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.

Unter OpenSuse Linux geht das ganz einfach:

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

Lo Date: Faket Koniguration Abhangigkeiten Apzoigon Curken DDM Crimere liestelletieren		YaST2	Sortware-Reposi	ισπ
Anzeigen - Suchen RPM-Gruppen Installationsü pgp Suchen Suchen in Suchen ✓ Schlüsselwörter Schlüsselwörter ✓ Zusammenfassung Beschreibung Beschreibung RPM "Bietet An" Dateiliste Suchmodus: Enthält ✓	 Paket nvidia-computeG03 enigmail libcryptui-data libcryptui-devel libopencdk10 libopencdk10-32bit nvidia-computeG02 python-gpgme seahorse-daemon seahorse-sharing typelib-1_0-CryptUI-0_(Zusammenfassung NVIDIA driver for computing OpenPGP addon for Thunde Library for prompting for PG Library for prompting for PG Library Providing Basic Part Library Providing Basic Part Library Providing Basic Part NVIDIA driver for computing A Python module for workin Library for prompting for PG Sharing of PGP public keys v D Library for prompting for PG Daten Abhängigkeiten Version O - Library for prompting for PG d for prompting for PGP keys.	g with GPGPU rbird and SeaMonkey 3P keys Data 3P keys Developmen 3P keys s of the OpenPGP Mes g with GPGPU g with OpenPGP mess 3P keys Daemon via DNS-SD and HKP 3P keys Introspection	Ins 33: (1.' (3.) (3.) (0.) (3.) (3.) (3.) (3.) (3.) (3.) (3.) (3
	Digitalkamora			Ab

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.

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.

```
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, I
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 🛛
Ihr Name ("Vorname Nachname"):
```