

# [de] Zertifikate - Beantragung SSL Zertifikate - CSR-Erstellung unter Unix (Konfig-Datei)

13.05.2024 19:25:55

FAQ-Artikel-Ausdruck

<b>Kategorie:</b>	IT-Sicherheit & Anmeldung an Diensten::PKI-Zertifikate	<b>Bewertungen:</b>	0
<b>Status:</b>	öffentlich (Alle)	<b>Ergebnis:</b>	0.00 %
<b>Sprache:</b>	de	<b>Letzte Aktualisierung:</b>	17:32:07 - 13.09.2023

## Schlüsselwörter

Zertifikatsbeantragung ACME CSR

## Lösung (öffentlich)

### CSR-Erstellung unter Unix (Konfig-Datei)

#### Voraussetzungen:

- OpenSSL installiert

1. Download der Vorlagen-Konfigurationsdatei: [1]HIER

(Um den Link zu öffnen, kann es notwendig sein Strg oder Shift zu drücken, während auf den Link geklickt wird (abhängig vom verwendeten Browser und Betriebssystem)).

2. Konfigurationsdatei anpassen, wenn SubjectAltNames (mehrere DNS-Namen) verwendet werden sollen:

o Zeile 34, Raute Symbol (#) vor „req\_extensions = v3\_req“ entfernen

o Zeile 67, Raute Symbol (#) vor „subjectAltName“ entfernen

o DNS-Namen durch gewünschte Werte ersetzen. Der primäre DNS-Name muss mit eingetragen werden. Formatierung muss beibehalten werden: DNS:XYZ1..., DNS:XYZ2..., DNS: XYZ3....

3. Befehl in Kommandozeile ausführen:

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

4. Folgende Werten sind bereits vorgegeben und müssen mit [ENTER] bestätigt:

Laendername

Bundesland

Ortsbezeichnung

Name der Organisation

5. Folgende Werte müssen manuell eingegeben werden:

Eindeutiger DNS-Name: XYZ.tu-dresden.de (vollständiger Hostname)

E-Mail-Adresse: admin@tu-dresden.de (E-Mail-Adresse des Ansprechpartners)

Hinweis: Der eindeutige DNS-Name muss auch manuell eingegeben werden, wenn dieser bereits in den SubjectAltNames verwendet wird

6. Im Verzeichnis befinden sich nun der Private-Key (privkey.pem) und der Zertifikatsantrag (certreq.pem)

[1] <https://tu-dresden.de/tu-dresden/organisation/ressourcen/dateien/sg-3-5-informationssicherheit/zih-generic-req.conf>