# Installation und Einrichtung des GnuPG-Verschlüsselungs-Programms (Dateien / E-Mails)

Bei dem GnuPG-Verschlüsselungsprogramm handelt es sich um eine freie Implementierung des OpenPGP-Verfahrens, das als eines der Standard-Verfahren im E-Mail-Bereich gilt und das eine sehr sichere Verschlüsselung von E-Mails ermöglicht. Dieses Programm ist eigentlich "stand-alone", d. h. es kann völlig autark Dateien verschlüsseln und signieren. Aber es ist auch möglich, über die mittlerweile realisierten PlugIn-Programme z. B. für den Mozilla Thunderbird (Enigmail-PlugIn) oder Microsoft Outlook (GpgOL-PlugIn) diese Verschlüsselung schnell und elegant für E-Mails zur Verfügung zu stellen. Im Folgenden soll die Vorgehensweise beschrieben werden, wie das Programm eingerichtet und konfiguriert werden kann.

## 1. Grundlagen der Verschlüsselung

Damit eine Verschlüsselung erfolgreich funktionieren kann, muss jeder Teilnehmer über 2 Schlüssel verfügen, die sich gegenseitig ergänzen:

- einen öffentlichen Schlüssel, der einmal mit den Partnern ausgetauscht werden muss (dabei ist es völlig in Ordnung, diesen Schlüssel per nicht verschlüsselter E-Mail auszutauschen!)
- einen geheimen Schlüssel (der bitte auch WIRKLICH GEHEIM bleiben muss!)

Diese beiden Schlüssel "ergänzen" sich, d. h. wurde ein Text mit dem öffentlichen Schlüssel verschlüsselt, so lässt er sich nur noch mit dem geheimen Schüssel entschlüsseln. Das Gleiche gilt jedoch auch umgekehrt: Ein Text, der mit dem geheimen Schlüssel verschlüsselt wurde, kann nur mit dem öffentlichen Schlüssel wieder entschlüsselt werden (z. B. für eine elektronische Unterschrift).

Will man eine verschlüsselte E-Mail an einen Partner schicken, so wird der öffentliche Schlüssel des Partners verwendet, um die E-Mail zu verschlüsseln. Anschließend kann die E-Mail noch signiert werden, d. h. es wird eine elektronische Unterschrift, die mit dem geheimen Schlüssel des Absenders erstellt wurde, angehängt. Danach kann die E-Mail verschickt werden.

Trifft diese nun beim Empfänger ein, so kann dieser anhand des öffentlichen Schlüssels des Absenders feststellen, dass der Absender korrekt ist. Danach wird der E-Mail-Inhalt mit dem geheimen Schlüssel dechiffriert und kann gelesen werden.

### 2. Download und Installation von GnuPG

Das Programm GnuPG ist unter allen gängigen Plattformen (Windows, Linux, Mac OS X, Android) auf <a href="https://www.gnupg.org/">https://www.gnupg.org/</a> verfügbar; stellvertretend soll hier die Windows-Variante beschrieben werden, die unter <a href="https://gpg4win.org/download.html">https://gpg4win.org/download.html</a> heruntergeladen werden kann. Zum Berichtszeitpunkt war die aktuelle Version <a href="https://gpg4win.org/download.html">Gpg4win 3.1.0 (Released: 2018-04-13)</a>) verfügbar.

Nach dem Download der Datei und dem Start des Installationsprogramms wird man mit folgendem Fenster zum Auswählen der Sprache begrüßt:



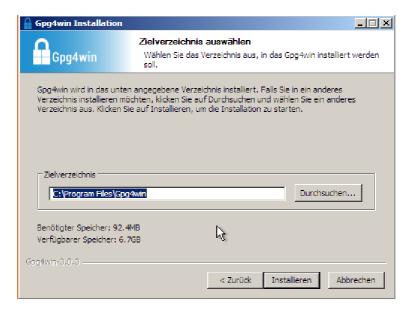
Nach der Sprachauswahl erscheint das Fenster



das mit Klick auf "Weiter" beantwortet werden kann. Die Auswahl der zu installierenden Komponenten ist ausreichend und kann unverändert übernommen werden:



Auch der Installationspfad kann in der Regel unverändert übernommen werden:

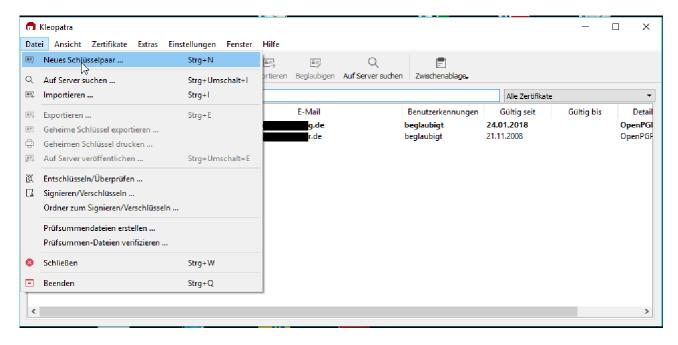


womit die Installation mit den folgenden Schritten abgeschlossen werden kann:



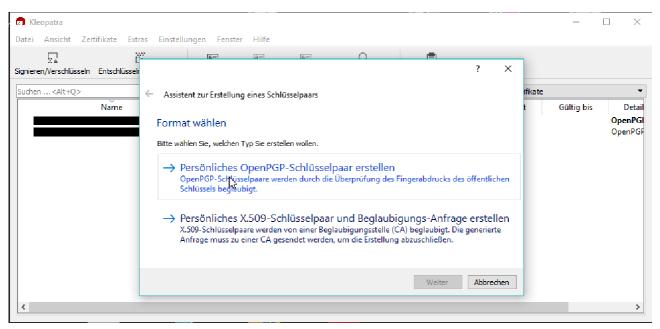
# 3. Erzeugung der eigenen Schlüsselpaare

Anschließend wird das Programm Kleopatra, das von Gpg4Win installiert wurde, gestartet, das dem Anwender die Schlüsselverwaltung ermöglicht:

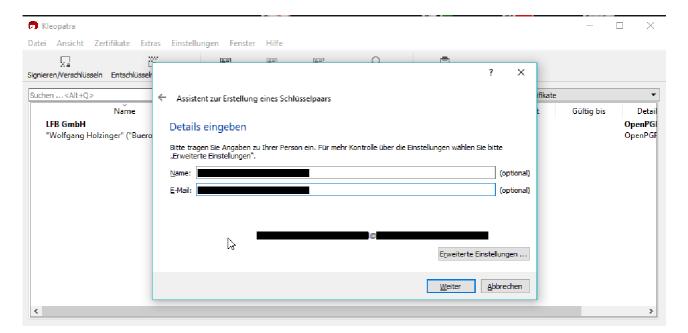


Mit diesem Programm kann ein Benutzer seinen persönlichen "Schlüsselbund" verwalten, d. h. er erhält eine Liste der bereits gespeicherten Schlüssel. Daneben können neue Schlüssel erzeugt und die Schlüssel von Partnern importiert werden.

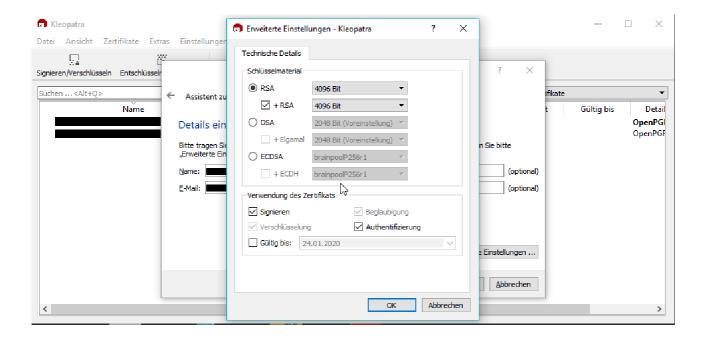
Zunächst soll jedoch ein neues OpenPGP-Schlüsselpaar erzeugt werden, um eine Kommunikation per E-Mail zu ermöglichen:



Dazu sollte Ihr Name und die mit dem Schlüssel verbundene E-Mail eingegeben werden:

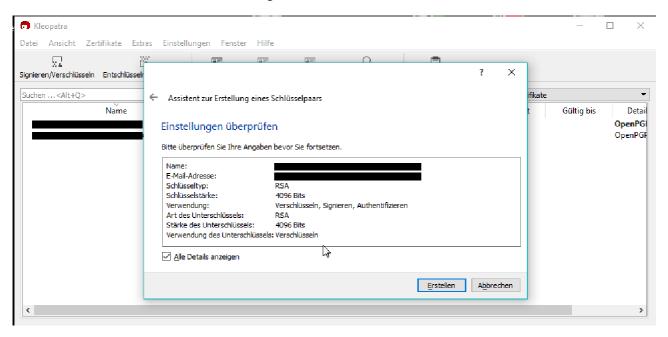


Mit dem Klick auf den Button "Erweiterte Einstellungen ..." kann ein Zusatzmenü geöffnet werden, mit dem man die folgenden Parameter einstellen kann:

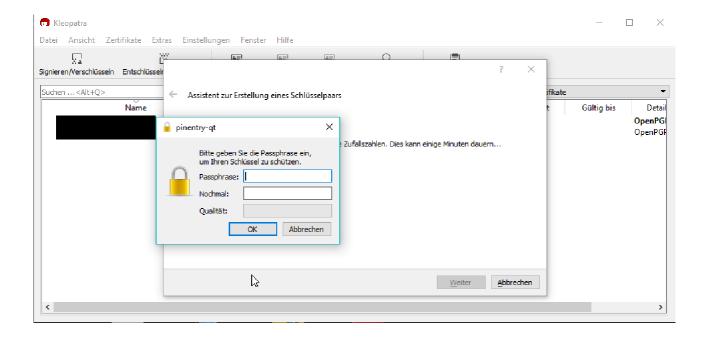


Anmerkung: Eine Schlüssellänge von 4096 Bit ist schon recht lang, bedeutet aber einen erheblichen Sicherheitsgewinn. Und wer weiß schon, wie lange ein Schlüssel verwendet wird, falls kein Ablaufdatum eingegeben wird ...

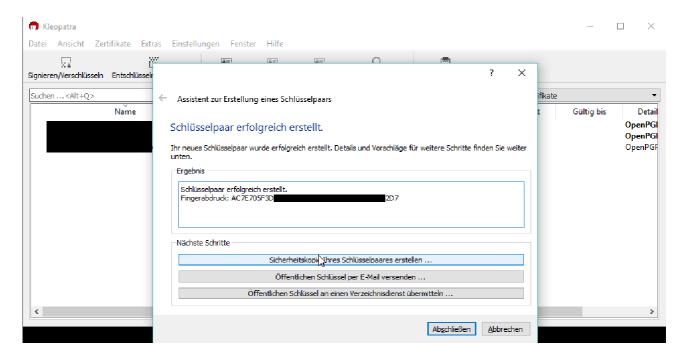
Nach einer letzten Kontrolle der Einstellungen ...



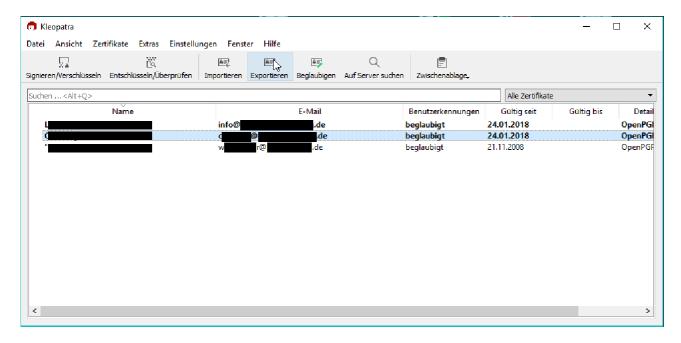
... kann ein Zugangspasswort bzw. Passphrase (bitte merken Sie sich dieses Kennwort und halten Sie es geheim!) für den Schlüsselbund vergeben werden ...



... womit die Schlüsselerzeugung beendet wird:



Zuletzt sollte die aktuelle Schlüsselliste - um den neuen Schlüssel ergänzt - angezeigt werden ...



... womit einer sicheren und verschlüsselten E-Mail-Übermittlung nichts mehr im Weg stehen sollte.

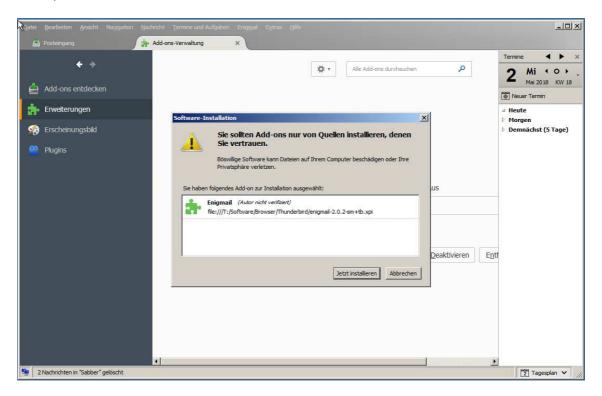
## 4. Verschlüsseltes E-Mailing

Im Folgenden soll anhand der beiden Programme Mozilla Thunderbird und Microsoft Outlook kurz gezeigt werden, wie die Verschlüsselung genutzt werden kann.

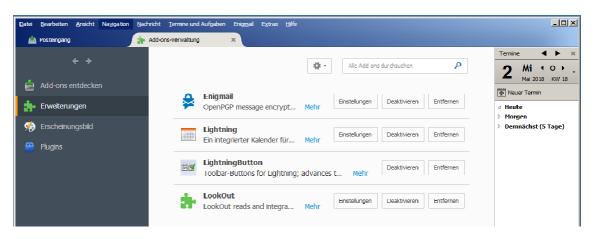
### 4.1. Mozilla Thunderbird

Bei diesem Programm handelt es sich um ein E-Mail-Programm der Mozilla Foundation, das mittlerweile auf allen gängigen Plattformen verfügbar ist und das über zahlreiche PlugIns erweitert werden kann.

Zum Verschlüsseln mittels GnuPG benötigt der Thunderbird das Enigmail-PlugIns (Download unter <a href="https://www.enigmail.net/index.php/en">https://www.enigmail.net/index.php/en</a> oder aber Installation direkt über die Add-On-Verwaltung des Thunderbird):



Nach einem Neustart wird dann das Enigmail-Plugin im Add-On-Menü in der Liste der Erweiterungen angezeigt:

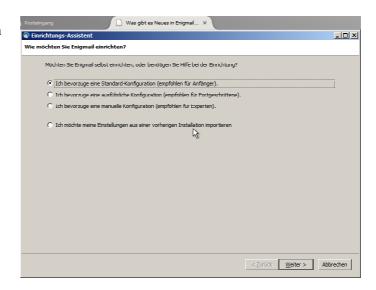


Nun muss das Enigmail-Plugin konfiguriert werden: Im Hauptmenü existiert jetzt der Menüeintrag "Enigmail", in dem es den "Einrichtungsassistenten" gibt, der die Basiskonfiguration ermöglicht:



Was gibt es Neues in Enigmail v2.0?

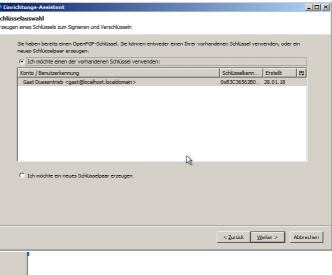
Hier reicht es, die Standard-Konfiguration durchzuführen, ...



... die den über Kleopatra erzeugten Schlüssel erkennen und verarbeiten kann, ...

Einrichtungs-Assiste

Enigmail ist nun fertig eingerichtet.

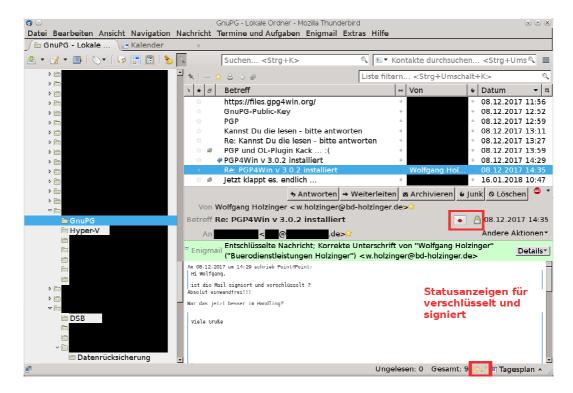


Danke, dass Sie Frigmail verwenden.

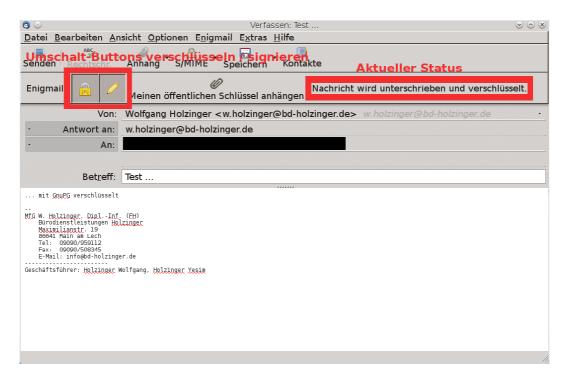
Für weitere Informationen zur Verwendung von Enigmail, beauchen Sie bitte https://www.enigmail.net/documentation/

... womit dann die Basiskonfiguration bereits abgeschlossen ist.

Damit ist die Installation von Enigmail abgeschlossen und es kann im Thunderbird eine Verschlüsselung mittels GnuPG realisiert werden:

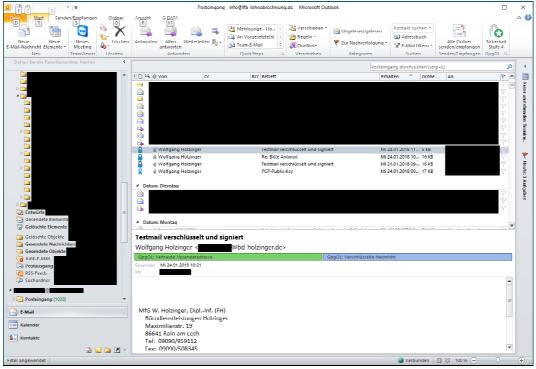


Beim Eingeben einer neuen E-Mail wird eine Statusleiste dargestellt, mit der man die Mail sowohl verschlüsseln als auch signieren kann. Zusätzlich wird der Status als "Button gedrückt" und im Beschreibungstext angezeigt.



#### 4.2. Microsoft Outlook

Auch für das bekannte MS-Outlook ist mittlerweile ein PlugIn verfügbar, der die Nutzung von GnuPG stark vereinfacht. Im Posteingang kann man die verschlüsselten E-Mails am "Vorhängeschloss" erkennen. Nach Eingabe des Schlüsselbund-Passworts wird die entschlüsselte E-Mail im Klartext angezeigt:



Will man jetzt eine neue E-Mail erstellen, dann wird das Vorhandensein des GpgOL-PlugIns in der Ribbons-Leiste rechts angezeigt. Mit diesem neuen Button kann man eine E-Mail verschlüsseln und signieren:

