

# ANLEITUNG AUSSTELLUNG EINES SERVERZERTIFIKATS ÜBER HARICA

## 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. Dabei ist zu beachten, dass momentan maximal 20 SANs durch Harica unterstützt werden. 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
CN = einrichtung.ruhr-uni-bochum.de (die Hauptdomain)
[v3_req]
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 das Harica-Portal unter <https://cm.harica.gr/Login> auf, und klicken Sie auf "Academic Login".

Suchen Sie anschließend nach "Ruhr-Universität Bochum" und wählen Sie diese aus.

Geben Sie Ihre RUB-LoginID (Benutzername) und das dazugehörige Passwort ein und klicken Sie auf "Anmelden".

Login

New to HARICA? [Sign Up](#)

Email address

Type your email address

Password

Type your password

[Forgot password?](#)

Login

Or

**Academic Login**

Sign in

GREEK UNIVERSITIES NETWORK (GUnet)  
General Commercial Registry Number: 160729401000

Find Your Institution

Your university, organization or company

ruhr-uni

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

Remember this choice [Learn More](#)

**Ruhr-Universität Bochum**

Willkommen an der Ruhr-Universität Bochum

ANMELDEN BEI HARICA

Benutzername

Benutzername

Passwort

Passwort

Anmeldung nicht speichern

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

[Neues Layout?](#)

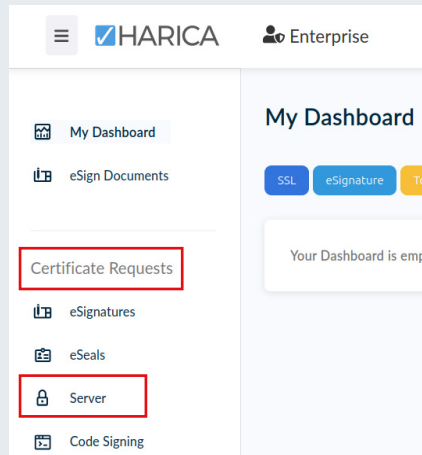
Anmelden

### Schritt 3

Wählen Sie nun "Server" auf der linken Seite unter "Certificate Requests" aus.

#### HINWEIS:

Da Harica die SANs nicht aus dem CSR übernimmt, müssen Sie die Domains **entweder** manuell eingeben, **oder** eine Datei hochladen, in der die Domains enthalten sind. Zu beachten ist hierbei, dass die Anzahl der SANs auf 20 beschränkt ist.



#### Variante 1: Manuelle Eingabe

Sie müssen für jede Domain angeben, ob auch die "www."-Domain hinzugefügt werden soll. Setzen Sie hierfür das Häkchen bei "Include www.ruhr-uni-bochum.de without additional cost" oder entfernen Sie dieses.

Klicken Sie anschließend auf "+ Add more domains". Sie müssen für jede Domain angeben, ob auch die "www."-Domain hinzugefügt werden soll. Wenn alle Domains eingetragen wurden, klicken Sie auf "Next".

#### Variante 2: Datei-Upload

Laden sie über "Download CSV Sample" die Beispiel-Datei herunter und befüllen Sie diese entsprechend.

Klicken Sie anschließend auf „Select file“ und laden Sie Ihre Datei hoch. Klicken Sie anschließend auf "Import".

#### Schritt 4

Wählen Sie nun die Art des Serverzertifikats aus, indem Sie beim gewünschten Zertifikat auf "Select" klicken.

Wir empfehlen ein OV-Zertifikat, da bei dieser Art des Zertifikats auch Organisationsinformationen und somit die Zugehörigkeit zur RUB in das Zertifikat geschrieben werden.

In einem DV-Zertifikat stehen nur die beantragten Domains und keine Organisationsinformationen.

Wenn Sie einen Zertifikatstyp ausgewählt haben, klicken Sie auf "Next".

Sie sehen anschließend die Informationen Ihrer Organisation, die in das Zertifikate geschrieben werden. Klicken Sie auf "Next".

Stimmen Sie den "Terms of Use", den "Certification Practices" und dem "Data Privacy Statement" zu, indem Sie das Häkchen setzen und klicken Sie auf "Next".

### Select the type of your certificate

**Domain-only (DV)**  
SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:  
• One or more domains

Select

Free

**For enterprises or organizations (OV)**  
SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:  
• One or more domains  
• Information of your organization that owns/controls the domains

Select

Free

**For enterprises or organizations (EV)**  
SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:  
• One or more domains  
• Information of your organization that owns/controls the domains  
• Official registry information of your organization

Select

from  
250€ year

### Select the type of your certificate

Edit

**For enterprises or organizations (OV)**  
SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:  
• One or more domains  
• Information of your organization that owns/controls the domains

Selected

Free

< Back

Next

### Organization information

**Legal name**  
Ruhr-Universitaet Bochum

**Country**  
DE

**State or province**  
Nordrhein-Westfalen

< Back

Next

### Review the application before submitting

Certificate Type	Service Duration
SSL OV	1 year

Domains  
sso-test.ruhr-uni-bochum.de

Organization Details  
**Legal name:** Ruhr-Universitaet Bochum  
**State or province:** Nordrhein-Westfalen  
**Country:** DE

I, \_\_\_\_\_, declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

< Back

Next

Wählen Sie nun "Submit CSR manually" aus. Fügen Sie anschließend Ihr CSR ein und stimmen Sie erneut den "Terms of Use", den "Certification Practices" und dem "Data Privacy Statement" zu, indem Sie das Häkchen setzen.

Klicken Sie anschließend auf "Submit request". Danach werden Sie auf das Dashboard weitergeleitet.

### Submit Request

What is a CSR?

Auto-generate CSR or **Submit CSR manually**

Use your (already created) CSR and submit it here.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICBTCCARQGCzCBMAQI...
-----END CERTIFICATE REQUEST-----
```

I, [Name], declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

[Back](#) **Submit request**

### Schritt 5

Sobald Ihr beantragtes Zertifikat erstellt wurde, erhalten Sie vom System eine E-Mail mit einem Link zum Dashboard.

Dort können Sie Ihr Zertifikat herunterladen, indem Sie rechts außen auf das Download-Symbol klicken.

Product	Validity	Information	
SSL DV	Valid	Information	
SSL DV	Valid	Information	
SSL DV	Valid	Information	
SSL DV	Valid	Information	

### HINWEIS:

Die aktuelle Zertifikaskette sollte an dieser Stelle auch immer heruntergeladen werden. Harica verwendet derzeit noch mehrere Root-CA's, sodass es nicht ausgeschlossen werden kann, dass es zu Änderungen an der Chain kommen kann.

Je nach Anwendung laden Sie entweder das Zertifikat mit Kette (PEM bundle) oder das Cert (PEM) und die Kette (chain) einzeln herunter.

Details Download Revocation Notifications Order

You can download your Certificate in a variety of formats, depending on your needs.

PEM

Typical text format

DER

Typical binary format

DER CA

Typical binary format of the Issuing Authority Certificate

PKCS#7 (chain)

Typical text format including all certificate chain

PEM bundle

Typical text format including all certificate chain along with the cross certificate

If your Certificate's Private Key is installed in a cryptographic device (token), you can download the DER and DER (CA) files and import them to your device through the token's management software. Otherwise, you can download the PEM, PEM bundle files and along with the Private Key file that you created earlier during the request process (privateKey.pem), visit <https://www.harica.gr/en/Tools/PemToP12> and convert them into a single .p12 file which is used by various operating systems/applications.

### KONTAKT & HILFE:

Bei Fragen und Problemen wenden Sie sich an unseren Helpdesk unter: [its-helpdesk@ruhr-uni-bochum.de](mailto:its-helpdesk@ruhr-uni-bochum.de)