

## [en] Certificate -SSL Certificate Request - CSR creation using Unix (Config-File)

08/08/2024 16:00:08

[FAQ Article Print](#)

<b>Category:</b>	IT-Sicherheit & Anmeldung an Diensten::PKI-Zertifikate	<b>Votes:</b>	0
<b>State:</b>	public (all)	<b>Result:</b>	0.00 %
<b>Language:</b>	en	<b>Last update:</b>	11:37:15 - 07/15/2024

### Keywords

Zertifikat Zertifikatsbeantragung ACME CSR

### Solution (public)

CSR creation using Unix (Config-File)

Requirements:

- OpenSSL installed

1. The download of the template configuration file can be found on the right under the attachments ( zih-generic-req.conf ).

2. Adjust configuration file if SubjectAltNames (multiple DNS names) are to be used:

o Line 34, remove hash symbol (#) before "req\_extensions = v3\_req"

o Line 67, remove hash symbol (#) before "subjectAltName"

o Replace DNS names with desired parameters. The primary DNS name must also be entered. Formatting must be kept as follows: DNS:XYZ1..., DNS:XYZ2..., DNS:XYZ3....

3. Execute command in command line:

```
openssl req -new -config zih-generic-req.conf -keyout privkey.pem -outform PEM  
-out certreq.pem -nodes
```

4. The following parameters are already set and must be confirmed with [ENTER]:

Country name

Federal state

Location name

Organization name

5. The following parameters must be entered manually:

Unique DNS name: XYZ.tu-dresden.de (complete host name)

E-mail address: admin@tu-dresden.de (E-mail address of the contact person)

Note: The 'Unique DNS Name' must also be entered manually if it is already used in the SubjectAltNames

When using Wildcard entries it is recommended to register a DNS entry for wildcard for Sectigo before in the DNS

6. The directory now contains the private key (privkey.pem) and the certificate request (certreq.pem)