LU06f - Dateien verschlüsseln

Mit einem Verschlüsselungsprogramm wie Kleopatra können wir Dateien verschlüsseln und signieren.

Einleitung

GPG steht für „GNU Privacy Guard“ und ist eine Open-Source-Implementierung des OpenPGP-Standards zum Verschlüsseln und Signieren von Daten und Kommunikation. Es wurde entwickelt, um die Privatsphäre und Sicherheit von E-Mails und anderen digitalen Nachrichten zu gewährleisten. Eine Reihe von Verschlüsselungsprogrammen implementieren GPG und bieten eine einfache Benutzeroberfläche an. Dabei sollte das Programm folgende Funktionen bieten:

- Dateien verschlüsseln und entschlüsseln,
- Dateien signieren und Signaturen prüfen,
- Verwaltung der Public- und Private-Keys.

Kleopatra (GPG4Win)

Für Windows bietet sich die Verwendung von Kleopatra an. Das Programm wird als Teil von Gpg4win installiert. Möglicherweise haben Sie Gpg4win bereits zum Verschlüsseln Ihrer Emails in Outlook installiert. In diesem Fall können Sie die nächsten zwei Schritte überspringen.

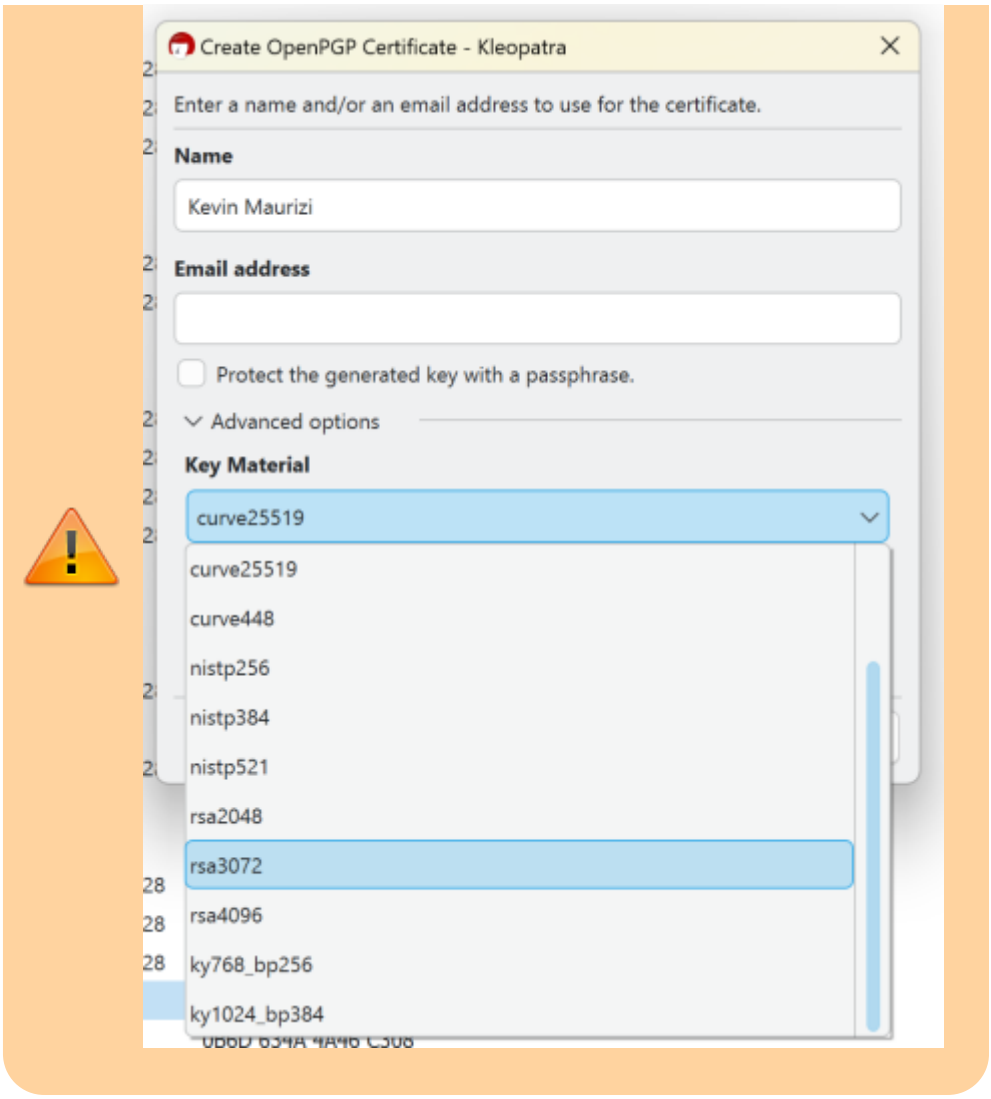
Installation und Konfiguration

Falls Sie Gpg4win noch nicht installiert haben, können Sie es herunterladen und die Installation starten (siehe https://www.youtube.com/watch?v=UYGzRbhmbhI. Bei der Auswahl der Komponenten müssen Sie **Kleopatra** auswählen.

Eigenes Schlüsselpaar erzeugen

Als Erstes benötigen Sie ein Schlüsselpaar (Public- und Private-Key).

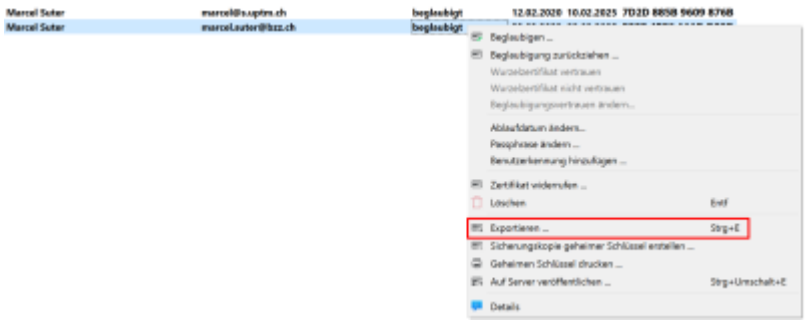
Verwenden Sie beim Erzeugen des Schlüsselpaars den RSA-Algorithmus. Gehen Sie dazu in die **Erweiterten Einstellungen** und kontrollieren Sie die Auswahl.



Schlüssel austauschen

Public Key exportieren

Um verschlüsselte und signierte Dateien auszutauschen, benötigen beide Parteien den Public Key des jeweiligen Gegenübers. Dazu müssen Sie zunächst Ihren Public Key exportieren. Machen Sie einen Rechtsklick auf Ihren Schlüssel (**fett** angezeigt) und wählen Sie „exportieren …“

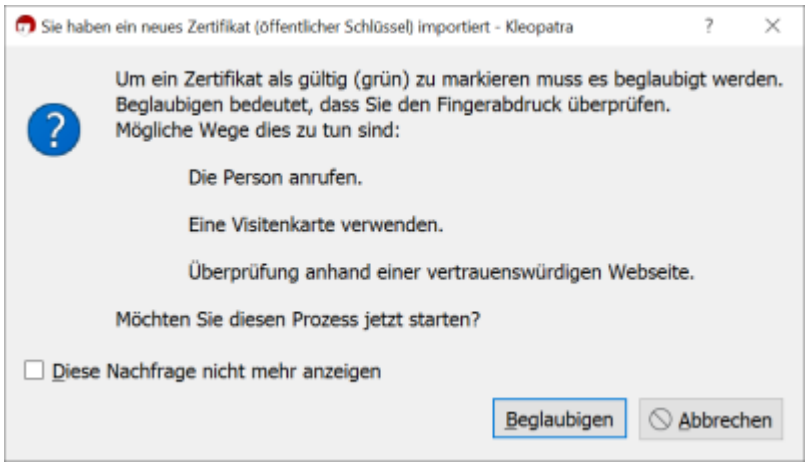


Speichern Sie die Datei. Nun können Sie diese Datei via Email, Teams, … an Ihren Partner senden.

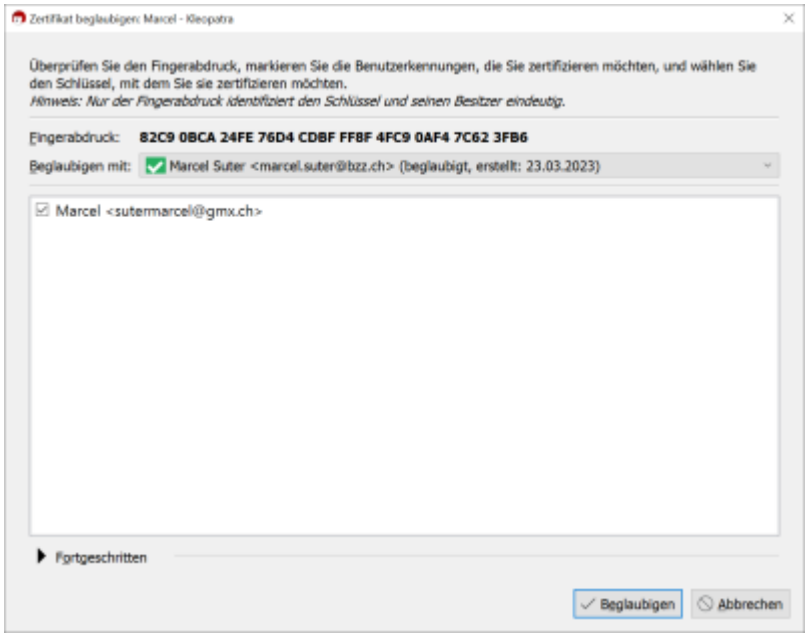
Public Key des Partners importieren

Nachdem Sie den Public Key Ihres Partners erhalten haben, können Sie diesen Importieren. Im Menu „Datei“ wählen Sie „Importieren …“ und wählen die Datei mit dem Public Key aus.

Nach dem Import werden Sie gefragt, ob Sie das Zertifikat beglaubigen möchten. Machen Sie dies nur, wenn Sie die Herkunft und Identität des Zertifikats auf einem separaten Weg überprüft haben.



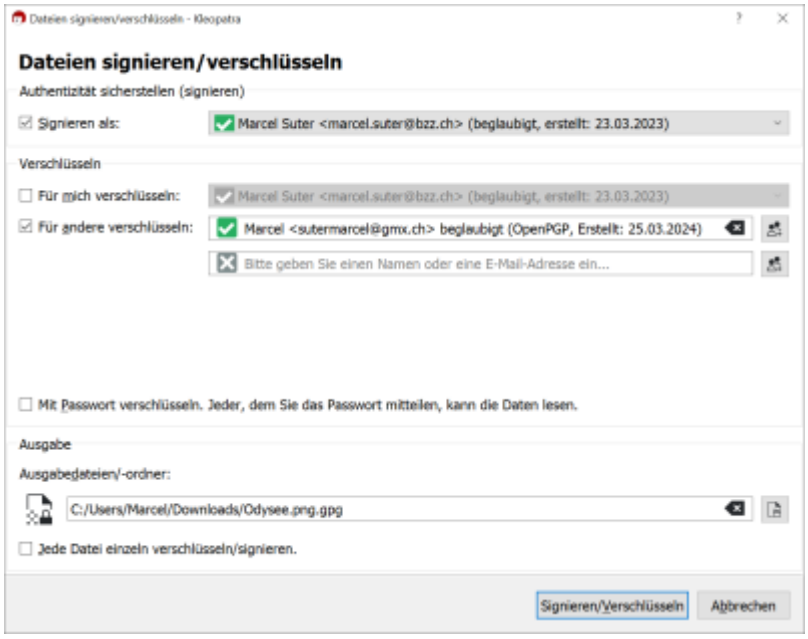
Um den Schlüssel zu beglaubigen, müssen Sie Ihren Private Key auswählen.



Dateien verschlüsseln und signieren

Über „Signieren/Verschlüsseln“ können Sie nun beliebige Dateien verschlüsseln und signieren.

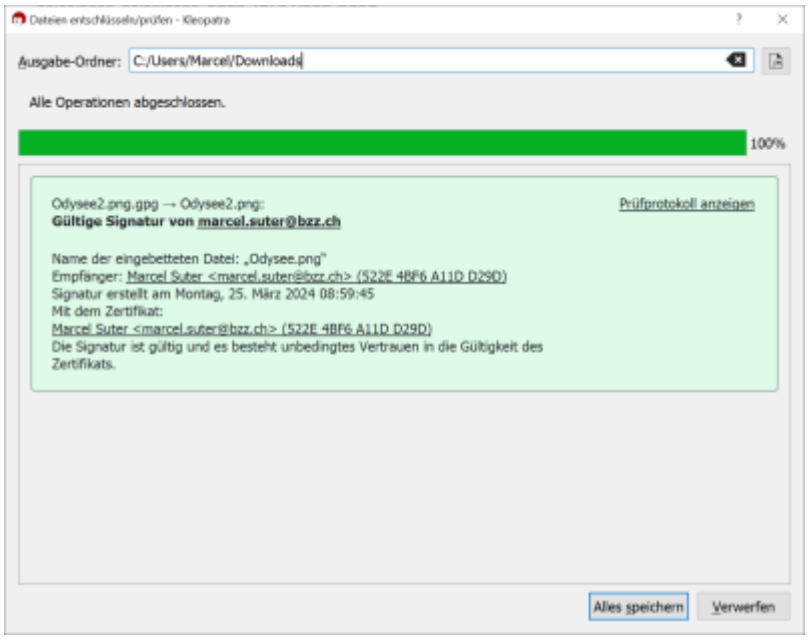
- Signieren Sie die Datei mit Ihrem Private Key.
- Wählen Sie den Public Key Ihres Partners zum Verschlüsseln aus.
- Ob Sie die Datei auch mit dem eigenen Key verschlüsseln, hängt von der Verwendung der Datei ab. Falls Sie die Datei selber nicht mehr entschlüsseln müssen, können Sie das Häkchen bei „Für mich selber verschlüsseln:“ entfernen.



Senden Sie nun die verschlüsselte und signierte Datei an Ihren Partner.

Datei entschlüsseln und Signatur prüfen

Über „Entschlüsseln/Prüfen“ können Sie die Datei Ihres Partners entschlüsseln und die Signatur prüfen. Wählen Sie die Datei aus und das Programm zeigt Ihnen an, ob die Signatur stimmt.



---

m114-A0G