

How to Generate a CSR and Private Key in Linux via Command Line

To issue a certificate, you need a certificate signing request, briefly a CSR file. Based on the data provided in the CSR file, the certificate issuer will issue the certificate that can later be used, among other things, to secure websites. The certificate signature request and associated private key can be generated at any time by a command line.

When generating a CSR file, a private key is created that will allow the certificate to be installed after the certificate is issued. After generating a private key, it is recommended to save the private key to a location where it is easy to find in the future. If the private key is missing then the certificate can not be installed, in which case the certificate release process must be repeated.

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 on the Microsoft Windows system?](#)

GENERATE PRIVATE KEY AND CSR FROM A LINUX ENVIRONMENT

To create the private key and the associated CSR file, follow these steps:

1. Log in to your account via SSH
2. 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.

3. 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 headquarters 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.
4. 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

```
cat 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 #7

Created 2023-10-19 13:32:34 CEST by DotRoll Knowledge Base

Updated 2026-05-14 14:11:37 CEST by DotRoll Knowledge Base