

# Comunicazioni e identità sicure: LE CHIAVI PGP E GPG uso e abuso

By Martino Colucci  
Linux Night 14 Aprile 2010  
martyn at ultrapowersystem dot it

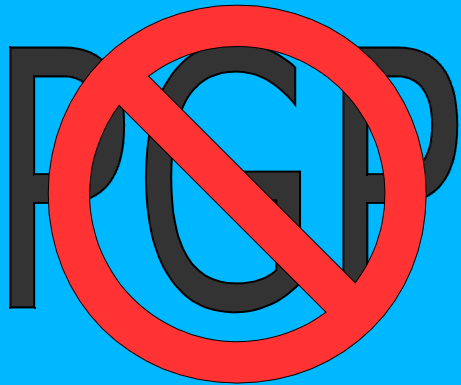


## Che cosa è PGP?

PGP significa PRETTY GOOD PRIVACY (privato sostanzialmente buono), è un sistema a chiavi asimmetriche per la criptazione e decriptazione di testi, viene usato anche per cifrare le e-mail, ma non solo... .  
può essere usato anche come “firma digitale” per “identificare” un dato utente.

Nato dalla mente di Phil Zimmermann nel 1991, il PGP intendeva rendere accessibile e semplice la crittografia in ambito informatico.

Un uso corretto di tale tecnologia, garantisce un buon livello di sicurezza.



Il diffondersi di tale tecnologia al di fuori dei confini USA, causò a Zimmermann, nel 1993, una indagine dal Governo degli Stati Uniti per “esportazioni di armi senza licenza”. Codifiche con chiavi oltre i 40 bit venivano considerate illegali in quanto vere e proprie armi, e nativamente PGP supportava chiavi che partivano da 128 bit.

Da PGP nacquero le specifiche e lo standard OpenPGP.

PGP è un prodotto commerciale brevettato, alcuni suoi “gap” hanno fatto nascere versioni alternative come GPG che seguono appieno lo standard OpenPGP

Per maggiori info su PGP: [http://it.wikipedia.org/wiki/Pretty\\_Good\\_Privacy](http://it.wikipedia.org/wiki/Pretty_Good_Privacy)  
<http://www.pgp.com/>

# Cos'è GPG?

GPG, ovvero Gnu Privacy Guard, è una alternativa libera al “brevettato” PGP, segue lo standard OpenPGP e lo standard IETF, è sostenuto dal Governo Tedesco e dalla Free Software Foundation e, ovviamente, ha una licenza GNU GPL

GPG è disponibile per Unix, Linux ma anche per MS Windows e Mac OS X.

Anche GPG usa chiavi asimmetriche per codificare i messaggi, un elemento di affidabilità e sicurezza, ed è un prodotto maturo e stabile.

GPG funziona sostanzialmente come il PGP, rendendo la crittografia semplice e la sicurezza accessibile a tutti.

Nel 2000 il Governo Tedesco a stanziato e finanziato il porting per piattaforme Microsoft Windows

The logo consists of the letters 'GPG' in a large, bold, black, sans-serif font. A yellow five-pointed star is positioned to the right of the second 'G', partially overlapping its right side.

Maggiori info:

<http://www.gnupg.org/index.html>

[http://it.wikipedia.org/wiki/GNU\\_Privacy\\_Guard](http://it.wikipedia.org/wiki/GNU_Privacy_Guard)

[http://it.wikipedia.org/wiki/Internet\\_Engineering\\_Task\\_Force](http://it.wikipedia.org/wiki/Internet_Engineering_Task_Force)

## OK, ora so cos' è il PGP e il GPG, ma come li uso?

Essenzialmente, per usare GPG, bisogna prima creare una coppia di chiavi, una pubblica e una privata.

Il comando per fare questo è: `$gpg --gen-key`

consiglio una chiave che abbia almeno 1024 bit di dimensione (una dimensione maggiore non fa male, anzi, aumenta la sicurezza della chiave stessa) ed una durata non infinita, 5 anni è un buon compromesso.

Il secondo passo è pubblicare la “chiave pubblica” su un server di chiavi.

```
$ gpg --keyserver [nome server] --send-key  
[id della chiave]
```

In questo modo potete far sì che chi voglia comunicare con voi possa scaricare la vostra chiave pubblica per inviarvi i messaggi crittografati.

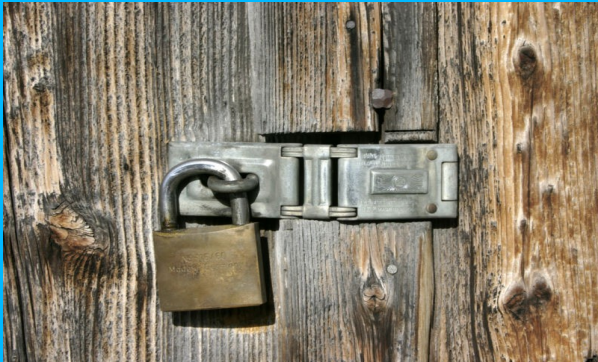


Andiamo avanti...

Il terzo passo è quello di far sapere a tutti quelli che conoscete dove trovare la vostra chiave pubblica, anche voi potete ricercare le chiavi dei vostri amici e conoscenti, o delle persone che volete comunicare in modo crittografico, sui server di chiavi.

Questo il comando:

```
$ gpg --keyserver [nome server] --search-keys [nome chiave o utente]
```



Due server dove potete cercare sono:

```
hkp://pgp.mit.edu:11371
```

```
ldap://keyserver.pgp.com
```

Ora avete tutte le informazioni per poter mandare messaggi crittografati.

Vi consiglio di leggere la guida di gpg, per il resto dei comandi, che potete avere dando questa stringa su terminale (bash o simile):

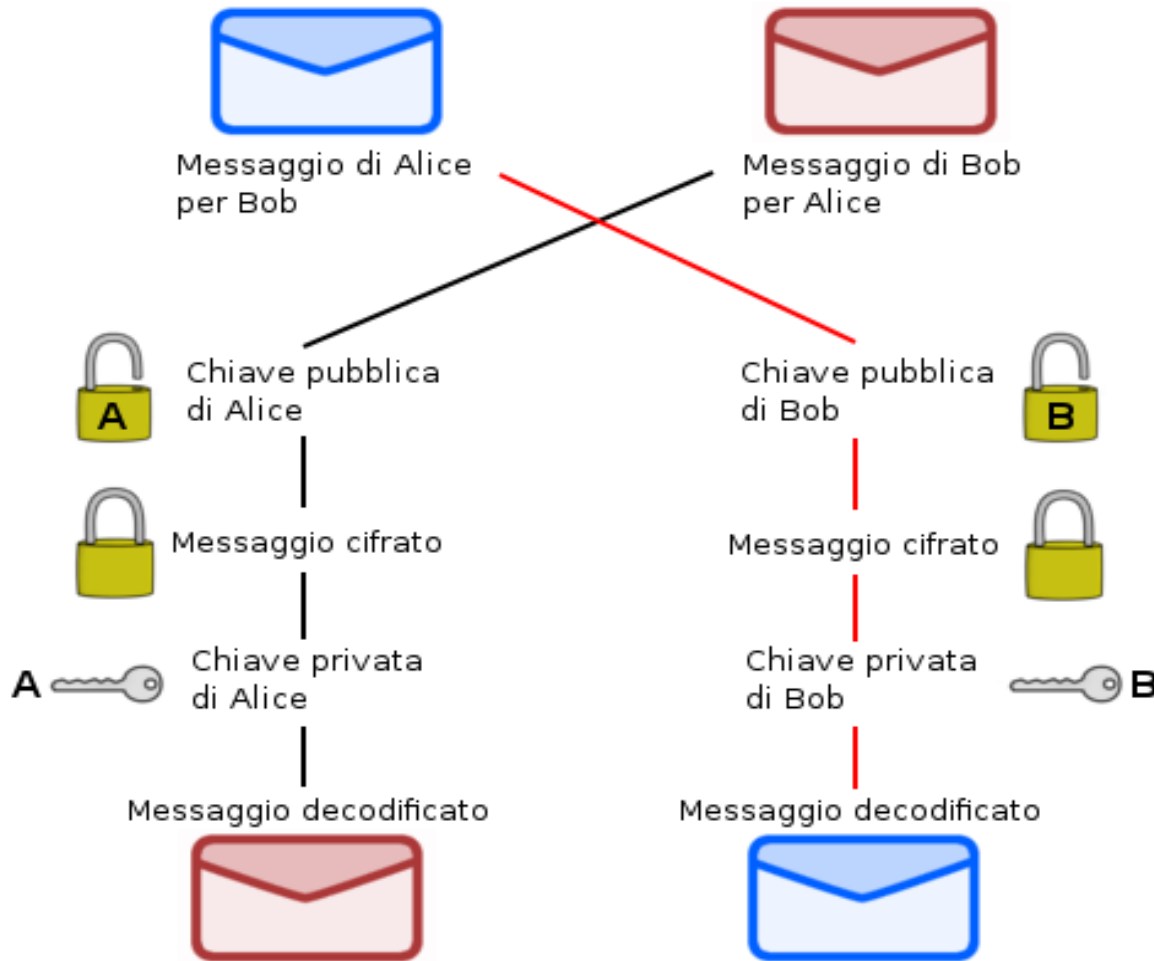
```
$man gpg
```

oppure questo per i comandi rapidi:

```
$gpg --help
```

# Ok! Ma come funziona?

Il meccanismo è semplice, dal keyserver si recupera la CHIAVE PUBBLICA dell'utente a cui si intende mandare il messaggio, si cripta il messaggio, lo si spedisce, all'arrivo l'utente usa la propria CHIAVE PRIVATA ( o SEGRETA) per decifrare il messaggio. Notare che una volta usata la chiave pubblica per criptare, la chiave pubblica non può decriptare il messaggio, serve la chiave privata. In poche parole un circuito a senso unico dove la chiave pubblica cripta e quella privata decrypta.



Nell'esempio qui a lato Bob spedisce un messaggio ad Alice usando la chiave pubblica di Alice. Alice leggerà il messaggio deciptando il tutto con la sua chiave privata. L'inverso sarebbe accaduto se Alice volesse mandare un messaggio a Bob. In questo caso Alice userebbe la chiave pubblica di Bob, e Bob la sua chiave privata per decodificare il messaggio.

Il circuito è a senso unico.

## Ok! Adesso so come funziona, cosa devo fare?

Adesso sei pronto a usare il tuo paio di chiavi per comunicare con il mondo in modo sicuro.

Ma abbiamo ancora una cosa da fare, creare una **RETE DI FIDUCIA**.

Una rete di fiducia è una interconnessione che si ha con diversi utenti, lo scopo primario è quello di **FIRMARE** le chiavi pubbliche di chi si conosce, o si è conosciuto. In questo modo vi garantisce che la chiave che usate è proprio della persona che volete contattare, date fiducia con la vostra firma.

Inoltre altre persone avranno firmato la chiave del vostro contatto, e magari li conoscete anche, e vi fidate di loro, quindi, pur non conoscendo la persona, potete "fidarvi" in quanto conoscete chi ha firmato la chiave pubblica di questo sconosciuto.

Per firmare una chiave, dopo che avete verificato che appartenga al proprietario, potete firmarla:

```
$gpg --sign-key [ID della chiave da firmare]
```

In questo modo firmerete con la vostra chiave privata, la chiave pubblica di un vostro conoscente, altri potranno vedere che avete firmato la chiave e, visto che vi conoscono, potranno "fidarsi" di voi.

Se avete più chiavi, il comando per selezionare la chiave è:

```
$gpg --default-key [chiave che si vuole usare] --sign-key [chiave da firmare]
```

Potete vedere i dettagli di una chiave firmando:

```
$gpg --fingerprint [ID della chiave]
```

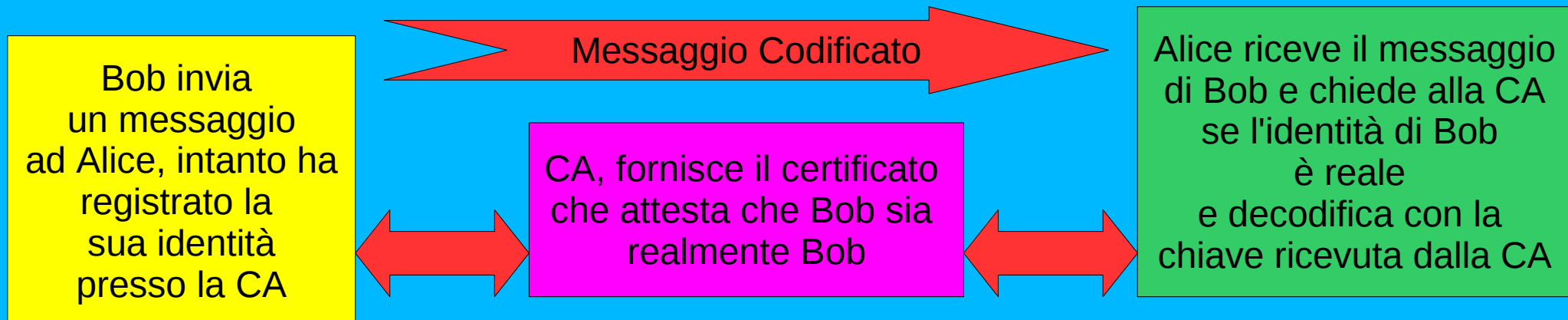
In questo modo potete anche vedere le eventuali firme fatte da altre persone con gli ID delle loro chiavi.

## Perché quindi un Key Sign Party?

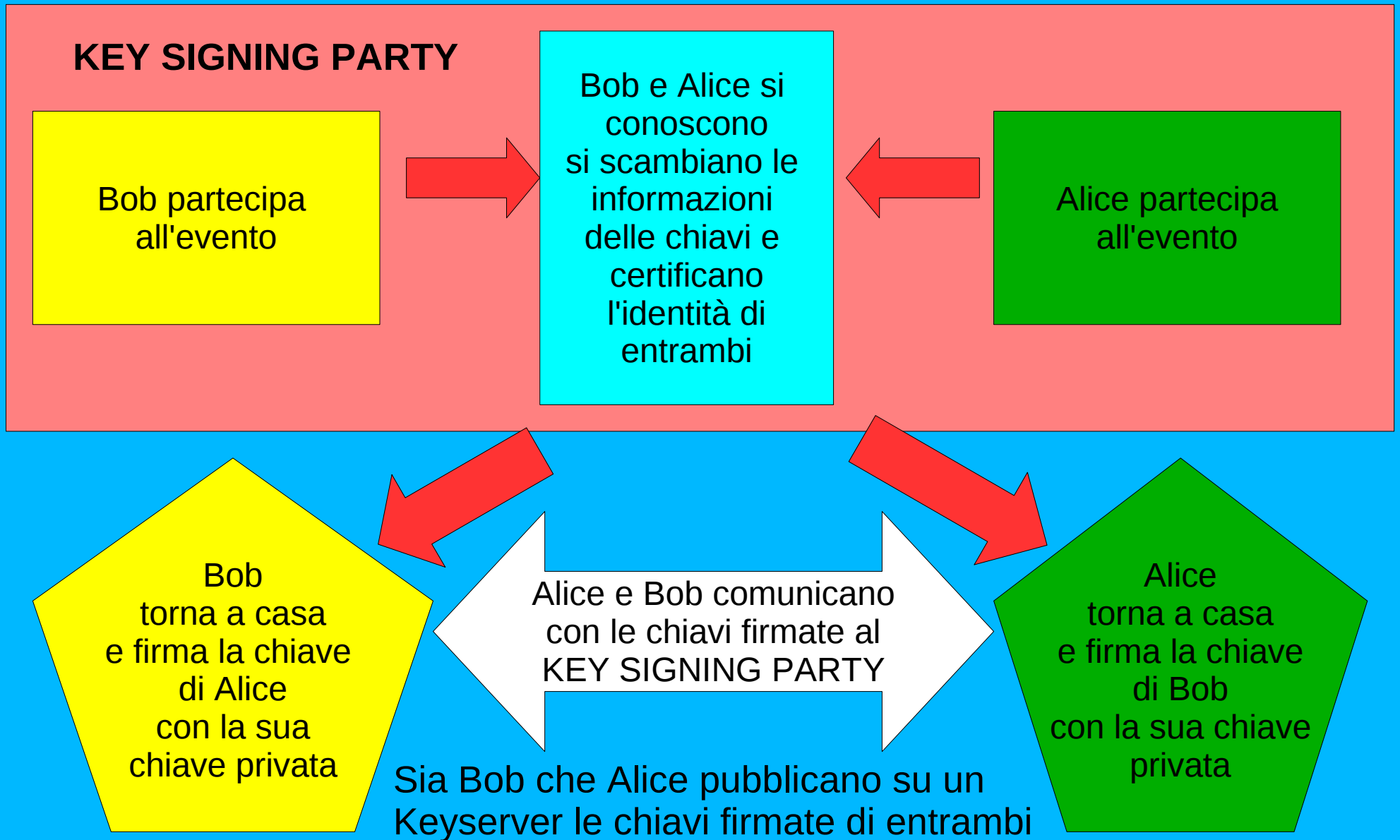
Ovvio! In un KEY SIGN PARTY potete conoscere di persona il proprietario della chiave, verificare che la chiave sia la sua.

In un contesto di sicurezza questo passo viene demandato a una CA (Certificate Authority) che certifica la chiave e l'identità del soggetto.

Il modello è quello che segue:



In un **KEY SIGNING PARTY** il processo è simile, ma diverso, il “certificate authority” viene sostituito dalle firme degli utenti che si conoscono all'evento, è la propria chiave privata a garantire per la chiave pubblica della persona conosciuta:



# Domande ?

Grazie per partecipato!

Per maggiori informazioni seguite questi link:

<http://www.gnupg.org/index.html>

[http://it.wikipedia.org/wiki/GNU\\_Privacy\\_Guard](http://it.wikipedia.org/wiki/GNU_Privacy_Guard)

[http://it.wikipedia.org/wiki/Internet\\_Engineering\\_Task\\_Force](http://it.wikipedia.org/wiki/Internet_Engineering_Task_Force)

[http://it.wikipedia.org/wiki/Pretty\\_Good\\_Privacy](http://it.wikipedia.org/wiki/Pretty_Good_Privacy)

<http://www.pgp.com/>

Queste diapositive sono create con Open Office.org 2.4, i contenuti sono stati elaborati da Martino Colucci, le immagini prese da Wiki Commons e rilasciate con licenza Creative Commons CC-BY-NC-SA oppure con CC-BY-SA

Quest'opera viene rilasciata sotto la licenza Creative Commons CC-BY-NC-SA

