Zertifizierungsstellen

Für eine ordnungsgemäße Funktion müssen die nachfolgenden Zertifizierungsstellen im Betriebssystem / in der verwendeten Software vorhanden sein. Falls eine oder mehrere Zertifizierungsstellen fehlen laden sie diese unten herunter und importieren sie entsprechend der Hinweise.

Öffentliche Zertifizierungsstellen

Öffentliche digitale Zertifikate an der Jade Hochschule werden in Zusammenarbeit mit dem DFN-CERT über 2 Verfahren ausgestellt.

DFN-PKI - Global G2

Öffentliche digitale Zertifikate der **DFN-PKI - Global G2** werden vom DFN-CERT in Verbindung mit der „T-Systems Enterprise Services GmbH“ ausgestellt. Daher erscheint deren Zertifizierungsstelle „T-TeleSec GlobalRoot Class 2“ als Stammzertifizierungsstelle und die beiden anderen als darunter stehende Zwischenzertifizierungsstellen. Es ergibt sich hier folgende Zertifizierungskette:

- T-TeleSec GlobalRoot Class 2
  - DFN-Verein Certification Authority 2
    - DFN-Verein Global Issuing CA

GÉANT-TCS - Sectigo

Öffentliche digitale Zertifikate vom **GÉANT-TCS - Sectigo** werden vom GÉANT in Verbindung mit „Sectigo“ ausgestellt. Daher erscheint deren Zertifizierungsstelle „AAA Certificate Services“ als Stammzertifizierungsstelle und die beiden anderen als darunter stehende Zwischenzertifizierungsstellen. Es ergibt sich hier folgende Zertifizierungskette:

- AAA Certificate Services
  - USERTrust RSA Certification Authority
    - GEANT OV RSA CA 4

In der Regel sind die öffentlichen Zertifizierungsstellen bereits in den Betriebssystemen enthalten.

Interne Zertifizierungsstellen

Interne digitale Zertifikate an der Jade Hochschule werden vom Hochschulrechenzentrum ausgestellt. Hier kommen diese Stammzertifizierungsstellen zum Einsatz:

- HS-WOE Certificate Authority (hs-woe.de)
- HS-WOE Certificate Authority (META)

Betriebssysteme

Microsoft Windows

Geräte im PC-Verbundsystem (z.B. Geräte in den Poolräumen / Virtuelle Desktops) sind bereits mit allen Zertifizierungsstellen ausgerüstet, hier ist also keine Änderung notwendig. Auf allen anderen Geräten müssen sie zur Integration von Zertifizierungsstellen als **Benutzer mit administrativen Rechten** angemeldet sein.

- Start → Computerzertifikate verwalten (eintippen)
- Zertifikate - Lokaler Computer
  - Vertrauenswürdige Stammzertifizierungsstellen → Zertifikate
    - AAA Certificate Services
    - HS-WOE Certificate Authority (hs-woe.de)
    - HS-WOE Certificate Authority (META)
    - T-TeleSec GlobalRoot Class 2
  - Zwischenzertifizierungsstellen → Zertifikate
    - DFN-Verein Certification Authority 2
    - DFN-Verein Global Issuing CA
    - GEANT OV RSA CA 4
    - USERTrust RSA Certification Authority

Fehlende Zertifizierungsstellen können Sie über einen Rechtsklick auf den jeweiligen Ordner Zertifikate → Alle Aufgaben → „Importieren…“ hinzufügen.

Apple iOS/iPadOS

- Einstellungen → Allgemein → Profile
  - AAA Certificate Services
  - DFN-Verein Global Issuing CA
  - DFN-Verein Certification Authority 2
  - HS-WOE Certificate Authority (META)
  - T-TeleSec GlobalRoot Class 2
- Einstellungen → Allgemein → Info → Zertifikatsvertrauenseinstellungen
  - AAA Certificate Services: aktiviert
  - HS-WOE Certificate Authority (META): aktiviert
  - HS-WOE Certificate Authority (hs-woe.de): aktiviert
  - T-TeleSec GlobalRoot Class 2: aktiviert

Fehlende Zertifizierungsstellen können am einfachsten von einem bestehenden (Mobilfunk-) Netzzugang aus auf das Gerät gebracht werden.

- Laden Sie die oben stehenden Zertifizierungsstellen mit Safari herunter
- Konfigurationsprofil laden: Zulassen
- Wechseln Sie in Einstellungen → Allgemein → Profile
- Tippen Sie auf das neue Profil
- Tippen Sie oben rechts auf „Installieren“ und folgen den Anweisungen
- Tippen Sie auf „Fertig“
- Wiederholen Sie den Vorgang mit den anderen Zertifizierungsstellen

- Wechseln Sie in Einstellungen → Allgemein → Info → Zertifikatsvertrauenseinstellungen
- Aktivieren Sie alle Zertifizierungsstellen

Apple macOS

Zur Integration von Zertifizierungsstellen müssen Sie als lokaler Benutzer mit administrativen Rechten angemeldet sein.

- Finder → Programme → Dienstprogramme → Schlüsselbundverwaltung
- Schlüsselbund System
    - AAA Certificate Services
    - DFN-Verein Certification Authority 2
    - DFN-Verein Global Issuing CA
    - HS-WOE Certificate Authority (hs-woe.de)
    - HS-WOE Certificate Authority (META)
    - T-TeleSec GlobalRoot Class 2

Fehlende Zertifizierungsstellen können am einfachsten von einem bestehenden Netzzugang aus auf das Gerät gebracht werden.

- Klicken Sie die oben stehenden Zertifizierungsstellen in einem Browser an
- Wählen Sie „Öffnen mit: Keychain Access“
- Verwenden Sie den Schlüsselbund „System“
- Wiederholen Sie den Vorgang für alle Zertifizierungsstellen

Google Android

- Einstellungen → Sicherheit → (Erweitert) → Verschlüsselung und Anmeldedaten
    - Vertrauenswürdige Anmeldedaten
        - AAA Certificate Services
        - T-Systems Enterprise Services GmbH - T-TeleSec GlobalRoot Class 2
    - Nutzeranmeldedaten
        - AAA Certificate Services - Installiert für WLAN
        - DFN-Verein Certification Authority 2 - Installiert für WLAN
        - DFN-Verein Global Issuing CA - Installiert für WLAN
        - HS-WOE Certificate Authority (META) - Installiert für WLAN
        - HS-WOE Certificate Authority (hs-woe.de) - Installiert für WLAN
        - T-TeleSec GlobalRoot Class 2 - Installiert für WLAN

Fehlende Zertifizierungsstellen können am einfachsten von einem bestehenden (Mobilfunk-) Netzzugang aus auf das Gerät gebracht werden. Laden Sie die oben stehenden Zertifizierungsstellen mit einem Browser herunter und öffnen Sie die heruntergeladene Datei. Es erscheint der der Dialog

„Zertifikat benennen“:

- Zertifikatname:
  - AAA Certificate Services
  - DFN-Verein Certification Authority 2
  - DFN-Verein Global Issuing CA
  - HS-WOE Certificate Authority (hs-woe.de)
  - HS-WOE Certificate Authority (META)
  - T-TeleSec GlobalRoot Class 2
- Verwendung der Anmeldedaten: WLAN

Ubuntu Linux

- Passwörter und Verschlüsselung
  - sudo apt install seahorse
- Einträge filtern (3 Punkte rechts oben) → Alle Anzeigen
- Zertifikate → Default Trust
  - T-TeleSec GlobalRoot Class 2
- Zertifikate → System Trust
  - AAA Certificate Services
  - DFN-Verein Certification Authority 2
  - DFN-Verein Global Issuing CA
  - HS-WOE Certificate Authority (hs-woe.de)
  - HS-WOE Certificate Authority (META)
  - T-TeleSec GlobalRoot Class 2

Fehlende Zertifizierungsstellen können am einfachsten von einem bestehenden Netzzugang aus auf das Gerät gebracht werden. Laden Sie die oben stehenden Zertifizierungsstellen mit einem Browser in den Downloads Ordner herunter. Fügen Sie sie dann systemweit ein:

```
cd ~/Downloads
sudo trust anchor aaa_certificate_services-2004-01-01.pem
sudo trust anchor usertrust_rsa_certification_authority-2019-03-12.pem
sudo trust anchor geant_ov_rsa_ca_4-2020-02-18.pem
sudo trust anchor t-telesec_globalroot_class_2-20081001.pem
sudo trust anchor dfn-verein_certification_authority_2-20160222.pem
sudo trust anchor dfn-verein_global_issuing_ca-20160524.pem
sudo trust anchor hs-woe_certificate_authority_hs-woe.de-20161121.pem
sudo trust anchor hs-woe_certificate_authority_meta-20140601.pem
```

Starten Sie zur Kontrolle die Anwendung „Passwörter und Verschlüsselung“ einmal neu.

Software

Mozilla Firefox

Mozilla Firefox ist für Apple macOS, Linux und Microsoft Windows verfügbar, benutzt aber in der Regel seinen eigenen, integrierten Zertifikatsspeicher.

- Anwendungsmenü (3 horizontale Striche) → Einstellungen → Datenschutz & Sicherheit → Zertifikate → Zertifikate anzeigen…
- Karte Zertifizierungsstellen:
  - Hochschule Wilhelmshaven/Oldenburg/Elsfleth
    - HS-WOE Certificate Authority (hs-woe.de)
    - HS-WOE Certificate Authority (META)
  - T-Systems Enterprise Services GmbH
    - T-Telesec GlobalRoot Class 2
    - DFN-Verein Certification Authority 2
  - The USERTRUST Network
    - GEANT OV RSA CA 4
  - Verein zur Foerderung eines Deutschen Forschungsnetzes e.V.
    - DFN-Verein Global Issuing CA

Fehlende Zertifizierungsstellen können Sie über den Button „Importieren…“ hinzufügen.