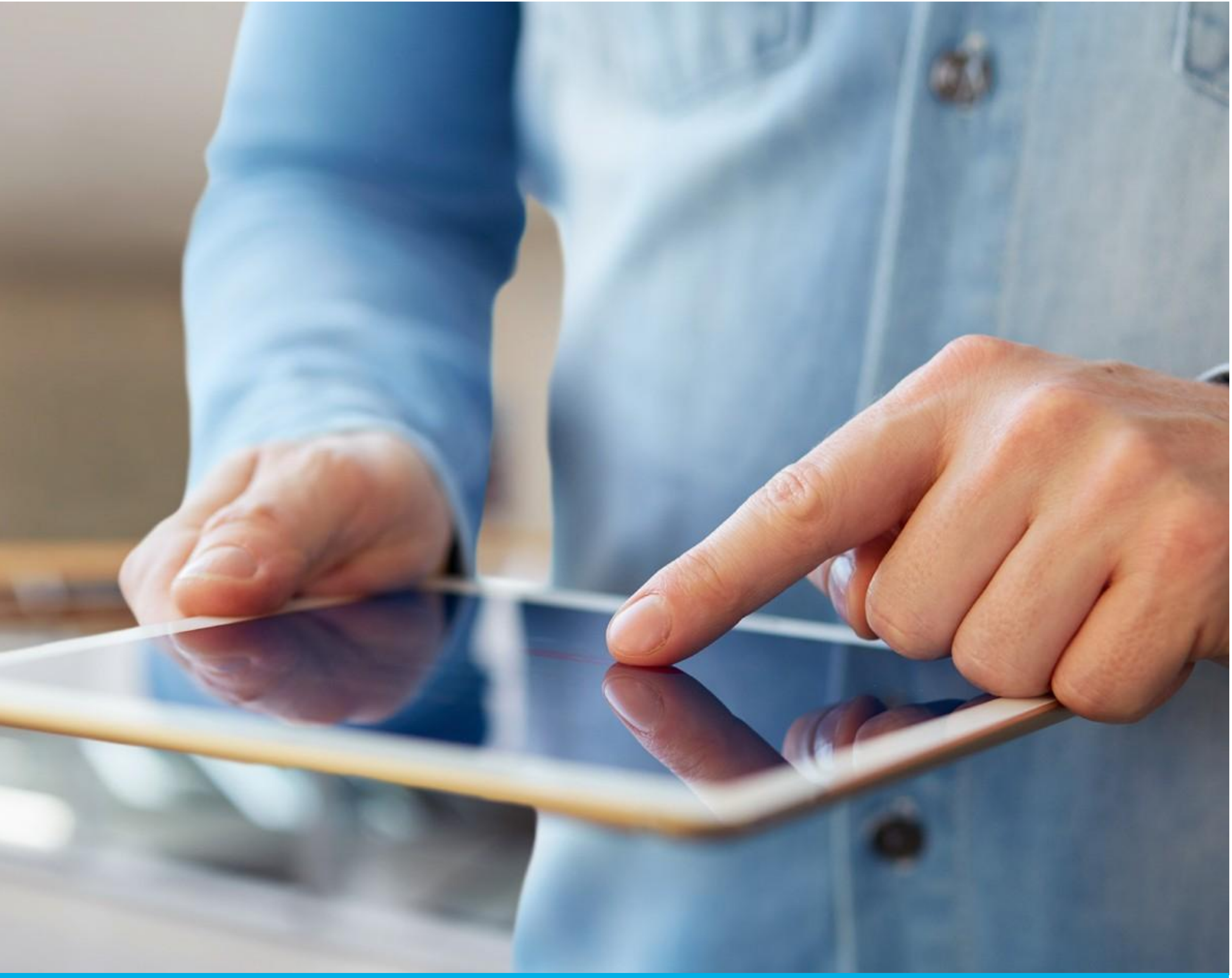


Instruction for generating CSR and PFX files using OpenSSL

Wer. 1.3

Certum

by asseco

Table of contents

1. Run OpenSSL tool

The instruction presents the process of generating CSR using the OpenSSL tool.

Note: Save the generated private key file as you will need it to install the certificate once it is issued. Create a folder in a location you know on your disk and save the generated files there.

The instructions were created using the installation package for OpenSSL, installed in a Windows environment. The OpenSSL installation steps may vary depending on the operating system, but the OpenSSL commands to generate the CSR are universal. Some operating systems have OpenSSL installed on the system by default.

Downloading OpenSSL

Download the OpenSSL tool from one of the distributors who offers the tool in the form of an installer, e.g. from https://slproweb.com/products/Win32OpenSSL.html. Choose the appropriate installation file compatible with the operating system on which you will run the process. A list of other sites hosting OpenSSL installers is available at: https://wiki.openssl.org/index.php/Binaries.

Note: We recommend using installation packages recommended by the OpenSSL team. Products recommended by OpenSSL developers are described as: [Recommended for users by the creators of OpenSSL].

OpenSSL installation and prepare to work

- Run the downloaded OpenSSL installation package
- Go through the installation wizard. If necessary, change the default options
- Finish the installation
- Create a folder in a known place on your disk, where you will store the CSR and the private key.

Running OpenSSL

Go to the folder where the program was installed. For Windows, the default path is usually: C:\Program Files\OpenSSL . Run *start.bat* file.

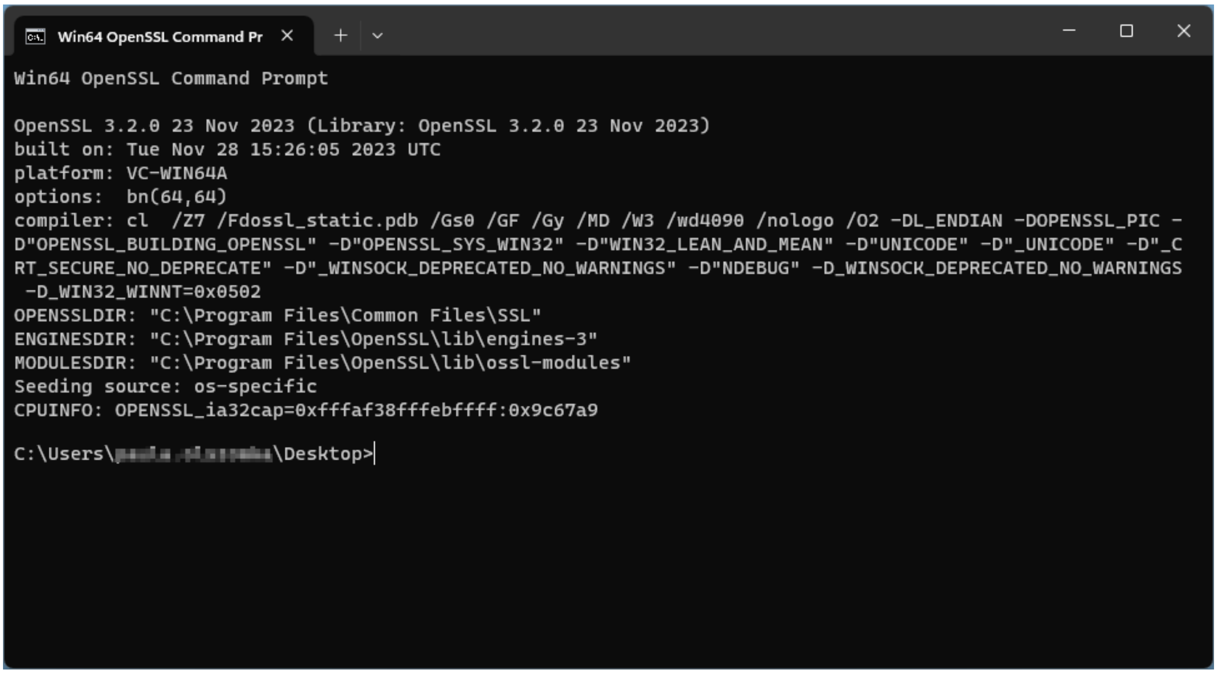
Alternatively, you can run the command line and then navigate to the OpenSSL folder with the command:

```
cd "path to the OpenSSL tool"
```

example:

```
cd "C:\Program Files\OpenSSL\bin".
```

As a result, you should have a command line terminal running, where you will execute OpenSSL commands.



```
Win64 OpenSSL Command Prompt

OpenSSL 3.2.0 23 Nov 2023 (Library: OpenSSL 3.2.0 23 Nov 2023)
built on: Tue Nov 28 15:26:05 2023 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"OPENSSL_BUILDING_OPENSSL" -D"OPENSSL_SYS_WIN32" -D"WIN32_LEAN_AND_MEAN" -D"UNICODE" -D"_UNICODE" -D"_C
RT_SECURE_NO_DEPRECATE" -D"_WINSOCK_DEPRECATED_NO_WARNINGS" -D"NDEBUG" -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=0xfffaf38fffebffff:0x9c67a9

C:\Users\[redacted]\Desktop>
```

2. Generating CSR file and the private key

CSR generation with RSA algorithm

a) In the OpenSSL console, use the following command and confirm by pressing **Enter**:

```
openssl req -new -newkey rsa:3072 -sha256 -nodes -keyout privatekey.key -
out CSR.csr
```

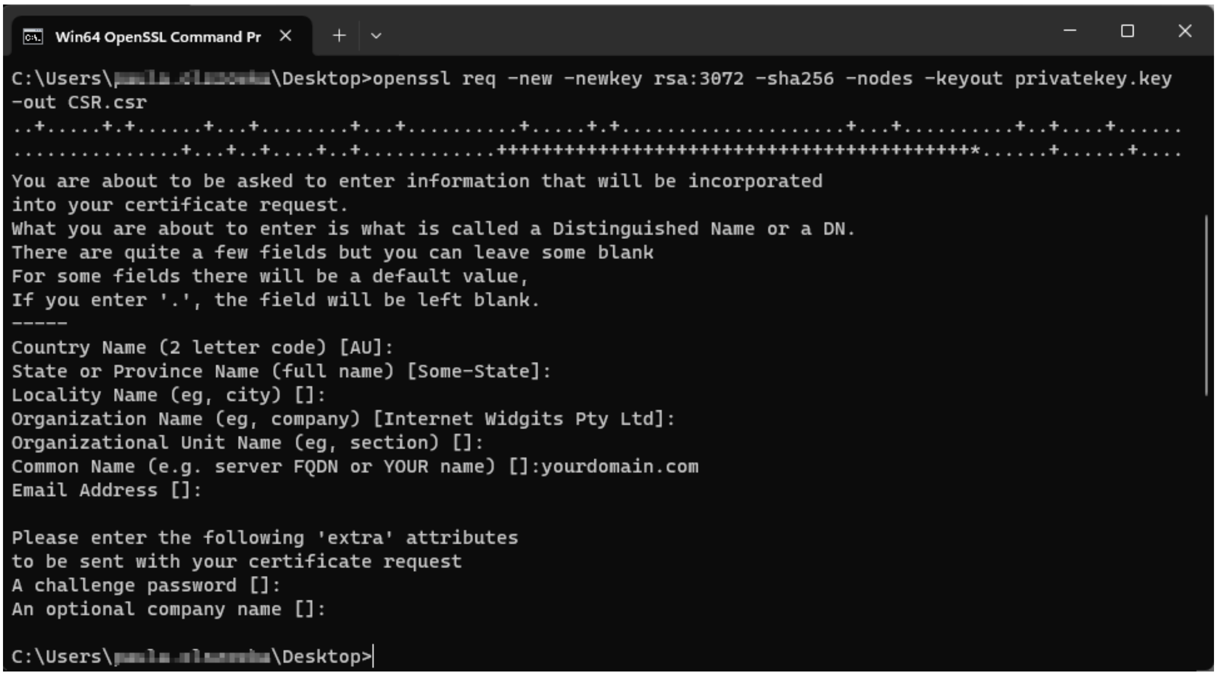
where:

- **3072** – it is the key length. If you need, you can use another value like 2048 or 4096 bit
- **privatekey**.key – it is the private key. You can set a different file name in the command. Save this file as you will need it to install the issued certificate

- CSR.csr – it is a CSR file. You can set a different file name in the command. You will use it to provide data to activate the certificate

b) When the console asks for field values to include in the CSR, provide at least the *Common name* value. You can skip values that are not required by clicking **Enter**. Certum systems offer to define the values of these fields when providing the data for the certificate and there is no need to provide them in the CSR.

c) After providing or skipping all required fields, two files will be generated in the folder where OpenSSL is running: CSR and a private key, with the names given in the command. You can copy them to the folder you created to save the files.



```
C:\Users\[redacted]\Desktop>openssl req -new -newkey rsa:3072 -sha256 -nodes -keyout privatekey.key
-out CSR.csr
..+.....+.+......+...+........+...+..........+.....+.+....................+...+..........+..+....+......
..............+...+..+....+..+............+++++++++++++++++++++++++++++++++++++++++++*......+......+....
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]:
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) []:yourdomain.com
Email Address []:

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

C:\Users\[redacted]\Desktop>
```

To use the generated CSR to provide data for certificate activation, open the CSR.csr file in a text editor e.g. Notepad and copy its content.

CSR generation with ECC algorithm

If you want to generate CSR with ECC keys which is required for e.g. for the National Node (Krajowy Węzeł Tożsamości) certificate, follow these steps:

a) In the OpenSSL console, use the following command to generate a configuration file for ECC keys and confirm by pressing **Enter**:

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

where:

- P-256 – it is the key length. If you need, you can use another value like P-384

- ECC.pem – it is a configuration file for generating CSR and private key with the EC algorithm. You can set a different file name in the command.

b) In the OpenSSL console, use the following command and confirm by pressing **Enter**:

```
openssl req -newkey ec:ECC.pem -keyout privatekey.key -out CSR.csr
```

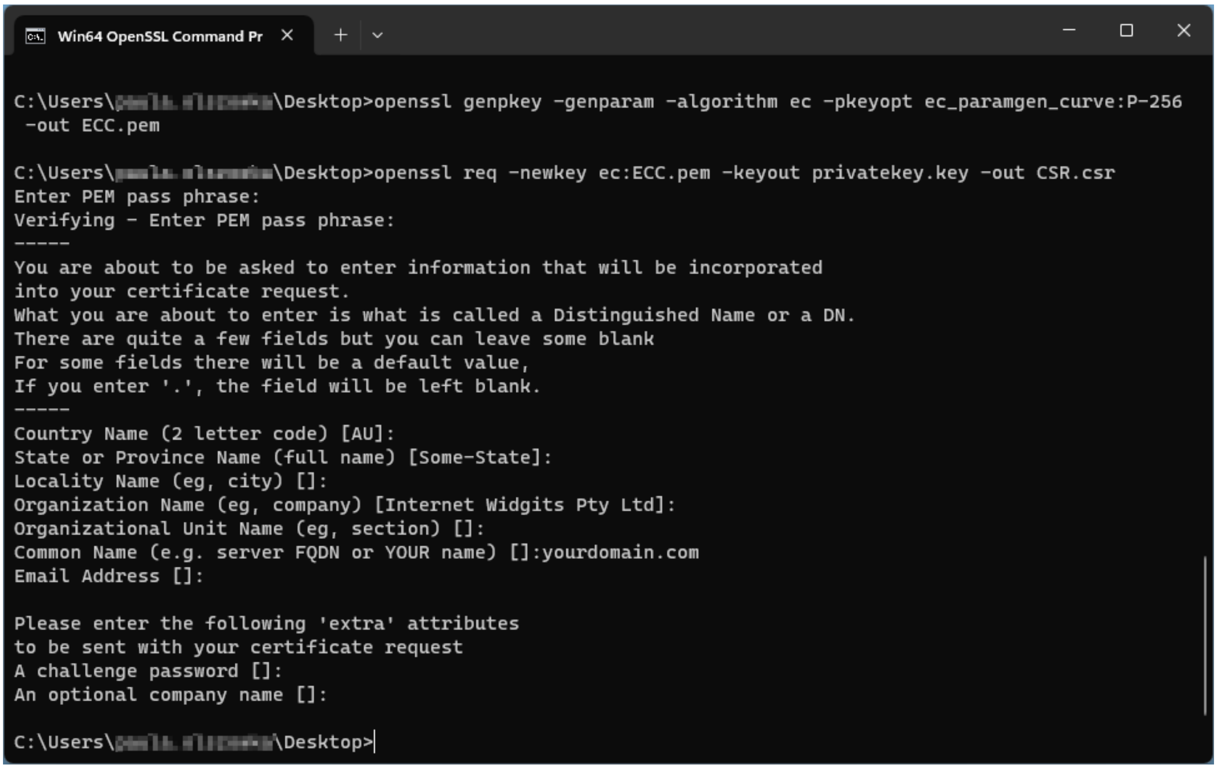
where:

- privatekey.key – it is the private key. You can set a different file name in the command. Save this file as you will need it to install the issued certificate
- CSR.csr – it is a CSR file. You can set a different file name in the command. You will use it to provide data to activate the certificate

c) Set a password for the private key file. Save it, as you will need it to install the issued certificate. The password you enter is not visible and it will be required to enter it twice

d) When the console asks for field values to include in the CSR, provide at least the *Common name* value. You can skip values that are not required by clicking **Enter**. Certum systems offer to define the values of these fields when providing the data for the certificate and there is no need to provide them in the CSR.

e) After providing or skipping all required fields, two files will be generated in the folder where OpenSSL is running: CSR and a private key, with the names given in the command. You can copy them to the folder you created to save the files.



```
C:\Users\[redacted]\Desktop>openssl genpkey -genparam -algorithm ec -pkeyopt ec_paramgen_curve:P-256
 -out ECC.pem

C:\Users\[redacted]\Desktop>openssl req -newkey ec:ECC.pem -keyout privatekey.key -out CSR.csr
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:
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) []:yourdomain.com
Email Address []:

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

C:\Users\[redacted]\Desktop>
```

To use the generated CSR to provide data for certificate activation, open the CSR.csr file in a text editor e.g. Notepad and copy its content.

3. Generating certificate in .pfx file

To install the certificate you will need the certificate file.

The issued certificate can be downloaded from the certificate creation e-mail or from the **Certificate details** view in the Data Security Products in your Certum store account, in a convenient **PEM** encoding.

From the **Certificate details** view you can also download subordinate certificates for your certificate to install them in your system.

a) Place the downloaded certificate file in the folder with the private key
b) In the OpenSSL console, use the following command and confirm by pressing **Enter**:

```
openssl pkcs12 -export -out certificate.pfx -inkey privatekey.key -in
cert.pem
```

where:

- certificate.pfx – it is the name which the .pfx file will be saved with
- privatekey.key – it is the name of the private key file generated with the CSR
- cert.pem – it is the name of the issued certificate

c) After you run the command, you will be asked to set a password for the .pfx file. Providing this password later will be required to install the certificate.

Once the request is completed, a .pfx file will be created with the specified name, in the same folder as the certificate and private key were saved.