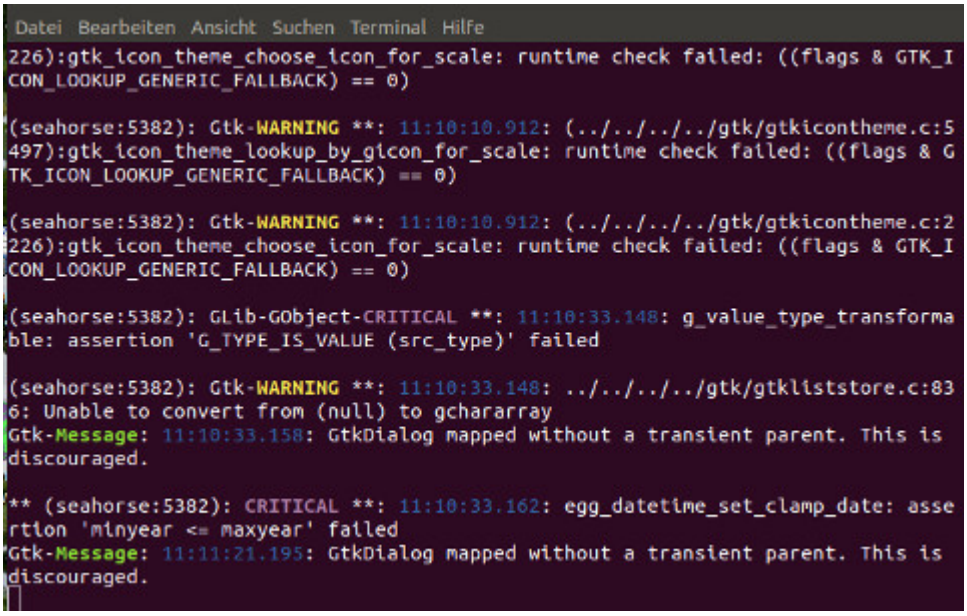
Discouraged [Update][2. Update]



Mein alter PGP-Schlüssel war abgelaufen. Ich habe einen neuen:

burks@burks.de (0x69152AA7DE1F513E) pub.asc – | ID DE1F513E | Fingerprint: 3D2A 0DFE D666 8237 5176 CD6B 6915 2AA7 DE1F 513E (Vgl. auch das Impressum.)

Natürlich ging wieder alles schief, was schief gehen konnte, und ich habe den halben Vormittag verschwendet.

Thunderbird bzw. Enigmail für Linux ist *nicht* in der Lage, einen 4096-Bit-Schlüssel zu erzeugen. Das Feature gibt es gar nicht, man wird auch nicht gefragt. (Dazu gibt es eine passende Website, har har: *class="client-nojs"*) Warum? Es weist auch nichts darauf hin.

Ich sprach so vor mich hin: Dann eben mit dem Terminal. Die Befehle weiß zwar niemand auswenig ausser Werner Koch, aber es gibt ja copy and paste.

gpg2 –full-gen-key
Das ist einfach, aber dann liest man:
Bitte wählen Sie, wie lange der Schlüssel gültig bleiben soll.

```
         0 = Schlüssel verfällt nie
       <n>  = Schlüssel verfällt nach n Tagen
       <n>w = Schlüssel verfällt nach n Wochen
       <n>m = Schlüssel verfällt nach n Monaten
       <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? (0)
```

Wie lautet es denn jetzt, wenn man fünf Jahre will? Muss das n in eckigen Klammern mit dazu? Kommen Leerzeichen hinter und vor das Anführungszeichen? Braucht man es überhaupt? Ich habe lange gebraucht, bis ich ein Beispiel gefunden habe, weil alle meine Versuche scheitern. Wer kein Mathematiker ist, versteht doch das mit dem Buchstaben n gar nicht! Und ich denke auch nicht so. Warum macht sich niemand Gedanken darüber, dass es sinnvoll wäre, einfach zu schreiben: 5y bedeutet: *Der Schlüssel wird nach fünf Jahren ungültig?!* Bei SELFHTML wird das auch so gemacht.

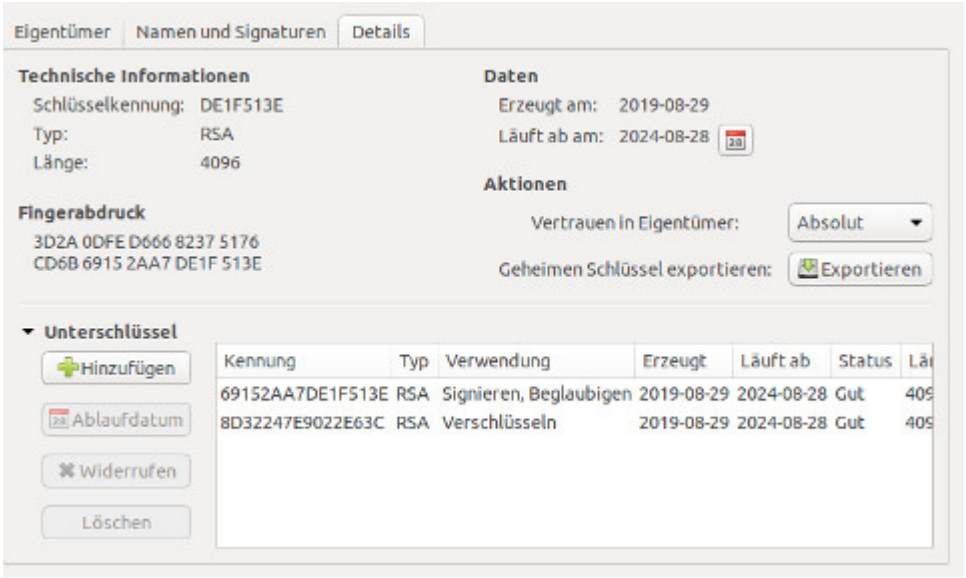
Ich habe es irgendwann aufgegeben, da ich vermutete, es müsse auch ein grafisches Frontend geben. Man kann übrigens nur *alle* geheimen Schlüssel in eine Datei exportieren, das wollte ich nicht.

Wenn man sich aber eine Liste dazu ansieht, wird einem ganz schlecht. Dieses kann das nicht, und jenes kann dieses nicht. Ich habe dan Seahorse genommen, das hatte ich eh schon installiert.

Ein Schlüsselpaar zu erzeugen, ist immer einfach, aber da beginnt das Problem erst. Was ist, wenn ich schon Dutzende von Schlüsselpaaren habe – seit 1995? Ich denke mir doch nicht jedes Mal einen neuen Namen für mich selbst aus, um den Schlüssel von den Software identifizieren zu lassen? Die Schlüssel-ID des neuen Schlüssels wurde auch nach einem Dutzend Versuchen nicht erkannt, so dass ich schon fast in der Laune des HB-Männchens war.

Ich halte es auch für einen Bug, wenn das Menü von Seahorse

anbietet, den *geheimen* Schlüssel zu exportieren, aber nicht verrät, wie man den *öffentlichen* Key in eine Datei bekommt (vgl. Screenshot unten). Irgendwann habe ich gemerkt, dass ich doch den gesamten Keyring exportiert hatte. Ein Anfänger hätte schon viel früher aufgegeben. So wird das nichts.



Update: Ein aufmerksamer Leser schickte mir einen Screenshot von Enigmail 2.1.2. Dort gibt es einen Tab mit der Option, auch 4096-Bit-Schlüssel zu erzeugen. In meinem Enigmail Version 2.0.8 gibt es den nicht. Ich frage mich, warum unter Ubuntu nicht die aktuellste Version angeboten wird?

[2. Update] Menschliches Versagen meinerseits, auf das mich ein aufmerksamer Leser hinwies. Wie man auf den Screenshots sieht, kann Thunderbird durchaus 4096-Bit-Schlüssel erzeugen. Das Feature ist nur sehr gut versteckt, warum auch immer – unter *Ablaufdatum* [sic! Sehr logisch!] und *erweitert*.