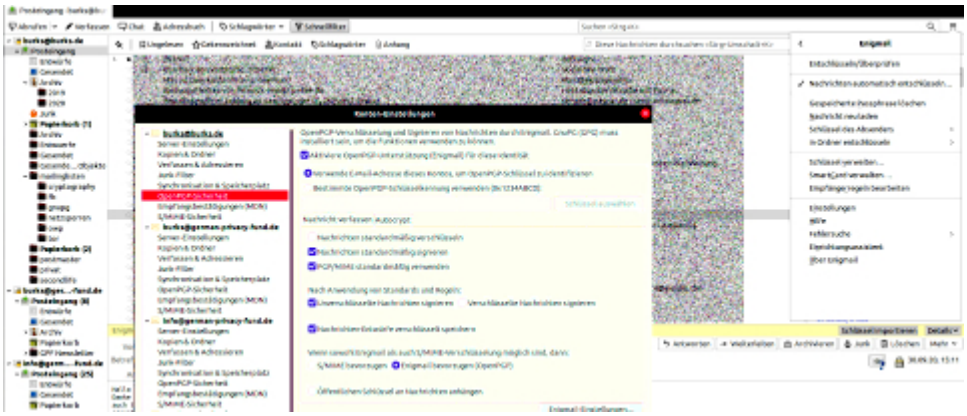
Spätere Fehler und frühere Fehler oder: E-Mails verschlüsseln unter Linux (Focal Fossa)

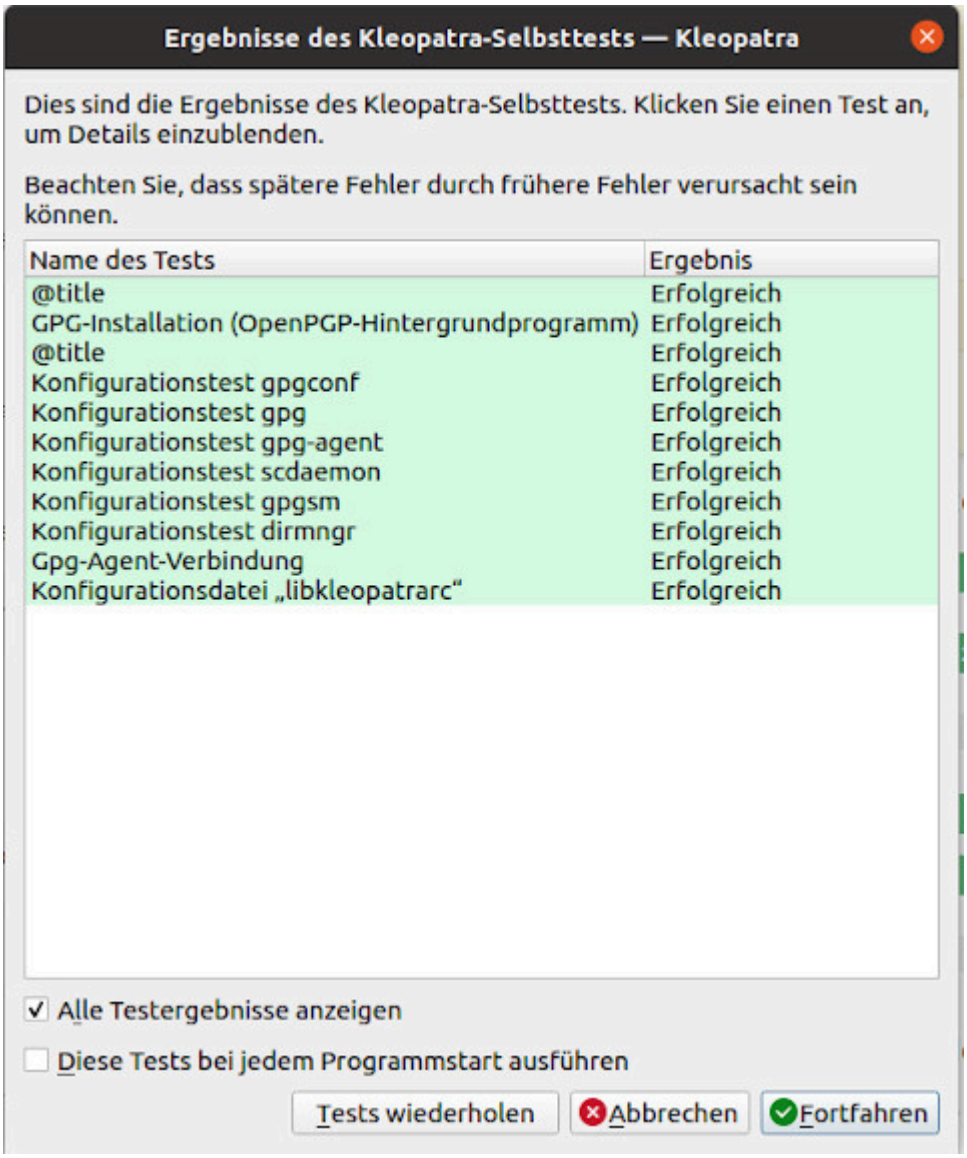


Immer ist irgendetwas. Ich plante, an diesem ruhigen Tag in der letzten Woche meines Urlaubs viel zu schreiben, wie immer eben. Jetzt habe ich nach dem Frühstück zwei Stunden meiner kostbaren Lebenszeit verplempert, um bei meinem neu eingerichteten Focal Fossa (Linux Ubuntu 20.04) wieder E-Mails verschlüsseln zu können. Man sollte denken, das sei einfach, zumal ich das seit exakt einem Vierteljahrhundert praktiziere. Aber das gilt nur theoretisch. Praktisch hat man dann mehrere Schlüssel, mehrere involvierte Programme, mehrere Rechner, mehrere Betriebssysteme, mehrere Versionen derselben, mehrere Backups, und schon bricht Chaos aus.

Die gute Nachricht: Nutzt man als E-Mail-Programm Thunderbird, braucht man bei Linux weiterhin das Add-on Enigmail. Das hört sich auf den verschiedenen Support-Websites ganz anders an: „Thunderbird's built-in OpenPGP support is not an exact copy of Thunderbird with Enigmail. Thunderbird wants to offer a fully integrated solution, and is no longer using GnuPG by default to avoid licensing issues. (This document explains the differences).“ Bedeutet das, man braucht das eigentliche

Verschlüsselungsprogramm GnuPG gar nicht mehr installieren? Und für welches Betriebssystem gilt das? (Wie das neue Thunderbird unter Windows verschlüsselt, beschreibe ich später in einem anderen Tutorial.)

Unter Linux stellt sich die Frage anders, da GnuPG bzw. OpenPGP „ab Werk“ ohnehin implementiert ist. Aber eben nicht komplett (vgl. Sceenshot unten). Das Paket scdaemon musste ich von Hand nachinstallieren, nachdem ich mir die gewohnte Benutzeroberfläche Kleopatra geholt hatte. Auch das Programm ist nicht automatisch in *Focal Fossa* enthalten. (Dann gibt es noch den zum Glück jetzt irrelevanten Unterschied zwischen GPG und GPG2.) Die glauben offenbar im Ernst, ich würde per Kommandozeile ein Programm bedienen wollen! Mach ich aber nicht.



Ich musste also, da ich kein Update von Ubuntu gemacht hatte, sondern eine komplette Neuinstallation, zunächst alle Schlüssel, inklusive des eigenen aktuellen Schlüsselpaars, mit Kleopatra importieren. Will man keine E-Mails, sondern Dateien verschlüsseln, braucht man eine grafische Oberfläche (Seahorse geht auch). Thunderbird kann das nicht, oder ich habe das Feature noch nicht gefunden.

Danach installiert man das Add-on Enigmail. Die Wikis und Manuals sind aber noch nicht für das neueste Ubuntu *Focal Fossa*; man muss also raten und vermuten. Wie aus dem vergrößerten Screenshot ganz oben ersichtlich sind alle Features an gewohnter Stelle.

Ich frage mich, warum die Thunderbird-Entwickler S/Mime ab Werk implementiert haben, aber nicht OpenPGP? Die können mir doch nicht erzählen, S/Mime würden mehr Leute nutzen? Die *usability* von S/MIME ist das Schlimmste, was man sich vorstellen kann – Finger weg! – es sei denn, man liebte die drohende Gefahr, in die Psychiatrie eingeliefert zu werden.

By the way: Außerdem habe ich mir das Leben schwer gemacht. Menschliches Versagen eben. Ich war am Rande des Nervenzusammenbruchs, als ich das halbe Dutzend meiner eigenen, zum Teil abgelaufenen Schlüsselpaare vor mir hatte, aber die Key-ID des aktuellen Schlüssels in meinem Impressum nicht wiederfand. Mein Konzept war und ist: alles Geheime sowie die Schlüssel sind in Veracrypt-Containern. Darin wiederum liegt eine verschlüsselte Datei, die KeepassXC anlegt. Dummerweise hatte ich bei der Neuinstallation ein veraltetes Backup genau jenes wichtigen Veracrypt-Containers benutzt, in dem mein aktueller geheimer Schlüssel nicht vorhanden war. Zum Glück habe ich noch ein kleines Netbook mit Linux Mint, auf dem ich erleichtert den „richtigen“ Container fand.

Jetzt brauch ich erst einmal noch mehr Kaffee… Vielleicht komme ich heute auch noch dazu, etwas nützliches zu tun.