Certification authorities

For proper functioning, the following certification authorities must be available in the operating system / software used. If one or more certification authorities are missing, download them below and import them according to the instructions.

Public certification authorities

⚠ Public certificate authorities are already included in the current operating systems.

Public digital certificates at Jade University are issued in cooperation with the DFN-CERT.

GÉANT-TCS - HARICA

Public digital certificates from **GÉANT-TCS - HARICA** are issued by GÉANT in conjunction with the "Hellenic Academic & Research Institutions Certification Authority" **since January 2025**. This results in the following certification chain:

- Hellenic Academic and Research Institutions RootCA 2015 (**Valid 2015-07-07 - 2040-06-30**)
    - HARICA TLS RSA Root CA 2021 (**Valid 2021-09-02 - 2029-08-31**)
        - GEANT TLS RSA 1 (**Valid 2025-01-03 - 2039-12-31**)

GÉANT-TCS - Sectigo

Public digital certificates from **GÉANT-TCS - Sectigo** were issued by GÉANT in conjunction with the company „Sectigo" **until the end of January 2025**.This results in the following certification chains:

Trust Path A:

- USERTrust RSA Certification Authority (**Valid 2010-02-01 - 2038-01-18**)
    - GEANT OV RSA CA 4 (Valid 2020-02-18 - 2033-05-01, for **server certificates**)
    - GEANT Personal CA 4 (Valid 2020-02-18 - 2033-05-01, for **user certificates**)
    - Sectigo RSA Organization Validation Secure Server CA (Valid 2018-11-02 - 2030-12-31, for **ACME server certificates**)

Trust Path C:

- AAA Certificate Services
(Valid 2004-01-01 - 2028-12-31)
    - USERTrust RSA Certification Authority
    (**Valid 2019-03-12 - 2028-12-31**)
        - GEANT OV RSA CA 4
        (Valid 2020-02-18 - 2033-05-01, for **server certificates**)
        - GEANT Personal CA 4
        (Valid 2020-02-18 - 2033-05-01, for **user certificates**)
        - Sectigo RSA Organization Validation Secure Server CA
        (Valid 2018-11-02 - 2030-12-31, for **ACME server certificates**)

DFN-PKI - Global G2

Public digital certificates of the **DFN-PKI - Global G2** were issued by DFN-CERT in conjunction with the company “T-Systems Enterprise Services GmbH” **until the end of July 2023**. Therefore, their certification authority “T-TeleSec GlobalRoot Class 2” appears as the root certification authority and the other two as intermediate certification authorities below it. This results in the following certification chain:

- T-TeleSec GlobalRoot Class 2
    - DFN-Verein Certification Authority 2
        - DFN-Verein Global Issuing CA

Internal certification bodies

Internal digital certificates at Jade University are issued by the University Computer Centre. These root certification authorities are used here:

- HS-WOE Certificate Authority (hs-woe.de)
- HS-WOE Certificate Authority (META)

Operating systems

Microsoft Windows

Devices in the PC network system (e.g. devices in the pool rooms / virtual desktops) are already equipped with all certification authorities, so no change is necessary here. On all other devices, they must be logged in as **users with administrative rights** to integrate certification authorities.

- Start → Manage Computer Certificates (type in)
- Certificates - Local Computer
    - Trusted Root Certification Authorities → Certificates
        - AAA Certificate Services
        - HARICA TLS RSA Root CA 2021

        - HS-WOE Certificate Authority (hs-woe.de)
        - HS-WOE Certificate Authority (META)
        - T-TeleSec GlobalRoot Class 2
    - Intermediate Certification Authorities → Certificates
        - DFN-Verein Certification Authority 2
        - DFN-Verein Global Issuing CA
        - GEANT OV RSA CA 4
        - USERTrust RSA Certification Authority

Missing certification authorities can be added by right-clicking on the respective folder Certificates → All tasks → „Import…“. add them.

Apple iOS/iPadOS

- Settings → General → Profiles
    - AAA Certificate Services
    - DFN-Verein Global Issuing CA
    - DFN-Verein Certification Authority 2
    - HARICA TLS RSA Root CA 2021
    - HS-WOE Certificate Authority (META)
    - T-TeleSec GlobalRoot Class 2
- Settings → General → Info → Certificate Trust Settings
    - AAA Certificate Services: enabled
    - HARICA TLS RSA Root CA 2021: enabled
    - HS-WOE Certificate Authority (META): enabled
    - HS-WOE Certificate Authority (hs-woe.de): enabled
    - T-TeleSec GlobalRoot Class 2: activated

The easiest way to get missing certificate authorities onto the device is from an existing (mobile) network access.

- Download the above certificate authorities with Safari.
- Load configuration profile: Allow
- Go to Settings → General → Profiles
- Tap on the new profile
- Tap on „Install“ in the upper right corner and follow the instructions
- Tap on „Done“
- Repeat the process with the other certification authorities.

- Go to Settings → General → About → Certificate Trust Settings
- Activate all certification authorities

Apple macOS

To integrate certification authorities, you must be logged in as a local user with administrative rights.

- Finder → Applications → Utilities → Keychain Administration
- Keychain System
    - AAA Certificate Services
    - DFN-Verein Certification Authority 2

    - DFN-Verein Global Issuing CA
    - HARICA TLS RSA Root CA 2021
    - HS-WOE Certificate Authority (hs-woe.de)
    - HS-WOE Certificate Authority (META)
    - T-TeleSec GlobalRoot Class 2

The easiest way to add missing certificate authorities to the device is from an existing network access.

- Click on the above certificate authorities in a browser.
- Select „Open with: Keychain Access“
- Use the „System“ keychain
- Repeat the process for all certificate authorities.

Google Android

- Settings → Security → (Advanced) → Encryption and Credentials
    - Trusted credentials
        - AAA Certificate Services
        - HARICA TLS RSA Root CA 2021
        - T-Systems Enterprise Services GmbH - T-TeleSec GlobalRoot Class 2
    - User credentials
        - AAA Certificate Services - Installed for WLAN
        - DFN-Verein Certification Authority 2 - Installed for WLAN
        - DFN-Verein Global Issuing CA - Installed for WLAN
        - HARICA TLS RSA Root CA 2021 - Installed for WLAN
        - HS-WOE Certificate Authority (META) - Installed for WLAN
        - HS-WOE Certificate Authority (hs-woe.de) - Installed for WLAN
        - T-TeleSec GlobalRoot Class 2 - Installed for WLAN

The easiest way to get missing certificate authorities onto the device is from an existing (mobile) network access. Download the above certificate authorities with a browser and open the downloaded file. The „Name Certificate“ dialogue appears:

- Certificate name:
    - AAA Certificate Services
    - DFN-Verein Certification Authority 2
    - DFN-Verein Global Issuing CA
    - HARICA TLS RSA Root CA 2021
    - HS-WOE Certificate Authority (hs-woe.de)
    - HS-WOE Certificate Authority (META)
    - T-TeleSec GlobalRoot Class 2
- Use of credentials: WLAN

Ubuntu Linux

- Passwords and encryption
    - sudo apt install seahorse
- Filter entries (3 dots top right) → Show all
- Certificates → Default Trust

    - T-TeleSec GlobalRoot Class 2
- Certificates → System Trust
    - AAA Certificate Services
    - DFN-Verein Certification Authority 2
    - DFN-Verein Global Issuing CA
    - HARICA TLS RSA Root CA 2021
    - HS-WOE Certificate Authority (hs-woe.de)
    - HS-WOE Certificate Authority (META)
    - T-TeleSec GlobalRoot Class 2

The easiest way to get missing certificate authorities onto the device is from an existing network access. Download the above certificate authorities to the Downloads folder using a browser. Then add them system-wide:

```
cd ~/Downloads
sudo trust anchor aaa_certificate_services-2004-01-01.pem
sudo trust anchor usertrust_rsa_certification_authority-2019-03-12.pem
sudo trust anchor geant_ov_rsa_ca_4-2020-02-18.pem
sudo trust anchor t-telesec_globalroot_class_2-20081001.pem
sudo trust anchor dfn-verein_certification_authority_2-20160222.pem
sudo trust anchor dfn-verein_global_issuing_ca-20160524.pem
sudo trust anchor hs-woe_certificate_authority_hs-woe.de-20161121.pem
sudo trust anchor hs-woe_certificate_authority_meta-20140601.pem
sudo trust anchor harica_tls_rsa_root_ca_2021_2021-02-19.pem
```

To check, restart the „Passwords and Encryption“ application once.

Software

Mozilla Firefox

Mozilla Firefox is available for Apple macOS, Linux and Microsoft Windows, but usually uses its own built-in certificate store.

- Application menu (3 horizontal bars) → Settings → Privacy & Security → Certificates → Show Certificates…
- Map certification authorities:
    - HARICA TLS RSA Root CA 2021
    - Wilhelmshaven/Oldenburg/Elsfleth University of Applied Sciences.
        - HS-WOE Certificate Authority (hs-woe.de)
        - HS-WOE Certificate Authority (META)
    - T-Systems Enterprise Services GmbH
        - T-Telesec GlobalRoot Class 2
        - DFN-Verein Certification Authority 2
    - The USERTRUST Network

        - GEANT OV RSA CA 4
    - Association for the Promotion of a German Research Network e.V.
        - DFN-Verein Global Issuing CA

Missing certification authorities can be added via the button „Import...“. button.

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

Permanent link:
https://hrz-wiki.jade-hs.de/en/tp/certificates/ca

Last update: **2025/03/19 12:56**