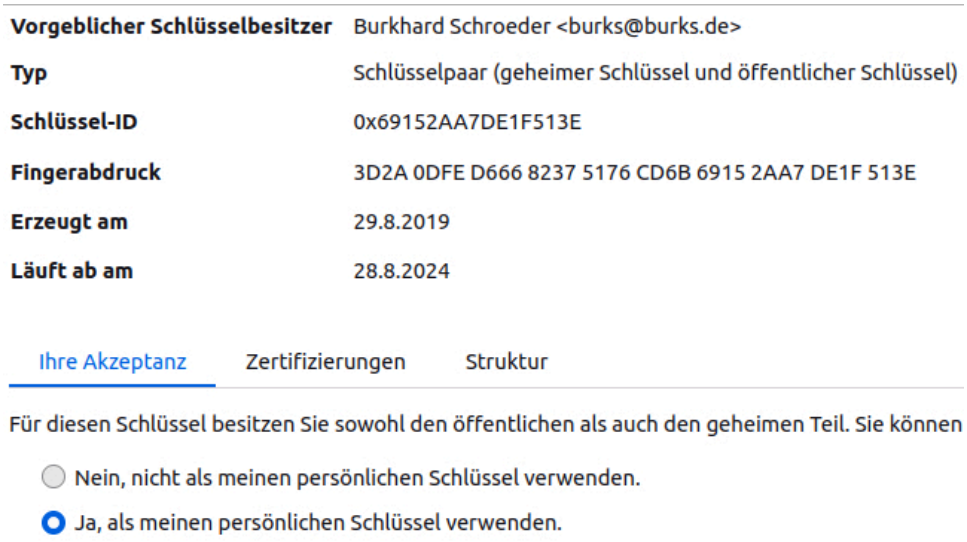
Unter vorgeblichen Schlüsselbesitzern



Die Weltläufte interessieren mich heute gar nicht. Wenn ich Tunten und Transen betrachten wollte, ginge ich in ein einschlägiges Etablissement, nicht aber zu Olympia. Ich habe gestern einen langen Artikel für ein Magazin geschrieben, der sich mit dem Einsatz künstlicher Intelligenz bei der Recherche beschäftigt, und war daher in einem technischen Stimmungsmodus. Heute also das, was mir mit meinem neuen „Kleine Hirse„-Handy noch fehlte: Verschlüsselung von E-Mails.

Was braucht man alles? Kleopatra für Linux, OpenPGP, Thunderbird und die OpenPGP-Schlüsselverwaltung davon, OpenKeychain für Android, FairEmail. Natürlich in meinem Fall Filezilla, um Daten vom Handy auf den PC zu spielen und zurück, und Gimp, um Grafiken zu bearbeiten. (Und Veracrypt, um an die Passwörterdatei von KeePass zu kommen.) Und ChatGPT. Für Neulinge ganz schön abschreckend.

Ich war auf alles vorbereitet, auch auf langwieriges Herumfummeln wie vor mehr als einem Jahrzehnt. Vorschau: Es war nicht so kompliziert, wie ich dachte, nur hatte ich einiges vergessen und musste mich erst erinnern/die künstliche Intelligenz fragen (siehe unten).

Um alle vorhandenen öffentlichen Schlüssel mit dem Programm Kleopatra auf einem Ubuntu-System in eine Datei zu exportieren, können Sie die folgenden Schritte ausführen:

1. **Kleopatra öffnen**:
   Starten Sie das Programm Kleopatra über das Anwendungsmenü oder über das Terminal mit dem Befehl:

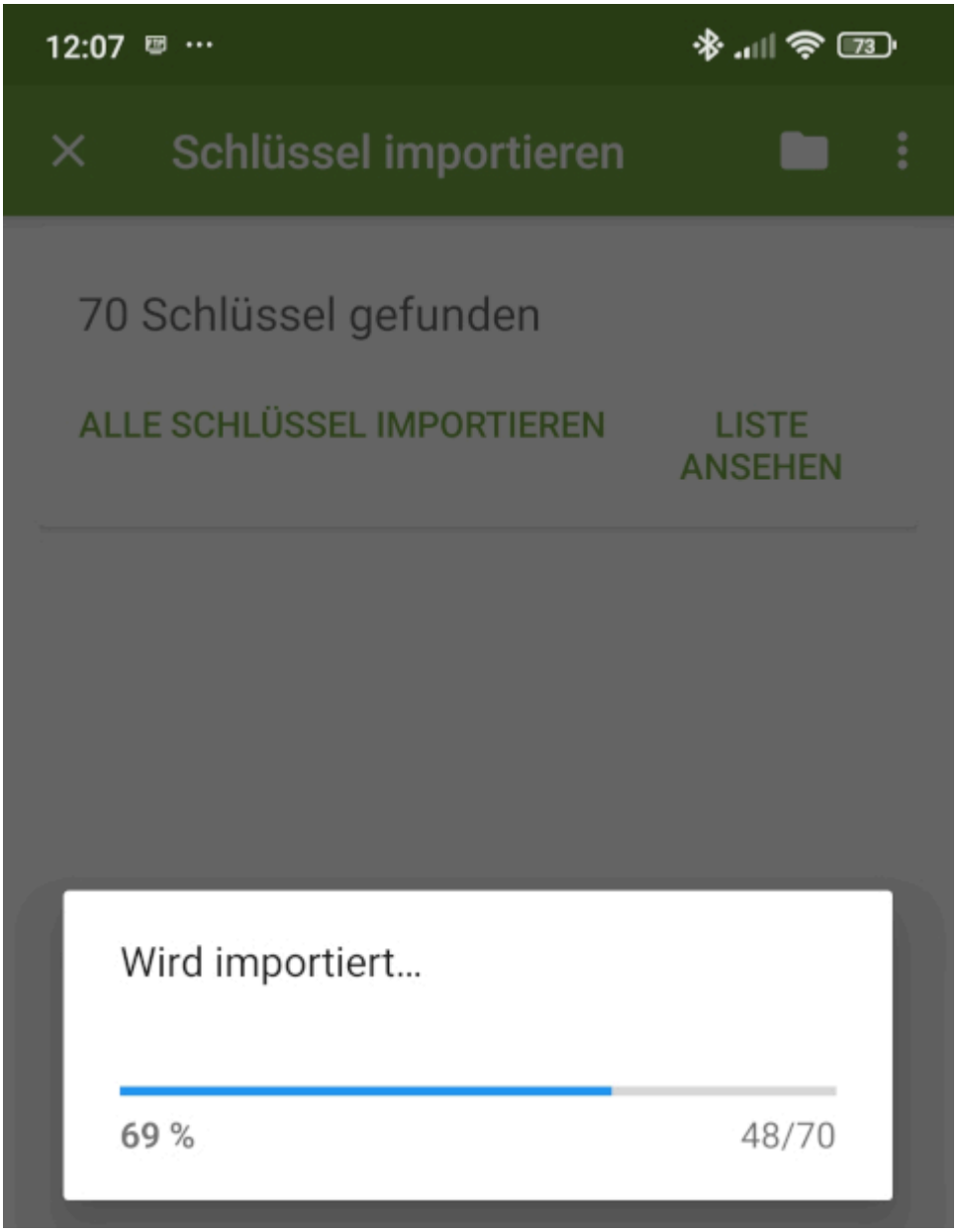
   bash — Code kopieren

   ```
   kleopatra
   ```

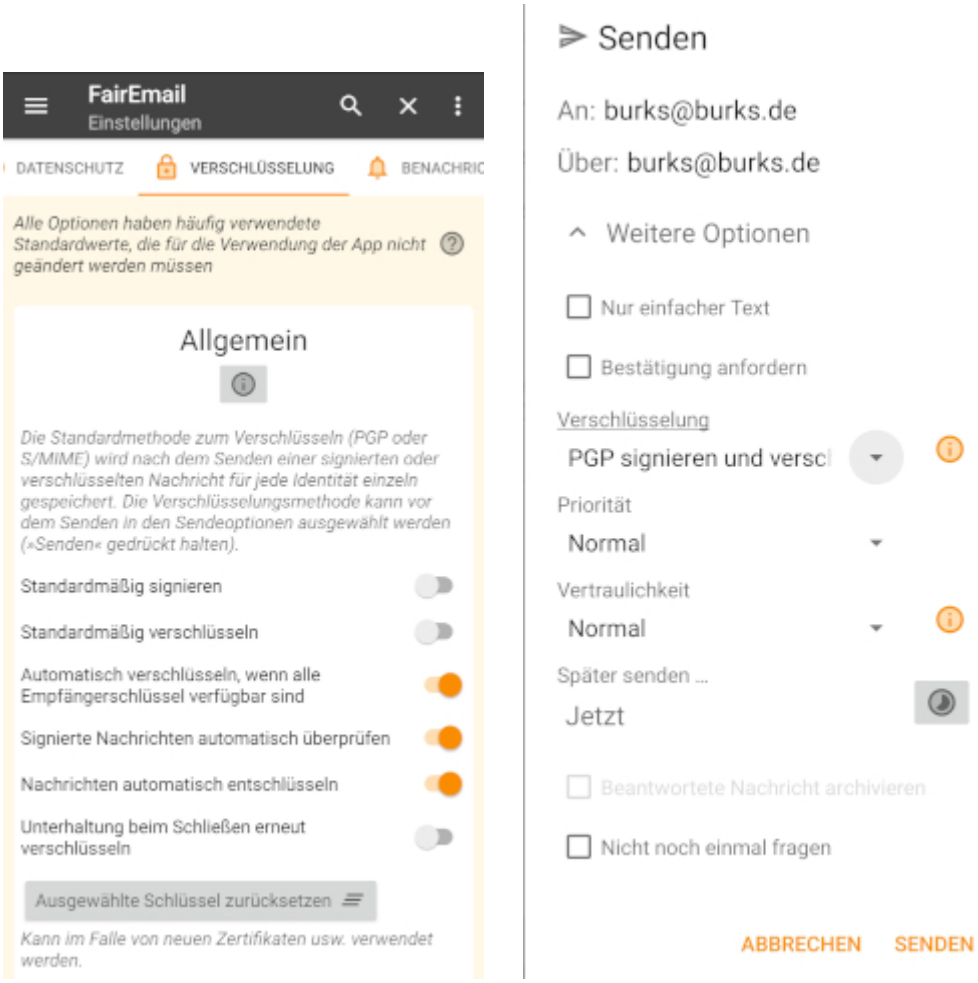
2. **Schlüsselliste anzeigen**:
   Wenn Kleopatra geöffnet ist, sollten alle Ihre Schlüssel angezeigt werden. Falls nicht, klicken Sie im Menü auf "Werkzeuge" und dann auf "Schlüssel verwalten", um die Schlüsselliste anzuzeigen.
3. **Öffentliche Schlüssel auswählen**:
   Markieren Sie alle öffentlichen Schlüssel, die Sie exportieren möchten. Sie können mehrere Schlüssel markieren, indem Sie die `Strg`-Taste (oder `Cmd`-Taste auf einem Mac) gedrückt halten und auf die einzelnen Schlüssel klicken.
4. **Schlüssel exportieren**:
   Gehen Sie nun in das Menü "Datei" und wählen Sie "Schlüssel exportieren". Alternativ können Sie mit der rechten Maustaste auf die markierten Schlüssel klicken und "Exportieren" wählen.
5. **Exportdatei wählen**:
   Ein Dialogfeld erscheint, in dem Sie den Speicherort und den Dateinamen für die exportierte Schlüsseldatei angeben können. Geben Sie den gewünschten Pfad und Dateinamen ein und klicken Sie auf "Speichern".
6. **Export abschließen**:
   Die öffentlichen Schlüssel werden nun in die angegebene Datei exportiert.

Zusammenfassend lässt sich sagen, dass Sie die Schlüssel in Kleopatra markieren, die Exportfunktion im Menü verwenden und die Datei speichern. Falls Sie eine detaillierte Anleitung mit Screenshots benötigen, sollten Sie in der Dokumentation von Kleopatra nachsehen oder eine Online-Suche nach Tutorials durchführen.

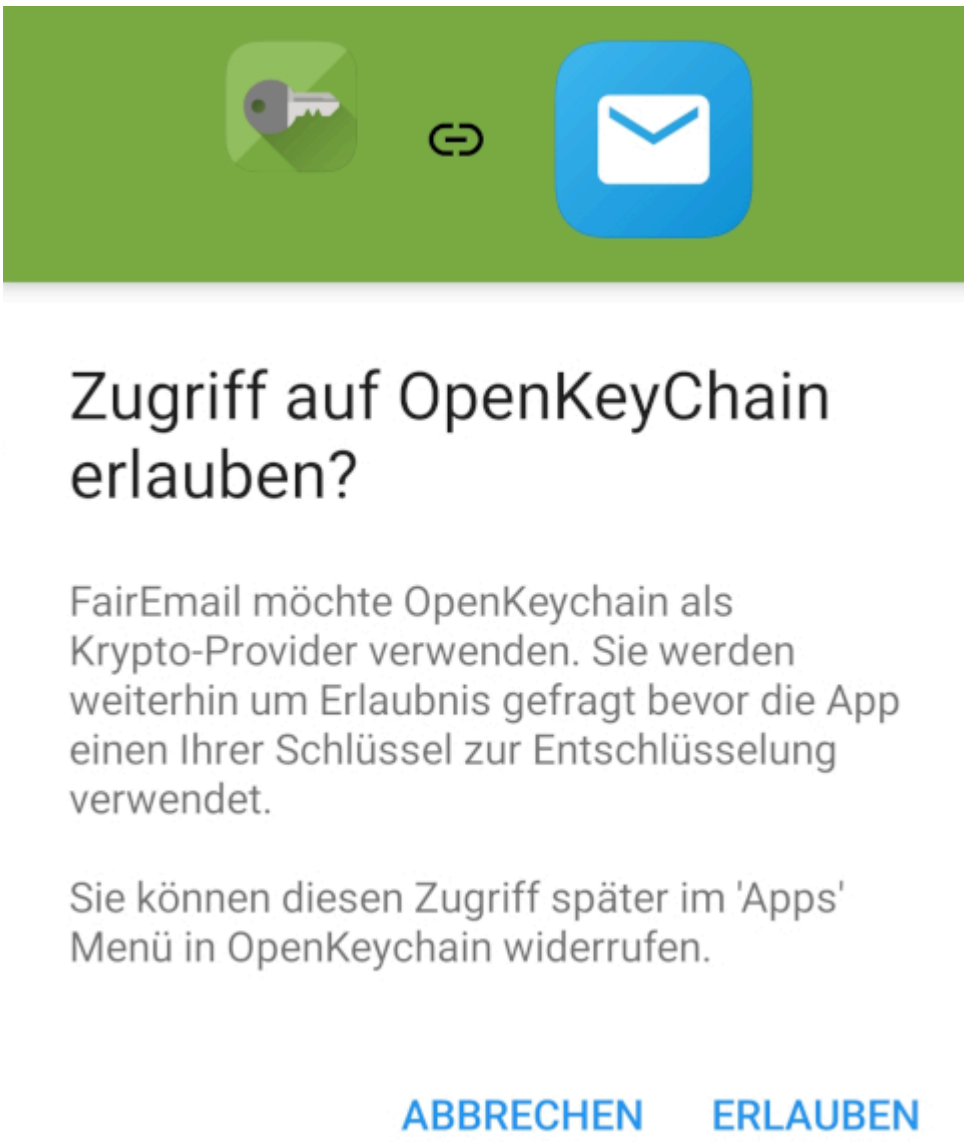
Das Kryptografie-affine Publikum wird ohnehin schon wissen, wie vorzugehen sei: Das eigene Schlüsselpaar per Kleopatra in eine Datei exportieren, danach alle anderen öffentlichen Schlüssel ebenfalls exportieren. Die ASCII-Dateien (das Format der Schlüssel) sollten dann in das DCIM-Verzeichnis des Smartphones.



OpenKeychain bindet dann alle vorhandenen Schlüssel ein. Ja, das ging ohne Probleme! Ich konnte es kaum glauben.



Kompliziert wurde es, mit FairEmail die Verschlüsselung einzurichten. Ich musste erst ~~einen Roboter~~ fragen. *Wenn Sie das Feature „Privatsphäre“ in den Einstellungen von FairEmail nicht finden, könnte es sein, dass die Option woanders platziert ist oder dass eine bestimmte Konfiguration erforderlich ist. Hier sind die Schritte, um PGP-Verschlüsselung in FairEmail einzurichten, falls die Menüpunkte abweichen blabla.* Nach ein paar Minuten kam ich drauf, dass man in den Einstellungen auch oben von links nach rechts scrollen kann. Dort taucht dann das Feature „Verschlüsselung“ auf.



Übrigens hasse ich es, auf einem Smartphone mein Passwort für meinen PGP-Schlüssel eintippen zu müssen. Es ist so lang, dass ich mit einem Finger immer einmal daneben tippe.

Ich habe für alles knapp eine Stunde gebraucht, falls das jemanden interessiert. Die verschlüsselte Test-E-Mail vom Handy zum PC kam korrekt an.