Dateien

Mit Hilfe eines X.509 Zertifikates können Sie unter anderem Dateien signieren und verschlüsseln.

Zertifikatsmanagement-Software

Zunächst müssen Sie eine geeignete Zertifikatsmanagement-Software auf Ihren PC installieren. Hier bietet sich zum Beispiel eine Software mit dem Namen „Kleopatra“ an. Kleopatra ist eine freie (im Sinne von Freiheit), quelloffene und zugleich kostenfreie Software.

- Unter Windows ist Kleopatra ein Teil des sogenannten „Gpg4win“ Paketes, welches „...zum Verschlüsseln und Signieren von E-Mails, Dateien und Ordnern unter Windows“ geeignet ist. Laden Sie sich das Gpg4win Paket hier herunter. Wenn Sie mögen, können Sie gerne für Gpg4win spenden, Sie können jedoch auch durch Auswahl von „0€“ den Download starten. Installieren Sie Gpg4win auf Ihrem PC. Bei der Installation können Sie alle Standardwerte übernehmen.
- Unter Linux installieren Sie mit Hilfe der integrierten Softwareverwaltung das Paket „kleopatra“.

Einrichtung der Software für X.509 Zertifikate

Zertifizierungsketten

Als erstes müssen Sie die 2 kompletten, ausstellenden Zertifizierungsketten der DFN-PKI für die Jade Hochschule in Kleopatra importieren. Die benötigten Dateien finden Sie innerhalb der Hochschule im PC-Verbundsystem und außerhalb der Hochschule über den WebFiler unter

- JADE-HS - Daten (X:) / HRZ-Support / Zertifikatsdienste

Importieren Sie dazu unter dem Kleopatra-Menüeintrag „Datei / Importieren“ die folgenden Dateien in dieser Reihenfolge:

- Im Unterordner DFN-Global-G1:
  - Deutsche_Telekom_Root_CA_2-19990709.der
  - DFN-Verein_PCA_Global_-_G01-20140722.der
  - HS-WOE_CA_-_G01-20140605.der
- Im Unterordner DFN-Global-G2:
  - T-Telesec_GlobalRoot_Class_2-20081001.der
  - DFN-Verein_Certification_Authority_2-20160222.der
  - DFN-Verein_Global Issuing_CA-20160524.der

Schließen Sie am Ende alle Registerkarten mit dem Namen „Importierte Zertifikate“. Lassen Sie lediglich die Karte „Alle Zertifikate“ geöffnet.

Zertifikatssperrlisten

Zur Zeit werden Zertifikatssperrlisten nicht unterstützt, daher müssen Sie die Prüfung abschalten:

- Im Kleopatra-Menüeintrag „Einstellungen / Kleopatra einrichten…“ wählen Sie die Gruppe „S/MIME-Prüfung“.
- Klicken Sie hier auf die Checkbox „Nie Sperrlisten zu Rate ziehen“ und dann auf den Button „OK“

Nutzerzertifikat

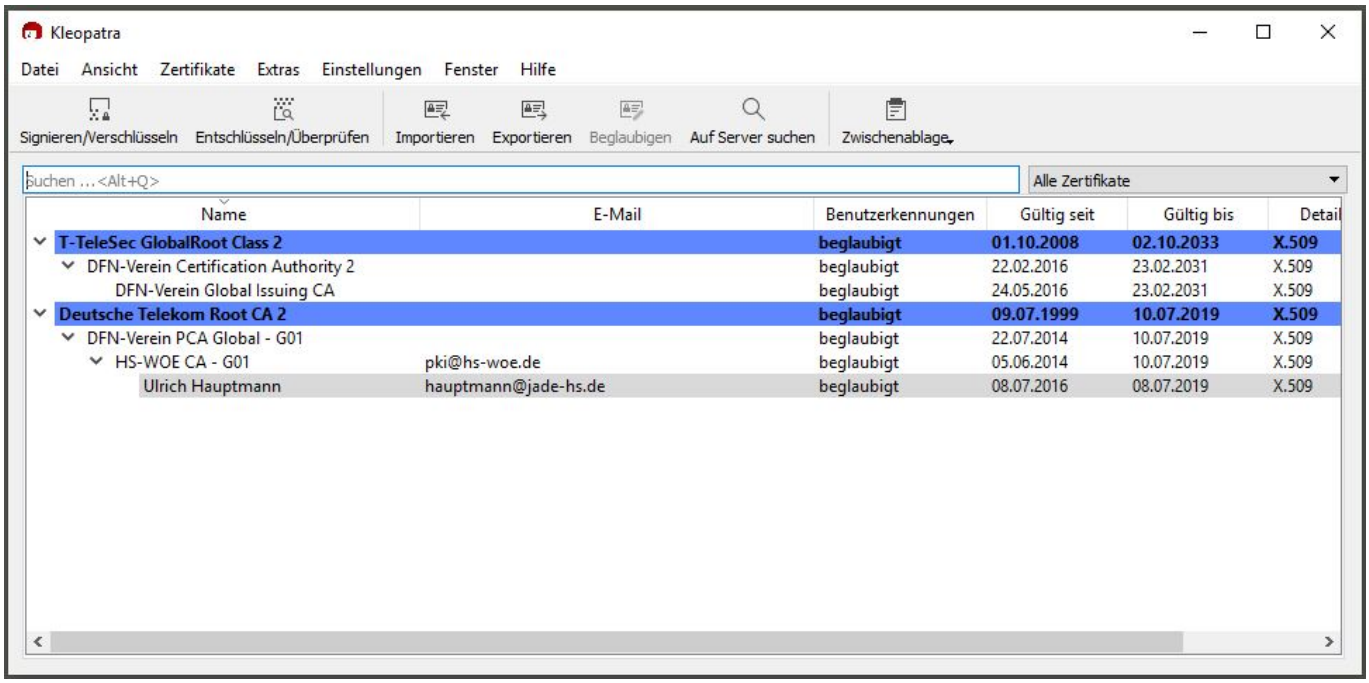
Im weiteren Verlauf müssen Sie Ihr X.509 Zertifikat mit Hilfe Ihrer unter Nutzerzertifikate (Abschnitt Sicherung) erstellten Zertifikatsdatei importieren:

Importieren Sie dazu unter dem Kleopatra-Menüeintrag „Datei / Importieren“ die unter Nutzerzertifikate (Abschnitt Sicherung) erstellte Zertifikatsdatei. Im Verlauf des Import-Dialoges werden Sie im Fenster „pinentry“ zur Eingabe einer Passphrase aufgefordert, es handelt sich hier um das Passwort, welches Sie ebenfalls bei der Erstellung des Nutzerzertifikates unter Sicherung eingegeben haben (möglicherweise müssen Sie dieses Kennwort weitere zwei Male eingeben).

Öffentliche Nutzerzertifikate

Falls Sie Dateien für andere Personen verschlüsseln möchten, müssen Sie die zur Verschlüsselung notwendigen öffentlichen Nutzerzertifikate des Empfängers besitzen und ebenfalls in Kleopatra importieren.

Nach der Einrichtung sollte das Hauptfenster von Kleopatra in etwa so aussehen:



Dateien signieren / verschlüsseln

Nun können Sie in Kleopatra Dateien signieren und/oder verschlüsseln:

- Klicken Sie dazu auf den Kleopatra-Menüeintrag „Datei / Signieren/Verschlüsseln…“ und wählen die zu signierende/verschlüsselnde Datei.
    - Authentizität sicherstellen (signieren)
        - Wählen sie die Checkbox „Signieren als:“ aus.
        - Klicken auf den Button „Signieren“.

        - Sie werden im Fenster „pinentry“ zur Eingabe einer Passphrase aufgefordert, geben Sie hier Ihr Zertifikatspasswort ein.
        - Neben der zu signierenden Datei entsteht nun eine weitere Datei mit dem gleichen Namen, ergänzt um den Zusatz
            - p7s bei X.509 (die signierte Datei im PKCS#7 Format)
        - Sie müssen die Original- und die Signaturdatei im selben Ordner bewahren.
    - Verschlüsseln:
        - Wählen Sie die Checkbox „Für mich verschlüsseln“ aus, wenn Sie für sich selbst verschlüsseln wollen.
        - Wählen Sie die Checkbox „Für andere verschlüsseln“ aus, wenn Sie für andere verschlüsseln wollen. Hierzu müssen Sie wie oben beschrieben das öffentliche Zertifikat der anderen Personen importieren und dieses dann hier auswählen.
        - Klicken auf den Button „Verschlüsseln“.
        - Neben der zu verschlüsselnden Datei entsteht nun eine weitere Datei mit dem gleichen Namen, ergänzt um den Zusatz
            - .p7m bei X.509 (die verschlüsselte Datei im PKCS#7 Format)

Dateien überprüfen / entschlüsseln

Nun können Sie in Kleopatra Dateien auf eine gültige Signatur überprüfen und/oder entschlüsseln:

- Klicken Sie dazu auf den Kleopatra-Menüeintrag „Datei / Entschlüsseln/Überprüfen...“.
    - Überprüfen
        - Wählen sie die Signaturdatei (mit der Endung .p7s) aus.
    - Entschlüsseln:
        - Wählen sie die verschlüsselte Datei (mit der Endung .p7m) aus.
- Es öffnet sich ein Hinweisfenster, welches den Status der Signatur / Verschlüsselung anzeigt.