Gruppenzertifikate

Voraussetzungen

Zur Erstellung eines Gruppenzertifikates müssen folgende Voraussetzungen erfüllt sein:

- Das freigegebene Postfach muss bereits existieren und die E-Mail Adresse bekannt sein
- Für das freigegebene Postfach muss eine hauptverantwortlich Person benannt werden
- Die hauptverantwortliche Person muss Zugriff auf das freigegebene Postfach haben

Beantragung

Zur Beantragung senden Sie eine E-Mail mit folgenden Daten an den HRZ-Servicedesk:

- Titel: Beantragung eines Gruppenzertifikates
- Inhalt: Geben Sie folgenden Daten zur Erstellung an:
  - E-Mail-Adresse des freigegebenen Postfachs
  - Vor- und Nachname der hauptverantwortlichen Person für das Gruppenzertifikat

Ausstellung

An die eingetragene E-Mail-Adresse wird nun eine Einladungsmail geschickt, und das Zertifikat kann von der für die Gruppe verantwortlichen Person erstellt werden.

- **Code**: wird nur angezeigt, im weiteren Verlauf nicht benötigt
- **Email**: wird nur angezeigt, ggfs. Kontrolle auf Richtigkeit
- **Password**: Passwort für den Schutz der Datei des Gruppenzertifikates (PKCS#12 Datei)
  - Hier ein Passwort setzen und und in geeigneter Weise dokumentieren
- **Passphrase**: Passwort, um das Gruppenzertifikat zu erneuern oder zurückzuziehen.
  - Hier ein Passwort setzen und und in geeigneter Weise dokumentieren
- Submit

Das Gruppenzertifikat wird nun generiert und automatisch als Datei im Format PKCS#12 (Dateiendung .p12) ausgestellt, mit dem Button „Download“ wird die Datei lokal heruntergeladen. Je nach Webbrowser Einstellung liegt die Zertifikatsdatei mit dem Namen **<E-Mail-Adress>.p12** in der Regel **im Ordner „Downloads“**.

- Benennen Sie die Zertifikatdatei nach folgender Notation um:
  - **GEANT-TCS-Sectigo_<E-Mail-Adresse>_<JJJJ-MM-TT>_<Nachname_Vorname>.p12**
- Speichern Sie die Zertifikatdatei an einem geeigneten Ort außerhalb Ihres PCs ab, z.B.
  - in der Collaboration Cloud im Ordner „Persönlich/Zertifikate“
  - im PC-Verbundsystem auf Laufwerk „Z:\Zertifikate“

Integration

Die Integration des digitalen Zertifikats hängt vom verwendeten Betriebssystem und der verwendeten Software ab.

> **Bitte bewahren Sie Ihre abgelaufenen digitalen Zertifikate auf**. Sie benötigen diese zur Kontrolle von Signaturen und zur Entschlüsselung von E-Mails.

Microsoft Windows

Das Betriebssystem Microsoft Windows speichert digitale Zertifikate und Zertifizierungsstellen an einer zentralen Stelle, dem Windows Zertifikatsspeicher (Cryptographic Service Provider). Sobald sie eine Software verwenden, die den Windows Zertifikatsspeicher nutzt müssen sie ihr digitales Zertifikat in diesen zentralen Zertifikatsspeicher importieren:

- Start > Internetoptionen (eintippen) > Karte: Inhalte
- Zertifikate > Karte „Eigene Zertifikate“ > Importieren…
  - Geben Sie bei der Passwortabfrage das bei der Ausstellung gewählte Passwort ein.
  - In den Importoptionen aktivieren sie **keinesfalls** das Feld „Schlüssel als exportierbar markieren“.

Software unter Microsoft Windows, die den zentralen Zertifikatsspeicher nutzt sind **Google Chrome , Microsoft Edge / Outlook**.