GnuPg, Enigmail, Posta Sicura

Zattara Stefano
stefano@zattara.org

Cos'è GnuPG 1

- “...GnuPG is the GNU project's complete and free implementation of the OpenPGP standard as defined by RFC2440 . GnuPG allows to encrypt and sign your data and communication....”
- GnuPG è il progetto GNU di una completa e libera implementazione dello standard OpenPGP come definito dall RFC2440. GnuPG permette di criptare e firmare i tuoi dati e le tue comunicazioni....

Cos'è GnuPG 2

- GnuPG è un sitema che, basandosi su una chiave pubblica e privata, permette di firmare i propri documenti (ovvero permette di autenticare il mittente e di impedire modifiche), e di criptarli, rendendoli leggibili solo a se stessi e/o solo ad altri.

Cos'è GnuPG 3

- Io utente creo una coppia di chiavi, ed un certificato di revoca, chiamate chiave pubblica e chiave privata. Volendo (consigliato) è possibile mettere una password sulla chiave privata.
- Come dice il nome, la chiave privata devo tenerla io, mentre la pubblica posso (devo) distribuirla.
- Uso la mia chiave privata per firmare i messaggi e chi li riceve li verifica con la mia chiave pubblica.

Chiave pubblica?!

- E' importante che io “distribuisca” la chiave pubblica, perché altrimenti chi riceve la mia mail non può autenticarla e quindi non serve a nulla.
- E' importante firmare le chiavi di cui si è certi, in modo da rendere più forte uno dei punti deboli del sistema.
- KeyServer.

EnigMail

- EnigMail permette di portare l'uso di GnuPG sulla posta con thunderbird, e quindi permette di gestire mail firmate/criptate.
- EnigMail perché è il più usato/conosciuto.
- Thunderbird perché è veloce, pratico, sicuro, facile da usare, bello.

Esempio Pratico:

```
guest@Tux ~ $ gpg –help
[.....]
Home: ~/.gnupg
Algoritmi gestiti:
A chiave pubblica: RSA, RSA-E, RSA-S, ELG-E, DSA
Cifrari: 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH
Hash: MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compressione: Non compresso, ZIP, ZLIB, BZIP2
[.....]
--gen-key               genera una nuova coppia di chiavi
[....]

guest@Tux ~ $ gpg --gen-key
Per favore scegli che tipo di chiave vuoi:
   (1) DSA and Elgamal (default)
   (2) DSA (firma solo)
   (5) RSA (firma solo)
Cosa scegli? 1
DSA keypair will have 1024 bits.
ELG-E keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2048
La dimensione richiesta della chiave è 2048 bit
```

Esempio Pratico:

Per favore specifica per quanto tempo la chiave sarà valida.
0 = la chiave non scadrà
<n> = la chiave scadrà dopo n giorni
<n>w = la chiave scadrà dopo n settimane
<n>m = la chiave scadrà dopo n mesi
<n>y = la chiave scadrà dopo n anni
Chiave valida per? (0) 1y
Key expires at dom 23 set 2007 12:30:20 CEST
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>"

Nome e Cognome: Zattara Stefano
Indirizzo di Email: stefano@swlibero.org
Commento: Chiave di prova
Hai selezionato questo User Id:
"Zattara Stefano (Chiave di prova) <stefano@swlibero.org>"

Modifica (N)ome, (C)ommento, (E)mail oppure (O)kay/(Q)uit? o
Ti serve una passphrase per proteggere la tua chiave segreta.

Inserisci la passphrase:

Esempio Pratico:

Dobbiamo generare un mucchio di byte casuali. È una buona idea eseguire
qualche altra azione (scrivere sulla tastiera, muovere il mouse, usare i
dischi) durante la generazione dei numeri primi; questo da al generatore di
numeri casuali migliori possibilità di raccogliere abbastanza entropia.

```
+++++++++++++++++++++++++++++++.+++++.+++++++++++++++++++++++++++++++++++++++.+++++..++
   +++++++++++++..+++++...+++++++++++++++.++++++++++.+++++.++++++++++++++++>+++++.+++++>+++
   ++>.+++++.....................................................................<+++++.................+++++^^^
```

gpg: key B6EE9B66 marked as ultimately trusted
chiavi pubbliche e segrete create e firmate.

gpg: controllo il 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: il prossimoi controllo del trustdb sarà fatto il 2007-09-23
pub   1024D/B6EE9B66 2006-09-23 [expires: 2007-09-23]
      Key fingerprint = 779E 98E4 3FC7 D943 495B 9873 B2A4 7892 B6EE 9B66
uid   Zattara Stefano (Chiave di prova) <stefano@swlibero.org>
sub   2048g/D9A73A34 2006-09-23 [expires: 2007-09-23]

guest@Tux ~ $ gpg --gen-revoke B6EE9B66

sec 1024D/B6EE9B66 2006-09-23 Zattara Stefano (Chiave di prova) <stefano@swlibero.org>

Create a revocation certificate for this key? (y/N)y

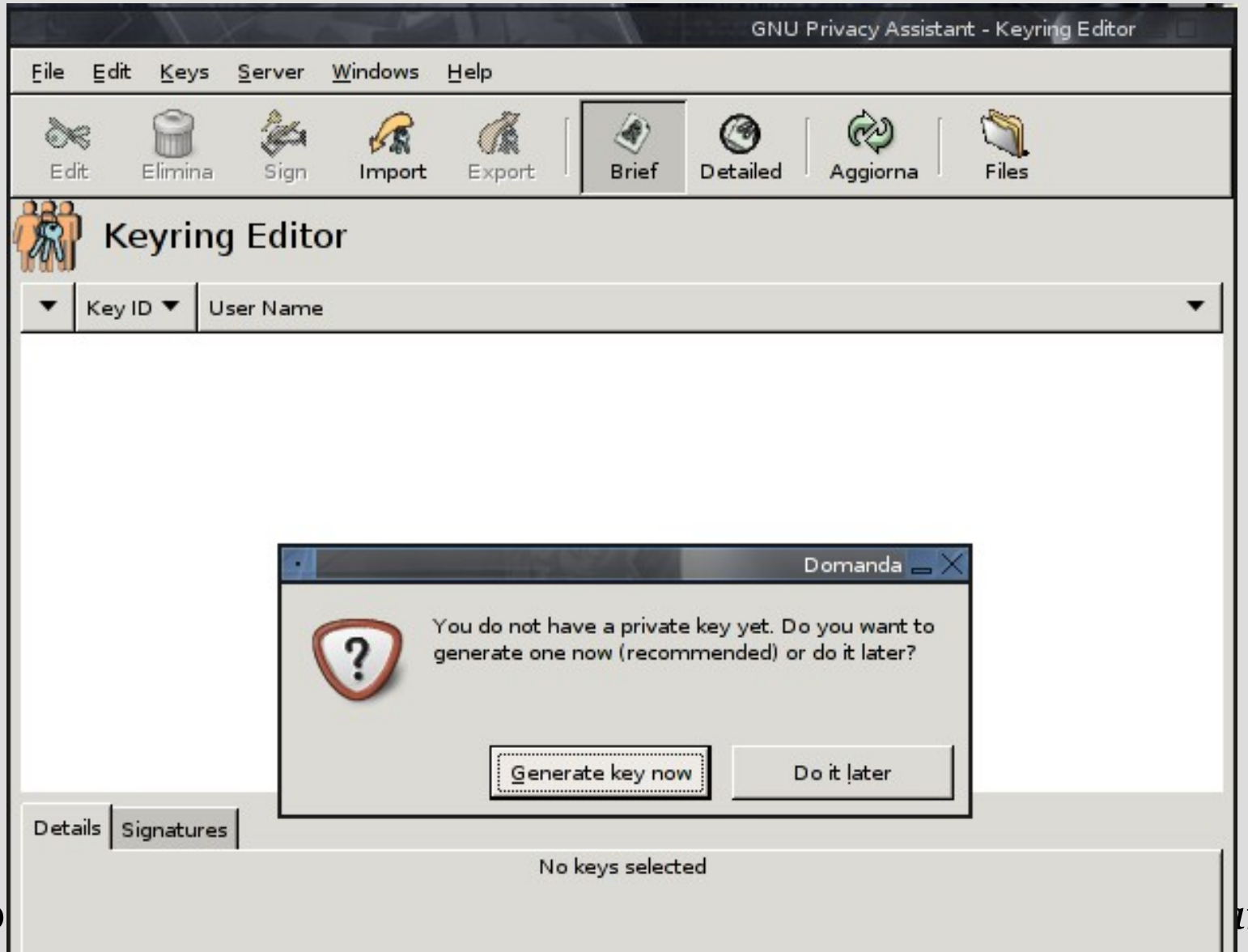
Esempio Pratico:

```
guest@Tux ~ $ gpg -k
/home/guest/.gnupg/pubring.gpg
------------------------------
pub   1024D/B6EE9B66 2006-09-23 [expires: 2007-09-23]
uid                  Zattara Stefano (Chiave di prova) <stefano@swlibero.org>
sub   2048g/D9A73A34 2006-09-23 [expires: 2007-09-23]

guest@Tux ~ $ gpg -K
/home/guest/.gnupg/secring.gpg
------------------------------
sec   1024D/B6EE9B66 2006-09-23 [expires: 2007-09-23]
uid                  Zattara Stefano (Chiave di prova) <stefano@swlibero.org>
ssb   2048g/D9A73A34 2006-09-23

guest@Tux ~ $ gpg --keyserver keyserver.linux.it –send-keys B6EE9B66
```

GPA

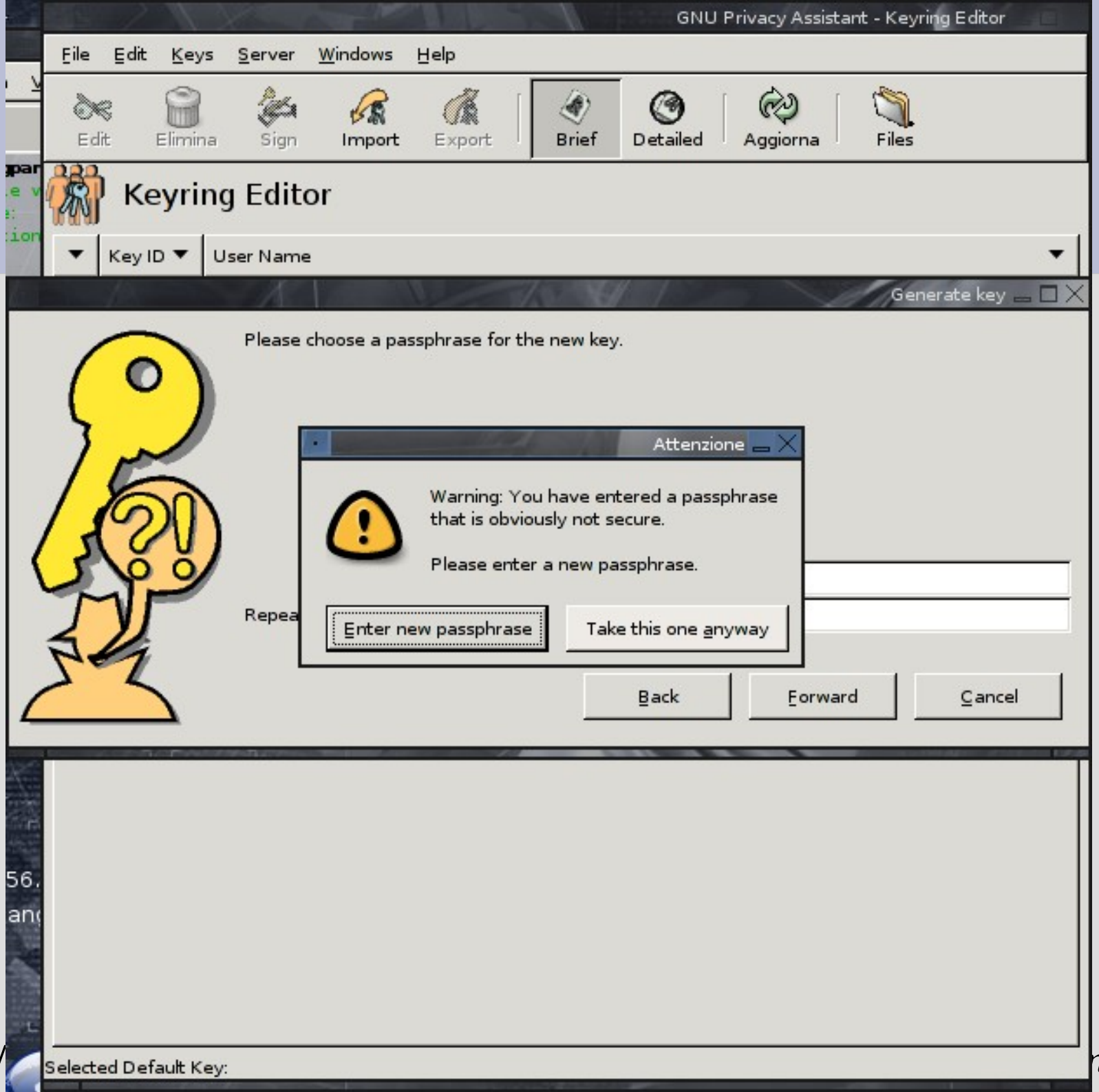
- Gnu Privacy Assistant (GPA) è una gui (Graphical User Interface) per GnuPG.
- Utilizza le gtk
- emerge -av gpa; apt-get install gpa; yum gpa

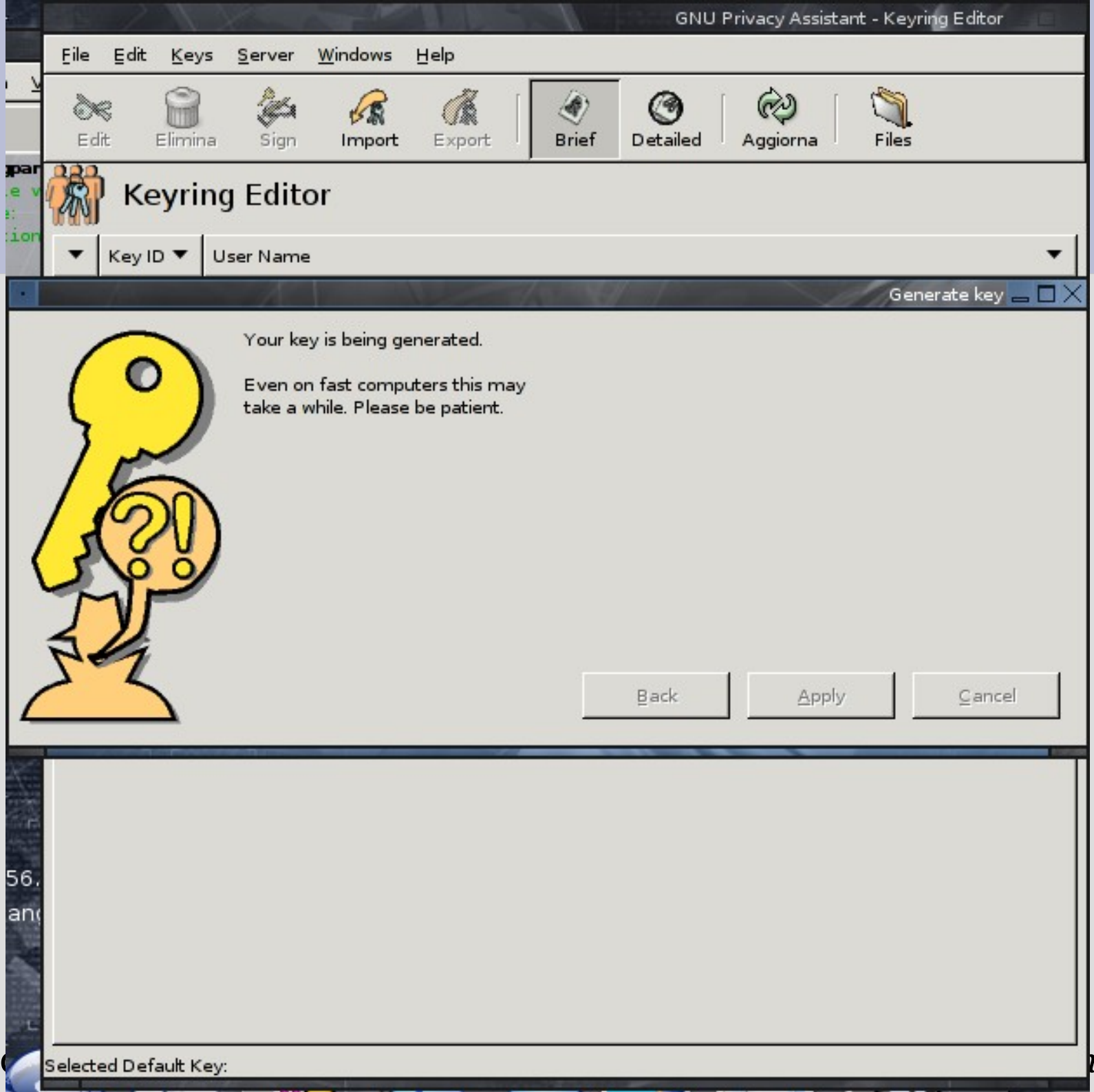
Creiamo una chiave:

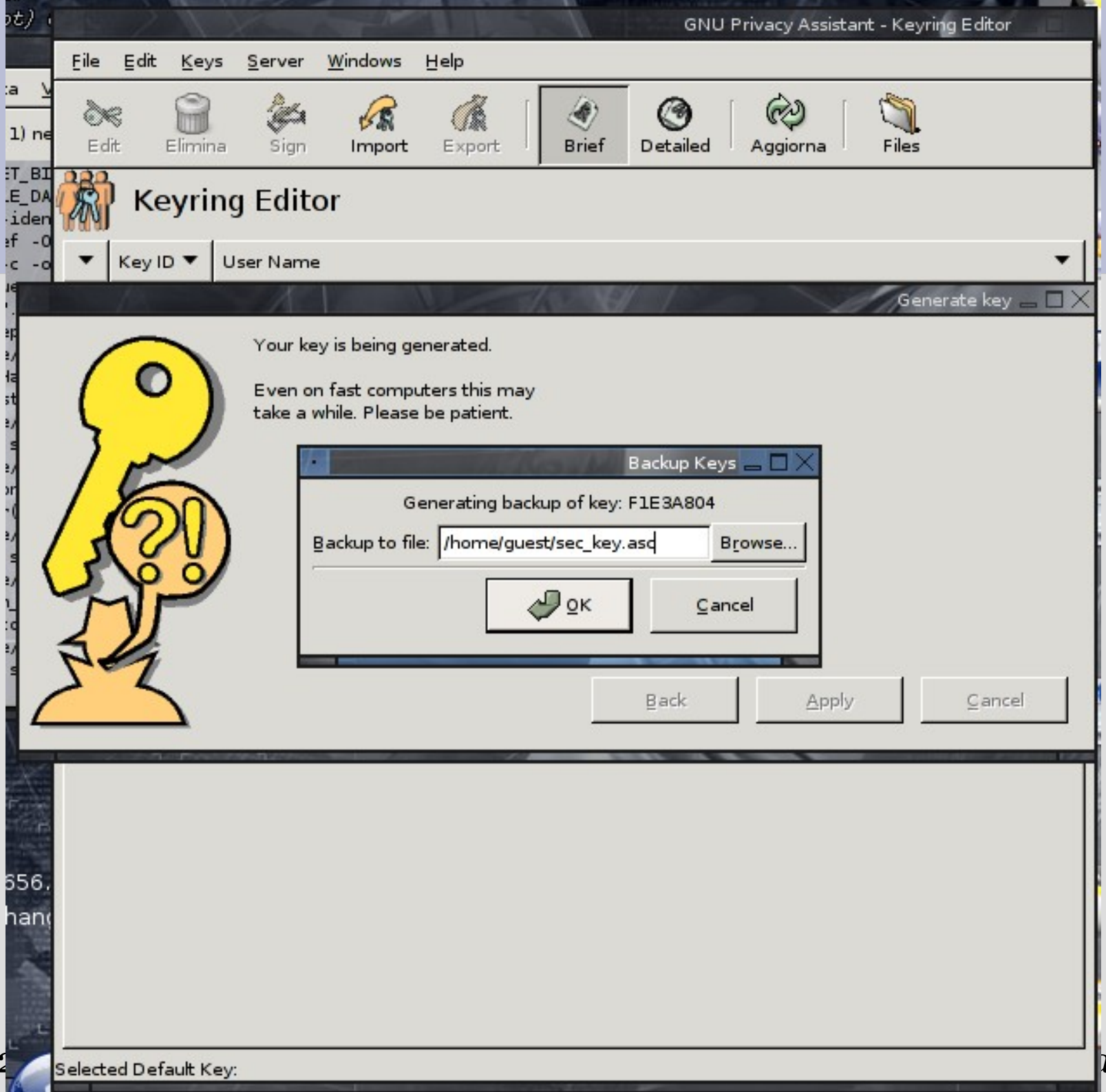


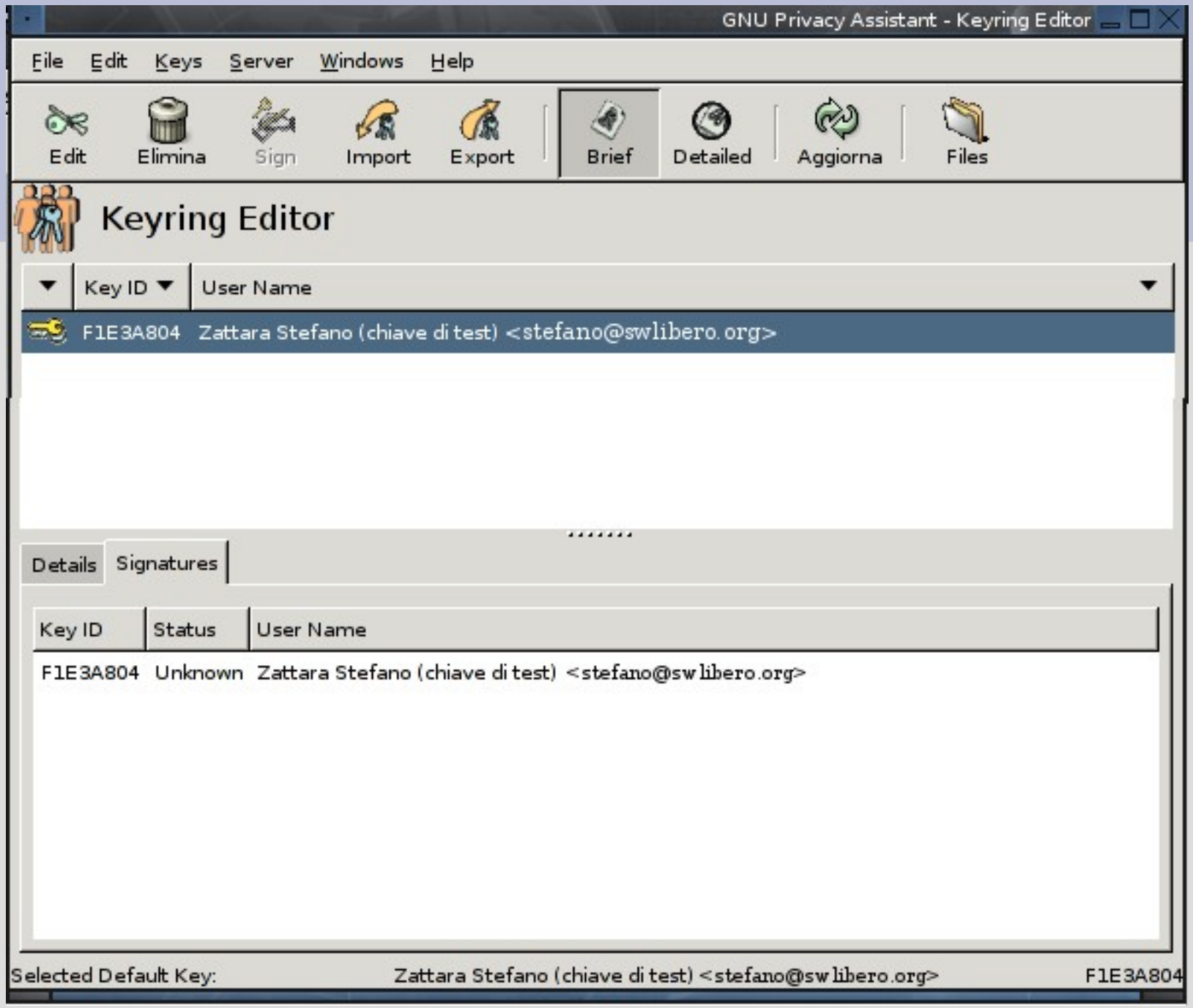

GNU Privacy Assistant - Keyring Editor
File Edit Keys Server Windows Help
Edit Elimina Sign Import Export Brief Detailed Aggiorna Files
Keyring Editor
Key ID
User Name
Generate key
Please insert your full name.
Your name will be part of the new key to make it easier for others to identify keys.
Your Name: Zattara Stefano (chiave di test)
Back Forward Cancel
Selected Default Key:


GNU Privacy Assistant - Keyring Editor
File Edit Keys Server Windows Help
Edit Elimina Sign Import Export Brief Detailed Aggiorna Files
Keyring Editor
Key ID
User Name
Generate key
Please insert your email address.
Your email address will be part of the new key to make it easier for others to identify keys. If you have several email addresses, you can add further email adresses later.
Your Email Address:
stefano@swlibero.org
Back
Forward
Cancel
Selected Default Key:

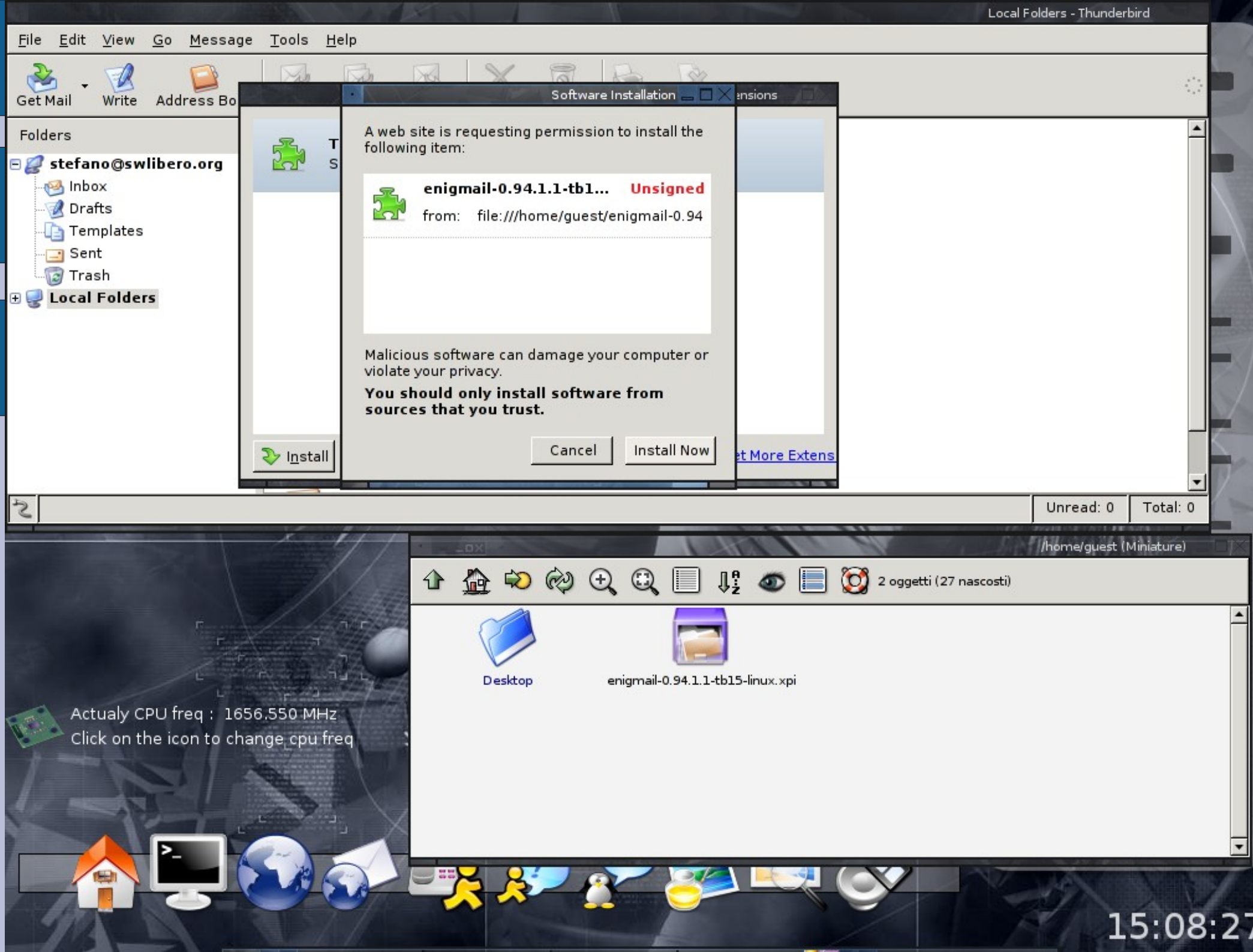

GNU Privacy Assistant - Keyring Editor
File Edit Keys Server Windows Help
Edit Elimina Sign Import Export Brief Detailed Aggiorna Files
Keyring Editor
Key ID
User Name
Generate key
Please choose a passphrase for the new key.
Attenzione
Warning: You have entered a passphrase that is obviously not secure.
Please enter a new passphrase.
Enter new passphrase
Take this one anyway
Repea
Back
Forward
Cancel
Selected Default Key:


GNU Privacy Assistant - Keyring Editor
File Edit Keys Server Windows Help
Edit Elimina Sign Import Export Brief Detailed Aggiorna Files
Keyring Editor
Key ID
User Name
Generate key
Your key is being generated.
Even on fast computers this may take a while. Please be patient.
Back
Apply
Cancel
Selected Default Key:

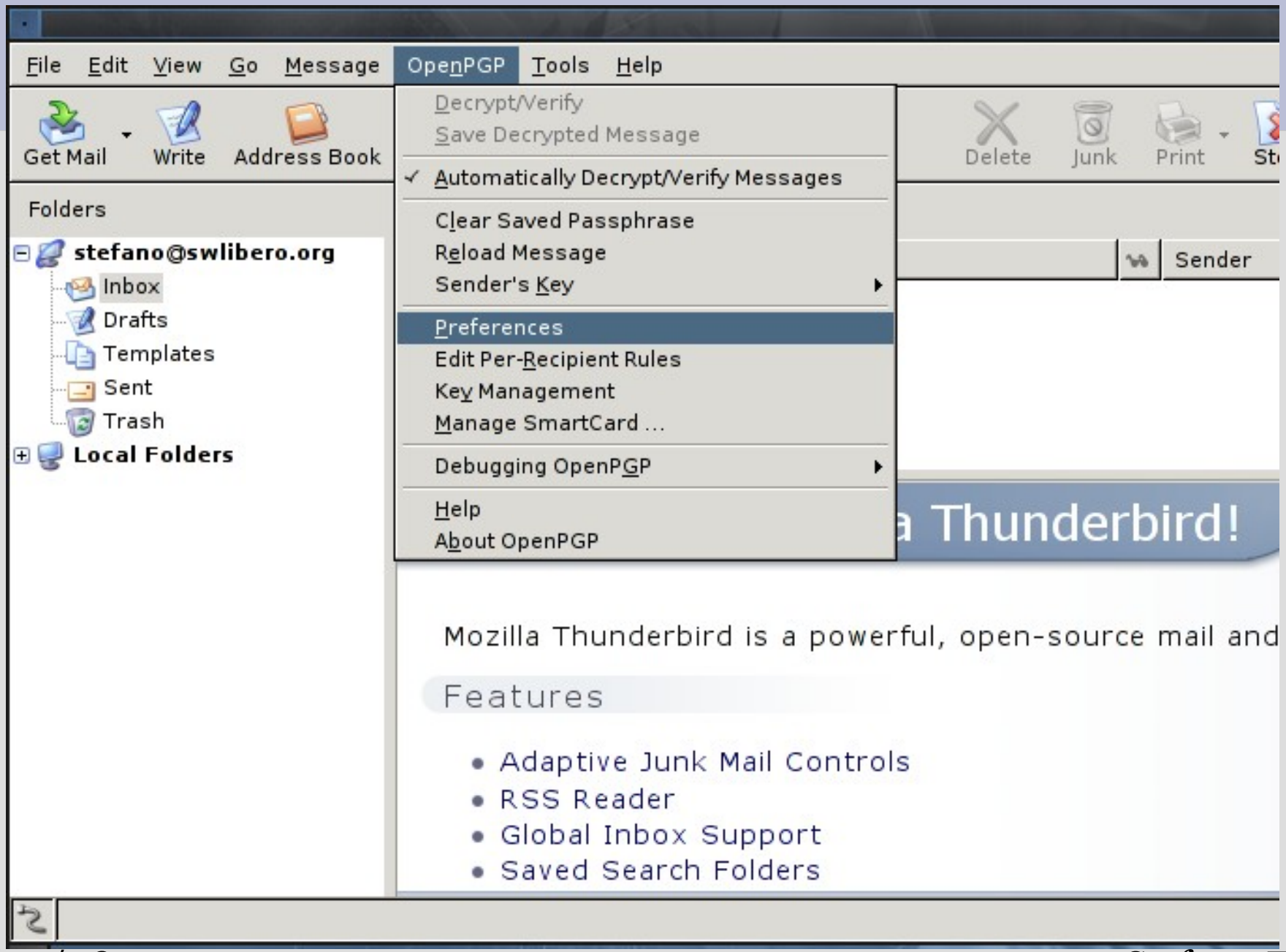

GNU Privacy Assistant - Keyring Editor
File Edit Keys Server Windows Help
Edit Elimina Sign Import Export Brief Detailed Aggiorna Files
Keyring Editor
Key ID
User Name
Generate key
Your key is being generated.
Even on fast computers this may take a while. Please be patient.
Backup Keys
Generating backup of key: F1E3A804
Backup to file: /home/guest/sec_key.asc
Browse...
OK
Cancel
Back
Apply
Cancel
Selected Default Key:


GNU Privacy Assistant - Keyring Editor
File Edit Keys Server Windows Help
Edit Elimina Sign Import Export Brief Detailed Aggiorna Files
Keyring Editor
Key ID
User Name
F1E3A804 Zattara Stefano (chiave di test) <stefano@swlibero.org>
Details Signatures
Key ID Status User Name
F1E3A804 Unknown Zattara Stefano (chiave di test) <stefano@swlibero.org>
Selected Default Key: Zattara Stefano (chiave di test) <stefano@swlibero.org> F1E3A804

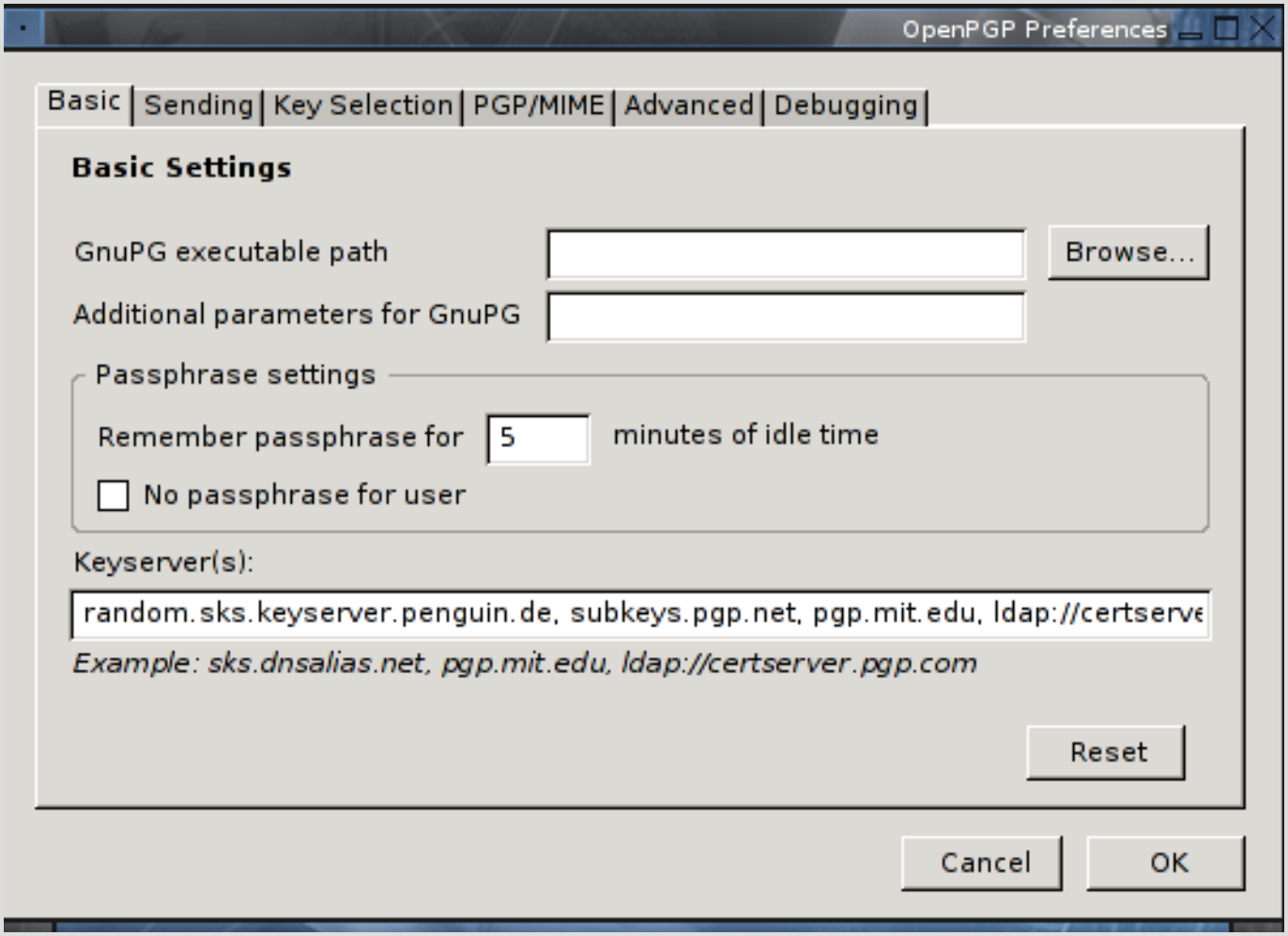
Impostazione Thunderbird


Local Folders - Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Bo
Folders
stefano@swlibero.org
Inbox
Drafts
Templates
Sent
Trash
Local Folders
Software Installation
A web site is requesting permission to install the following item:
enigmail-0.94.1.1-tb1...
Unsigned
from: file:///home/guest/enigmail-0.94
Malicious software can damage your computer or violate your privacy.
You should only install software from sources that you trust.
Cancel
Install Now
Install
Unread: 0
Total: 0
/home/guest (Miniature)
2 oggetti (27 nascosti)
Desktop
enigmail-0.94.1.1-tb15-linux.xpi
Actualy CPU freq : 1656,550 MHz
Click on the icon to change cpu freq
15:08:27

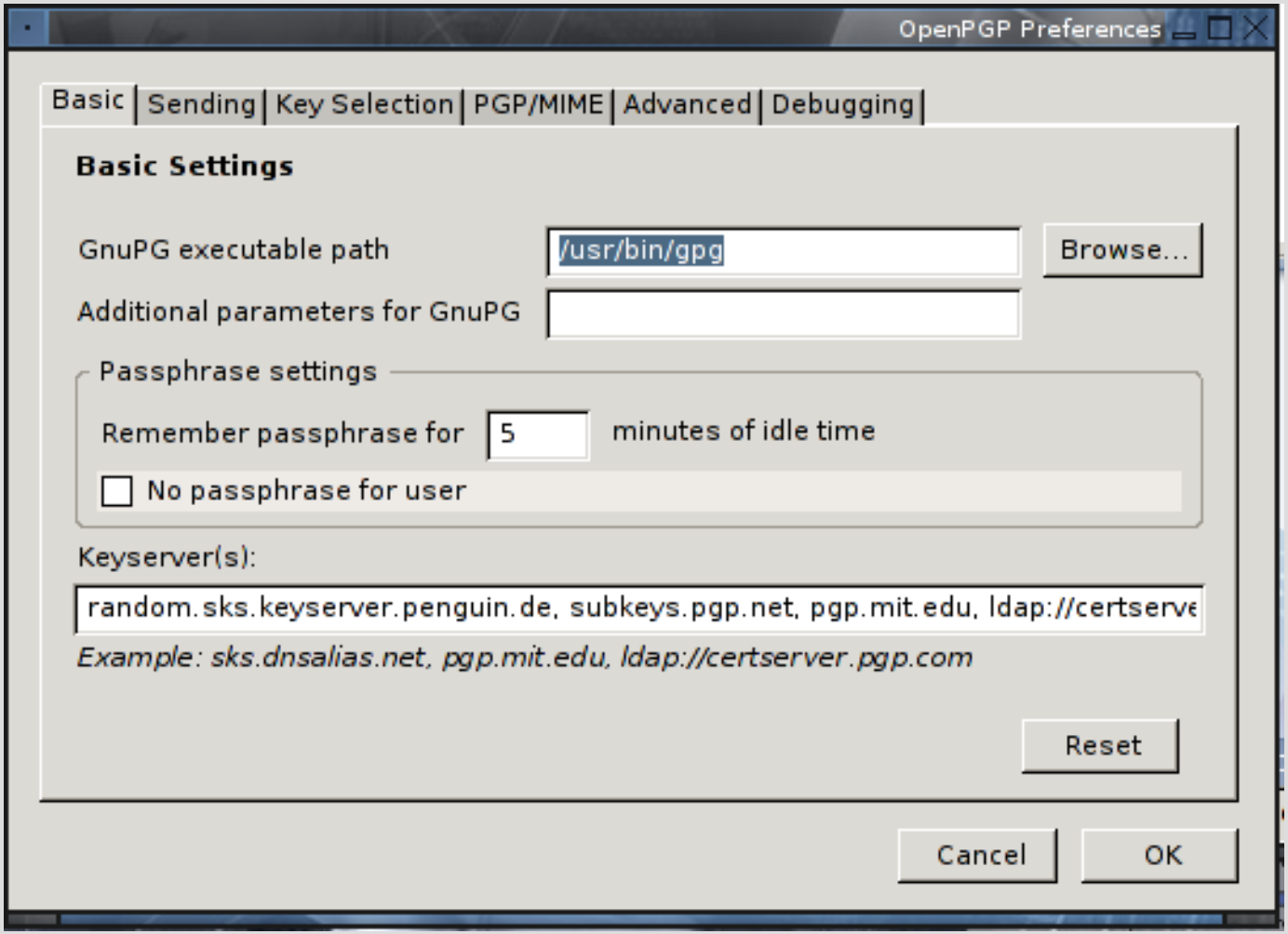
Impostazioni:



Finestra Impostazioni 1



Finestra Impostazioni 2



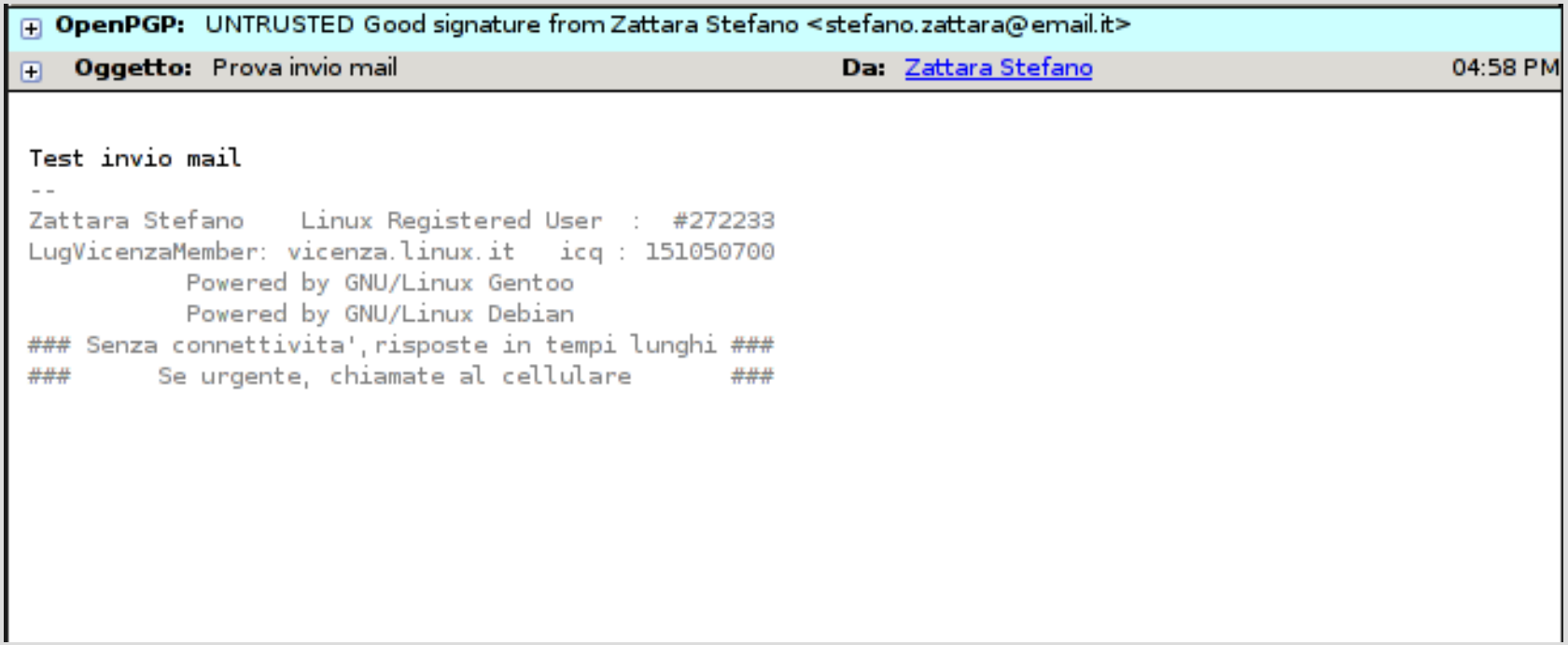
Messaggio Firmato

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Test invio mail
- --
Zattara Stefano    Linux Registered User  :  #272233
LugVicenzaMember: vicenza.linux.it   icq : 151050700
           Powered by GNU/Linux Gentoo
           Powered by GNU/Linux Debian
### Senza connettivita', risposte in tempi lunghi ###
###      Se urgente, chiamate al cellulare       ###


-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.5 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org

iD8DBQFFF+6GOyFeqbwEdJERAswlAJwJK3BXnnvim6CpwELXOKvbx7yVSQCfXOz+
VUdsz81mRVs79Sa0JF2WVcY=
=PaTl
-----END PGP SIGNATURE-----
```

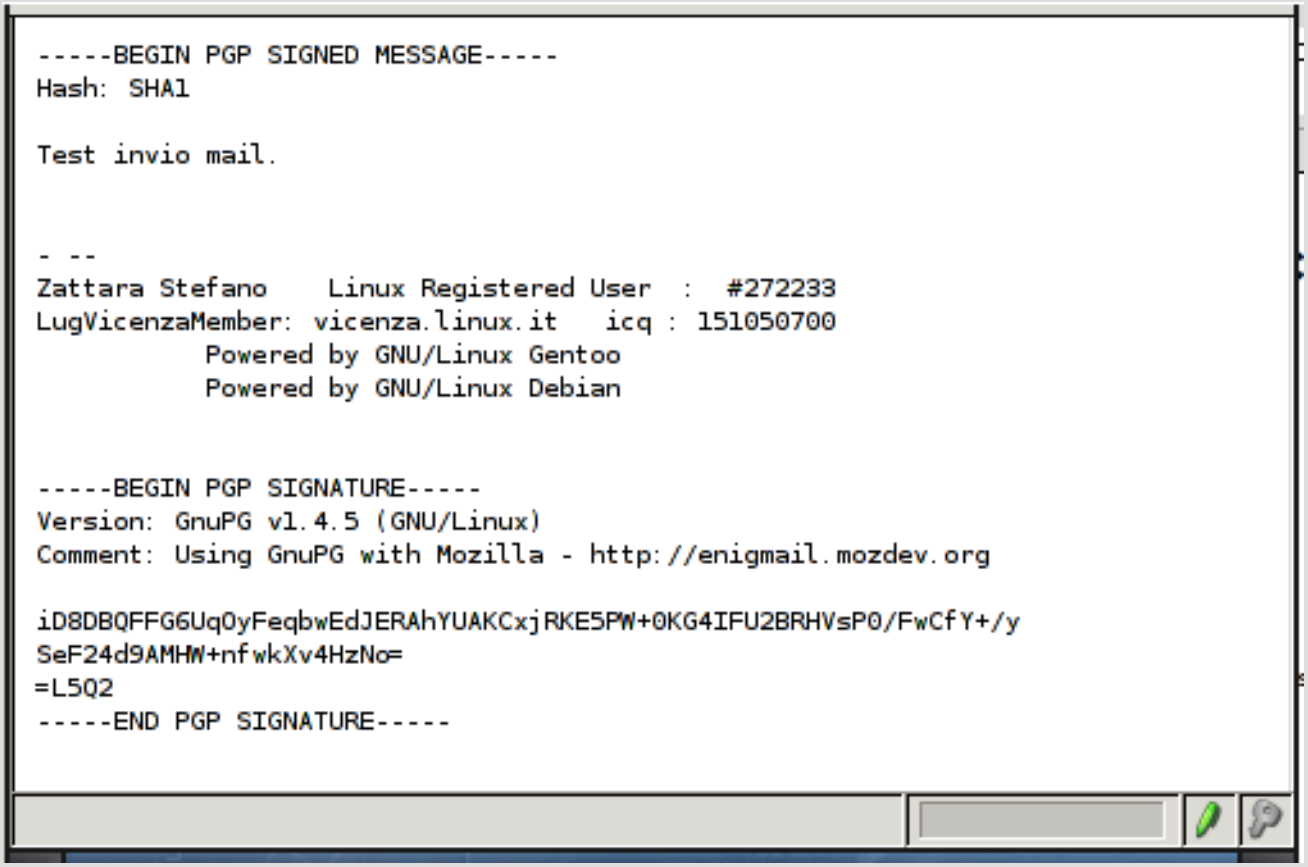
Messaggio Criptato

```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-15
Version: GnuPG v1.4.5 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org

hQQOAwTjPlo4HbeAEA//dCwmW9PupIDjIa2QyvcCToQlWtRCJprmgol7P+4klzit
Q4iZO6LYsk4pYsKOAXWcM4qjk4Gfg7aTrn+0jYLbt6Cf6CflGnyEAWgGTqstgMFq
mQNCSE5ic/SdX2emUpn5zXYHcwsLRgt06cl6LIGtxQhX4Xl6su15XIJcRQMnta2x
3fpe3sTqSmvZR6Go3Gyg/3Fjq6XuD0neyekFUwYbpSE2x866VhX3510wTQciWZ8T
HL5jGQqktZP9jHTlgel2nMXHNK2MaZUO7wqlixYP6xLgaEv76IRp3ePZyWPfErIv
HCttzluUeSo0f+RZ3p7WL9RzgVEB4UkaahQM3MpMWuXOq2xstvLEMx4FOubjQuGG
c69BDHqhvcGAuW5c0mtcBG2slbvUhtyXq56qMg98foc1BPa/wUvOSaebyYZaey6O
oz+QmASCgP7IEMxLnlQ0MoYrtsRYiXas5Jqo2wh3vhMZJoQ4HC6bydcoy3On1j13
OlBkETeIaV46ouXatZNB984oLQDbpMxX1g6eWX5PoAha5MrA8GOosdEnoBqNDaZl
g6QEEg+IyDSOaILqBzigQPoCIKonyvkpITmifYVaR8yonBXWyixv73gfBvch6St+
75QDH5CBJREPHK57KWFn9O/0w6eV/mcvu3YuXz9PZ1+8Zz090MCpgct4kG5elMQQ
AMKy+ZVRpU4Kf3z1ZKEzDtJgrCuxmZ5VZ82wdYzp8LYEcwgbPa5kdgTihxjsAPxj
ah+GIzRxh0HdQPNSZA2J8qQwXvKPMYEOUDkTKRPH3fCu4TzonZWTVHuZXPcKkVtY
jAfF4AfYng4dt5LQd5LSBMd9EiNLvCJkM+IbFIH901bknm0dHiaacFCuKc5x+U2z
3kNfUms7nroAAJ+kLV+w6czz6J9LqC7JY77L3uzASOybmBIkELnrTfbJFSkpAvrf
HOtz0UOcKakllkOStGR6ADH4i6CCBTARfyZKddpcPUcm7MUOMN9SukgpFAIGswrQ
```

Messaggio firmato e verificato

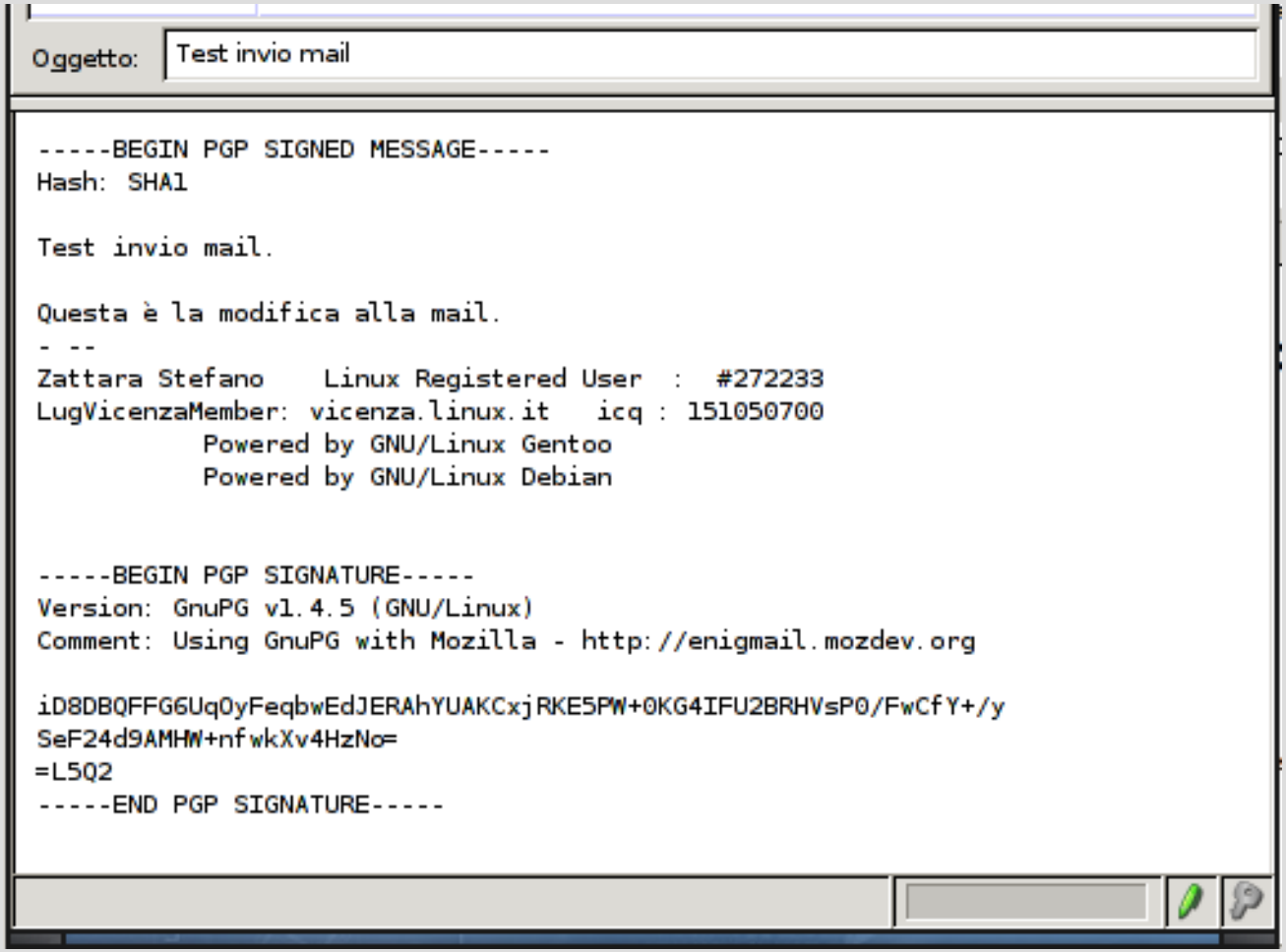


Alterazione messaggio

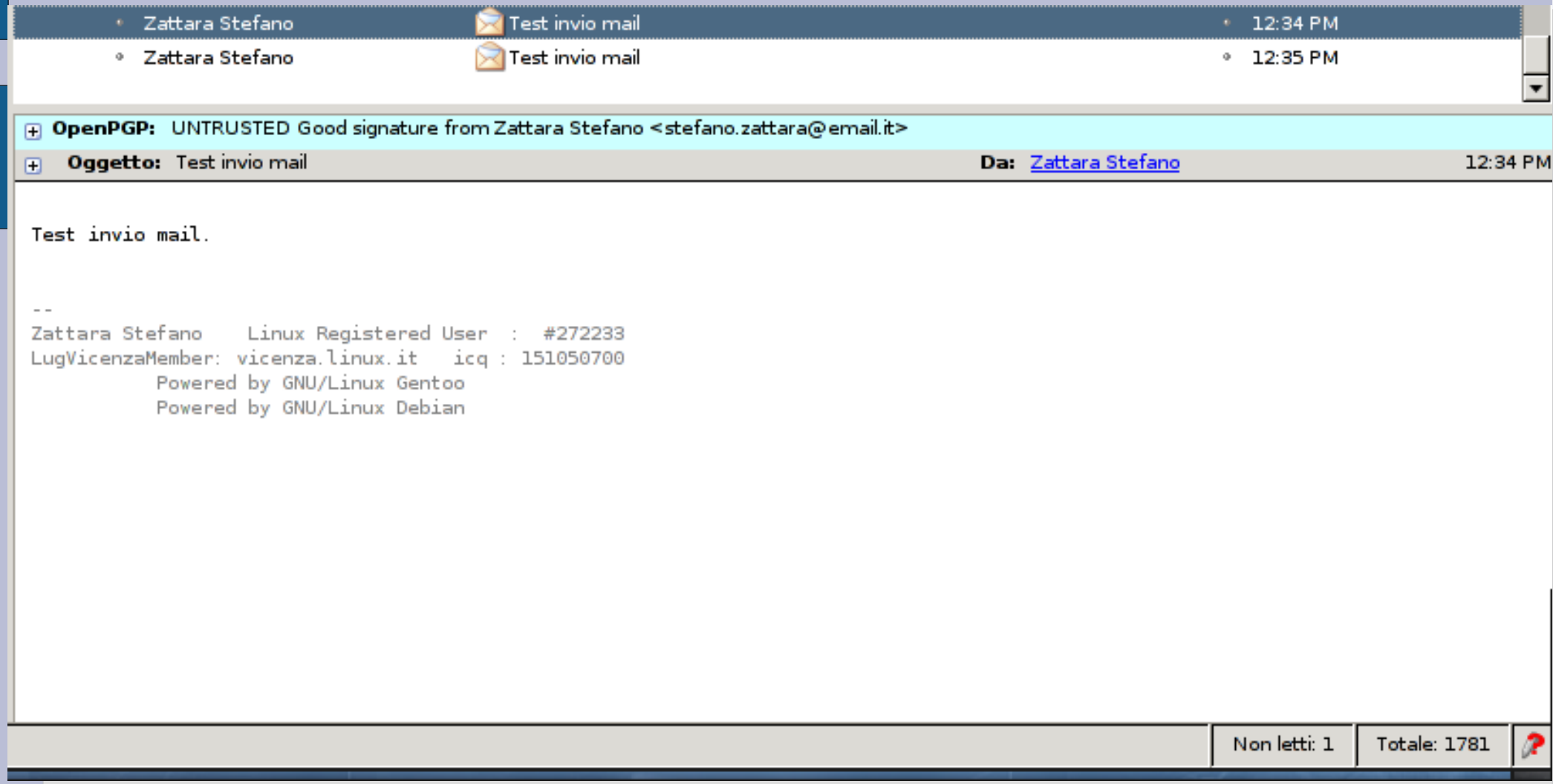


```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Test invio mail.


- --
Zattara Stefano    Linux Registered User  :  #272233
LugVicenzaMember: vicenza.linux.it   icq : 151050700
           Powered by GNU/Linux Gentoo
           Powered by GNU/Linux Debian


-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.5 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org

iD8DBQFFG6UqOyFeqbwEdJERAhYUAKCxjRKE5PW+0KG4IFU2BRHVsP0/FwCfY+/y
SeF24d9AMHW+nfwkXv4HzNo=
=L5Q2
-----END PGP SIGNATURE-----
```

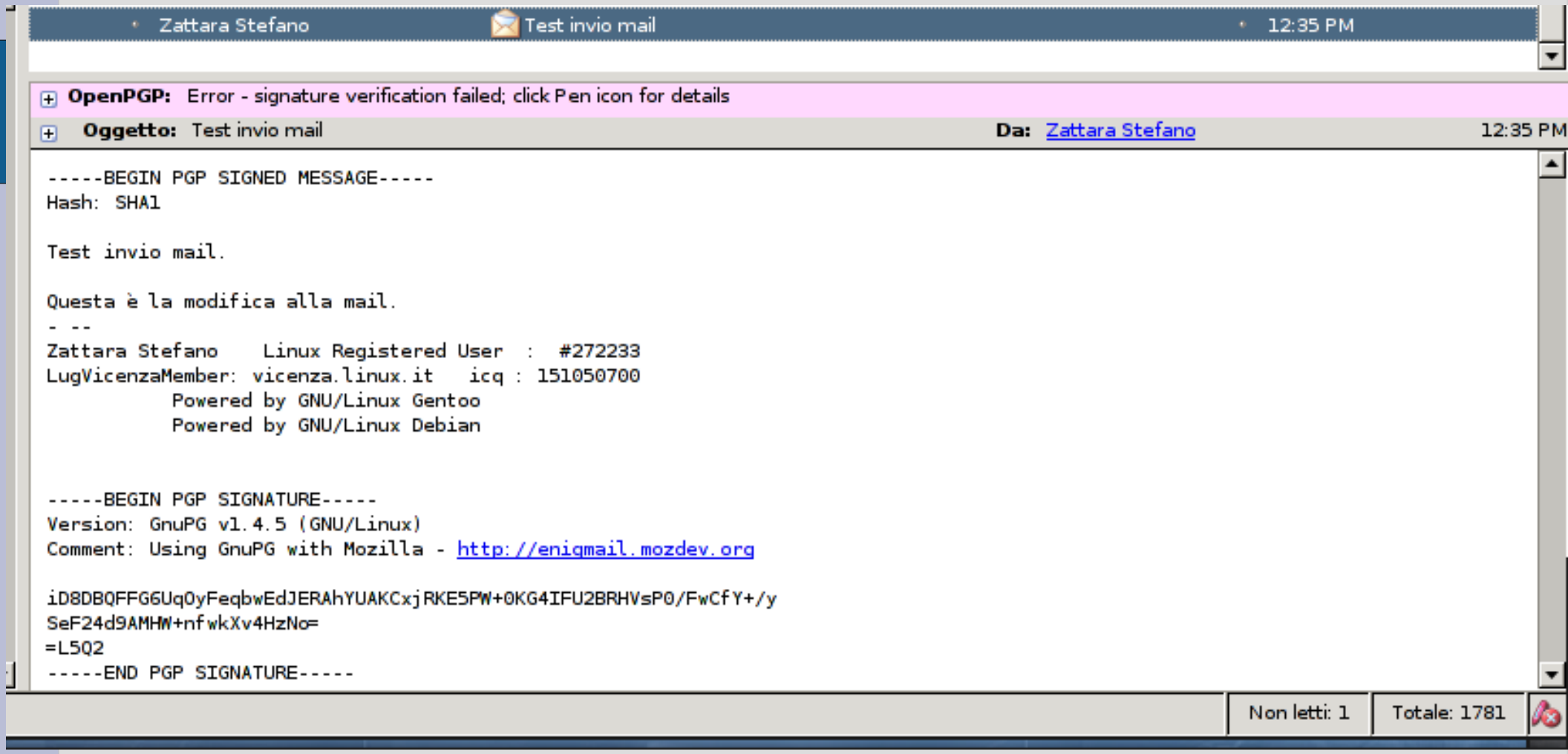
Alterazione messaggio



Validazione messaggio



Errore sul messaggio



Fonti

- http://www.gnupg.org
- http://keyserver.linux.it
- http://it.wikipedia.org/wiki/RSA
- http://www.google.it/linux
- IRC
- ICQ

Domande e Risposte teoria

Next Step: Esempio veramente pratico