HAWK Fakultät Ingenieurwissenschaften und Gesundheit Göttingen

PGP Mailverschlüsselung

1. Was ist PGP und wie funktioniert PGP-Mailverschlüsselung?

PGP steht für Pretty Good Privacy und kann zum Signieren und Verschlüsseln von Mails verwendet werden. Durch PGP wird sichergestellt, dass nur der Sender und Empfänger sicherheitsrelevante Daten, welche per E-Mail versendet werden, lesen können. Dafür wird von jedem Nutzer durch ein Programm ein Schlüsselpaar erstellt. Dieses Schlüsselpaar besteht aus einem Public und einem Private Schlüssel. In diesem Schlüssel kann zudem der Name und die E-Mail Adresse hinterlegt werden, zu welchem der Schlüssel gehört. Abbildung 1 verdeutlicht vereinfacht gesehen die Funktionsweise von PGP (tatsächlich ist der Vorgang ein bisschen komplizierter). Der Public Key ist ein Schlüssel (2048-4096 Bit), welchen jeder kennen muss, der dem Empfänger eine verschlüsselte Nachricht senden will. Diesen Schlüssel kann man problemlos unverschlüsselt per Mail versenden oder auf einen öffentlich zugänglichen Server zur Verfügung stellen. Der Public Schlüssel wird verwendet, um mit einer mathematischen Operation die Daten unlesbar zu machen. Aus „Hallo Du“ wird zum Beispiel „AxBr26>Jsw/swß“. Nur der Empfänger kann mit seinem Private Key die Daten wieder entschlüsseln. Der Private Key ist der Key, den nur der Empfänger haben darf. Das heißt jeder Kommunikationsteilnehmer behält sein Private Key für sich. Verliert man den Private Key, kann man nicht mehr auf seine empfangenen verschlüsselten Nachrichten zugreifen. Deswegen sollte man den Schlüssel irgendwo sicher aufbewahren (Zum Beispiel auf einen nur dafür vorgesehenen USB Stick oder CD zuhause oder in der Schreibtischschublade, wo keiner drankommt). Gelangt der Schlüssel in die Hand einer anderen Person, kann diese die Nachrichten entschlüsseln. Deswegen sollte man den Private Key auch nicht auf einer Cloud o.ä. ablegen.

Wichtig zu wissen ist, der Verschlüsselungsweg ist eine Einbahnstraße. Mit dem Public Key, zum Verschlüsseln der Daten, kann die E-Mail nicht wieder entschlüsselt werden.

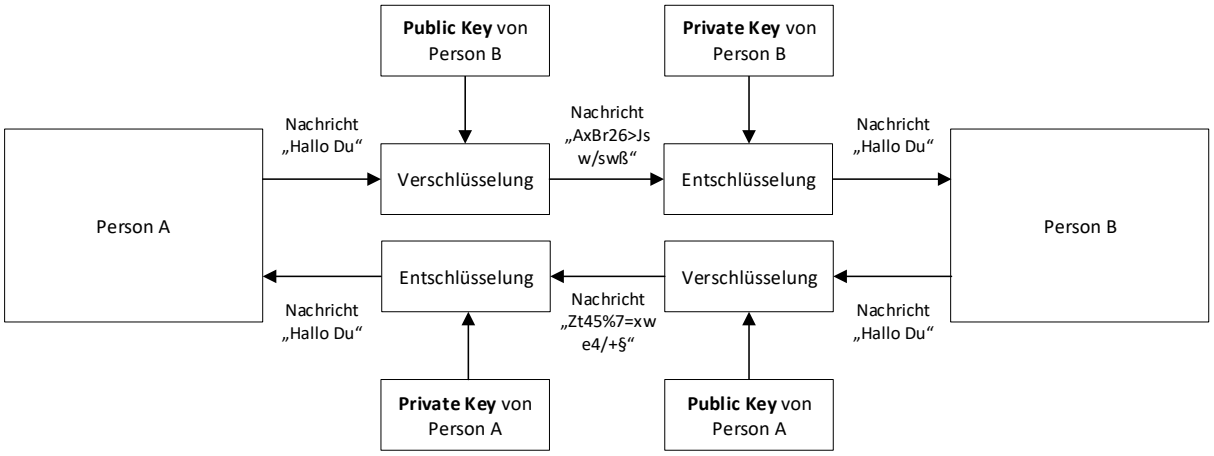


Abbildung 1: Vereinfachte Funktionsweise von PGP Mailverschlüsselung

Von Mario Hesse und Jannik Schulz

Der Key kann zum Beispiel, wie in Textfeld 1 und Textfeld 2 gezeigt, aussehen und in einer Textdatei oder Textbasierten Datei abgelegt sein. Wichtig ist hier nochmal! Den Private Key niemals irgendjemand anderem schicken. Wenn einem dies passiert, sollte man sich gleich ein neues Schlüsselpaar erstellen und den alten Schlüssel gegenüber allen Kommunikationspartnern als ungültig erklären.

Textfeld 1: Beispiel Public Key

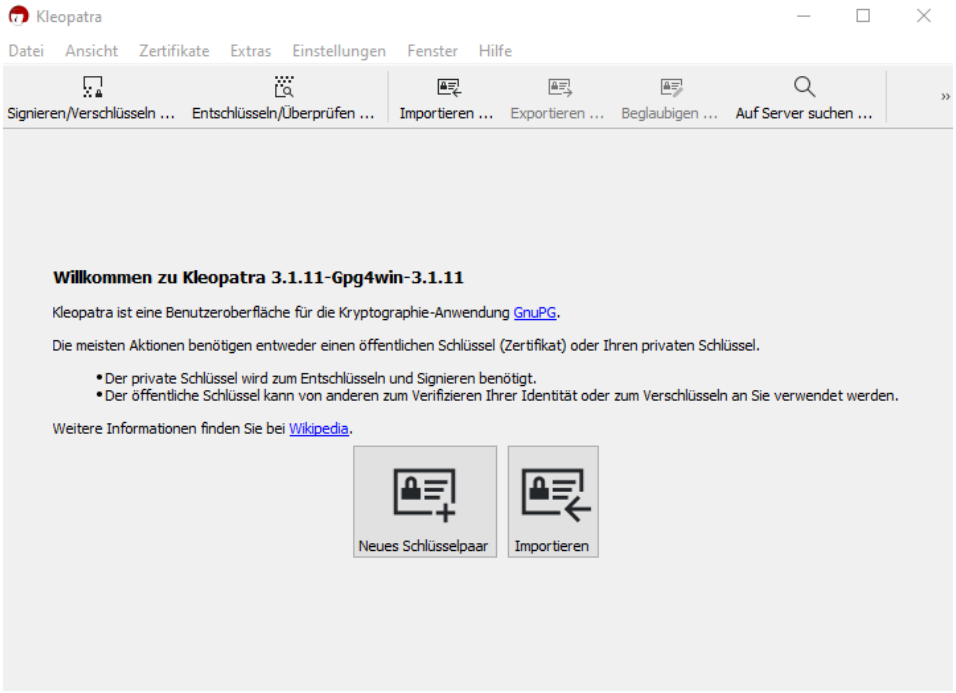
```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBF38vs8BEADLTjokLO7Bhhuy4nJQ9UyNduZZJN1BYqjWluS0i1dgChjG2EJ/
[…]
/0uDwPcOhKdIH5MBL7kmLscsNQnUYCZ6aa5a2fEyoyKVYvyWf6NSwWaNFQTn+Cz0
uHeQ3/Uph5V5EeIMS0g=
=huWO
-----END PGP PUBLIC KEY BLOCK-----
```

Textfeld 2: Beispiel Private Key

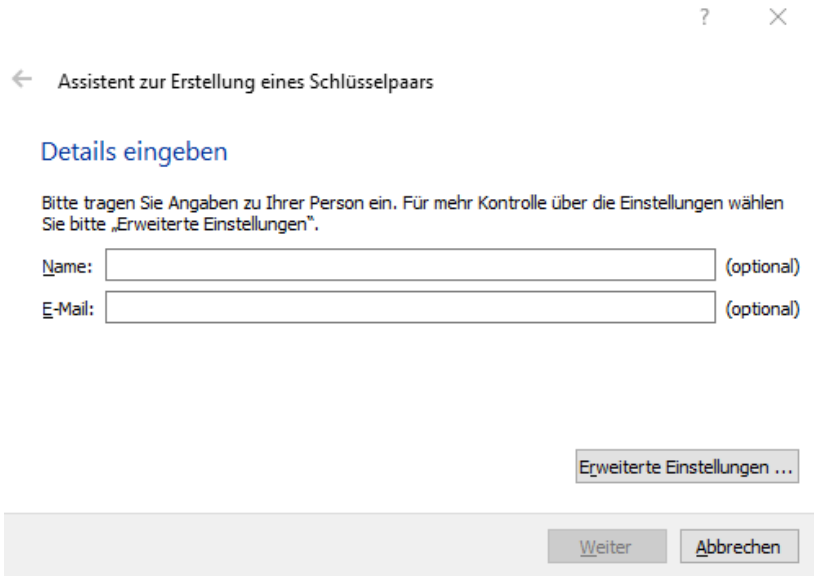
```
-----BEGIN PGP PRIVATE KEY BLOCK-----

mQINBF38vs8BEADLTjokLO7Bhhuy4nJQ9UyNduZZJN1BYqjWluS0i1dgChjG2EJ/
[…]
/0uDwPcOhKdIH5MBL7kmLscsNQnUYCZ6aa5a2fEyoyKVYvyWf6NSwWaNFQTn+Cz0
uHeQ3/Uph5V5EeIMS0g=
=huWO
-----END PGP PRIVATE KEY BLOCK-----
```

2. Anleitung zum Einrichten in Outlook und unter Windows

1. Downloaden und installieren Sie PGP4Win unter https://www.gpg4win.de/download-de.html (Behalten Sie dabei einfach alle Standardeinstellung bei der Installation bei).
2. Starten Sie das mitinstallierte Programm Kleopatra (Kleopatra ermöglichst es dem Nutzer die PGP Schlüssel zu erstellen und zu importieren und zu verwalten).
3. Wenn Sie noch kein Schlüsselpaar haben, klicken Sie auf „Neues Schlüsselpaar“

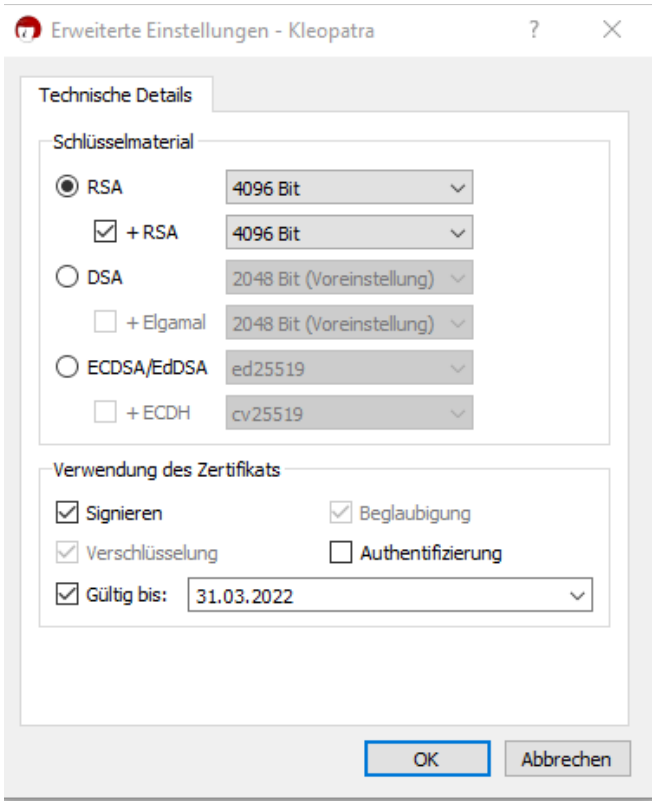


4. Tragen Sie beim aufkommenden Fernster Ihren Namen und Email Adresse ein

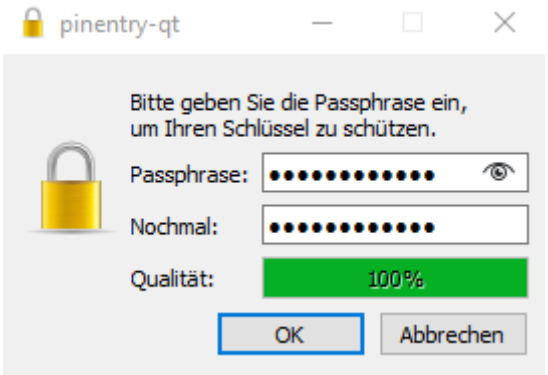


Von Mario Hesse und Jannik Schulz

5. Unter den erweiterten Einstellungen können Sie den Schlüssel auf 4096 Bit umstellen.

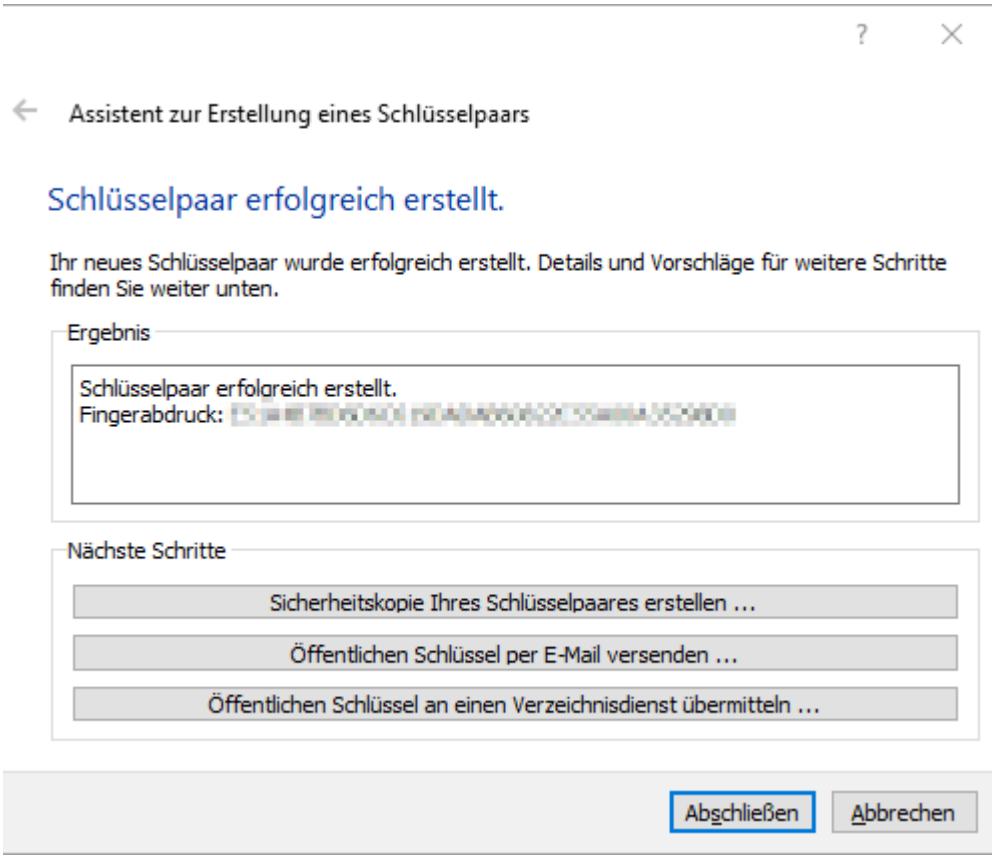


6. Das Gültigkeitsdatum kann bestehen bleiben. Dies stellt nur sicher, dass der Key nach Ablauf der der Gültigkeitsfrist unbrauchbar wird, sollten Sie den Schlüssel nicht mehr verwenden oder wenn er Ihnen verloren geht. Sie können das Gültigkeitsdatum auch später nochmal verlängern.
7. Bestätigen Sie alle Fenster und klicken Sie auf Erstellen bis die Aufforderung kommt eine Passphase (Password) zu erstellen. Vergeben Sie hier ein starkes Password und bestätigen Sie!

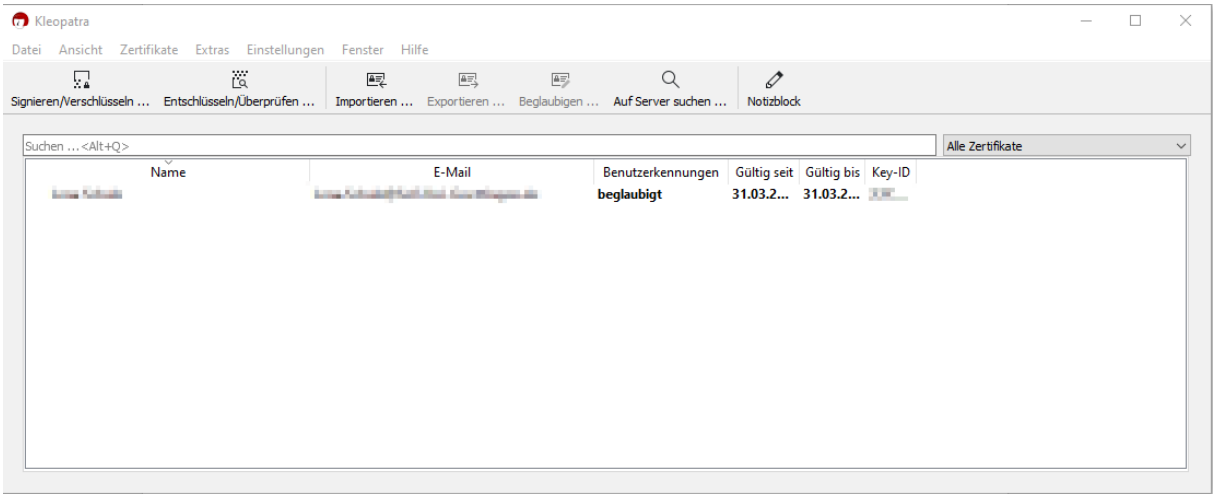


8. Erststellen Sie eine Sicherheitskopie Ihres Schlüssels und bestätigen Sie dies mit Ihrer Passphrase. Legen Sie diesen Schlüssel sicher irgendwo ab. Der soeben exportierte Schlüssel ist Ihr privater Key und darf von niemand anderes als Ihnen in Besitz gelangen. Ergänzen Sie

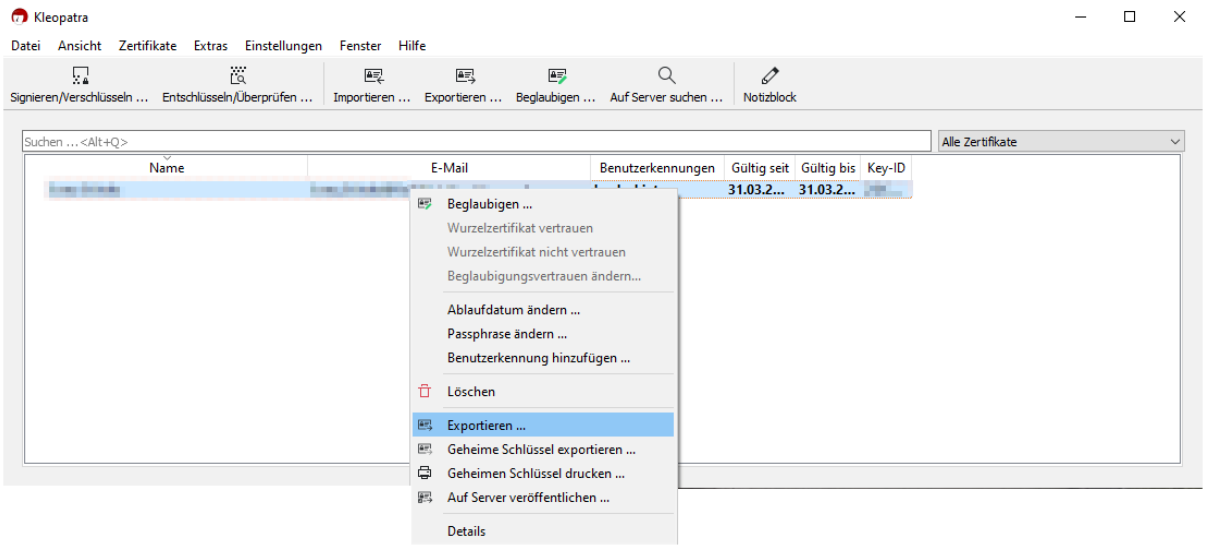
dabei den Dateinamen um das Wort Private, damit Sie die Schlüssel nicht selbst verwechseln können.



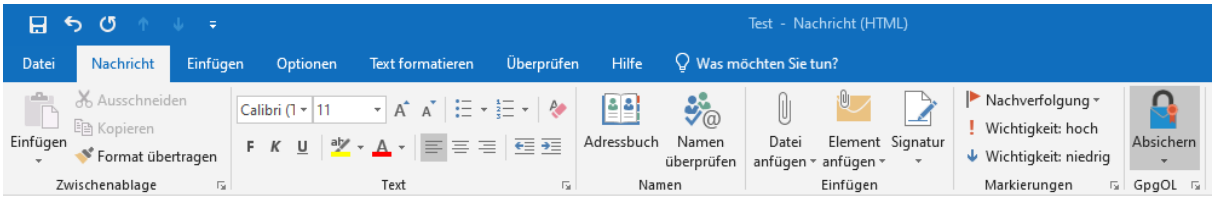
9. Klicken Sie auf Abschließen. Sie gelangen damit auf den Hauptbildschirm von Kleopatra



10. Der „Fett“ formatierte Schlüssel ist Ihrer. Machen Sie einen Rechtsklick und exportieren Sie Ihren Public Key. Ergänzen Sie dabei den Dateinamen um das Wort Public, damit Sie die Schlüssel nicht selbst verwechseln.



11. Die Datei mit dem Public Key können Sie nun ungehindert Ihren Kollegen unverschlüsselt per Mail zusenden. Diese können den Key dann über die Import Schaltfläche von Kleopatra importieren. Seien Sie sich jedoch beim Importieren eines Schlüssels sicher, dass dieser von der entsprechenden Person kommt. Importierte Schlüssel werden in Kleopatra nicht „Fett“ markiert.
12. Starten Sie den PC neu, um sicherzustellen, dass alle Einstellungen und Konfigurationen übernommen worden sind.
13. Starten Sie Outlook. Es sollte sich ein Outlook Add-In mit installiert haben.
14. Schreiben Sie zum Test eine E-Mail an einen Kollegen, dessen Schlüssel Sie bereits importiert haben. Es sollte oben rechts die Schaltfläche für das Add-In „GpgOL“ aufgetaucht sein



15. Beim Absenden und aktivierter Add-In Schaltfläche sollte die E-Mail nun automatisch verschlüsselt werden.

Hinweis: Zum lesen verschlüsselter Nachrichten muss der Empfänger PGP Entschlüsselung auf dem Endgerät unterstützen. Es empfiehlt sich nicht jede E-Mail zu verschlüsseln, sondern nur die sicherheitsrelevanten. Da viele Empfänger Ihre Emails auch gerne vom Smartphone oder Tablet aus lesen, aber nicht jede Email Software auf diesen Endgeräten PGP unterstützt, kann die E-Mail Verschlüsselung schnell zum Kommunikationshindernissen führen. Eine E-Mail-App, die PGP Verschlüsselung unterstützt und für die meisten mobilen Geräte verfügbar ist, ist K-9 Mail.

Von Mario Hesse und Jannik Schulz

3. Anleitung zum Einrichten unter Thunderbird und Windows und Linux

1. Überleg dir ein gutes Passwort
    - min. 8 Zeichen, große und kleine Buchstaben, Zahlen und Sonderzeichen
    - Tipp: Sinnlose alberne Passphrasen gespickt mit Abkürzungen und Sonderzeichen Bsp.: dA1stZahn-Wach5imfö(h)n -> Klartext: Da ist Zahnwachs im Föhn; klar, klingt albern, bleibt aber im Kopf :-)
2. Installiere Thunderbird
    - https://www.thunderbird.net/de/
3. Installiere gpg4win
    - Windows:
        - https://www.gpg4win.org/download.html
    - Linux:
        - `sudo apt-get install gnupg2`
4. Füge zu Thunderbird das Addon Enigmail zu Thunderbird hinzu
    - https://www.enigmail.net/index.php/en/ oder
    - https://addons.mozilla.org/de/thunderbird/addon/enigmail/
5. Nach dem erfolgreichen installieren von Enigmail öffnet sich ein Assistent zum Einrichten eines PGP-Schlüsselpaares. Folge dem Assistenten und verwende einfach die Standardeinstellungen. Am Ende dieses Schritts ist die Einrichtung abgeschlossen und E-Mails können verschlüsselt und entschlüsselt werden.
6. Um die Verwendung der PGP-Verschlüsselung noch etwas komfortabler zu gestalten können noch die folgenden Einstellungen in Thunderbird getroffen werden.
    - Menü -> Einstellungen -> Kontoeinstellungen -> OpenPGP-Sicherheit: ✔ Nachrichten standardmäßig verschlüsseln
    - Neue E-Mail -> Menü -> Ansicht -> Symbolleiste -> Anpassen: Füge die Buttons Verschlüsseln, Nachricht signieren und Eigenen Schlüssel anhängen per Drag and Drop zur Symboleiste hinzu. -> Die hinzugefügten Sybole zeigen an, ob die Nachricht verschlüsselt und/oder signiert wurde sowie, ob der eigene öffentliche Schlüssel mit angehangen worden ist. Das ist übersichtlich und praktisch!

4. Weblinks

- Schönes einfaches Erklärvideo zu PGP: https://www.youtube.com/watch?v=tamRqD43D3o
- Gute interaktive PGP Erklärseite von Jugend hackt: https://howtopgp.jugendhackt.de/#/
- Schritt für Schritt Videoanleitung für Thunderbird in Windows: https://youtu.be/ieuHHu4MoMo
- Schritt für Schritt Anleitung für Windows, Mac, Android und iPhone https://netzpolitik.org/2013/anleitung-so-verschlusselt-ihr-eure-e-mails-mit-pgp/
- Eine sehr ausführliche Erklärung in 8 Eskalationsstufen: https://blogs.itemis.com/de/openpgp-im-berufsalltag-teil-1-was-ist-das

Von Mario Hesse und Jannik Schulz