

Serverzertifikate

Allgemeines

Mit Hilfe der GÉANT Trusted Certificate Services (GÉANT-TCS) in Verbindung mit HARICA wird die Ausstellung von SSL Serverzertifikaten ermöglicht.

Hinweise:

- Die Ausstellung von SSL Serverzertifikaten seitens GÉANT-TCS in Verbindung mit der Firma Sectigo endete am 10.01.2025.
- Die Ausstellung von SSL Serverzertifikaten seitens des DFN in der DFN-PKI endete am 31.08.2023.

Die bis zu diesem Datum beantragten SSL Serverzertifikate sind (trotzdem) 1 Jahre ab Ausstellung gültig.

Vorbereitung

Download von OpenSSL: <https://wiki.openssl.org/index.php/Binaries>

Variablen:

- **<Servername>**: Der Servername incl. Domain, z.B. server1.hs-woe.de
- **<Datum>**: Das Datum im ISO-Format, z.B. 20220326

```
# Ordner <Servername> anlegen und in den Ordner wechseln
mkdir <Servername>
cd <Servername>
#
# Schlüsselpaar (Key) erzeugen
openssl genrsa -out HARICA-<Servername>-<Datum>-key.pem 4096
#
# Zertifikatsrequest (Certificate Signing Request - CSR) erzeugen
openssl req -new -key HARICA-<Servername>-<Datum>-key.pem -out HARICA-
<Servername>-<Datum>-csr.pem
```

- Country Name: DE
- State or Province Name: Niedersachsen
- Locality Name: Wilhelmshaven oder Oldenburg oder Elsfleth
- Organization Name: Jade Hochschule Wilhelmshaven / Oldenburg / Elsfleth
- Organizational Unit Name: <keine>
- Common Name: <Servername>
- Email-Address: <keine>

Der Zertifikatsrequest liegt nun im o.a. Ordner als HARICA-<Servername>-<Datum>-csr.pem vor.

Beantragung

Bei der Beantragung eines SSL Serverzertifikates wird der von Ihnen erzeugte Zertifikatsrequest im HARICA Certificate Manager signiert und ausgestellt.

- Öffnen Sie die Webseite des [HARICA Certificate Manager](#) und klicken auf „**Academic Login**“
 - Find Your Institution: **Jade Hochschule**
 - Melden Sie sich mit Ihren **Anmeldedaten der Jade Hochschule** an
 - Im Fenster „An den Dienst zu übermittelnden Informationen“ klicken Sie auf **Akzeptieren**
- Klicken Sie links in der Menüleiste unter Certificate Requests auf **Server**
- 1. Request
 - Domains
 - Friendly name (optional): einen beliebigen Namen zur einfachen Identifikation im Dashboard angeben
 - **Add Domains Manually** or via Import: **CN eintragen**
 - **Include www.: Deaktivieren**
 - **Add more domains: weitere SANs eintragen**
 - Next
 - Produkt
 - **For Enterprises or organisations (OV):** Select
 - Next
 - Details
 - Organization information: Jade Hochschule Wilhelmshaven / Oldenburg / Elsfleth
 - Next
 - Authorization: ist bereits durch Anmeldung mit einer E-Mail Adresse der Jade Hochschule erfolgt
 - Summary
 - Review the application before submitting
 - Read and agree to Terms of Use: aktiviert
 - Next
 - Submit
 - **Submit CSR manually: den Inhalt des zuvor generierten CSRs einfügen**
 - Read and agree to Terms of Use: aktiviert
 - **Submit request**

Im Dashboard erscheint das beantragte SSL Serverzertifikat unter **Pending Certificates**

Ausstellung

Nach der Beantragung melden Sie sich bitte im HRZ bei den Herren [Früchtenicht](#) oder [Manemann](#) zur Ausstellung des SSL Serverzertifikates.

Sicherung

Im Anschluß an die Ausstellung bekommt die beantragende Person eine E-Mail, in der die erfolgreiche SSL Serverzertifikatausstellung beschrieben ist. Im Dashboard kann das SSL Serverzertifikat in

verschiedenen Formaten heruntergeladen werden.

Format	Download	Umbenennen in	Anwendung
PEM	Cert.pem	HARICA-<Servername>-<Datum>-cert.pem	nginx mit extra CA-File
DER	Cert_binary.cer	HARICA-<Servername>-<Datum>-cert.der	
DER CA	Issuer.cer	HARICA-<Servername>-<Datum>-ca.der	
PKCS#7 (chain)	Cert_chain.p7b	HARICA-<Servername>-<Datum>.p7b	Microsoft IIS
PEM bundle	Cert_bundle.pem	HARICA-<Servername>-<Datum>-cert+chain.pem	Apache & nginx (Certificate w/ issuer after)

Nach dem Download sollte das Zertifikat entsprechend umbenannt und gesichert werden. Je nach Webbrowser Einstellung liegt die Zertifikatsdatei in der Regel im Ordner „Downloads“.

- Benennen Sie die Zertifikatsdatei nach oben angegebener Notation um
- Speichern Sie die Zertifikatsdatei und auch die beiden weiter oben erzeugten Dateien (Key & CSR) an einem geeigneten Ort außerhalb Ihres PCs ab, z.B.
 - in der [Collaboration Cloud](#) im Ordner „Persönlich/Zertifikate“
 - im [PC-Verbundsystem](#) auf Laufwerk „Z:\Zertifikate“

From:

<https://hrz-wiki.jade-hs.de/> - **HRZ-Wiki**

Permanent link:

<https://hrz-wiki.jade-hs.de/de/tp/certificates/servercert>

Last update: **2025/03/19 09:11**

