

Controle van de authenticiteit

Na het downloaden wordt eerst de integriteit van alle bestanden gecontroleerd. Daarvoor dienen we de juiste sleutel te downloaden. Deze wordt onder andere verspreid door een aantal zogenoemde key-servers en hij kan met het volgende commando, dat op www.kernel.org staat vermeld, worden ingelezen:

```
jeroen@server:~> gpg --keyserver wwwkeys.pgp.net --recv-keys 0x517D0F0E
gpg: Let op: er wordt onveilig geheugen gebruikt!
gpg: opvragen van sleutel 517D0F0E van wwwkeys.pgp.net ...
gpg: sleutel 517D0F0E: openbare sleutel geïmporteerd
gpg: Totaal aantal behandeld: 1
gpg: geïmporteerd: 1
jeroen@server:~>
```

Dat we de sleutel hebben gekregen kunnen we controleren met behulp van het volgende commando.

```
jeroen@server:~> gpg -kv
gpg: Let op: er wordt onveilig geheugen gebruikt!
/home/jeroen/.gnupg/pubring.gpg
-----

pub 1024D/F8EE10B4 2001-12-14 Jeroen Baten (kwoot) <jbaten@i2rs.nl>
sub 1024g/F43B4ACE 2001-12-14

pub 1024D/517D0F0E 2000-10-10 Linux Kernel Archives Verification Key <ftpadmin@kernel.org>
sub 4096g/E50A8F2A 2000-10-10
jeroen@server:~>
```

Zoals u ziet hebben we nu twee sleutels: de eerste is die van de auteur en de tweede is van de kernel-ontwikkelaars. Nu we de beschikking hebben over een sleutel die we vertrouwen¹⁸, kunnen we de gedownloade bestanden controleren:

```
jeroen@server:~> gpg --verify linux-2.4.18.tar.bz2.sign linux-2.4.18.tar.bz2
gpg: Let op: er wordt onveilig geheugen gebruikt!
gpg: Ondertekening gemaakt op ma 25 feb 2002 20:42:45 CET met DSA sleutel nummer 517D0F0E
gpg: Correcte ondertekening van "Linux Kernel Archives Verification Key
<ftpadmin@kernel.org>"
Kon geen pad vinden dat leidt tot vertrouwen van de sleutel. Laten we
eens proberen of we wat missende waarden kunnen invullen.

Geen pad gevonden dat leidt naar een van onze sleutels.

gpg: LET OP: Deze sleutel is niet getekend met een betrouwbare ondertekening!
gpg: Er is geen indicatie dat deze ondertekening van de eigenaar is.
gpg: Vingerafdruk: C75D C40A 11D7 AF88 9981 ED5B C86B A06A 517D 0F0E
jeroen@server:~> gpg --verify patch-2.4.19.bz2.sign patch-2.4.19.bz2
```