# Server certificates

## General

The GÉANT Trusted Certificate Services (GÉANT-TCS) in combination with HARICA enables the issuing of SSL server certificates.

**Notes**:

- The issuance of SSL server certificates by GÉANT-TCS in conjunction with the company Sectigo ended on 10.01.2025.
- The issuance of SSL server certificates by DFN in the DFN-PKI ended on 31.08.2023.

SSL server certificates requested up to this date are (nevertheless) valid for 1 year from the date of issue.

## Preparation

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

Variables:

- **<server name>**: The server name incl. domain, e.g. server1.hs-woe.de
- **<Date>**: The date in ISO format, e.g. 20220326

```
# Create folder <servername> and change to the folder
mkdir <servername>
cd <servername>
#
# Generate key pair (key)
openssl genrsa -out HARICA-<servername>-<date>-key.pem 4096
#
# Generate Certificate Signing Request (CSR)
openssl req -new -key HARICA-<servername>-<date>-key.pem -out HARICA-
<servername>-<date>-csr.pem
```

- Country name: DE
- State or province name: Niedersachsen
- Locality name: Wilhelmshaven oder Oldenburg oder Elsfleth
- Organization Name: Jade Hochschule Wilhelmshaven/Oldenburg/Elsfleth (ENG: Jade University Wilhelmshaven/Oldenburg/Elsfleth)
- Organizational Unit Name: <keine> (ENG: <none>)
- Common Name: <Servername>
- Email-Address: <keine> (ENG: <none>)

The certificate request is now in the above-mentioned folder as HARICA-<servername>-<date>-csr.pem.

# Request

When requesting an SSL server certificate, the certificate request you generate is signed and issued in the HARICA Certificate Manager.

- Open the website of the HARICA Certificate Manager and click on "**Academic Login**"
  - Find Your Institution: **Jade University**
  - Log in with your **Jade University** credentials
  - In the window „Information to be transmitted to the service" click on **Accept**
- Click on **Server** in the menu bar on the left under Certificate Requests
- 1st request
  - Domains
    - Friendly name (optional): enter any name for easy identification in the dashboard
    - **Add Domains Manually** or via Import: **Enter CN**
    - **Include www.: Deactivate**
    - **Add more domains: enter more SANs**
    - Next
  - Product
    - **For Enterprises or organizations (OV)**: Select
    - Next
  - Details
    - Organization information: Jade University of Applied Sciences Wilhelmshaven / Oldenburg / Elsfleth
    - Next
  - Authorization: has already been done by registering with an e-mail address of Jade University
  - Summary
    - Review the application before submitting
    - Read and agree to Terms of Use: activated
    - Next
  - Submit
    - **Submit CSR manually: insert the content of the previously generated CSR**
    - Read and agree to Terms of Use: activated
    - **Submit request**

The requested SSL server certificate appears in the dashboard under **Pending Certificates**

# Issuance

After the application, please contact Mr. Früchtenicht or Mr. Manemann at the HRZ for the issuance of the SSL server certificate.

# Backup

After the certificate has been issued, the applicant will receive an e-mail describing the successful SSL server certificate issue. The SSL server certificate can be downloaded in various formats from the

dashboard.

| Format | Download | Rename to | Application |
|---|---|---|---|
| **PEM** | Cert.pem | HARICA-<Servername>-<Datum>-crt.pem | nginx with extra CA-File |
| **DER** | Cert_binary.cer | HARICA-<Servername>-<Datum>-crt.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>-crt+chain.pem | Apache & nginx (Certificate w/ issuer after) |

After the download, the certificate should be renamed and saved accordingly. Depending on the web browser settings, the certificate file is usually located in the “Downloads” folder.

- Rename the certificate file according to the above notation
- Save the certificate file and the two files created above (Key & CSR) in a suitable location outside your PC, e.g.
  - in the Collaboration Cloud in the „Personal/Certificates“ folder
  - in the PC network system on the „Z:\Certificates“ drive

From:
https://hrz-admin-wiki.jade-hs.de/ - **HRZ-Admin-Wiki**

Permanent link:
**https://hrz-admin-wiki.jade-hs.de/en/tp/certificates/servercert**

Last update: **2025/03/23 09:49**