How to generate a private key and CSR on the Microsoft Windows system?

In order to be able to obtain the private key required to use the SSL certificate and later use Microsoft Windows, and the CSR must install the OpenSSL binary. After installation, we will be able to create the certificate signing request and the associated private key.

There are several options for creating a private key and its associated CSR file:

- How to generate a private key and CSR file with cPanel?
- How to generate a private key and CSR from the Linux command line?

1. INSTALL OPENSSL

1. Open the following link in your browser:

   https://slproweb.com/products/Win32OpenSSL.html
2. On the page that appears, select the OpenSSL for the operating system architecture
   - for a 32-bit operating system: Win32 OpenSSL v1.0.2p Light
   - for a 64-bit operating system: Win64 OpenSSL v1.0.2p Light

   and then download it.
3. Run the downloaded installation file and follow the installer instructions.

2. SET UP THE OPENSSL

After installing OpenSSL, it is necessary to set up the location of the OpenSSL configuration file for use. To do this, follow the steps below:

1. Click the **Start** menu, then the **Run** command
2. In open box type: `cmd`, then, click **OK**
3. A command prompt window appears type the following command at the prompt and press enter:
   - 32 bit version: `cd \OpenSSL-Win32`
   - 64 bit version: `cd \OpenSSL-Win64`

>

> If OpenSSL is installed in another directory during installation, then the current path may differ from the above path

4. Type the following command at the prompt and press enter:
   - 32 bit version: `set OPENSSL_CONF=c:\OpenSSL-Win32\bin\openssl.cfg`
   - 64 bit version: `set OPENSSL_CONF=c:\OpenSSL-Win64\bin\openssl.cfg`
5. Restart computer (mandatory).

3. GENERATE PRIVATE KEY AND CSR UNDER MICROSOFT WINDOWS

Follow the steps below to complete the private key and the associated CSR file:

1. Click the **Start** menu, then find the majd keresse meg a **Command Prompt** item, then right click and select **Run as administrator** option. Then follow the on-screen instructions.
2. In open box type: `cmd`, then, click **OK**
3. A command prompt window appears type the following command at the prompt and press enter
   - 32 bit version: `cd \OpenSSL-Win32\bin`
   - 64 bit version: `cd \OpenSSL-Win64\bin`

> If OpenSSL is installed in another directory during installation, then the current path may differ from the above path

4. At the command prompt, type the following command: `openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.crt`

> The above command will help you create a private or a CSR file. The generated private key file is named *server.key*, while the CSR file is named *server.csr*. Instead of naming the example, we recommend that you provide names that can easily be identified by the CSR file or the private key.

5. The command is started by pressing the enter key. The program initially prepares the private key and requests the data needed to create the CSR file. After entering the data, press enter to enter.
   - **Country Name**: You must enter the
     - the two capital letters of the headquarters of the organization
     - in case of a person, two capital letters of the country of residence

>

> Make sure you enter two uppercase country codes (for example, HU or FR) The full country code list is available through the following link: https://www.iso.org/obp/ui/#search

- **State or Province Name**: Provide the state or county in which:
  - the headquarters of the organization
  - in the case of a natural person, the state or county of the city to which it belongs belongs
- **Locality Name**: Enter the
  - organization headquaters city
  - in the case of a natural person, the city in which you are staying
- **Organization Name**: Enter the
  - organization's full or abbreviated name
  - in the case of a natural person, his full name
- **Organizational Unit Name**: you can enter the name of the department within that organization.
- **Common Name**: In this field, you must enter the domain name or subdomain name for which the certificate will be issued by the certificate issuer. This field does not need to enter "http://" "https://" prefixes.

> The common name field should normally be the domain name, for example: example.com. If you require an SSL certificate for a subdomain, you must enter the subdomain.example.com. If you want to request a wildcard SSL certificate, you should start with *, for example: *.example.com where example.com represents the domain name.

- **Email Address**: You can specify an email address that can be used to contact you.
- **Challenge password**: It is enough to leave the field empty, press enter to move on.
- **Optional company name**: It is enough to leave the field empty, press enter to move on.

6. OpenSSL creates and saves the private key as *server.key* after the data is provided, while the CSR file is named *server.csr*. Then, when ordering the SSL certificate, you must submit the contents of the *server.csr* file to issue the dance. You do not have to send the private key.
   After generating, use the following command to display the contents of the CSR file

```
notepad server.csr
```

   it looks like the next one:

```
-----BEGIN CERTIFICATE REQUEST-----
CSR CODE
-----END CERTIFICATE REQUEST-----
```

The information given in the certificate signup request can be viewed using the following command:

```
openssl req -noout -text -in server.csr
```

Revision #2
Created 18 October 2023 12:48:09 by Judit Pásztor
Updated 25 October 2023 15:56:01 by Judit Pásztor