User certificates

General

With the help of the GÉANT Trusted Certificate Services (GÉANT-TCS) in conjunction with the company Sectigo, user certificates for advanced electronic signatures are made possible. Legal principles regarding electronic signatures and their characteristics can be found in the Documentation of the DFN-PKI.

The issuance of user certificates by DFN in the DFN-PKI ended on August 31, 2023. DFN user certificates applied for up to this date are still valid for 3 years from the date of issue.

Application & Issuance

When applying for a digital user certificate, a key pair is generated on your PC under your user ID and in the web browser you are using, which is then signed and issued in the Sectigo Certificate Manager (SCM).

- Open the website Sectigo Certificate Manager (SCM).
- If you have not already done so, log in to the SCM.
    - In the „**Find Your Institution**“ field, select „**Jade Hochschule**“
    - Log in with your **Jade University of Applied Sciences** username and password.
- The „Digital Certificate Enrollment“ window appears.
    - Check the correctness of the information here
        - **Name: Your first and last name**
        - **Organization: Jade University of Applied Sciences Wilhelmshaven/Oldenburg/Elsfleth**
            - Note: the additional backslashes are a display error.
        - **Email: Your email address**
    - Select the **Certicate Profile „GÉANT Personal Certificate „**.
    - Select the **Term „1095 days „**
    - Select the **Enrollment Method „Key Generation „**
    - Select the **Key Type „RSA - 4096“**.
    - To be able to download the user certificate later and to protect the private key, enter a **Password of your choice**.
    - Agree to the terms of use of the EULA by **checking the checkbox**.
    - Submit the form by **clicking on the „Submit „** button.

The user certificate is now generated and automatically issued as a file in PKCS#12 format (file extension .p12). Depending on the web browser setting, the certificate file with the name **certs.p12** is usually **in the „Downloads „** folder.

- Rename the certificate file according to the following notation:

    - **<YYYY-MM-DD>_GEANT-TCS-Sectigo_<FirstName_LastName>.p12**
- Save the certificate file in a suitable location outside your PC, e.g.
    - in the Collaboration Cloud in the folder „Personal/Certificates“.
    - in PC-Verbundsystem on drive „Z:\Zertifikate“ (certificates)
    - Remember the corresponding password to be able to restore the digital user certificate if necessary.

Integration

The integration of the digital user certificate depends on the operating system and software used.

Please keep your expired digital user certificates. You will need them to check signatures and decrypt emails.

Microsoft Windows

The Microsoft Windows operating system stores digital user certificates and certificate authorities in a central location, the Windows Certificate Store (Cryptographic Service Provider). As soon as you use software that uses the Windows certificate store, you must import your digital user certificate into this central certificate store:

- Start → Internet Options (type in) → Map: Contents
- Certificates → „Own certificates“ card → Import…
    - When prompted for a password, enter the password you chose when the certificate was issued.
    - In the import options, also activate the field „Mark key as exportable“.

Software under Microsoft Windows that uses the central certificate store are **Google Chrome , Microsoft Edge / Outlook**.

Apple iOS/iPadOS

The Apple iOS & iPadOS operating systems store digital user certificates and certificate authorities in a central location in the operating system. You must therefore bring your digital user certificate to the device in order to store it in this central certificate store:

- Send yourself and **only via the Jade University email system** an email to which you attach your digital user certificate.
- In the „Mail“ app, open the received email and tap on the attached user certificate. The operating system confirms the integration with the message „Profile loaded …“.
- Go to Settings → General → Profiles.
- Here you will find a new identity certificate:
    - Tap „Install“ at the top right (the prompt may be repeated).
    - Enter the password you chose when it was issued and tap „Next“

  - Finish installing the new profile by tapping „Done“.

Apple macOS

The Apple macOS operating system stores digital user certificates and certification authorities in a central location, the key ring management. Therefore, import your digital user certificate into this central certificate store:

- Double-click the digital user certificate file.
- The keyring management tries to change the system keyring, so you have to log in.
  - Use the password of your local Apple user here.
- You will be prompted for the password for your digital user certificate.
  - Enter the password you chose when you were issued the certificate.
- Check: Your digital user certificate appears in the key ring management in the key ring „System“ and the category „My certificates“.

Google Android

The Google Android operating system stores digital user certificates and certificate authorities in a central location in the operating system. You must therefore bring your digital user certificate to the device in order to store it in this central certificate store:

- Send yourself and **only via the Jade University email system** an email to which you attach your digital user certificate.
- On your Google Android device, open the received email and save the attached user certificate in the file system.
- Go to Settings → Security → (Advanced) → Encryption and Credentials.
- Tap on „Install from SD card“ and point to the previously saved file of your digital user certificate.
- In the „Extract Certificate“ window, enter the password you chose when the certificate was issued and tap „Next“.
- In the „Name Certificate“ window, enter the following:
  - Certificate name: GEANT-TCS-Sectigo (your email address).
  - Use of credentials: VPN and Apps
- Finish the installation by tapping OK.

You can then find the installed digital user certificate under Settings → Security → (Advanced) → Encryption and Credentials → User Credentials.

Linux

Linux stores digital user certificates and certification authorities in a central location, the application „Passwords and Encryption“ shows them. However, importing your digital user certificate is currently not possible, i.e. it cannot be stored in this central certificate store. You must therefore import your digital user certificate into the respective application (e.g. Evolution or Firefox).

Use

After the integration of the digital user certificates, they can be used to increase security in the following services:

- Signing & Encrypting Files
- Signing & Encrypting Emails

Electronic signing of documents in Adobe products is not supported, notes on this can be found in the DFN-PKI TCS FAQ at Document Signing.