Group certificates

Prerequisites

To create a group certificate, the following requirements must be met:

- The shared mailbox must already exist and the e-mail address must be known.
- A person with primary responsibility must be named for the shared mailbox.
- The person with primary responsibility must have access to the shared mailbox.

Request

To apply, send an e-mail with the following data to the HRZ-Helpdesk:

- Title: Application for a group certificate.
- Content: Provide the following data for creation:
  - E-mail address of the shared mailbox
  - First and last name of the person primarily responsible for the group certificate

Issue

An invitation email is now sent to the registered email address and the certificate can be created by the person responsible for the group.

- **Code**: is only displayed, not required in the further course.
- **Email**: is only displayed, check for correctness if necessary
- **Password**: Password for the protection of the group certificate file (PKCS#12 file).
  - Set a password here and document it in a suitable manner.
- **Passphrase**: Password to renew or revoke the group certificate.
  - Set a password here and document it appropriately.
- Submit

The group certificate is now generated and automatically issued as a file in PKCS#12 format (file extension .p12), the file is downloaded locally using the „Download“ button. Depending on the web browser setting, the certificate file with the name **<email address>.p12** is usually **in the „Downloads „** folder.

- Rename the certificate file according to the following notation:
  - **GEANT-TCS-Sectigo_<email-address>_<YYYY-MM-DD>_<surname_first_name>.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 network System on drive „Z:\Certificates“.

Integration

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

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

Microsoft Windows

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

- Start > Internet Options (type) > Map: Contents
- Certificates > „My Certificates“ tab > Import...
  - At the password prompt, enter the password you chose when the certificate was issued.
  - In the import options, do **not** activate the field „Mark key as exportable“.

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