User certificates

General

With the help of the GÉANT Trusted Certificate Services (GÉANT-TCS) in conjunction with the company HARICA, 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.

Notes:

- The issuance of S/MIME user certificates by GÉANT-TCS in conjunction with the company Sectigo ended on 10.01.2025.
- The issuance of S/MIME user certificates by DFN in the DFN-PKI ended on 31.08.2023.

The S/MIME user certificates applied for up to this date are (nevertheless) valid for 3 years from the date of issue.

Request

When applying for an S/MIME 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 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 login details**
  - In the window "Information to be transmitted to the service" click on **Accept**
- Click on **Email** in the menu bar on the left under Certificate Requests
- 1st request
  - Select the type of your certificate: **Email-only > Select**
  - Enter your email address: **Is prefilled > Next**
  - Select a method to validate your email address(es): Validate via email to selected email address > **Next**
  - Review the application before submitting
  - **Read and agree to Terms of Use: activated**
  - Click on **Submit**
- The requested certificate appears in the dashboard under **Pending Certificates**

Issuance

After submitting your application, you will receive an email from the HARICA Certificate Manager with the subject "HARICA - Email confirmation for certificate issuance"

- Check the content of this email for correctness and then click on "**Confirm**"

- In the “Validate your email address” window, check that your email address is correct again and then click on “**Confirm**”
- The requested product now appears in the dashboard under “Ready Certificates”: **S/MIME with your e-mail address**
- Click on “**Enroll your Certificate**” under Actions
- Click on **Generate Certificate** in the “Certificate Enrollment” window
    - Algorithm: **RSA**
    - Key size: **4096**
    - Set a passphrase: **<your desired password for this certificate>**
    - Confirm passphrase: **<your desired password for this certificate>**
    - I understand that this passphrase is under my sole knowledge and HARICA does not have access to it: **enabled**
    - Click on **Enroll Certificate**
- Click **Download** in the “Get your certificate” window and save the user certificate locally.
- Click on **Close**
- The requested certificate now appears in the dashboard under **Valid Certificates**

Backup

An S/MIME user certificate was 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 **Certificate.p12** is usually **in the “Downloads ”** folder.

- Rename the certificate file according to the following notation:
    - **<YYYY-MM-DD>_GEANT-TCS-HARICA_<first name_last name>.p12**
- Save the certificate file in a suitable location outside your PC, e.g.
    - in the Collaboration Cloud in the “Personal/Certificates” folder
    - in the PC network system on drive “Z:\Certificates”
    - Make a note of the corresponding password so that you can restore the S/MIME 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“.

Note for Apple systems: Under Apple operating systems (iOS, macOS etc.), an error message regarding an incorrect password may appear when importing the certificate. In this case, the user certificate issued by Sectigo must also be converted once.

openssl pkcs12 -in cert.p12 -out cert-new.pem

openssl pkcs12 -export -in cert-neu.pem -out cert-apple.p12

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-HARICA (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

The electronic signing of documents in Adobe products is not supported, please refer to the document Document Signing.

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

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

Last update: **2025/03/05 11:11**