Anleitung zur Nutzung von PGP mit Mail in Mac Os

Installation von GPG Tools

Für die Verwaltung deiner Schlüssel und das ent- bzw. verschlüsseln benötigst du das Programm GPG Tools.

- Download GPG Tools: https://gpgtools.org
- Installiere GPG Tools so wie alle Programme

Nach der Installation solltest du ein Programm mit dem Namen GPG Keychain im Programme Ordner finden. Hier werden später deine Schlüssel gespeichert.

Außerdem sollte eine Erweiterung in deinem Mail Programm (zu finden in den Einstellungen) installiert sein.

Einrichten von GPG Tools

Um verschlüsselte Emails zu versenden, benötigst du ein Schlüsselpaar. Dieses erstellst du im Programm GPG Keychain.

- Öffne GPG Keychain
- Klick (oben links) auf Neu oder Ablage > Neuer Schlüssel
- gib alle Informationen ein und klicke Schlüssel erstellen

Du solltest folgendes Fenster sehen und kannst dich jetzt entscheiden, ob dein Schlüssel auf einen Schlüsselserver hochgeladen werden soll. Dies erleichtert anderen Menschen deinen Schlüssel zu finden. (Achtung: Einmal hochgeldaden kann ein Schlüssel nicht wieder gelöscht werden. Also gut überlegen, ob der angegebene Name dauerhaft mit dieser Emailadresse in Verbindung gebracht werden soll. Im Zweifel lieber nicht hochladen. Geht auch später noch!)

Dein Schlüsselpaar ist jetzt erstellt und sollte in deiner Keychain zu finden sein.

Für den Fall der Fälle sollte noch ein Widerrufszertifikat erstellt werden. Damit kann der Schlüssel bei Verlust widerrufen werden. Das sorgt dafür, dass andere Nutzer*innen wissen, dass Mails nicht mehr mit diesem Schlüssel verschlüsselt werden sollten. Die Zertifikatsdatei sollte an einem sicheren Ort gespeichert werden.

- rechtsklick auf deinen Schlüssel
- Widerrufszertifikat erstellen
- Datei auf einem verschlüsselten USB Stick oder im KeePassX speichern

Was ist ein Schlüsselpaar?

Dein Schlüsselpaar besteht aus einem öffentlichen und einem privaten Schlüssel. Der Private muss immer in deinem Besitz bleiben und darf dein Gerät nicht verlassen. Solltest du den Verdacht haben, dass der Schlüssel doch irgendwie die Beitzer*in gewechselt haben könnte, ist es Zeit den Schlüssel mit dem Widerrufszertifikat zu widerrufen und ein neues Schlüsselpaar anzulegen.

Dein öffentlicher Schlüssel wird benötigt, um dir verschlüsselte Emails zu senden. Diesen kannst du also an alle Freund*innen senden (und ggf. auf den Schlüsselserver hochladen).

Das ganze kannst du dir so vorstellen, dass dein öffentlicher Schlüssel ein offenes Schloss ist, welches du einer Freundin gibst. Diese schreibt etwas und verschließt das geschreibene mit diesem Schloss, in dem sie es 'zu klickt'. Nun bist du die einzige Person die dieses Schloss, mit deinem privaten Schlüssel, öffnen kann.

Deinen öffentlichen Schlüssel kannst du versenden, in dem du rechtsklick auf deinen Schlüssel in GPG Keychain klickst und Öffentlichen Schlüssel per E-Mail senden. Du kannst den öffentlichen Schlüssel auch Exportieren und als Emailanhang versenden oder auf deine Website stellen.

Versenden einer verschlüsselten Email

Damit du einer Person eine verschlüsselte Nachricht senden kannst benötigst du also ihren öffentlichen Schlüssel. Schau doch mal auf dem Schlüsselserver, ob deine Freund*innen einen hochgeladen haben.

Angenommen du hast den Schlüssel einer Person per Email bekommen, kannst du ihn einfach in deine GPG Keychain ziehen oder mit Ablage > Importieren die Datei importieren. Dieser sollte in der GPG Keychain angezeigt werden. Manchmal werden die Schlüssel auch kryptisch dargestellt (zB auf den Schlüsselservern).

Diese kannst du einfach kopieren und dann in GPG Keychain wechseln. Das Programm erkennt automatisch, dass du einen Schlüssel kopiert hast und fragt, ob du ihn einfügen möchtest.

Zum versenden einer Email:

- Öffne Mail
- Klicke auf neue Email
- Empfänger*in eingeben (von der du den Schlüssel hast)
- Schloss Symbol aktivieren
- absenden

Achtung: Der Betreff ist immer unverschlüsselt!

Was bedeutet signieren?

Eine weiter Funktion ist das signieren. Du kannst Emails immer signieren, egal ob du den Schlüssel der Empfänger*in hast oder nicht. Wenn du einer Person ermöglichen möchtest zu Prüfen, ob deine Email auf dem Weg verändert wurde, kannst du die Email mit deinen Schlüsseln signieren. Die Empfänger*in kann nun die Signatur prüfen und weiß somit, ob die Email so angekommen ist, wie du sie losgeschickt hast.

Deine Signatur kannst du aktivieren indem du das Haken Symbol neben dem Schloss Symbol aktivierst.

Externe Links

- GPGTools einrichten
- Screencast zu GPGTools
- E-Mail-Verschlüsselung mit Thunderbird unter Mac OS