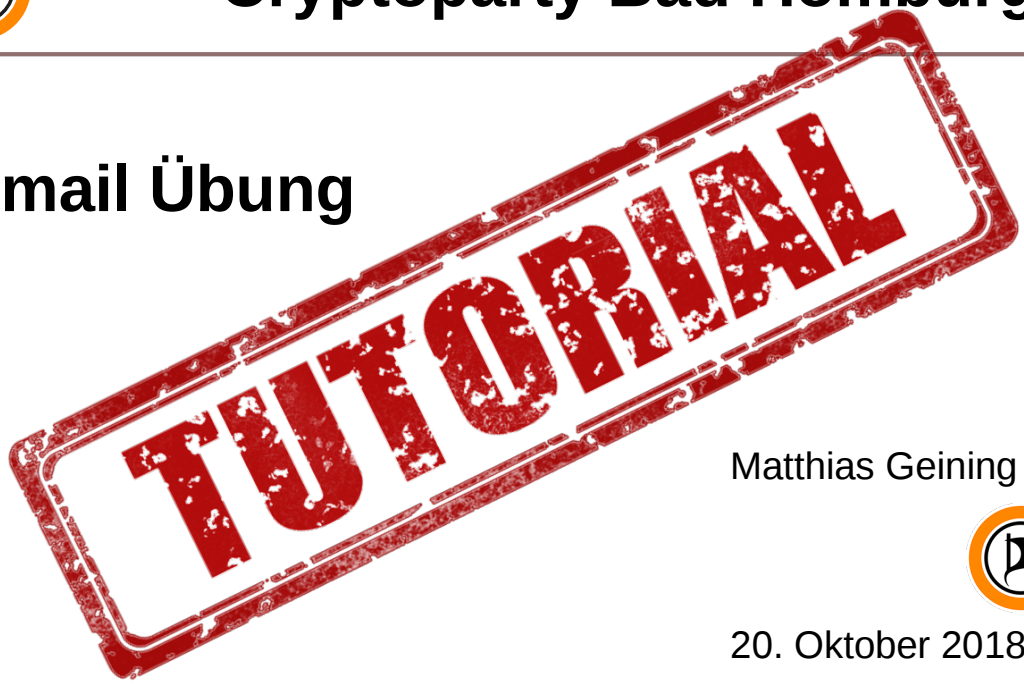
Cryptoparty Bad Homburg

Email Übung



Matthias Geining &

PIRATENPARTEI
KV Hochtaunus- & Main-Taunus-Kreis

20. Oktober 2018, Bad Homburg

Ziel

- GPG benutzen
- Eigenes Schlüsselpaar erzeugen
- Schlüssel im- und exportieren
- Mail verschlüsseln und unterschreiben
- Mail entschlüsseln und Sender überprüfen

Voraussetzung

- Mail Programm ist installiert
  - Thunderbird und/oder
  - Outlook
- Email Adresse ist angelegt
  - Dummy Adresse ist ok
- Passwort ist bekannt
- Email abholen funktioniert mit Thunderbird und/oder Outlook
  - POP/IMAP konfiguriert beim Provider
    bei z.B. web.de, google.com muss POP/IMAP eingeschaltet sein
  - POP/IMAP lokal konfiguriert und getestet

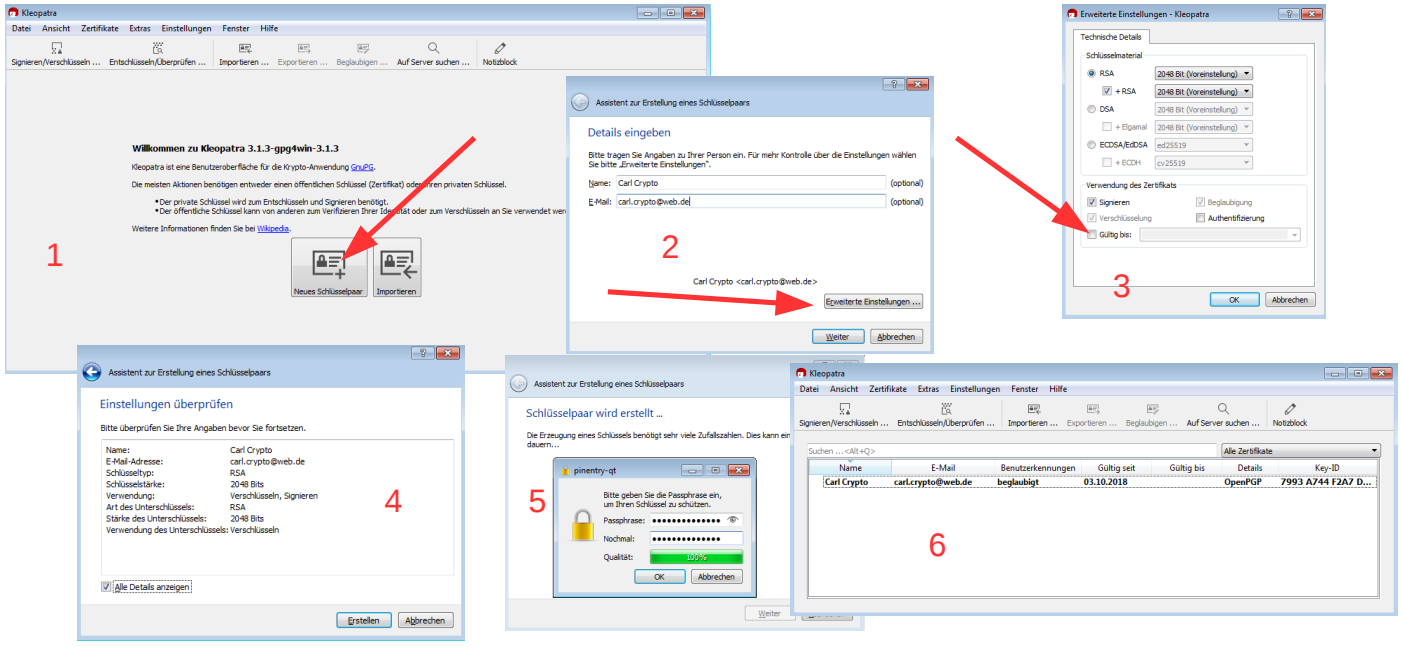
Download

- Gpg4Win
  https://www.gpg4win.org/
- EnigMail
  https://www.enigmail.net/index.php/en/

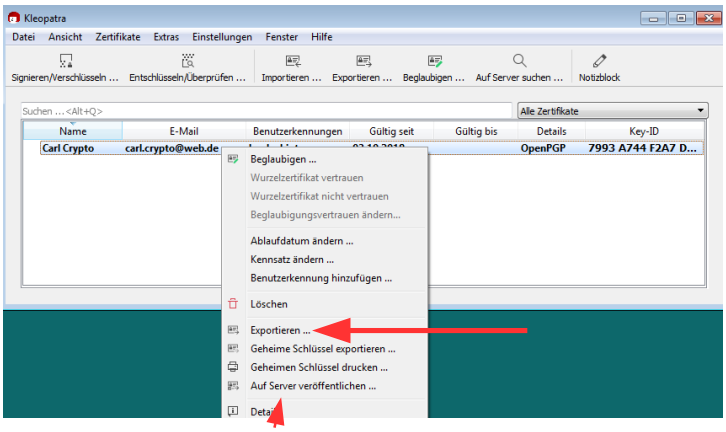
Gpg4Win installieren

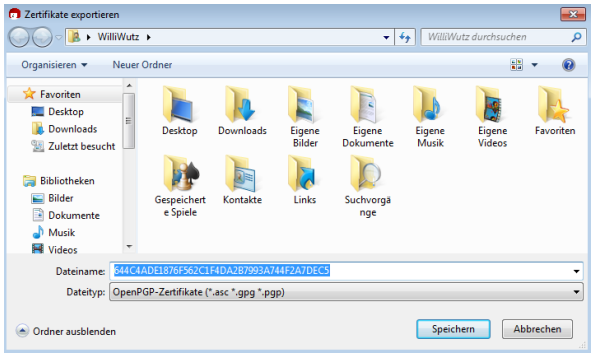
Eigenen Schlüssel erzeugen

(öffentlich und privat)



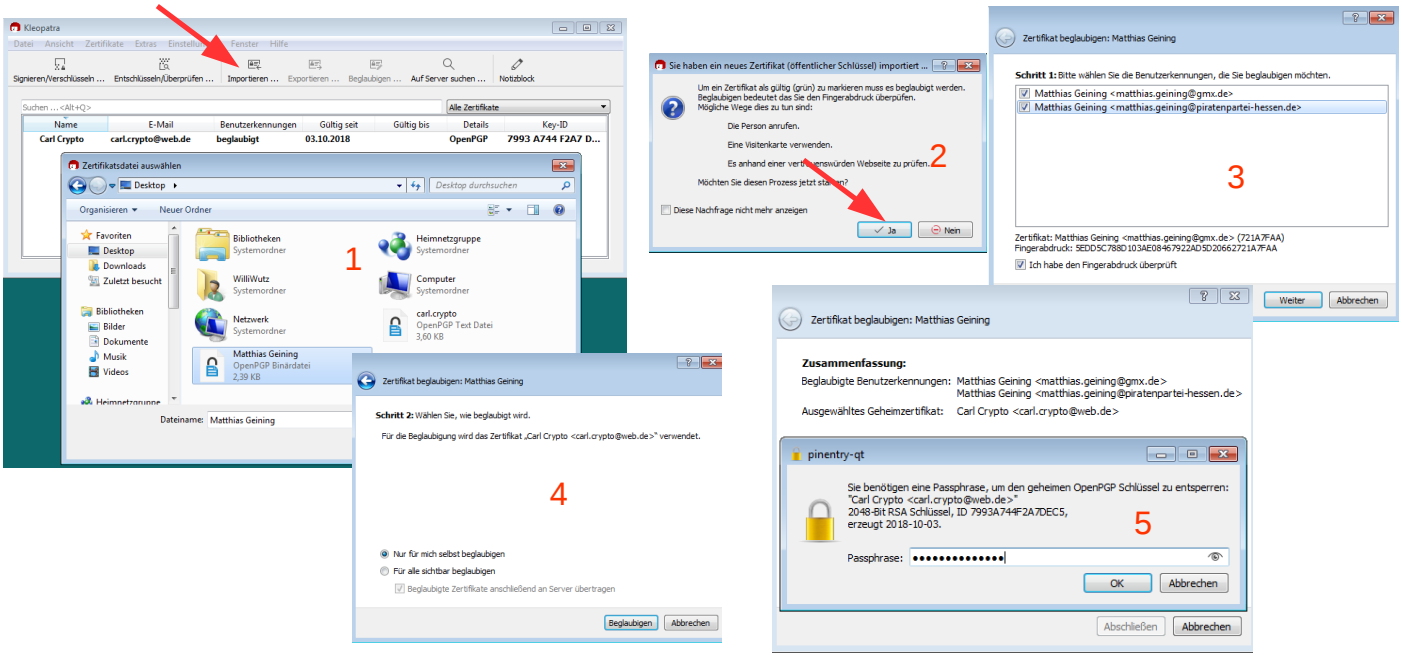
Eigenen öffentlichen Schlüssel exportieren



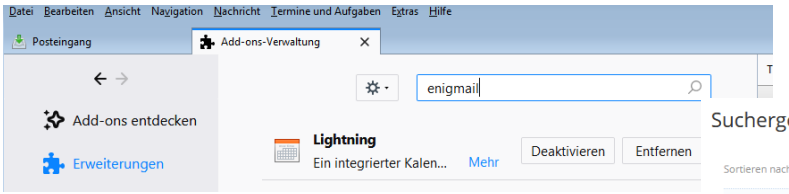


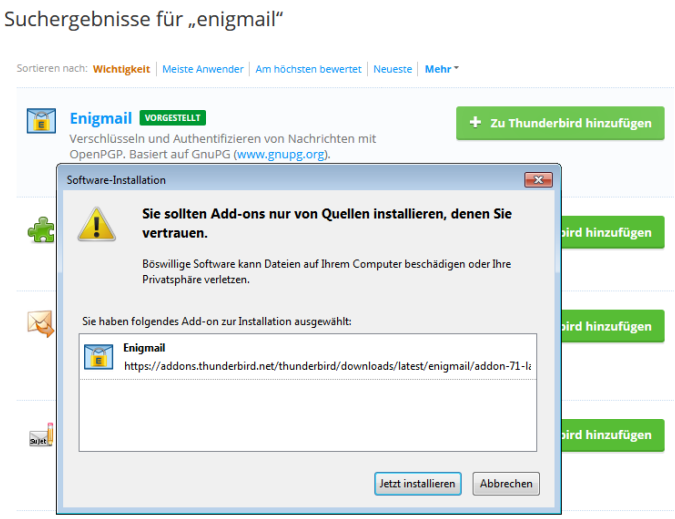
Frage: Was bedeutet „Auf Server veröffentlichen ...“

Fremden öffentlichen Schlüssel importieren



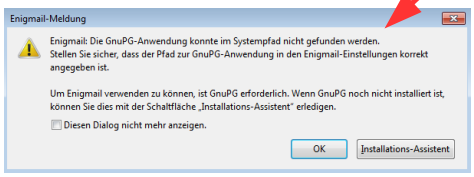
EnigMail installieren



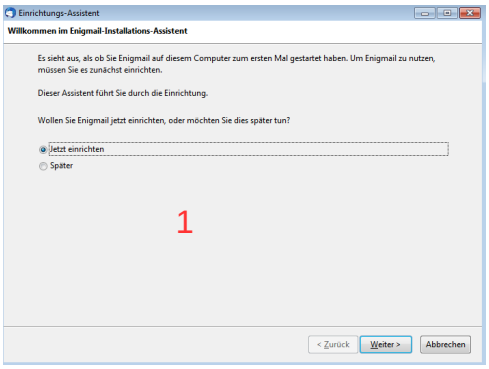


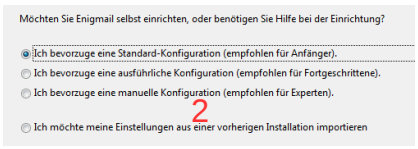
- Thunderbird starten
- Extras → Add-On
- Erweiterungen → EnigMail suchen
- EnigMail zu Thunderbird hinzufügen

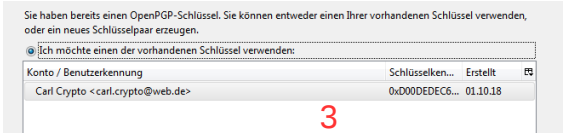
- EnigMail installiert fehlenden Komponenten automatisch
  - GnuPG bzw. gpg4win installieren
  - EnigMail Installationsassistent pausieren, bis gpg4win installiert ist

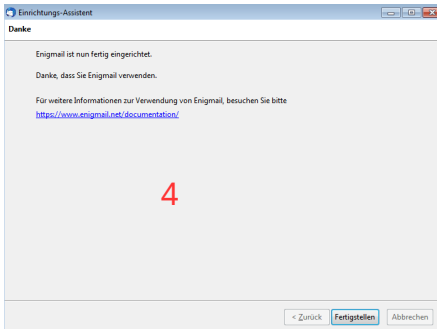


EnigMail Einrichtungsassistent



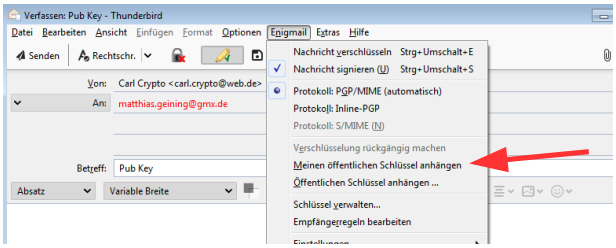






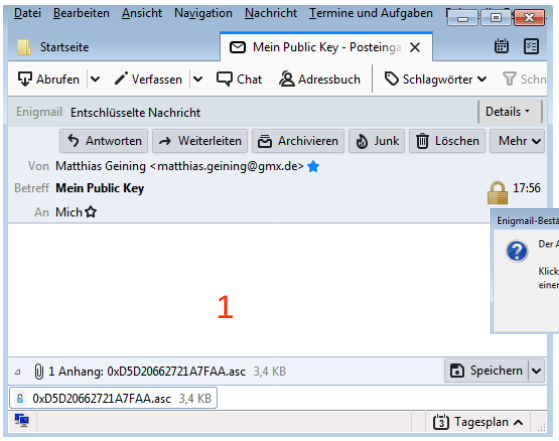
Eigenen öffentlichen Schlüssel verschicken

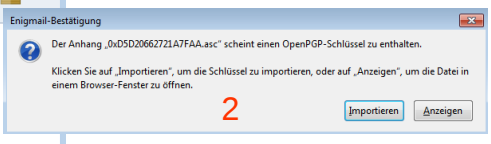
- Neue Mail erstellen
- Eigenen öffentlichen Schlüssel anhängen



Fremden öffentlichen Schlüssel importieren

Mail mit Thunderbird öffnen



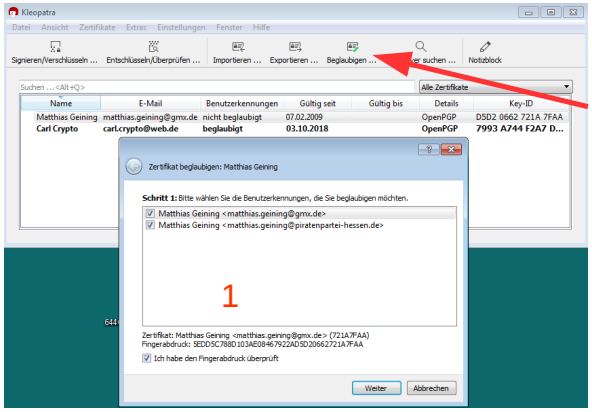


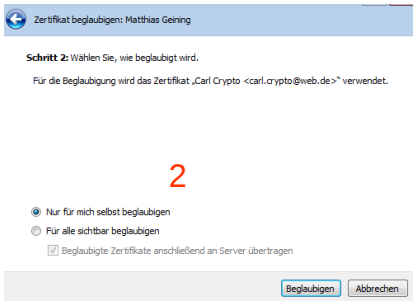
Fingerabdruck verifizieren mit dem Besitzer des öffentlichen Schlüssels

- z.B. telefonisch, auf einer Webseite, persönlich
- Nicht Email, sondern anderes Kommunikationsmittel benutzen

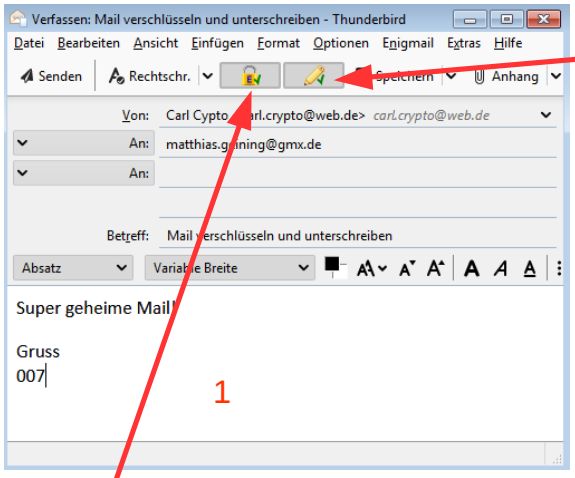
Fremden öffentlichen Schlüssel beglaubigen

Kleopatra starten



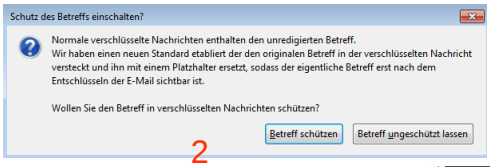


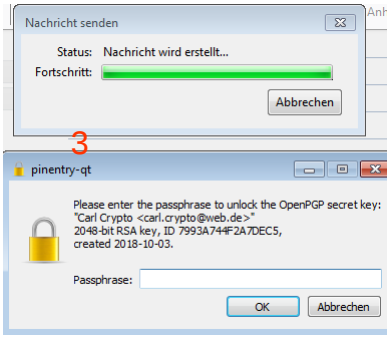
Mail verschlüsseln und unterschreiben



Unterschreiben

Verschlüsseln

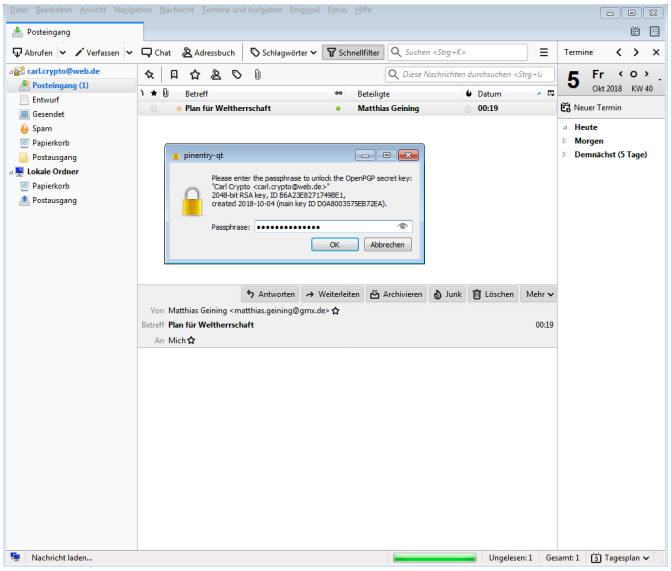


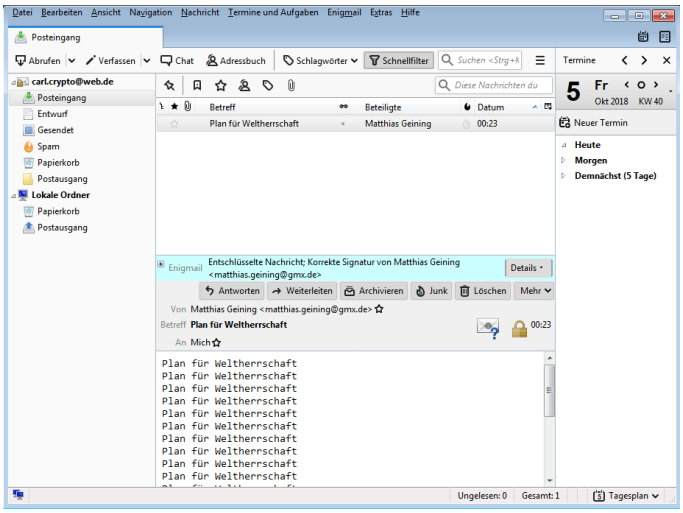


Verschlüsseln und Unterschreiben sind unabhängig voneinander

- Verschlüsseln ohne unterschreiben → geht
- Unterschreiben ohne verschlüsseln → geht auch

Mail entschlüsseln und Unterschrift prüfen

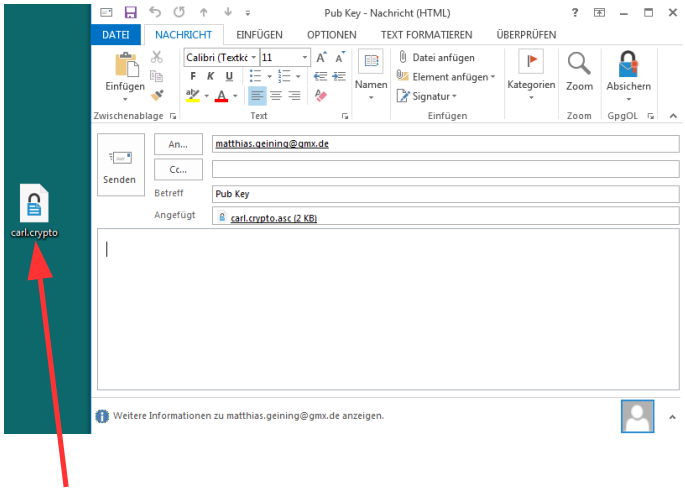




GnuPG unter Outllook

- Outlook muss installiert sein
- Gpg4Win installieren (wie vorher beschrieben)
- Anschließend eigenen Schlüssel erzeugen (öffentlich und privat) (wie vorher beschrieben)
- Eigenen öffentlichen Schlüssel exportieren (wie vorher beschrieben)
- Outlook starten

Eigenen öffentlichen Schlüssel versenden

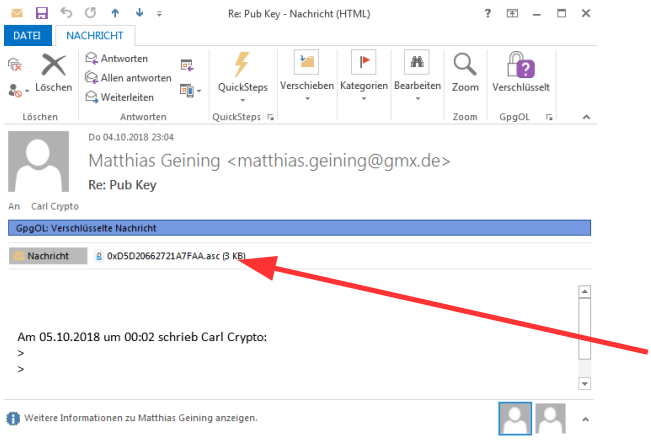


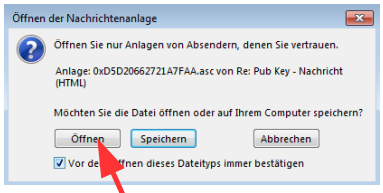
- Neue Mail erstellen
- Eigenen öffentlichen Schlüssel anhängen

Eigenen öffentlichen Schlüssel an Mail anhängen

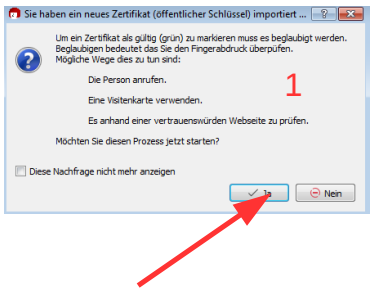
Frage: Könnten auch andere öffentliche Schlüssel anhangen werden und macht das Sinn?

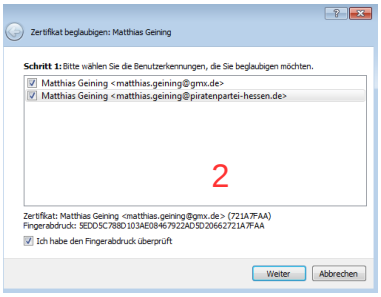
Fremden öffentlichen Schlüssel importieren

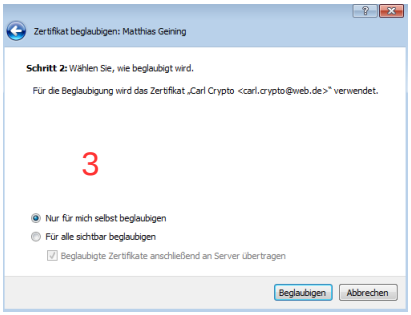


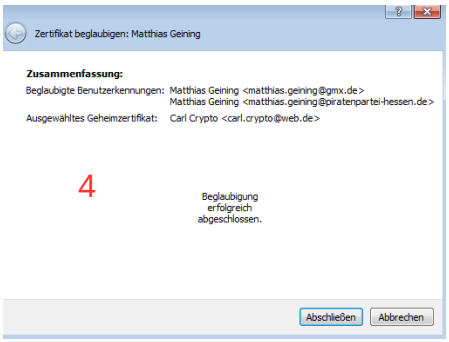


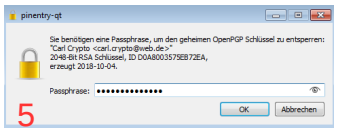
Fremden öffentlichen Schlüssel importieren



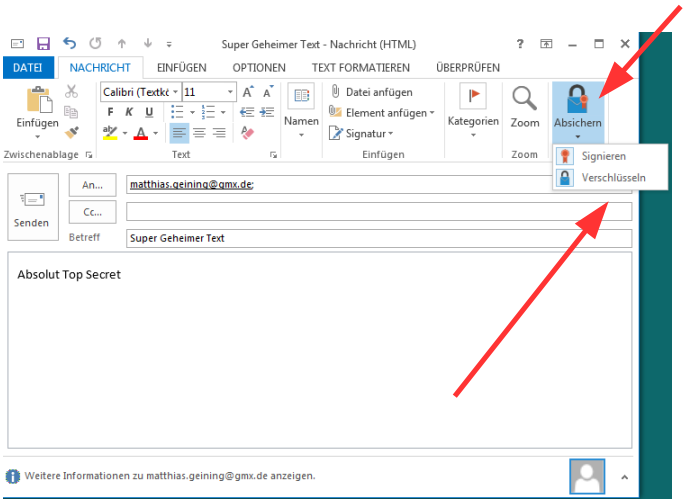


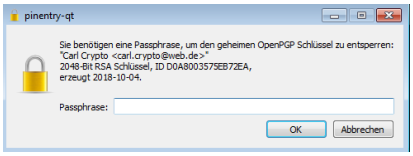






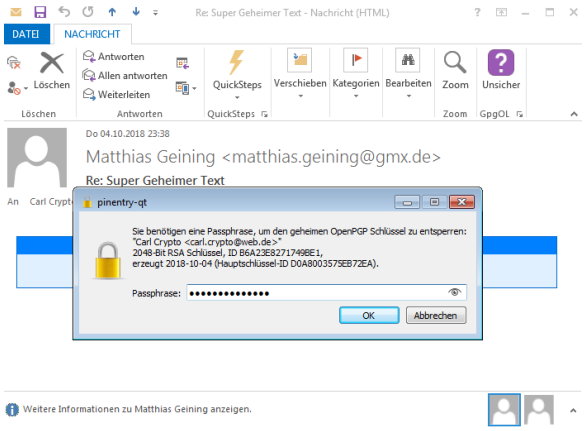
Mail verschlüsseln und unterschreiben

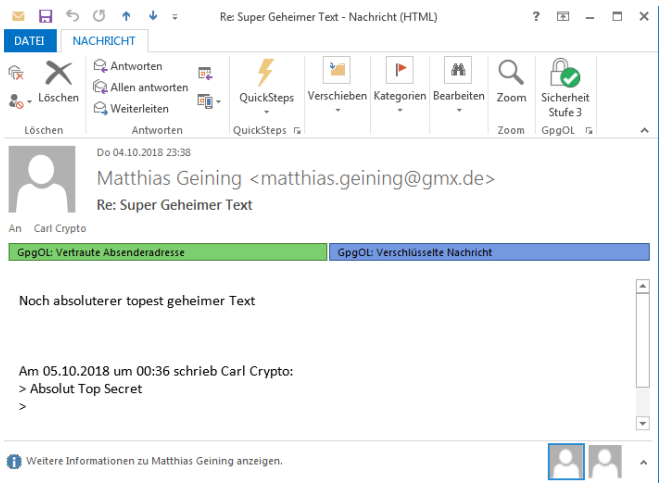




Frage: Wenn ich nur verschlüssele aber nicht unterschreibe, werde ich nicht nach meinem Passwort gefragt!
Warum?

Mail entschlüsseln und Unterschrift prüfen





Zum Selbermachen

- Mail mit eigenem öffentlichen Schlüssel als Anhang an edward-de@fsf.org schicken
- Antwort kommt mit eigenem Schlüssel verschlüsselt zurück
- Mail mit öffentlichen Schlüssel von edward-de@fsf.org verschlüsselt an edward-de@fsf.org schicken
- Antwort zeigt ob es geklappt hat

Weitere Infos: https://emailselfdefense.fsf.org/de/

Weitere Test Adresse: adele@gnupp.de

Cryptoparty Bad Homburg

Kontakt:	Matthias Geining
eMail:	matthias.geining@gmx.de
PGP Fingerprint:	5EDD 5C78 8D10 3AE0 8467 922A D5D2 0662 721A 7FAA
Messager:	Signal, Telegram, kein WhatsUp