

SelfLinux-0.12.2



Installation von GnuPG



Autor: Mike Ashley ()
Formatierung: Matthias Hagedorn (matthias.hagedorn@selflinux.org)
Lizenz: GFDL

1 Anhang C Installation von GnuPG

Dieses Kapitel beschreibt die Installation von GnuPG auf verschiedenen Plattformen. Die Beschreibung bezieht sich auf die Version 1.0.1 von GnuPG. Bitte lesen Sie auf jeden Fall auch die Dateien **README** und **INSTALL** im GnuPG Source-Verzeichnis. Wo Sie aktuelle Versionen von GnuPG als TAR-Archiv, RPM oder Binary für Win32 bekommen, können Sie im [Anhang B](#) nachlesen.

1.1 Unix und GNU/Linux

Bevor Sie mit der Installation beginnen, stellen Sie bitte sicher, daß Ihre Sourcefiles nicht modifiziert wurden. Das ist ein sehr wichtiger Schritt, denn nur so können Sie sicherstellen, dass niemand irgendwelche Hintertüren oder absichtlich Schwachstellen in den Code eingebaut hat.

Wenn Sie bereits eine Version von GnuPG installiert haben, können Sie einfach die Signatur überprüfen. **Benutzen Sie jedoch niemals die Version, die Sie gerade Installieren möchten, für diese Überprüfung.** Der Schlüssel mit dem die Signatur erzeugt wurde [wohl eher der dazugehörige öff. Schlüssel] ist:

```
pub 1024D/57548DCD 1998-07-07 Werner Koch (gnupg sig) <dd9jn@gnu.org>
```

Sollten Sie diesen Schlüssel noch nicht in Ihrem öffentlichen Schlüsselbund haben, müssen Sie ihn zuerst aus der Datei [g10/pubring.asc](#) aus den Sourcen importieren:

```
user@linux ~/ $ gpg --import src/gnupg-1.0.0/g10/pubring.asc
```

oder von einem Key Server holen, also beispielsweise:

```
user@linux ~/ $ gpg --keyserver blackhole.pca.dfn.de --recv-keys  
0x57548DCD
```

Dann können Sie die Signatur überprüfen mit

```
user@linux ~/ $ gpg --verify gnupg-1.0.1.tar.gz.asc
```

Sollten Sie eine überprüfte [trusted] Version von PGP 2 oder PGP 5 installiert haben, können Sie die PGP 2 Signatur [gnupg-1.0.1.tar.gz.sig](#) überprüfen:

```
user@linux ~/ $ pgp gnupg-1.0.1.tar.gz.sig gnupg-1.0.1.tar.gz
```

Falls Sie weder GnuPG noch PGP installiert haben, dann Benutzen Sie den MD5 Hashalgorithmus um eine Prüfsumme des Tar-Files zu erzeugen.

```
user@linux ~/ $ md5sum gnupg-1.0.1.tar.gz  
37eeae62c1823edc787996bfee70351a  gnupg-1.0.1.tar.gz
```

Vergleichen Sie dann bitte die Checksumme mit der, die Sie unter  <http://www.gnupg.org/download.html> finden.

Nehmen wir an, Sie möchten GnuPG systemweit installieren, so dass es für alle User nutzbar ist und nehmen wir weiterhin an, bei Ihrem System befinden sich die Sourcen für lokal installierte Software unter `/usr/local/src/`. Kopieren Sie das TAR-File nach `/usr/local/src`; dann wechseln Sie in das Verzeichnis und entpacken dort das TAR-File:

```
root@linux ~/ # cd /usr/local/src/  
root@linux ~/ # gzip -d gnupg-1.0.1.tar.gz  
root@linux ~/ # tar xvf gnupg-1.0.1.tar
```

Danach wechseln Sie in das neu angelegte Unterverzeichnis `gnupg-1.0.1/` und führen dann nacheinander:

```
root@linux ~/ # ./configure  
root@linux ~/ # make  
root@linux ~/ # make install
```

aus. Die ausführbare Datei **gpg** befindet sich dann in `/usr/local/bin`. Für weitere Optionen von `configure` benutzen Sie die Option `--help` und lesen die Datei **INSTALL**.

Um zu verhindern, dass vertrauliche Daten auf die Swap-Partition ausgelagert werden, empfiehlt es sich das **Set-User-ID Bit** für **gpg** zu setzen:

```
root@linux ~/ # chmod u+s /usr/local/bin/gpg
```

GnuPG verhindert dann, dass Teile seines Speicherbereichs auf die Festplatte ausgelagert werden. Wenn Sie dies nicht tun möchten, können Sie die Option `no-secmem-warning` in die Datei `~/.gnupg/options` einfügen, dann bekommen Sie diesbezüglich auch keine Warnmeldungen mehr.

Sollten Sie keine Root-Rechte auf dem System haben oder der Systemadministrator nicht gewillt sein, GnuPG systemweit zu installieren, besteht immer noch die Möglichkeit zu einer User-Installation. Legen Sie dazu am Besten ein Unterverzeichnis `src/` in Ihrem Home-Verzeichnis an, wenn Sie dies nicht schon haben. Entpacken Sie das Tar-File in `~/src` und führen dann:

```
user@linux ~/ $ ./configure --prefix=$HOME
```

aus. Dann können Sie genau wie oben ein `make` und `make install` durchführen. `make install` legt dann die Unterverzeichnisse `bin/ lib/ man/ share/` in Ihrem Home-Verzeichnis an. Die ausführbare Datei befindet sich dann unter `$HOME/bin/gpg`. `$HOME/bin` sollte natürlich in Ihrem Pfad liegen.