Nutzerzertifikate

Allgemeines

Mit Hilfe der GÉANT Trusted Certificate Services (GÉANT-TCS) in Verbindung mit der Firma Sectigo werden Nutzerzertifikate für fortgeschrittene elektronische Signaturen ermöglicht. Rechtliche Grundlagen in Bezug auf elektronische Signaturen und deren Ausprägungen sind in der Dokumentation der DFN-PKI nachzulesen.

> **Die Ausstellung von Nutzerzertifikaten seitens des DFN in der DFN-PKI endete am 31.08.2023. Die bis zu diesem Datum beantragten Nutzerzertifkate des DFN sind trotzdem noch 3 Jahre ab Ausstellung gültig.**

Beantragung & Ausstellung

Bei der Beantragung eines digitalen Nutzerzertifikats wird auf Ihrem PC unter Ihrer Benutzerkennung und in dem von Ihnen verwendeten Webbrowser ein Schlüsselpaar generiert, welches im weiteren Verlauf im Sectigo Certificate Manager (SCM) signiert und ausgestellt wird.

- Öffnen Sie die Webseite Sectigo Certificate Manager (SCM).
- Falls noch nicht geschehen melden Sie sich im SCM an
  - Im Feld „**Find Your Institution**“ wählen Sie „**Jade Hochschule**“
  - Melden Sie sich mit Ihrem **Benutzernamen und Passwort der Jade Hochschule** an.
- Es erscheint das Fenster „Digital Certificate Enrollment“
  - Prüfen Sie hier die Richtigkeit der Angaben
    - **Name: Ihr Vor- und Nachname**
    - **Organization: Jade Hochschule Wilhelmshaven/Oldenburg/Elsfleth**
      - Hinweis: bei den zusätzlichen Backslashes handelt es sich um einen Anzeigefehler
    - **Email: Ihre E-Mail Adresse**
  - Wählen Sie das **Certicate Profile „GÉANT Personal email signing and encryption“**
  - Wählen Sie den **Term „730 days“**
  - Wählen Sie als **Enrollment Method „Key Generation“**
  - Wählen Sie als **Key Type „RSA - 4096“**
  - Um das Nutzerzertifikat später herunterladen zu können und den privaten Schlüssel zu schützen vergeben Sie ein **Passwort Ihrer Wahl**
  - Wählen Sie als **Key protection algorithm „Secure AES256-SHA256“**
  - Stimmen Sie den Nutzungsbedingungen der EULA durck **Aktivierung der Checkbox** zu
  - Übermitteln Sie das Formular durch einen **Klick auf die Schaltfläche „Submit“**

Das Nutzerzertifikat wird nun generiert und automatisch als Datei im Format PKCS#12 (Dateiendung .p12) ausgestellt. Je nach Webbrowser Einstellung liegt die Zertifikatsdatei mit dem Namen **certs.p12** in der Regel **im Ordner „Downloads“**.

- Benennen Sie die Zertifikatdatei nach folgender Notation um:
  - **<JJJJ-MM-TT>_GEANT-TCS-Sectigo_<Vorname_Nachname>.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“
  - Merken Sie sich das dazugehörige Passwort, um das digitale Nutzerzertifikat im Bedarfsfall wiederherstellen zu können.

Integration

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

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

Microsoft Windows

Das Betriebssystem Microsoft Windows speichert digitale Nutzerzertifikate 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 Nutzerzertifikat 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 zusätzlich das Feld „Schlüssel als exportierbar markieren“.

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

Apple iOS/iPadOS

Die Betriebssysteme Apple iOS & iPadOS speichern digitale Nutzerzertifikate und Zertifizierungsstellen an einer zentralen Stelle im Betriebssystem. Sie müssen daher ihr digitales Nutzerzertifikat auf das Gerät bringen, um es in diesem zentralen Zertifikatsspeicher abzuspeichern:

- Schicken Sie sich selbst und **ausschließlich über das E-Mail-System der Jade Hochschule** eine E-Mail, an der Sie ihr digitales Nutzerzertifikat anhängen.
- In der App „Mail“ öffnen Sie die empfangene E-Mail und tippen auf das angehangene Nutzerzertifikat. Das Betriebssystem bestätigt die Integration mit der Meldung „Profil geladen …“
- Wechseln Sie in Einstellungen → Allgemein → Profile

- Hier finden Sie ein neues Identitätszertifikat:
    - Tippen Sie oben rechts auf „Installieren“ (die Aufforderung wird möglicherweise wiederholt)
    - Geben Sie das bei der Ausstellung gewählte Passwort ein und tippen auf „Weiter“
    - Beenden Sie die Installation des neuen Profils durch tippen auf „Fertig“

Apple macOS

Das Betriebssystem Apple macOS speichert digitale Nutzerzertifikate und Zertifizierungsstellen an einer zentralen Stelle, der Schlüsselbundverwaltung. Importieren Sie daher ihr digitales Nutzerzertifikat in diesen zentralen Zertifikatsspeicher:

- Doppelklicken Sie auf die digitale Nutzerzertifikatsdatei
- Die Schlüsselbundverwaltung versucht den Systemschlüsselbund zu verändern, daher müssen Sie sich anmelden
    - Verwenden Sie hier das Passwort ihres lokalen Apple Benutzers.
- Es erscheint die Abfrage des Passwortes für ihr digitales Nutzerzertifikat.
    - Geben Sie das bei der Ausstellung gewählte Passwort ein.
- Kontrolle: Ihr digitales Nutzerzertifikat erscheint in der Schlüsselbundverwaltung im Schlüsselbund „System“ und der Kategorie „Meine Zertifikate“

Google Android

Das Betriebssystem Google Android speichert digitale Nutzerzertifikate und Zertifizierungsstellen an einer zentralen Stelle im Betriebssystem. Sie müssen daher ihr digitales Nutzerzertifikat auf das Gerät bringen, um es in diesem zentralen Zertifikatsspeicher abzuspeichern:

- Schicken Sie sich selbst und **ausschließlich über das E-Mail-System der Jade Hochschule** eine E-Mail, an der Sie ihr digitales Nutzerzertifikat anhängen.
- Auf Ihrem Google Android Gerät öffnen Sie die empfangene E-Mail und speichern das angehangene Nutzerzertifikat im Dateisystem.
- Wechseln Sie in Einstellungen → Sicherheit → (Erweitert) → Verschlüsselung und Anmeldedaten
- Tippen Sie auf „Von SD-Karte installieren“ und zeigen auf die vorher gespeicherte Datei Ihres digitalen Nutzerzertifikates.
- Im Fenster „Zertifikat extrahieren“ geben Sie das bei der Ausstellung gewählte Passwort ein und tippen auf „Weiter“
- Im Fenster „Zertifkat benennen“ geben Sie folgendes ein:
    - Zertifikatname: GEANT-TCS-Sectigo (Ihre E-Mail-Adresse)
    - Verwendung der Anmeldedaten: VPN und Apps
- Beenden Sie die Installation durch Tippen auf OK.

Das installierte digitale Nutzerzertifikat finden Sie dann unter Einstellungen → Sicherheit → (Erweitert) → Verschlüsselung und Anmeldedaten → Nutzeranmeldedaten.

Linux

Linux speichert digitale Nutzerzertifikate und Zertifizierungsstellen an einer zentralen Stelle, die Anwendung „Passwörter und Verschlüsselung“ zeigt diese. Der Import ihres digitalen Nutzerzertifikat

ist allerdings zur Zeit nicht möglich, d.h. das es nicht in diesem zentralen Zertifikatsspeicher gespeichert werden kann. Sie müssen daher ihr digitales Nutzerzertifikat in die jeweilige Anwendung (z.B. Evolution oder Firefox) importieren.

Nutzung

Nach der Integration der digitale Nutzerzertifikate können diese zur Erhöhung der Sicherheit in folgenden Diensten genutzt werden:

- Signieren & Verschlüsseln von Dateien
- Signieren & Verschlüsseln von E-Mails

> Das elektronische Signieren von Dokumenten in Adobe Produkten wird nicht unterstützt, Anmerkungen dazu sind in der DFN-Dokumentation unter DFN-PKI > GEANT Trusted Certificate Services (TCS) > TCS FAQ > Dokumentensignatur in GEANT TCS (Document Signing) nachzulesen.