

PGP für Linux

Hier geht es darum seine Mails zu verschlüsseln damit nicht jeder (NSA) mitlesen kann !

Das Internet ist noch nie sicher gewesen und die meisten private Datenkommunikation läuft nach wie vor ungeschützt durch das Internet.

Ich beschäftige mich gerade mit der Sicherheit in der Kommunikation und auch E-Mail daher dieser Artikel.

Vorbereitung:

Zuerst muss man sich die pakete von openPGP installieren.

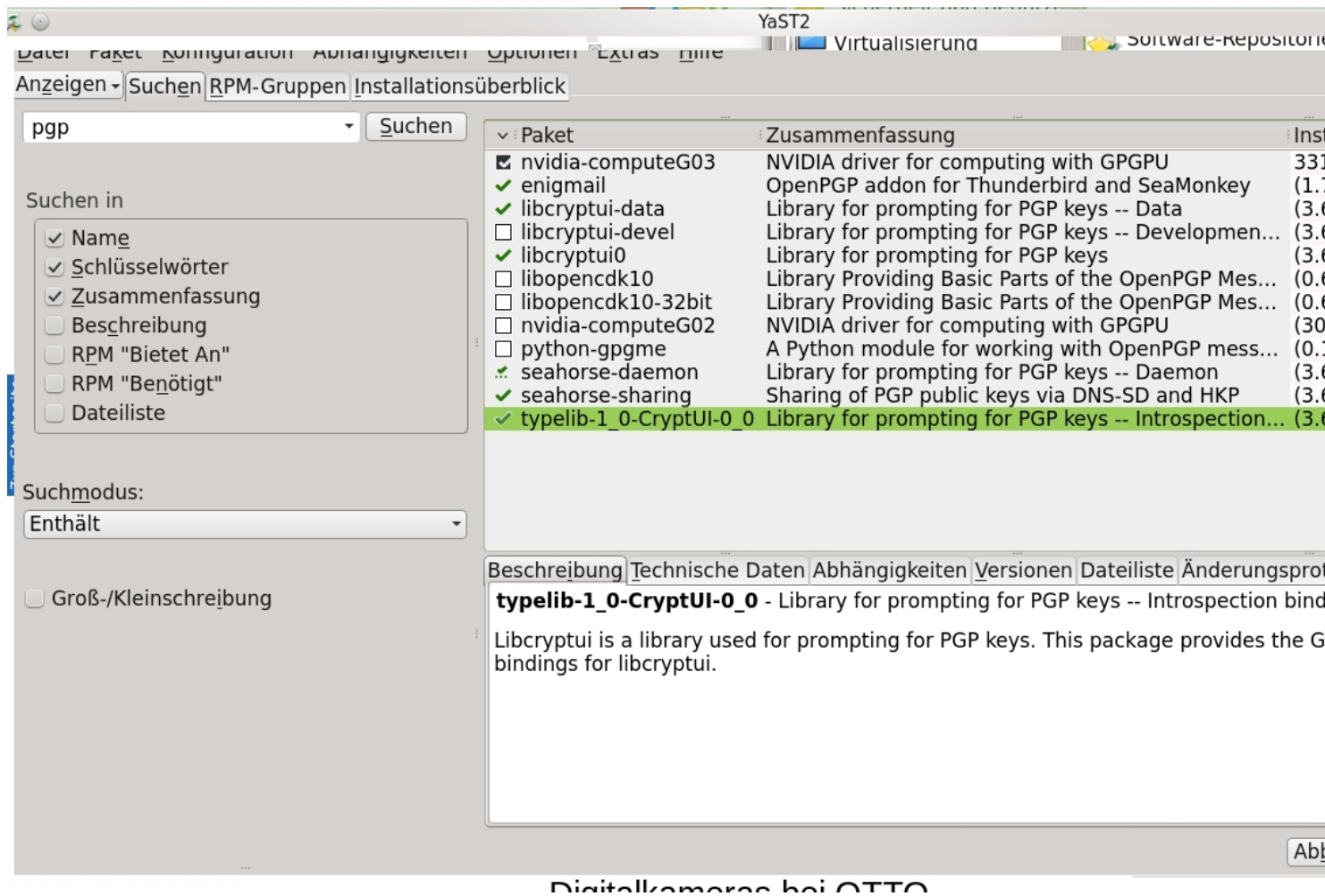
pgp unter linux einrichten

Geschrieben von: Administrator

Sonntag, den 03. August 2014 um 13:18 Uhr - Aktualisiert Sonntag, den 03. August 2014 um 13:58 Uhr

Unter OpenSuse Linux geht das ganz einfach:

Yast starten und pgp in der Softwareauswahl suchen. Dann die Pakete installieren. (Abb.1)



Das Paket enigmail für Thunderbird habe ich ebenfalls gleich ausgewählt, da ich die E-Mail Verschlüsselung nutzen möchte.

Anschliessend werden die ausgewählten Pakete per Yast eingespielt.

pgp unter linux einrichten

Geschrieben von: Administrator

Sonntag, den 03. August 2014 um 13:18 Uhr - Aktualisiert Sonntag, den 03. August 2014 um 13:58 Uhr

Dann geht es auf die Konsole wenn die Software installiert ist.

Mit dem Befehl: **gpg --list-keys** lässt man sich seine Schlüssel anzeigen.

Mit dem Befehl **gpg --gen-key** wird ein interaktiver Dialog aufgerufen.

pgp unter linux einrichten

Geschrieben von: Administrator

Sonntag, den 03. August 2014 um 13:18 Uhr - Aktualisiert Sonntag, den 03. August 2014 um 13:58 Uhr

```
wolfgang@schlepptop04:~/gnupg> gpg --gen-key -n
gpg (GnuPG) 2.0.19; Copyright (C) 2012 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Bitte wählen Sie, welche Art von Schlüssel Sie möchten:

- (1) RSA und RSA (voreingestellt)
- (2) DSA und Elgamal
- (3) DSA (nur signieren/beglaubigen)
- (4) RSA (nur signieren/beglaubigen)

Ihre Auswahl? 1

RSA-Schlüssel können zwischen 1024 und 4096 Bit lang sein.

Welche Schlüssellänge wünschen Sie? (2048) 4096

Die verlangte Schlüssellänge beträgt 4096 Bit

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) 0

Schlüssel verfällt nie

Ist dies richtig? (j/N) j

GnuPG erstellt eine User-ID um Ihren Schlüssel identifizierbar zu machen

Ihr Name ("Vorname Nachname"): ■

Bitte geben Sie eine E-Mail-Adresse ein, die mit dem Schlüssel verknüpft werden soll. (Optional: Geben Sie eine Beschreibung ein, die mit dem Schlüssel verknüpft werden soll.)