Instructions for generating a CSR file for certificates in the Data Security category

version 1.1

Certum
by asseco

Table of contents

1.   Scope of the instruction

The instruction includes
- a description of "Certum Tools"
- a CSR file using "Certum Tools"
- creating a .pfx certificate file with the Open SSL tool

2.   Product description

Certum's "Certum Tools" application that enables generating the CSR request necessary to issue the following certificates from the Data Security category:
- SSL
- E-Mail ID (S/MIME)
- Code Signing
- National Node
- VPN

The result of the application is the generation of the content of a CSR request and a private key that can be copied/saved.

Requirements: You need a current version of Java to run the application.
Certum also supports java 8: 202

3.   Using the application

a)   Launching the application

Download the application from the https://www.support.certum.eu/en/what-is-csr/ website, run it and install it.
Next, download the "certum-tools-1.0.0-launcher.bat" file. To download this file, right-click on the download file and then select "Save File". Save both files in the same location. Always run the application from the .bat file using a double-click.

b)   Changing the language

The application is available in two language versions: Polish and English.
When you open the application, you will see its simple interface. If you want to change the application language, use the "Język" command. The application starts in Polish by default.

c) Start generating a CSR

To generate the CSR and private key, start filling in the various fields you need for the certificate. Note that you will be able to overwrite all fields, except the Name (CN), from within the store.

In the Name (CN) field, depending on the certificate, enter:

- For SSL Commercial (DV), Trusted (OV) and Premium (EV) certificates: the name of the main domain (for a Wildcard certificate, remember the asterisk)
- For the Mail ID (S/MIME) Individual certificate: the eMail ID address
- For the eMail ID (S/MIME) Business certificate: Name and surname
- For the Code Signing certificate: First and last name or company name.
- For the National Node certificate: Name of Institution/Company
- For the VPN certificate: device/card name, etc.

Complete the following fields according to your needs and the scope of the data you want to have in the certificate.

After completing the fields, select the key algorithm and its length.

NOTE: Remember that EC is required for the National Node certificate.

After completing all the necessary fields, click Generate.

d) Saving a file

When you click Generate, the following files will be generated:

- A CSR, the content of which should be copied, save and included in the Certum form

- A private key to be stored on your computer. It will be necessary to create the certificate after Certum has signed the .csr file

After clicking Save, the files are saved in the specified folder in the .pem format

The private key will be saved under the default name privateKey.pem

NOTE: The files should be saved in the User folder. To select it go to:

Local disk (C:)-> Users->Your folder

C:\Users\your.folder

4. Creating a certificate file with the Open SSL tool

The .pfx file is needed to install the certificate. It should be created with a previously saved private key (generated previously from within the application) and a certificate file, available for download after issuing from the client's account on the Certum store.

a) Once the certificate is issued, download the certificate file in binary or text form from the Certificate Management tab.
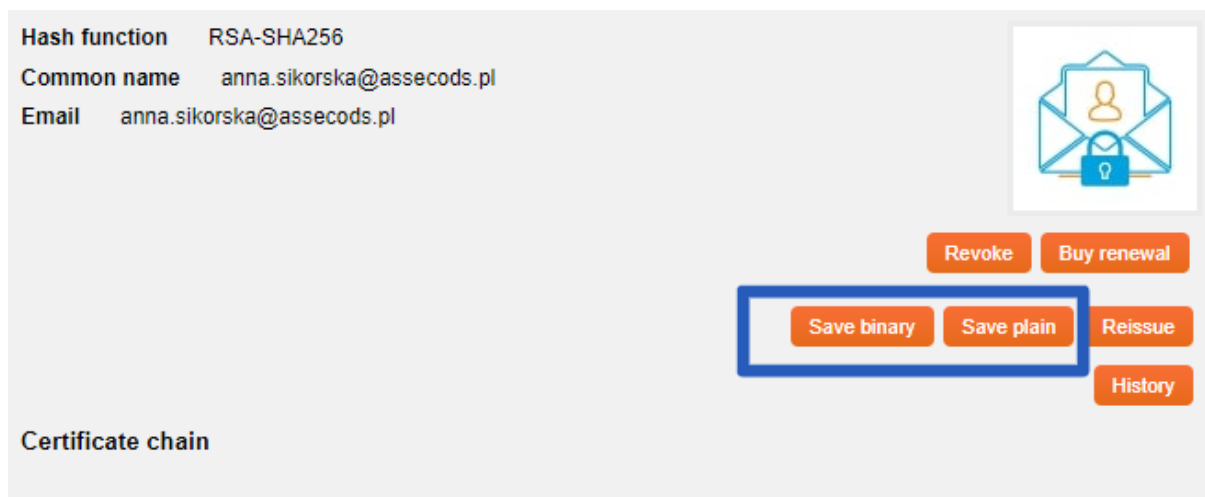

Note: The file should be saved in the same location as the previously saved private file, i.e. in the User folder. C:\Users\your.folder

You will need the OpenSSL tool to create the .pfx file

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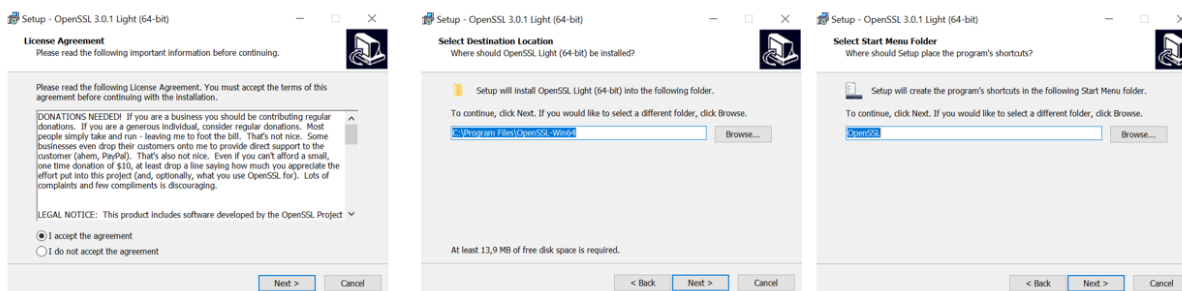
- Choose the method of running the program (We recommend the OpenSSL binaries)
- Install the program by clicking Install

- If you wish to make donations, please select the option you want. Click Finish to complete the installation.
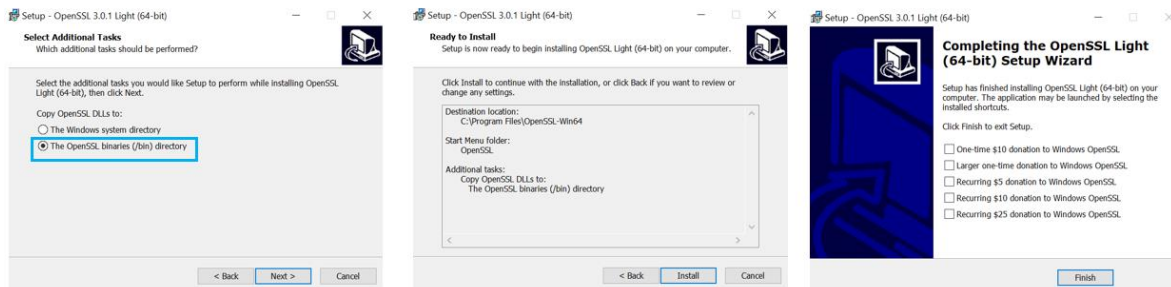
- Navigate to the folder where the program was installed. The default value is: C:\Program Files\OpenSSL
- Run the start.bat file

📁 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

c) Creating a pfx file from the console

After running the file, the console will appear.

Enter the following command into the console, keeping in mind the values of the variables:

openssl pkcs12 -export -out certificatepfx -inkey privateKey -in 1f1da808028adaae5d5ced0679e04657.cer

The values in bold mean:
certificatepfx – 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 store