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" app
- creating a CSR file necessary to issue a certification request on Certum store
- creating the .pfx certificate

2. Product description

Certum's "Certum Tools" application 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
- Generating a .pfx file

The result of the application is the generation of the content of a CSR request and a private key and a .pfx file based on the public part of the certificate and matching private key necessary to install the certificate

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.
If you downloaded the .exe file, open the application normally,

If you are using the .jar version, 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

Generated CSR

```
-----BEGIN CERTIFICATE REQUEST-----
MIICVzCCAT8CAQAwFDESMBAGA1UEAwwJY2VydHVtLnBsMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAp2MhDt1ZWrFXBWo3f9pN+eA9/vEpQ6dUkeLq+gp7
FPB9bbS3BnBMi7BIr7vlJkmhoh71M7zH52dsgJnJcafQDslCmEui1sW84C4MXj8q
Kfi48fC7+uWPsbyHqx4XjppTTx8DeouLhrWU8ZRqlwibZHuCNXf8HtFBWt04qmI6
s001Z+7t7RaT4egGyJ6RlzgNbZ43QWH9Iw3TYGAas76tduEikK/klScBTZWBLmMo
4ODTAXO1G2OGvEvJN/IgnnMmMsR2wZ0vGkxtrIwVZJdqiWHzGRb6VAJX+wrT8XcC
d9oUpZ6Cfrvc1J7aGU44NZSv7ZsfS1Fh2yjSLtXG7R16PwIDAQABMA0GCSqGSIb3
DQEBCwUAA4IBAQBLhCdDfxNDoV89YJMZUfBoPMP+Hr8XUk1Ca5laPsfHeoxwtT2G
```


Generated private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAp2MhDt1ZWrFXBWo3f9pN+eA9/vEpQ6dUkeLq+gp7FPB9bbS3
BnBMi7BIr7vlJkmhoh71M7zH52dsgJnJcafQDslCmEui1sW84C4MXj8qKfi48fC7
+uWPsbyHqx4XjppTTx8DeouLhrWU8ZRqlwibZHuCNXf8HtFBWt04qmI6s001Z+7t
7RaT4egGyJ6RlzgNbZ43QWH9Iw3TYGAas76tduEikK/klScBTZWBLmMo4ODTAXO1
G2OGvEvJN/IgnnMmMsR2wZ0vGkxtrIwVZJdqiWHzGRb6VAJX+wrT8XcCd9oUpZ6C
frvc1J7aGU44NZSv7ZsfS1Fh2yjSLtXG7R16PwIDAQABAoIBAQCEIMeziB5EbMAY
UiPFFHmAyPWnDI5aDPfAwLJi9Wr6uGsJ8iCXQlXrrhdyQHRZZL3lzzIWyOmzS/xl
9v8AbErboRqkRPAhQK06+J5ittF9mAvFTxXTkum+juc4t+Q4eLFSP1TrosNcbnFH
0LOHPAANbUD3G+M0IFHKe92DAU78wKqdF9Kq6IAZMInFjL9XF4B8/00eQJyTsVtO
Lo5rOsrmwUel/pKcOHmT38aZiIRByM6L0qTkihpDN
```


4. Creating a .pfx files

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.

Hash function   RSA-SHA256
Common name   anna.sikorska@assecods.pl
Email   anna.sikorska@assecods.pl

Revoke   Buy renewal

Save binary   Save plain   Reissue

History

Certificate chain

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

The file can be saved in two formats:

- The file downloaded using the "Save Binary" option has extension .cer

- The file downloaded with the "Save as text" option has extension .pem. The pem file can be opened with notepad, e.g. to copy its contents.

Note: If you do not know where the downloaded files are stored, check the Downloads folder.

b)   Create a .pfx file

Open Certum Tools. Select the Generator pfx tab (p12)

- In the "Certificate" part load the file with the certificate, that is the public part of the certificate, downloaded in the previous step from the Certum store.

- In the "Private Key" part load the private key file previously generated from Certum.

Set the password. Remember it! You will need it to install the certificate. You will not be able to complete the process without it. After clicking "Generate", the file will be available for download.