

ANLEITUNG AUSSTELLUNG EINES SERVERZERTIFIKATS ÜBER SECTIGO

ABLAUF

Schritt 1

Erstellen Sie ein Schlüsselpaar und ein Certificate Signing Request (CSR) auf dem Server, auf dem das Zertifikat installiert werden soll. Dazu erstellen Sie als erstes eine config-Datei. Diese Datei muss folgendes beinhalten:

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
utf8 = yes
[req_distinguished_name]
C = DE
ST = Nordrhein-Westfalen
L = Bochum
O = Ruhr-Universität Bochum
OU = Ihre Einrichtung
CN = einrichtung.ruhr-uni-bochum.de (die Hauptdomain)
[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = einrichtung.ruhr-uni-bochum.de
DNS.2 = www.einrichtung.ruhr-uni-bochum.de
DNS.3 = einrichtung.rub.de
DNS.4 = www.einrichtung.rub.de
DNS.5 = anderes.einrichtung.rub.de
```

Speichern Sie die Datei als Konfigurationsdatei z.B. als "csr.conf".

Private Key erstellen:

```
openssl genrsa -out einrichtung.rub.de.key 4096
```

Um ein CSR (Certificate Signing Request) zu erstellen müssen Sie folgenden Befehl ausführen:

```
openssl req -new -out einrichtung.rub.de.csr -key einrichtung.rub.de.key -config csr.conf
```

Schritt 2

Rufen Sie nun das Sectigo-Portal unter

<https://cert-manager.com/customer/DFN/ssl/sslsaml/login>

auf, und klicken Sie auf „Your Institution“. (a)

Suchen Sie anschließend nach „Ruhr-Universität Bochum“ und wählen Sie diese aus. (b)

Geben Sie Ihre RUB-LoginID (c) und das dazugehörige Passwort (d) ein und klicken Sie auf „Anmelden“ (e).

Wählen Sie nun unter "Select Enrollment Account" den Account "RUB SSL Web Form" (f) aus und klicken Sie anschließend auf "Next" (g).

Welcome to SSL Certificate Management

Before enrolling or managing existing certificates you must authenticate.

Identity Provider

You can select to authenticate with your company's identity provider.

Your Institution (a)

Find Your Institution

Your university, organization or company

 (b)

Examples: Science Institute, Lee@uni.edu, UCLA

Remember this choice [Learn More](#)

Ruhr-Universität Bochum
ruhr-uni-bochum.de

Willkommen an der Ruhr-Universität Bochum

ANMELDEN BEI SECTIGO CERTIFICATE MANAGER

Benutzername (c)

Passwort (d)

 Anmeldung nicht speichern
 Die zu übermittelnden Informationen anzeigen, damit ich die Weitergabe gegebenenfalls ablehnen kann.

Neues Layout?

Anmelden (e)

Sectigo Certificate Manager

SSL Certificate Enrollment

Enroll with Access Code

An access code will grant you access to a protected enrollment account.

Access code

Select Enrollment Account

Select from the following enrollment accounts to continue.

Account (f)

RUB SSL Web Form

Next (g)

Schritt 3

Füllen Sie das Formular wie im Folgenden beschrieben aus.

1. Organization, Department, Email: Die Organisation, das Department sowie die E-Mail-Adresse für die Domäne Ihrer Organisation werden automatisch ausgefüllt.

2. Certificate Profile: Wählen Sie das auszustellende Zertifikatsprofil aus.

3. Certificate Term: Wählen Sie die Laufzeit des Zertifikats aus.

4. Upload CSR: Sie können den als .txt-Datei gespeicherten CSR hochladen, anstatt den CSR zu kopieren und in das CSR-Feld einzufügen.

5. CSR: Geben Sie ein CSR (der Request) ein, auf dessen Grundlage Sectigo Ihren Antrag bearbeiten und das Zertifikat für die Domain ausstellen soll. Der CSR kann entweder durch direktes Einfügen in das Feld oder durch Hochladen des CSR als .txt-Datei mit **Upload CSR** (siehe Nr. 4) eingegeben werden.

Beim Hochladen oder Einfügen des CSR analysiert das Formular den CSR automatisch. Bei Anträgen auf Multi-Domain-Zertifikate (MDC) muss der von Ihnen generierte CSR nur für einen einzigen allgemeinen Namen (auch bekannt als primärer Domainname) gelten. Sie sollten die zusätzlichen Domains, die Sie benötigen, in das Feld "Subject Alternative Name" (siehe Nr. 7) eingeben.

6. Common Name: Der richtige vollqualifizierte Domainname für die Organisation oder Abteilung wird automatisch nach hochladen des CSR ausgefüllt.

7. Subject Alternative Names (Obligatorisch für MDC): Wenn das Zertifikatsprofil auf Multi-Domain-Zertifikat (MDC) eingestellt ist, sollten Sie die zusätzlichen Domainnamen hier (durch Kommas getrennt) auflisten.

8. External Requester: Geben Sie hier die vollständige E-Mail-Adresse der Person ein, in deren Namen Sie den Antrag einreichen. Die E-Mail-Adresse muss aus derselben Domain stammen, für die das Zertifikat beantragt wird. Die E-Mail zur Zertifikatssammlung wird an diese E-Mail-Adresse gesendet. Für gewöhnlich ist es Ihre eigene E-Mail-Adresse. Wenn Sie dieses Feld leer lassen, wird automatisch die E-Mail-Adresse von oben (siehe Nr. 1) genutzt.



SSL Certificate Enrollment

Please complete this form to enroll for a certificate. Your certificate will be associated with the organization/department shown below.

If the certificate can be issued immediately you will be able to download it after submitting. If the certificate requires approval you will be notified by email to the address below when its issued.

1 Organization Ruhr-Universität Bochum
Department None
Email [redacted]

2 Certificate Profile *
OV Multi-Domain

3 Certificate Term *
1 Year

4 Upload CSR

5 CSR *

6 Common Name

7 Subject Alternative Names

8 External Requesters

9. Comments: Hier können Sie zusätzliche Informationen, die Sie dem/der genehmigenden Administrator*in bereitstellen möchten, eingeben.

9

Comments



10. Auto Renew: Hier können Sie festlegen, ob das Zertifikat vor Ablauf automatisch verlängert werden soll. Geben Sie die Anzahl der Tage vor Ablauf an, wann der Erneuerungsprozess beginnen soll. Am geplanten Tag reicht SCM den Erneuerungsantrag automatisch mit einem CSR, der mit den gleichen Parametern wie das vorhandene Zertifikat generiert wurde, bei der CA ein.

10

Auto Renew

11. Submit: Klicken Sie nun auf "Submit".

11

Submit

Schritt 4

Sobald Ihr beantragtes Zertifikat erstellt wurde, erhalten Sie vom System eine E-Mail, um Ihr Zertifikat herunterzuladen. Diese E-Mail enthält folgende Informationen:

1. Die **Certificate ID**, z. B. 4011274. Sie benötigen diese ID, um ein Zertifikat über das Portal herunterzuladen, zu erneuern oder zu widerrufen.
2. Verschiedene **Links**, mit denen ein Zertifikat über diese E-Mail heruntergeladen werden kann.

Hinweis: Da Sectigo momentan zwei gültige Zertifikatsketten anbietet und hier die ältere mitgegeben wird, empfehlen wir nur das Zertifikat herunterzuladen(Certificate only, PEM encoded) und die modernere Zertifikatskette zu verwenden.

[Zum Download](#)

Es gibt folgende Formate:

- **Certificate only, PEM encoded:**
nur eigenes Zertifikat
- **Certificate (w/issuer after), PEM encoded:**
eigenes Zertifikat und Herausgeberzertifikate
- **Certificate (w/chain), PEM encoded:**
Wurzelzertifikat, Herausgeberzertifikate und eigenes Zertifikat (Zertifikatskette)
- **PKCS#7:**
für Microsoft IIS , binär
- **PKCS#7, PEM encoded:**
für Microsoft IIS
- **Intermediate(s)/Root only, PEM encoded:**
Herausgeberzertifikate und Wurzelzertifikat
- **Root/Intermediate(s) only, PEM encoded:**
Wurzelzertifikat und Herausgeberzertifikate

Bei Fragen & Problemen

Bei Fragen und Problemen können Sie sich an unseren Helpdesk wenden: its-helpdesk@ruhr-uni-bochum.de.