Breve guida all'uso di gnupg

Generare una nuova chiave con gpg

Al prompt di sistema:

```
provagpg@nekkar:~$ gpg --gen-key
gpg (GnuPG) 1.4.6; Copyright (C) 2006 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

gpg: directory `/t/home/provagpg/.gnupg' created
gpg: can't open `/gnupg/options.skel': No such file or directory
gpg: keyring `/t/home/provagpg/.gnupg/secring.gpg' created
gpg: keyring `/t/home/provagpg/.gnupg/pubring.gpg' created
Please select what kind of key you want:
   (1) DSA and Elgamal (default)
   (2) DSA (sign only)
   (5) RSA (sign only)
Your selection? <invio>
DSA keypair will have 1024 bits.
ELG-E keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) <invio>
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)  10y
Key expires at dom 15 lug 2018 09:51:39 UTC
Is this correct? (y/N)  y
You need a user ID to identify your key; the software constructs the user ID
```

```
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Pinco Pallino
Email address: pinco.pallino@mailinator.com
Comment: <invio>
You selected this USER-ID:
    "Pinco Pallino <pinco.pallino@mailinator.com>"



Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
You need a Passphrase to protect your secret key.

Enter passphrase: oov0eiV6QuaeGoy6
Repeat passphrase: oov0eiV6QuaeGoy6

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++.+++++.++++++++++++++++++++.+++++...++++++++++++++>++++++++++.....
.....+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++..++++++++++.+++++.++++++++++..+++++.+++++.++++++++++++++++++++++++.+++++
...++++++++++++++++++++++++.+++++.++++++++++++++++++..++++++++++++++..+++++
+++++>++++++++++>....+++++....>.+++++..............<+++++............>+++++.
.<.+++++....>+++++..............+++++^^^
gpg: /t/home/provagpg/.gnupg/trustdb.gpg: trustdb created
gpg: key B9DDE7AD marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
```

```
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2018-07-15
pub   1024D/B9DDE7AD 2008-07-17 [expires: 2018-07-15]
      Key fingerprint = 9ABA AC2B EF7D D0BC 876F  2C20 DED9 F369 B9DD E7AD
uid                  Pinco Pallino <pinco.pallino@mailinator.com>
sub   2048g/91EFF221 2008-07-17 [expires: 2018-07-15]

provagpg@nekkar:~$
```

A questo punto la nuova coppia di chiavi è stata generata, essa viene identificata tramite il fingerprint. La chiave pubblica viene aggiunta alla base dati pubring.gpg, mentre la chiave privata viene salvata in secring. gpg. La parte privata viene cifrata e protetta con la password, tuttavia è bene mantenere sempre al sicuro la chiave privata.

Rivediamola:

```
provagpg@nekkar:~$ gpg --list-keys
/t/home/provagpg/.gnupg/pubring.gpg
---------------------------------
pub   1024D/B9DDE7AD 2008-07-17 [expires: 2018-07-15]
uid                  Pinco Pallino <pinco.pallino@mailinator.com>
sub   2048g/91EFF221 2008-07-17 [expires: 2018-07-15]
```

Questi sono i file che contengono i dati:

```
provagpg@nekkar:~$ ls -l .gnupg/
total 20
-rw------- 1 provagpg provagpg 1188 2008-07-17 09:59 pubring.gpg
-rw------- 1 provagpg provagpg  600 2008-07-17 09:59 random_seed
-rw------- 1 provagpg provagpg 1337 2008-07-17 09:59 secring.gpg
-rw------- 1 provagpg provagpg 1280 2008-07-17 09:59 trustdb.gpg
```

Caricare una chiave su un keyserver

provagpg@nekkar:~$ **gpg --keyserver keyserver.linux.it --send-keys B9DDE7AD**

```
gpg: sending key B9DDE7AD to hkp server keyserver.linux.it
```

Ora la chiave si trova sul keyserver. In realtà la chiave di questo esempio non è effettivamente stata caricata sul keyserver, per evitare di riempirlo con dati inutili, per cui non la troverete nel caso in cui la cerchiate.

Cercare una chiave in un keyserver e importarla

provagpg@nekkar:~$ **gpg --keyserver keyserver.linux.it --search bisetto**

```
provagpg@nekkar:~$ gpg --keyserver keyserver.linux.it --search bisetto
gpg: searching for "bisetto" from hkp server keyserver.linux.it
(1)    oMrca Bisetto <mbiso@libero.it>
 oMrca Bisetto <oMrca@folgorante.net>
   1024 bit DSA key CCFDB381, created: 2003-02-04
(2)    oMrca Bisetto <mbiso@usa.net>
   1024 bit DSA key 08C9F40F, created: 1999-02-15 (revoked)
Keys 1-2 of 2 for "bisetto".  Enter number(s), N)ext, or Q)uit > q
provagpg@nekkar:~$ gpg --keyserver keyserver.linux.it --search bisetto
gpg: searching for "bisetto" from hkp server keyserver.linux.it
(1)    oMrca Bisetto <mbiso@libero.it>
 oMrca Bisetto <oMrca@folgorante.net>
   1024 bit DSA key CCFDB381, created: 2003-02-04
(2)    oMrca Bisetto <mbiso@usa.net>
   1024 bit DSA key 08C9F40F, created: 1999-02-15 (revoked)
Keys 1-2 of 2 for "bisetto".  Enter number(s), N)ext, or Q)uit > 1
gpg: requesting key CCFDB381 from hkp server keyserver.linux.it
gpg: key CCFDB381: public key "oMrca Bisetto <oMrca@folgorante.net>" imported
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2018-07-15
gpg: Total number processed: 1
gpg:               imported: 1
```

Ottenere liste delle chiavi presenti nella base dati locale

Le proprie chiavi:

```
provagpg@nekkar:~$ gpg --list-secret-keys
```

```
/t/home/provagpg/.gnupg/secring.gpg
---------------------------------
sec   1024D/B9DDE7AD 2008-07-17 [expires: 2018-07-15]
uid                  Pinco Pallino <pinco.pallino@mailinator.com>
ssb   2048g/91EFF221 2008-07-17
```

Tutte le chiavi:

```
provagpg@nekkar:~$ gpg --list-keys
/t/home/provagpg/.gnupg/pubring.gpg
---------------------------------
pub   1024D/B9DDE7AD 2008-07-17 [expires: 2018-07-15]
uid                  Pinco Pallino <pinco.pallino@mailinator.com>
sub   2048g/91EFF221 2008-07-17 [expires: 2018-07-15]

pub   1024D/CCFDB381 2003-02-04 [expires: 2013-02-01]
uid                  oMrca Bisetto <oMrca@folgorante.net>
uid                  oMrca Bisetto <mbiso@libero.it>
sub   1024g/9D040459 2003-02-04 [expires: 2013-02-01]
```

Le chiavi con un criterio di ricerca:

```
provagpg@nekkar:~$ gpg --list-keys bisetto
pub   1024D/CCFDB381 2003-02-04 [expires: 2013-02-01]
uid                  oMrca Bisetto <oMrca@folgorante.net>
uid                  oMrca Bisetto <mbiso@libero.it>
sub   1024g/9D040459 2003-02-04 [expires: 2013-02-01]

provagpg@nekkar:~$ gpg --list-keys 91EFF221
pub   1024D/B9DDE7AD 2008-07-17 [expires: 2018-07-15]
uid                  Pinco Pallino <pinco.pallino@mailinator.com>
sub   2048g/91EFF221 2008-07-17 [expires: 2018-07-15]
```

Firmare un testo facendo copia-incolla

```
provagpg@nekkar:~$ gpg --armor --sign
```

```
You need a passphrase to unlock the secret key for
user: "Pinco Pallino <pinco.pallino@mailinator.com>"
1024-bit DSA key, ID B9DDE7AD, created 2008-07-17

Enter passphrase: oov0eiV6QuaeGoy6

provagpg@nekkar:~$ gpg --armor --sign

You need a passphrase to unlock the secret key for
user: "Pinco Pallino <pinco.pallino@mailinator.com>"
1024-bit DSA key, ID B9DDE7AD, created 2008-07-17

Testo di prova.
Ciao.

Pinco
^D
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.6 (GNU/Linux)

owGbwMvMwCR47+bnzJ13n69lPK2cxOBRbyoXklpckq+QkqlQUJRflqjH5ZyZmK/H
xRWQmZecz9Vhz8wKUmUH0ybI5LSDYTar3K6E1ayhujF9WbLxH/ZNK2acpcGwYE21
zN/MCZ02QX9uxXdbVif1McWsBgA=
=3/YU
-----END PGP MESSAGE-----
```

Decrittare un testo facendo copia-incolla

```
provagpg@nekkar:~$ gpg --decrypt
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.6 (GNU/Linux)
```

```
owGbwMvMwCR47+bnzJ13n69lPK2cxOBRbyoXklpckq+QkqlQUJRflqjH5ZyZmK/H
xRWQmZecz9Vhz8wKUmUH0ybI5LSDYTar3K6E1ayhujF9WbLxH/ZNK2acpcGwYE21
zN/MCZ02QX9uxXdbVif1McWsBgA=
=3/YU
-----END PGP MESSAGE-----
^D
Testo di prova.
Ciao.

Pinco
gpg: Signature made gio 17 lug 2008 12:04:14 UTC using DSA key ID B9DDE7AD
gpg: Good signature from "Pinco Pallino <pinco.pallino@mailinator.com>"
```

Verificare una firma facendo copia-incolla

```
provagpg@nekkar:~$ gpg --verify
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.6 (GNU/Linux)

owGbwMvMwCR47+bnzJ13n69lPK2cxOBRbyoXklpckq+QkqlQUJRflqjH5ZyZmK/H
xRWQmZecz9Vhz8wKUmUH0ybI5LSDYTar3K6E1ayhujF9WbLxH/ZNK2acpcGwYE21
zN/MCZ02QX9uxXdbVif1McWsBgA=
=3/YU
-----END PGP MESSAGE-----
^D
gpg: Signature made gio 17 lug 2008 12:04:14 UTC using DSA key ID B9DDE7AD
gpg: Good signature from "Pinco Pallino <pinco.pallino@mailinator.com>"
```

Apporre la propria firma per certificare la chiave di qualcun altro

Per firmare la chiave di qualcuno la dovete scaricare da un keyserver, oppure la ottenete con altri mezzi e la inserite nel vostro database locale. Per essere certi dell'autenticità della chiave dovete essere sicuri che i dati contenuti nella chiave corrispondano con quelli dichiarati, per cui dovete conoscere la persona la cui chiave state per firmare. Se la chiave vi è stata consegnata tramite un canale sicuro, potete procedere senza indugio,

se invece l'avete ottenuta in altro modo, per esempio posta elettronica o un keyserver, dovete verificarne l'integrità tramite il controllo del fingerprint attraverso un canale sicuro, di solito il telefono è quel che basta. Ecco come ottenere il fingerprint di una chiave:

```
provagpg@nekkar:~$ gpg --fingerprint bisetto
pub   1024D/CCFDB381 2003-02-04 [expires: 2013-02-01]
      Key fingerprint = E9B9 A8F6 86CE 855F E79D  20C8 D9A8 8FBA CCFD B381
uid                  oMrca Bisetto <oMrca@folgorante.net>
uid                  oMrca Bisetto <mbiso@libero.it>
sub   1024g/9D040459 2003-02-04 [expires: 2013-02-01]
```

Quando siete sicuri dell'autenticità della chiave, potete apporvi la vostra firma:

```
provagpg@nekkar:~$ gpg --sign-key bisetto

pub  1024D/CCFDB381  created: 2003-02-04  expires: 2013-02-01  usage: SCA
                     trust: unknown       validity: unknown
sub  1024g/9D040459  created: 2003-02-04  expires: 2013-02-01  usage: E
[ unknown] (1). oMrca Bisetto <oMrca@folgorante.net>
[ unknown] (2)  oMrca Bisetto <mbiso@libero.it>

Really sign all user IDs? (y/N) y

pub  1024D/CCFDB381  created: 2003-02-04  expires: 2013-02-01  usage: SCA
                     trust: unknown       validity: unknown
 Primary key fingerprint: E9B9 A8F6 86CE 855F E79D  20C8 D9A8 8FBA CCFD B381

     oMrca Bisetto <oMrca@folgorante.net>
     oMrca Bisetto <mbiso@libero.it>

This key is due to expire on 2013-02-01.
Are you sure that you want to sign this key with your
key "Pinco Pallino <pinco.pallino@mailinator.com>" (B9DDE7AD)

Really sign? (y/N) y

You need a passphrase to unlock the secret key for
```

```
user: "Pinco Pallino <pinco.pallino@mailinator.com>"
1024-bit DSA key, ID B9DDE7AD, created 2008-07-17

Enter passphrase: oov0eiV6QuaeGoy6


provagpg@nekkar:~$
```

Avete certificato la chiave. Lo si può vedere:

```
provagpg@nekkar:~$ gpg --list-sigs bisetto
pub   1024D/CCFDB381 2003-02-04 [expires: 2013-02-01]
uid                  oMrca Bisetto <oMrca@folgorante.net>
sig          8265A67E 2008-04-19  [User ID not found]
sig          C8D4619B 2008-04-20  [User ID not found]
sig 3        8918B376 2008-04-19  [User ID not found]
sig 3        CCFDB381 2005-05-29  oMrca Bisetto <oMrca@folgorante.net>
sig          B9DDE7AD 2008-07-17  Pinco Pallino <pinco.pallino@mailinator.com>
uid                  oMrca Bisetto <mbiso@libero.it>
sig          08C9F40F 2003-02-04  [User ID not found]
sig          7692CB1E 2003-03-08  [User ID not found]
sig          8265A67E 2008-04-19  [User ID not found]
sig          C8D4619B 2008-04-20  [User ID not found]
sig 3        8918B376 2008-04-19  [User ID not found]
sig          F73AD152 2003-03-08  [User ID not found]
sig 3        B97B65A4 2003-03-08  [User ID not found]
sig 3        33DAD598 2003-03-14  [User ID not found]
sig 3        CCFDB381 2003-02-04  oMrca Bisetto <oMrca@folgorante.net>
sig 3        CCFDB381 2003-02-04  oMrca Bisetto <oMrca@folgorante.net>
sig 3        CCFDB381 2003-02-04  oMrca Bisetto <oMrca@folgorante.net>
sig          B9DDE7AD 2008-07-17  Pinco Pallino <pinco.pallino@mailinator.com>
sub   1024g/9D040459 2003-02-04 [expires: 2013-02-01]
sig          CCFDB381 2003-02-04  oMrca Bisetto <oMrca@folgorante.net>

provagpg@nekkar:~$
```

Ora, per far sapere a tutto il mondo che avete apposto la vostra firma sulla chiave, la potete nuovamente caricare su un keyserver, con la procedura vista in precedenza:

```
gpg --keyserver keyserver.linux.it --send-keys bisetto
```

Mantenere aggiornate le chiavi

Per avere le versioni aggiornate delle chiavi pubbliche, compresa la vostra, su cui possono essere state apposte firme di altri, eseguite il seguente comando:

```
provagpg@nekkar:~$ gpg --keyserver keyserver.linux.it --refresh-keys
gpg: refreshing 2 keys from hkp://keyserver.linux.it
gpg: requesting key B9DDE7AD from hkp server keyserver.linux.it
gpg: requesting key CCFDB381 from hkp server keyserver.linux.it
gpgkeys: key 9ABAAC2BEF7DD0BC876F2C20DED9F369B9DDE7AD not found on keyserver
gpg: key CCFDB381: "oMrca Bisetto <oMrca@folgorante.net>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
```

Per continuare

`gpg --help`

`man gpg`