

Beantragung mit einem Zertifikatsantrag (CSR)

Erstellen einer CSR-Datei

Haben Sie die Beantragung durch einen Zertifikatsantrag gewählt, müssen Sie zuerst einen solchen erstellen. Dazu gehen Sie bitte wie folgt vor.

1. Laden Sie sich folgenden OpenSSL .cnf-Datei runter: [smime_config.cnf](#)
2. Öffnen Sie die Datei mit einem Texteditor und passen Sie folgende Textzeilen an:

- Erforderlich:

- OU =

```
openssl req -new -newkey rsa:4096 -keyout <certificate_key>.key -out  
<certificate_request>.csr -config <smime_config>.cnf
```

- CN =

- emailAddress =

- Optional, falls Sie eine oder zwei alternative Email-Adressen eintragen möchten:

- Entfernen Sie die Raute (#) aus dem Anfang der letzten Zeile (`#subjectAltName = @alt_names`) sowie die Rauten vor email.1 bzw. email.2, je nachdem, welche Sie benutzen.

- email.1 =

- email.2 =

3. Belassen Sie den Rest der Datei mit den bereits eingetragenen Werten und speichern sie diese unter einem beliebigen Namen ab.
4. Öffnen Sie das Terminal auf Ihrem Computer.
5. Mit folgendem Befehl erstellen Sie eine CSR-Datei:

```
openssl req -nodes -newkey rsa:4096 -keyout <certificate_key>.key -out  
<certificate_request>.csr -config <smime_config>.cnf
```

6. Die beiden Dateien `<certificate_key>.key` und `<certificate_request>.csr` finden Sie nun in dem Verzeichnis, aus dem Sie den Befehl ausgeführt haben.

Mit dem Befehl unter Punkt 5 wird ein Zertifikatsantrag mit privatem Schlüssel ohne Passwort erstellt. Für den Fall, dass ein privater Schlüssel mit Passwort gewünscht ist, nutzen Sie bitte folgenden Befehl:

```
openssl req -new -newkey rsa:4096 -keyout <certificate_key>.key -out <certificate_request>.csr  
-config <smime_config>.cnf
```

Beantragung des Zertifikates

Kehren Sie nun zur Beantragungsoberfläche zurück und kopieren Sie den CSR in das dafür vorgesehene Feld. Nur personenbezogene Email-Adressen sind berechtigt und werden hier aufgelistet. Fehlt eine Ihrer Email-Adressen, wenden Sie sich bitte per Email an noc@tu-braunschweig.de.

**Technische
Universität
Braunschweig**

maxmuste >

Toolbox Network
Operation Center

Navigation

Home

WIFI-Services

S/MIME Certificates

Contact NOC

Create S/MIME Certificate

What happens here?
You can request a S/MIME certificate by providing certificate signing request. For more information, please refer to the [documentation](#). (Login required.)

Request by password

Request by csr

Create S/MIME Certificate by CSR

Information
Up to 3 of the following emails are allowed in your CSR

- certbot@tu-braunschweig.de
- certrequests@tu-braunschweig.de
- max.mustermann@tu-braunschweig.de
- m.mustermann@tu-braunschweig.de

CSR ?

Paste your CSR here.

Nach erfolgreicher Beantragung gelangen Sie auch hier wieder zurück auf die Übersichtsseite und können dort Ihr P7B-Zertifikat herunterladen. Um dieses Zertifikat nutzen zu können, müssen sie zusammen mit dem privaten Schlüssel zuerst ein P12-Zertifikat erstellen. Die Anleitung dazu finden Sie weiter unten.

+ Request certificate

What happens here?

You can get an overview of your S/MIME certificates, request new or revoke existing certificates.

Current and valid S/MIME certificates

ID	Serial	CommonName	Status	Valid to	Type		
1	b4e6c400-xxxx						

Konvertieren der erhaltenen P7B-Datei

Nach erfolgreicher Beantragung eines Zertifikats mit eigenem CSR erhalten sie eine Datei mit der Endung ".p7b". Der Dateiname entspricht der ID des erstellten Zertifikates. Hierbei handelt es sich noch nicht um ein vollständiges Zertifikat. Sie müssen aus dieser Datei und dem bei Erstellung des CSRs erzeugten privaten Schlüssel erst noch eine Datei mit der Endung ".p12" erstellen. Dazu gehen Sie wie folgt vor:

1. Konvertieren der P7B-Datei in das PEM Format:

```
openssl pkcs7 -print_certs -in <cert_id>.p7b -out <cert_id>.pem -inform der
```

2. Exportieren der PEM Dateien in das P12 Format:

```
openssl pkcs12 -export -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -nomac -inkey  
<certificate_key>.key -in <cert_id>.pem -out <cert_id>.p12
```

Bei diesem Befehl werden Sie aufgefordert, ein Passwort einzugeben. Dieses Passwort schützt Ihr Zertifikat vor Missbrauch. Es wird gebraucht, um es in den Zertifikatsspeicher Ihres Betriebssystems zu importieren.