# Exercise Sheet 0x03

## PSI-AdvaSP-M: Advanced Security and Privacy

Privacy and Security in Information Systems Group

*By Isabell Sailer (1863490),*
*Tobias Schwartz (1738195),*
*Barbara Hoffmann (1759786),*
*Sascha Riechel (1740803)*

The code that we received through the encrypted and signed email: **8eWsDoonqXrYzWU.**

### OpenPGP

Since I use Windows 10 as an operating system, I had to install a software for creating a PGP key pair. The software that I used in this case was GPG4Win, which is an open source privacy and encryption software[1]. After installing the software, I could create a new keypair with the GPG4Win GUI Kleopatra, by opening the assistant for creating a new keypair. I chose RSA 2048 Bit encryption and set an expiration date on the 04.01.2019 (see fig. 1).

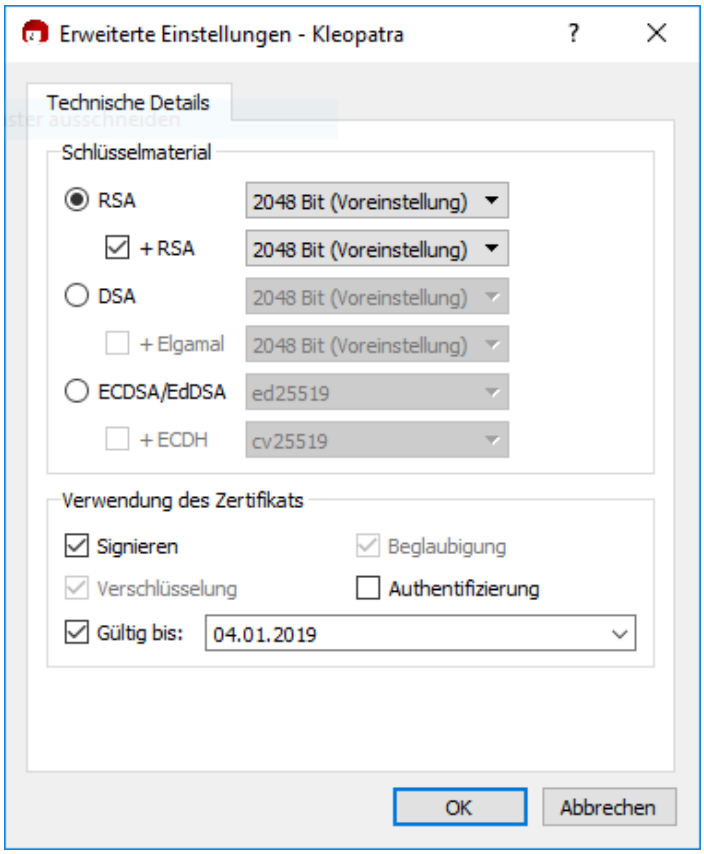
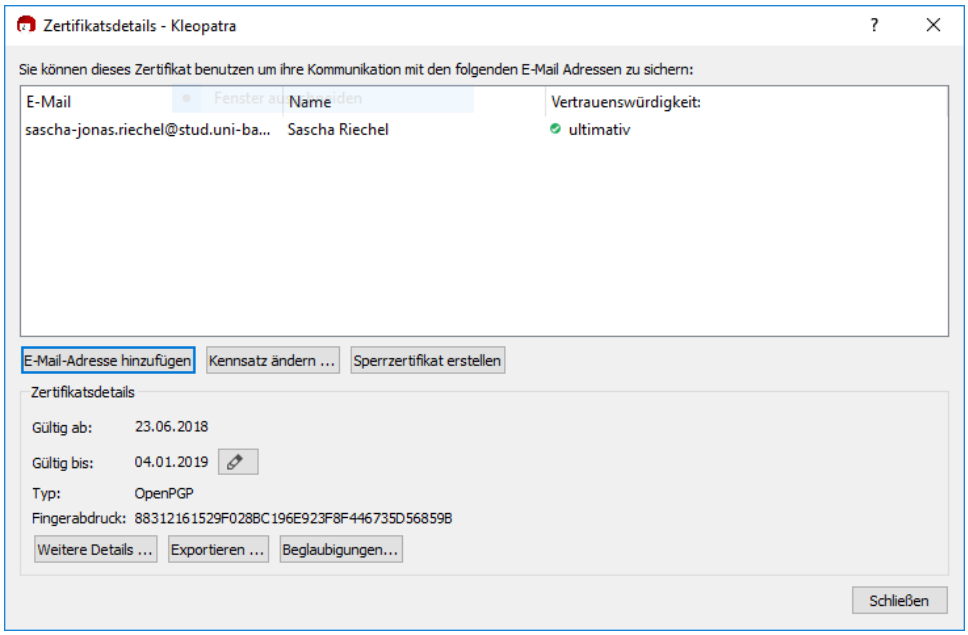


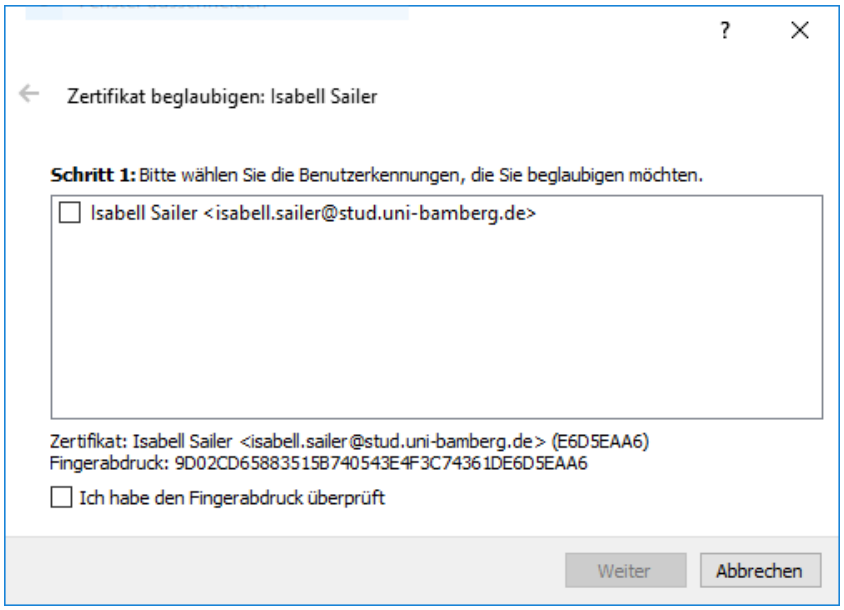

*Figure 1 Settings for OpenPGP key generation*

[1] https://www.gpg4win.org/

To create a revocation certificate, the generated Key has to be right-clicked in the Kleopatra key list and “details” should be selected. There, the option “Sperrzertifikat erstellen” (create revocation) needs to be clicked and the passphrase for the key and the output file has to be entered.




To sign the keys of the other group members, we send around our keys and signed them by importing the keys into Kleopatra, right-clicking the key to be signed and choose “Beglaubigen…” (sign). Then you need to verify that you have checked the fingerprint of the chosen public key and sign it finally by entering the own private key passcode.




When all keys have been signed, an email can be encrypted and signed with the use of the GPGol Outlook Plugin.

**S/MIME**

To get a certificate from the computer center, the following manual has to be followed:

https://www.uni-bamberg.de/fileadmin/rz/zertifizierung/Outlook_zertifikat_importieren.pdf

In short, a form has to be filled out and handed in to the computer center with a personal id card.