HACKMEETING 2007

francesco@cybervalley.eu

LFG

HACKMEETING 2007

introduzione alle implementazioni per la cifratura della posta elettronica applicate a due client di posta elettronica

Mozilla Thunderbird

LFG

File Modifica Visualizza Vai Segnalibri Schede Aiuto

Indietro Avanti Ferma Aggiorna Home Cronologia Segnalibri Trova

http://www.mozillaitalia.it/thunderbird/ Vai

FLUG Primipassi Yahoo! Super Norvegia IP TTips WP Yahoo! WEB CAM AINEVA powder T.tribe LRadio

mozilla thunderbird

de | en | es | fr | **it** | ja | nl | zh

Menù principale

Home
Funzionalità
Download
Documentazione
Scorciatoie da tastiera
Scorciatoie da mouse
Consigli e trucchi
Condivisione posta
Protezione della privacy
Posta in arrivo globale
Posta indesiderata
RSS
Raggruppamento messaggi
Ricerche come cartelle
Supporto
FAQ di Thunderbird
Modifica file di config.
Estensioni
Temi

Link

Progetto Thunderbird
Forum di Thunderbird
Mozilla.org
Mozilla Italia
Mozilla Firefox Help

Info sul sito

Informazioni sul sito
Novità sul sito

Mozilla Thunderbird Help

Benvenuti in Mozilla Thunderbird Help! Questo sito è dedicato a Thunderbird, il nuovo client di posta e news reader da Mozilla.org. Il sito è progettato per chi vuole imparare a configurare Thunderbird affinché venga incontro alle proprie esigenze.

Mozilla Thunderbird - Il Nuovo Client di Posta da Mozilla

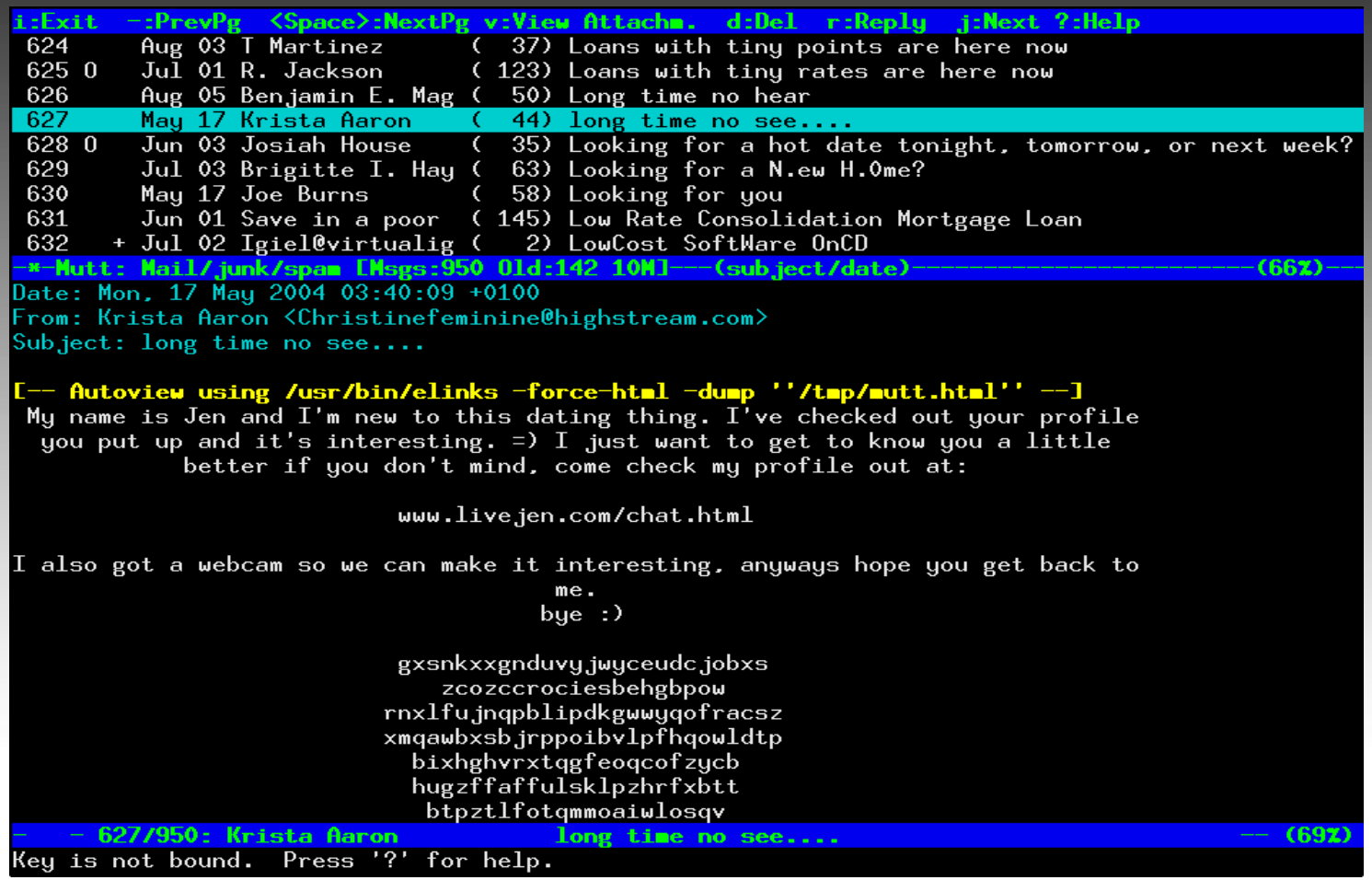
Mozilla Thunderbird è un client di posta e news reader gratuito, open-source e multi-piattaforma per i principali sistemi operativi correnti tra cui, ma non solo, Windows, Linux e Macintosh. Offre vari vantaggi rispetto agli altri client di posta, tra cui la classificazione dello spam. Realizzato a partire dal codice di Mozilla, Mozilla Thunderbird usa Gecko, il motore di rendering più rispettoso degli standard in assoluto.

Ultime notizie

Select Style: Default Style | Locked Menu | Classic | Classic with Locked Menu

LFG

HACKMEETING 2007



alcuni comandi per generare una coppia di chiavi pubblica/privata per l'utilizzo del gpg con riga di comando

I

su qualsiasi sistema operativo é possibile utilizzare client di posta elettronica che hanno la possibilità di utilizzare estensioni/eseguibili per la cifratura della posta elettronica

Il

esempio di creazione di una coppia di chiavi con un client di posta abbastanza comune:

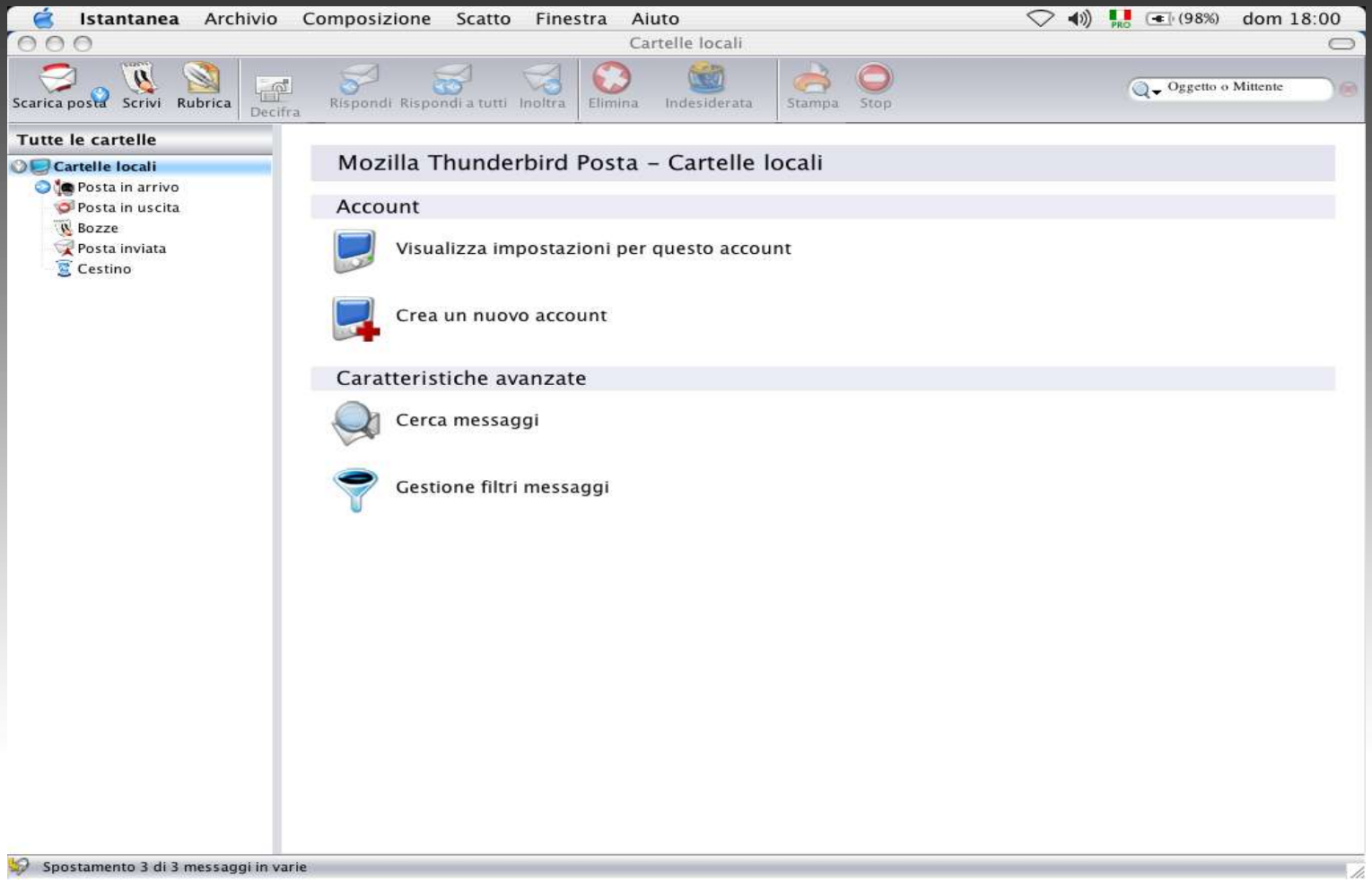
Mozilla Thunderbird

III

passo zero :

scaricare l'applicativo installarlo e configurarlo per il proprio account di posta

HACKMEETING 2007

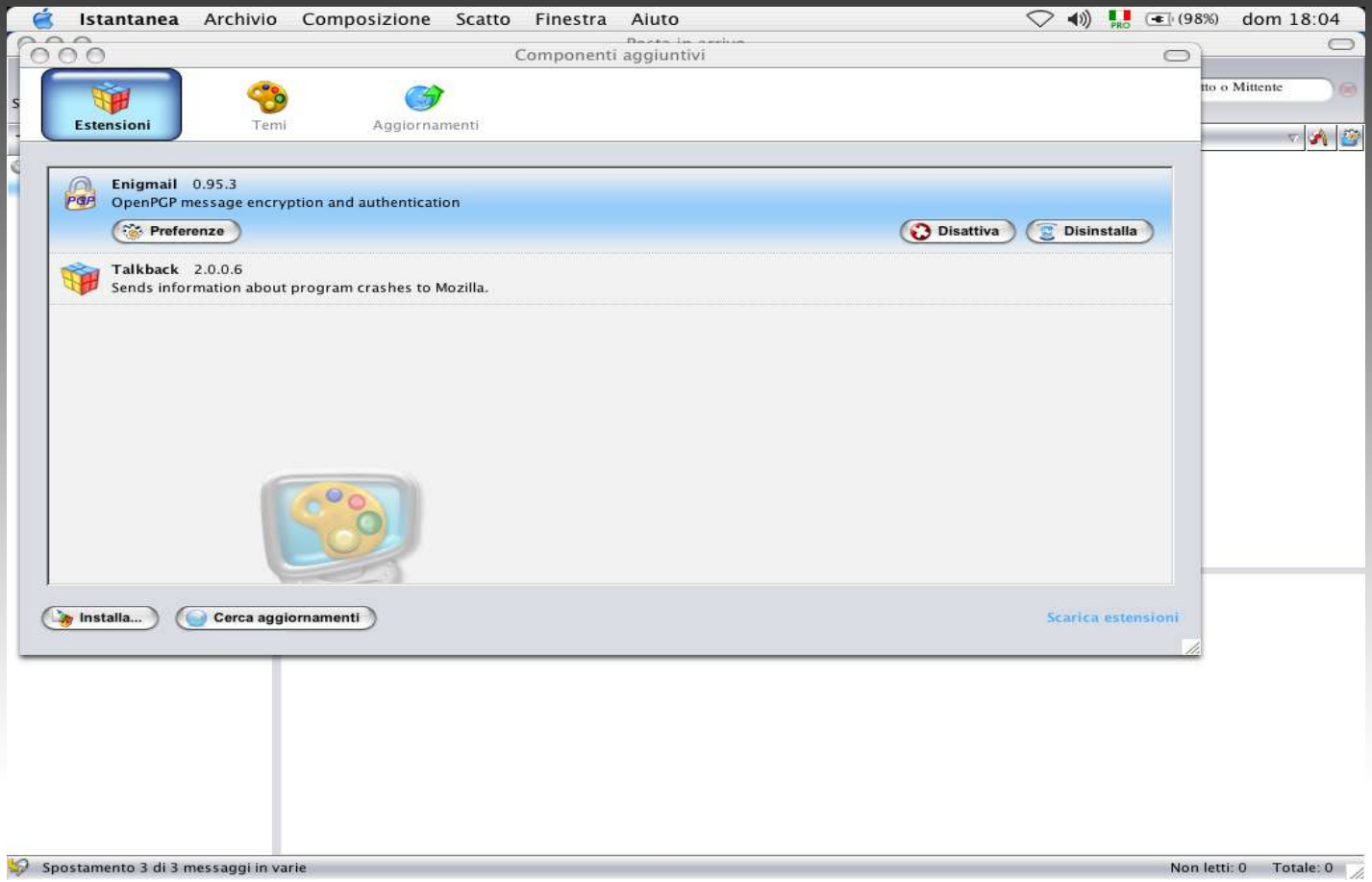


passo uno:

scaricare dal sito l'estensione per la cifratura della posta elettronica,

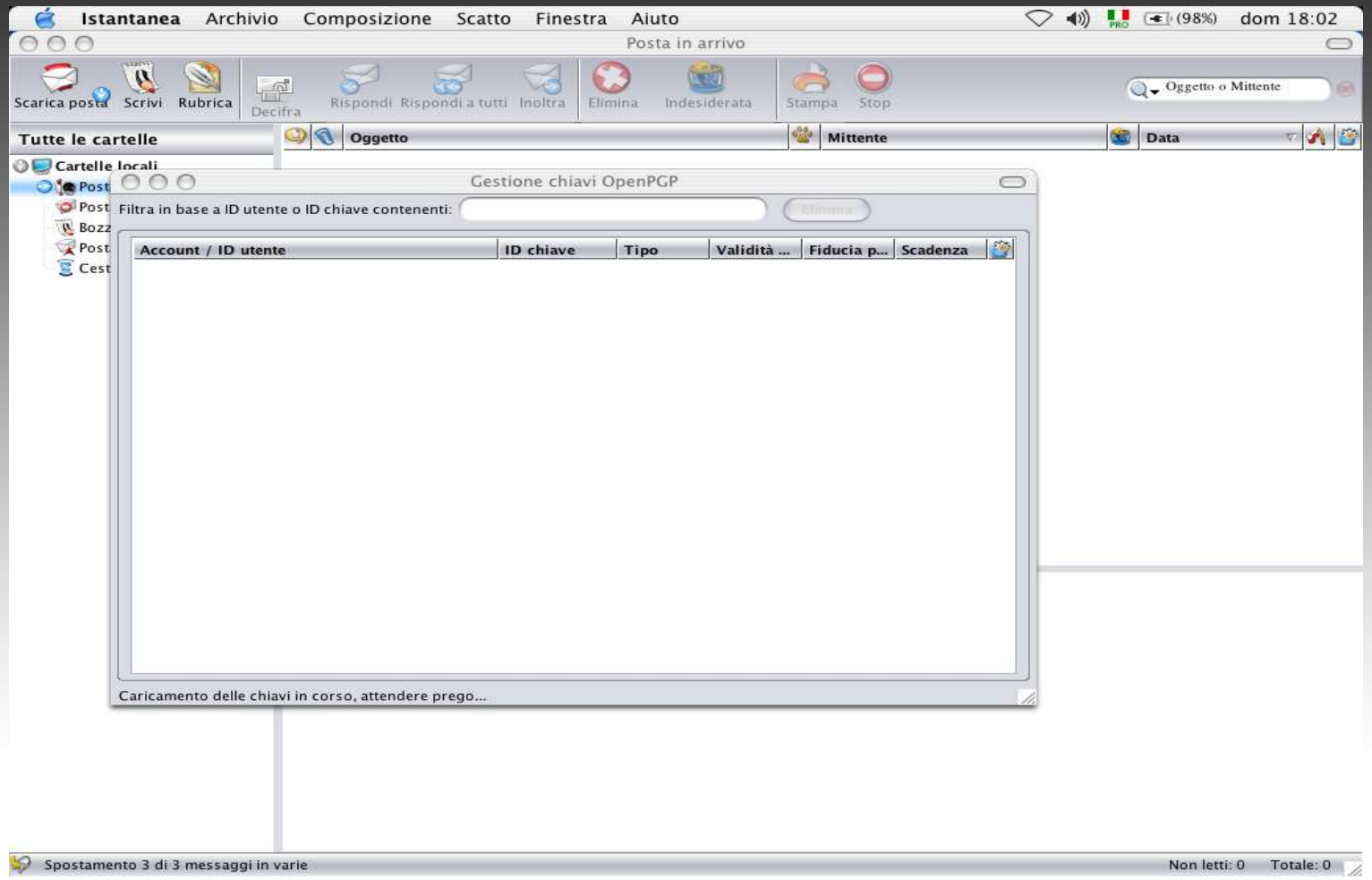
Enigmail

HACKMEETING 2007



LFG

HACKMEETING 2007



LFG

é possibile scaricarlo:

https://addons.mozilla.org

https://addons.mozilla.org/en-US/thunderbird/search?q=enigmail&status=4

IV

creazione di una coppia di chiavi in maniera grafica

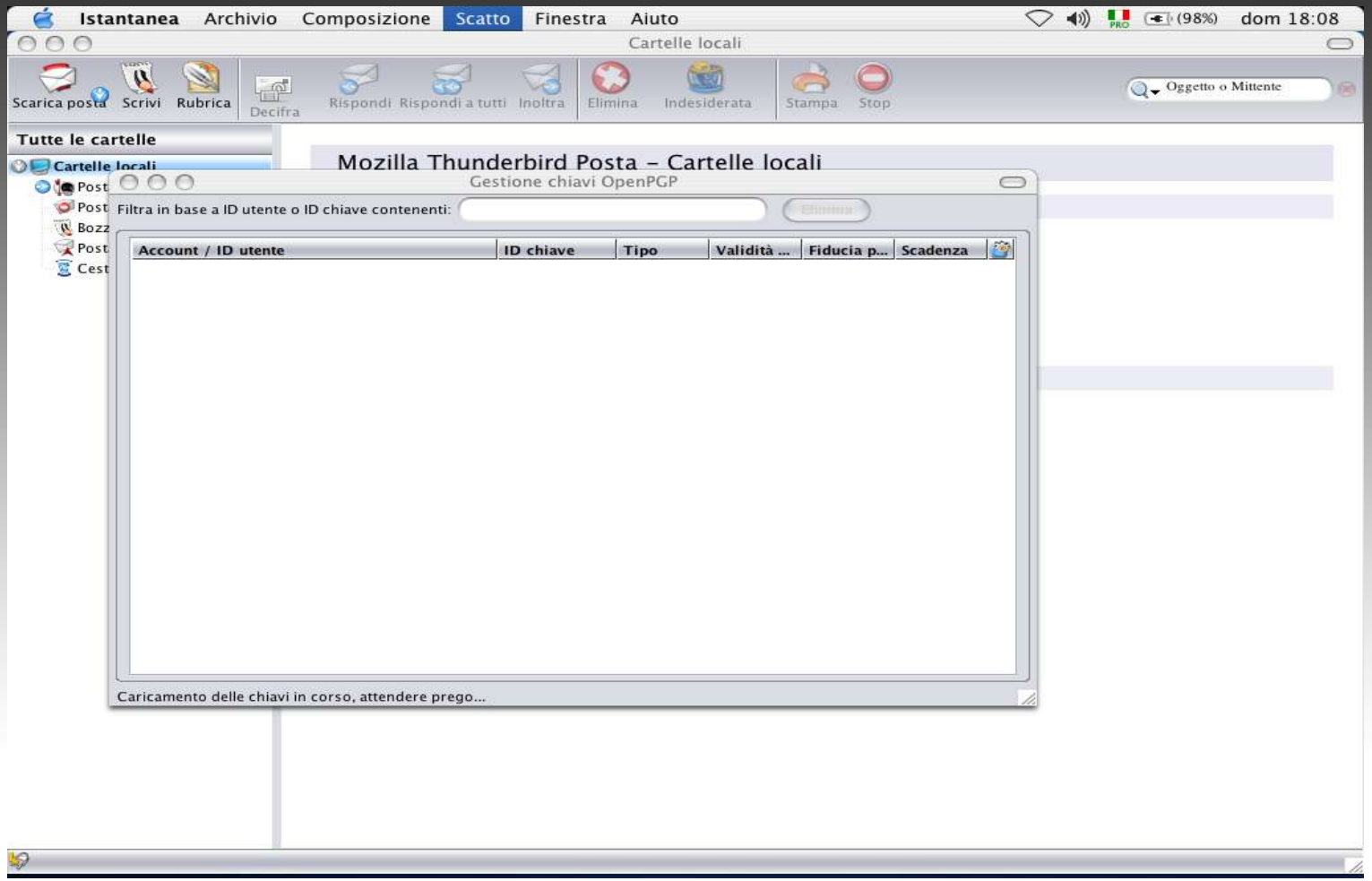
(Thunderbird)

basta aprire

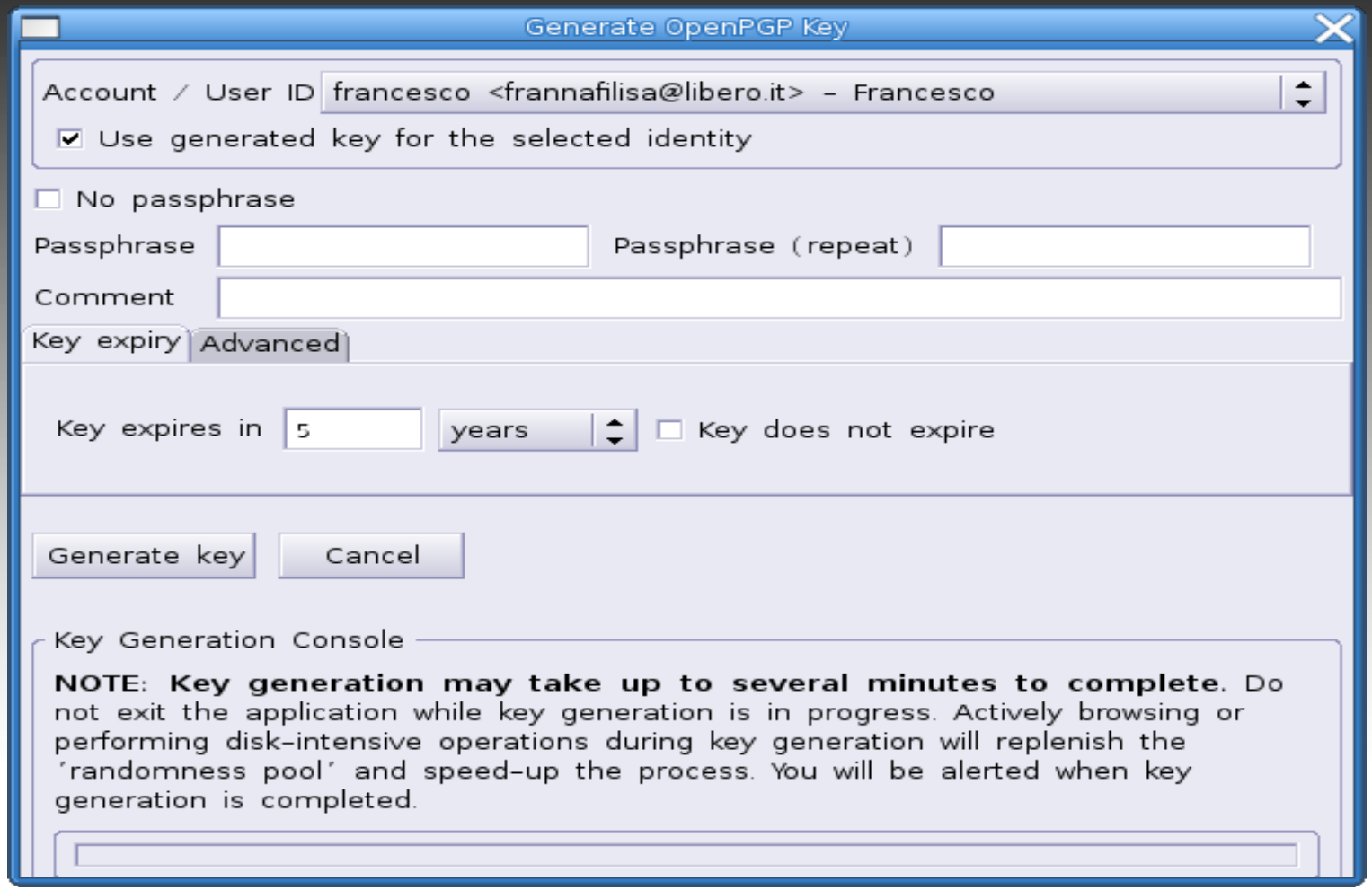
menu

genera coppia chiavi

HACKMEETING 2007



HACKMEETING 2007



LFG

generare una coppia di chiavi con la riga di comando :

```
francesco@xxxx:~$ 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.
```

tipo di chiave:

```
Please select what kind of key you want:
   (1) DSA and Elgamal (default)
   (2) DSA (sign only)
   (5) RSA (sign only)
Your selection? 1
DSA keypair will have 1024 bits.
ELG-E keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
Requested keysize is 2048 bits
```

validità della chiave gpg:

```
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)
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y
```

```
Key is valid for? (0) 1y
Key expires at lun 22 set 2008 18:28:09 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>"
```

```
Real name: miaobau
Email address: miaobau@ciccio.eu
Comment: hm '07
You selected this USER-ID:
    "miaobau (hm '07) <miaobau@ciccio.eu>"
```

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

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: key 0612FBDB marked as ultimately trusted
public and secret key created and signed.
```

```
gpg: checking the trustdb
gpg:3 marginal(s)needed,1complete(s)needed,PGPtrustmodel
gpg: depth: 0valid:4signed: 21 trust:0-,0q, 0n, 0m, 0f,4u
    gpg: depth:1 valid:21signed:21trust: 14-, 0q, 0n, 5m, 2f,
0u
gpg: depth: 2  valid:3  signed:  16  trust: 1-, 0q, 0n, 1m,
1f, 0u
gpg: depth: 3  valid: 2  signed:   5  trust: 1-, 0q, 0n, 1m,
0f, 0u
gpg: depth: 4valid: 1 signed: 6 trust: 1-, 0q, 0n, 0m, 0f,0u
gpg: next trustdb check due at 2007-11-04
pub1024D/0612FBDB 2007-09-23 [expires: 2008-09-22]
Key fingerprint = 89A1 9440 2DB8 E7C9 8F07  EBFB 843D FCA9
0612 FBDB
uidmiaobau (hm '07) <miaobau@ciccio.eu>
sub2048g/6A8E0798 2007-09-23 [expires: 2008-09-22]
```

http://www.gnupg.org/

http://www.mozillaitalia.it/thunderbird/

http://www.mutt.org/

http://enigmail.mozdev.org/

https://addons.mozilla.org/en-US/thunderbird

https://addons.mozilla.org/en-US/thunderbird/search?q=enigmail&status=4