Nutzerzertifikate

Allgemeines

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

Hinweise:

- Die Ausstellung von S/MIME Nutzerzertifikaten seitens GÉANT-TCS in Verbindung mit der Firma Sectigo endete am 10.01.2025.
- Die Ausstellung von S/MIME Nutzerzertifikaten seitens des DFN in der DFN-PKI endete am 31.08.2023.

Die bis zu diesem Datum beantragten S/MIME Nutzerzertifkate sind (trotzdem) 3 Jahre ab Ausstellung gültig.

Beantragung

Bei der Beantragung eines S/MIME Nutzerzertifikats wird auf Ihrem PC unter Ihrer Benutzerkennung und in dem von Ihnen verwendeten Webbrowser ein Schlüsselpaar generiert, welches im weiteren Verlauf im HARICA Certificate Manager signiert und ausgestellt wird.

- Öffnen Sie die Webseite des HARICA Certificate Manager und klicken auf “**Academic Login**”
  - Find Your Institution: **Jade Hochschule**
  - Melden Sie sich mit Ihren **Anmeldedaten der Jade Hochschule** an
  - Im Fenster “An den Dienst zu übermittelnden Informationen” klicken Sie auf **Akzeptieren**
- Klicken Sie links in der Menüleiste unter Certificate Requests auf **Email**
- 1. Request
  - Select the type of your certificate: **Email-only > Select**
  - Enter your email address: **Ist vorausgefüllt > 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: aktiviert**
  - Klicken Sie auf **Submit**
- Im Dashboard erscheint das beantragte Zertifkat unter **Pending Certificates**

Ausstellung

Im Anschluß an die Beantragung erhalten Sie eine E-Mail vom HARICA Certificate Manager mit dem Betreff “HARICA - Email confirmation for certificate issuance”

- Überprüfen Sie den Inhalt dieser E-Mail auf Richtigkeit und klicken dann auf “**Confirm**”
- Im Fenster “Validate your email address” kontrollieren sie erneut die Richtigkeit ihrer E-Mail Adresse und klicken dann auf “**Confirm**”
- Im Dashboard erscheint nun unter “Ready Certificates” das beantragte Produkt: **S/MIME mit ihrer E-Mail-Adresse**
- Klicken Sie unter Actions auf “**Enroll your Certificate**”
- Klicken Sie im Fenster “Certificate Enrollment” auf **Generate Certificate**
    - Algorithm: **RSA**
    - Key size: **4096**
    - Set a passphrase: **<Ihr gewünschtes Passwort für dieses Zertifikat>**
    - Confirm passphrase: **<Ihr gewünschtes Passwort für dieses Zertifikat>**
    - I understand that this passphrase is under my sole knowledge and HARICA does not have access to it: **aktiviert**
    - Klicken Sie auf **Enroll Certificate**
- Klicken Sie im Fenster “Get your certificate” auf **Download** und speichern das Nutzerzertifikat lokal.
- Klicken auf **Close**
- Im Dashboard erscheint das beantragte Zertifkat nun unter **Valid Certificates**

Sicherung

Bei der Ausstellung wurde ein S/MIME Nutzerzertifikat generiert und automatisch als Datei im Format PKCS#12 (Dateiendung .p12) ausgestellt. Je nach Webbrowser Einstellung liegt die Zertifikatsdatei mit dem Namen **Certificate.p12** in der Regel **im Ordner “Downloads”**.

- Benennen Sie die Zertifikatdatei nach folgender Notation um:
    - **<JJJJ-MM-TT>_GEANT-TCS-HARICA_<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 S/MIME 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”

Hinweis für Apple Systeme: Unter den Apple Betriebssystemen (iOS, macOS usw.) kommt es beim Import des Zertifikates unter Umständen zu einer Fehlermeldung bzgl. eines falschen Kennworts. In diesem Fall muss das von Sectigo ausgestellte Nutzerzertifikat einmal zusätzlich gewandelt werden.

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

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

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-HARICA (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 im Dokument Document Signing nachzulesen.

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

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

Last update: **2025/07/02 11:41**