Cleopatra

With the help of a digital user certificate according to the X.509 standard, you can sign and encrypt files, among other things. The software Kleopatra is suitable for convenient signing/encryption and checking/decryption of files.

Requirements

- Valid digital user certificate

Installation

Microsoft Windows

Under Microsoft Windows, Kleopatra is part of the so-called "Gpg4win" package. If you like you can donate for Gpg4win, but you can also start the download by selecting „0€“. Install Gpg4win on your PC, you can accept all default values during the installation.

Linux

Under Linux, install the package „kleopatra“ with the help of the integrated software management.

Configuration

Certification authorities

For proper functioning, you must integrate the certification authorities into Kleopatra. Add them to the software under the Kleopatra menu item „File / Import“. At the end, close all tabs named „Imported certificates“ and leave only the „All certificates“ tab open.

Certificate revocation lists

Currently, certificate revocation lists are not supported, so you need to disable the check:

- In the Kleopatra menu item „Settings / Set up Kleopatra…“ select the group „S/MIME check“.
- Click on the checkbox „Never consult revocation lists“ and then on the button „OK“.

User certificate

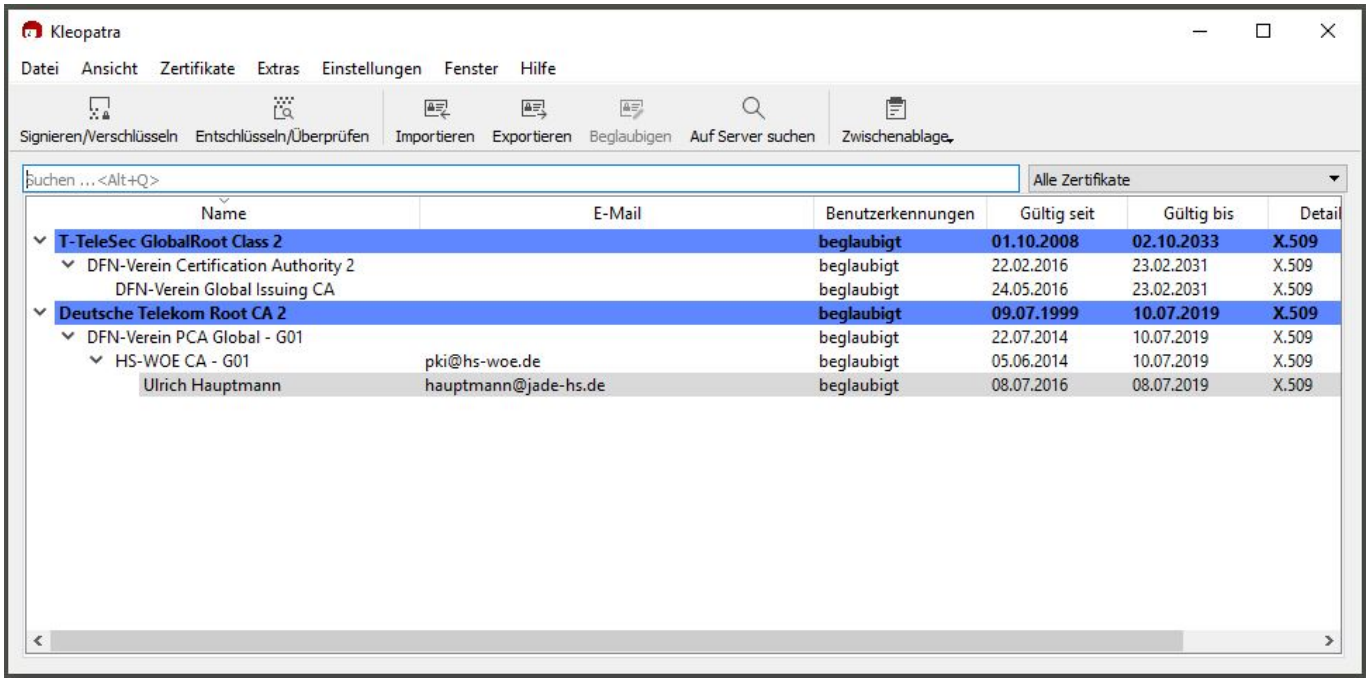
In the further course, you must create a digital user certificate using your certificate created under User Certificates (section Backup) to import the certificate file:

To do this, import the certificate file created under User Certificates under the Kleopatra menu item „File / Import“. (section Backup). In the course of the import dialogue, you will be asked to enter a passphrase in the „pinentry“ window; this is the password that you also entered when creating the user certificate under Backup (you may have to enter this password two more times).

User certificates of other persons

If you want to encrypt files for other people, you need to have the public part of the user certificate of the person you are receiving and import it into Kleopatra as well.

After the setup, the main window of Kleopatra should look something like this:



Sign / Encrypt

You can now sign and/or encrypt files in Kleopatra:

- To do this, click on the Kleopatra menu item „File / Sign/Encrypt...“ and select the file to be signed/encrypted.
  - Ensure authenticity (sign)
    - Select the checkbox „Sign as:“.
    - Click on the „Sign“ button.
    - You will be prompted to enter a passphrase in the „pinentry“ window: enter your certificate password.
    - Next to the file to be signed, another file with the same name is now created, supplemented by the suffix
      - p7s for X.509 (the signed file in PKCS#7 format)
    - You must keep the original and the signature file in the same folder.
  - Encrypt:

- Select the „Encrypt for me“ checkbox if you want to encrypt for yourself.
- Select the „Encrypt for others“ checkbox if you want to encrypt for others. As described above, you must import the other people's public certificate and then select this.
- Click on the „Encrypt“ button.
- Next to the file to be encrypted, another file with the same name will now be created, supplemented by the suffix
    - .p7m for X.509 (the encrypted file in PKCS#7 format)

Verify / Decrypt

Now you can check files in Kleopatra for a valid signature and/or decrypt them:

- To do this, click on the Kleopatra menu item „File / Decrypt / Verify…“.
    - Check
        - Select the signature file (with the extension .p7s).
    - Decrypt:
        - Select the encrypted file (with the extension .p7m).
- A message box opens showing the status of the signature / encryption.