

MOCA 2008



francesco@cybervalley.eu

Leandro Noferini Inoferin@cybervalley.org



M O C A 2008

Premessa

**la posta elettronica non è una
comunicazione sicura**

**i protocolli sono normalmente tutti
in chiaro**



MOCA 2008

Con pochissimo sforzo è possibile intercettare e registrare:

- i partecipanti alla discussione
- il contenuto dei messaggi
- orari di spedizione e ricevimento



MOCA 2008

Con pochissimo sforzo in più è possibile:

- modificare il contenuto del messaggio
- falsificare l'origine del messaggio



MOCA 2008

Precauzioni

Introdurre “strati” di cifratura nei vari livelli

- ssl/tls per il trasporto dei messaggi
- pgp/gpg per il contenuto dei messaggi

Non coprono in ogni caso tutte le debolezze
(remailer)



MOCA 2008

Di cosa parleremo

Protezione del contenuto
del messaggio usando
Gnu Privacy Guard



Integrazione in alcuni
programmi di posta



MOCA 2008



Buste chiuse

e

Cartoline



MOCA 2008

Cosa otteniamo

Cifratura – il corpo del messaggio diventa leggibile solo dai destinatari

Firma - Verifica che il corpo del messaggio non è stato modificato



MOCA 2008

Non copriremo tutte le tracce perché
rimarrà sempre possibile

- conoscere i partecipanti alla discussione
 - conoscere gli orari di spedizione e ricevimento
 - intercettare il messaggio



MOCA 2008

From: Francesco <francesco@firenze.linux.it>
To: Francesco <francesco@firenze.linux.it>
Subject: pizza....
Message-ID: <20080714151218.GA12855@jibby.cybervalley.org>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Disposition: inline
X-GPG-Fingerprint: 87E7 B7CE 577A EAD9 4744 F69F 22C2 AA92 26762990
User-Agent: Mutt/1.5.13 (2006-08-11)

Salve domenica andiamo a mangiare la pizza ????

--

Francesco

Key-id 26762990

Key fingerprint = 87E7 B7CE 577A EAD9 4744 F69F 22C2 AA92 2676 2990



M O C A 2008

From: Francesco <francesco@firenze.linux.it>
To: Francesco <francesco@firenze.linux.it>
Subject: pizza.....
Message-ID: <20080714151350.GB12855@jibby.cybervalley.org>
MIME-Version: 1.0
Content-Type: multipart/encrypted; protocol="application/pgp-encrypted";
boundary="0XfL5xGRrasGEqWY"
Content-Disposition: inline
X-GPG-Fingerprint: 87E7 B7CE 577A EAD9 4744 F69F 22C2 AA92 2676 2990
User-Agent: Mutt/1.5.13 (2006-08-11)

--0XfL5xGRrasGEqWY
Content-Type: application/pgp-encrypted
Content-Disposition: attachment

--0XfL5xGRrasGEqWY
Content-Type: application/octet-stream
Content-Disposition: inline; filename="msg.asc"

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

hQE0AxwKRZC7vMj fEAQAKvcJIJEl+MkbtD8zfoDGxcX/i694CkUHgGskCAhNUIms
GNwruiEZCqfyWBz+PDZuajYUmQS8XzL1Z0x3XgvLz8+64NwlnvN4DFhAVUZducFn
5NTp8yVPAQhn0qozN8TFc9do04ZqWdJSsoXBACeyMcQtR7D6IRUZJlmj0StFLpYE
A0EjFDSCQTLlj00IbnNQP6EU4X5f3jykTji2NLUKDxlCFgXvIxxPwxewR+CD8zLm
L9FLyPxGjulFV8iCMLiArEeAx/1TgZf0fXcUUL4ncnLsxWMGSEUtYbtKU4Eilkr0
DBAmQJ22Z+/7G8txR4dLRnQosAmxxD5y9ci74jgmsHjE0sDJAUerTfo0QBQlmXh4
SgbQ11BK0o/qeTWmq2tr3C976N6QzszPojGpEjSt5hb6Uj6ZPrnDoCoeUr5iNLjy
4X2YY3aDjTq3oafbdddYIoYLEhUxbceJRkaTTpBBX+MeIM9F3G0GYxAdc4XgMLjzg
9cl2XsfMWUKcoUhwstsrcJqRxxc5Lyr54u2ABLu3kTHIU70pZ1Ip/fuAWsG9DK1L
USGpb7C6780leZxsG4DaWZ0+L6ikzep407t8rNtu7JgQl4aiKhfGspE/VI0q/UeR



M O C A 2008

Pretty Good Privacy - PGP

Il primo programma ad usare la chiave pubblica/privata per uso “personale” è stato PGP di Philip Zimmermann ma:

- ha avuto una storia (lunga) molto tormentata
- ha subito molti cambi di gestione del programma
 - ha subito molti cambi di licenza
- ci sono state alcune versioni con caratteristiche discutibili
 - attualmente non è più sviluppato



M O C A 2008

Gnu Privacy Guard - GnuPG

GnuPG è un'implementazione del
paradigma della
chiave pubblica/chiave privata

- licenza libera (GPL)
- attivamente sviluppato
- disponibile per (tutti?) i sistemi operativi e distribuzioni
 - molte interfacce semplificate
- buona integrazione con molti client di posta elettronica



MOCA 2008



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



MOCA 2008

**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.
```



MOCA 2008

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

MOCA 2008

Utente:

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>"

LFG

MOCA 2008

Modifica dati:

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? 0
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.



MOCA 2008

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.

LFG

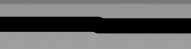
MOCA 2008

```
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]
```

LFG

MOCA 2008

Riassunto delle caratteristiche

- Tipo di algoritmo  Va bene il default
- Indirizzo utente  Indirizzo di posta elettronica con il quale verrà usato
- Dimensione della chiave  A seconda della paranoia personale
- Scadenza  Numero di giorni oltre il quale la chiave diventerà inutilizzabile
- Passphrase  Permette lo sblocco e perciò l'uso della chiave privata (decifrare e firmare)
- Fingerprint  Hash della chiave pubblica
Indentificativo



MOCA 2008

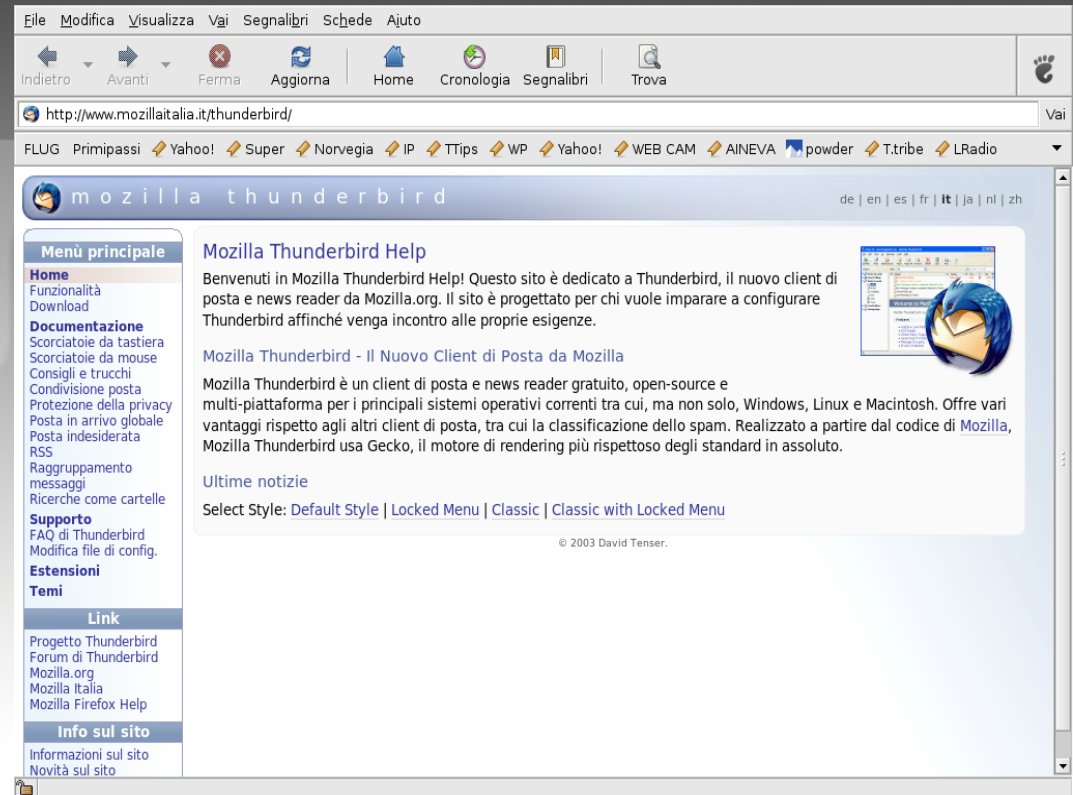
Thunderbird + Enigmail

Client di posta elettronica
basato su Mozilla

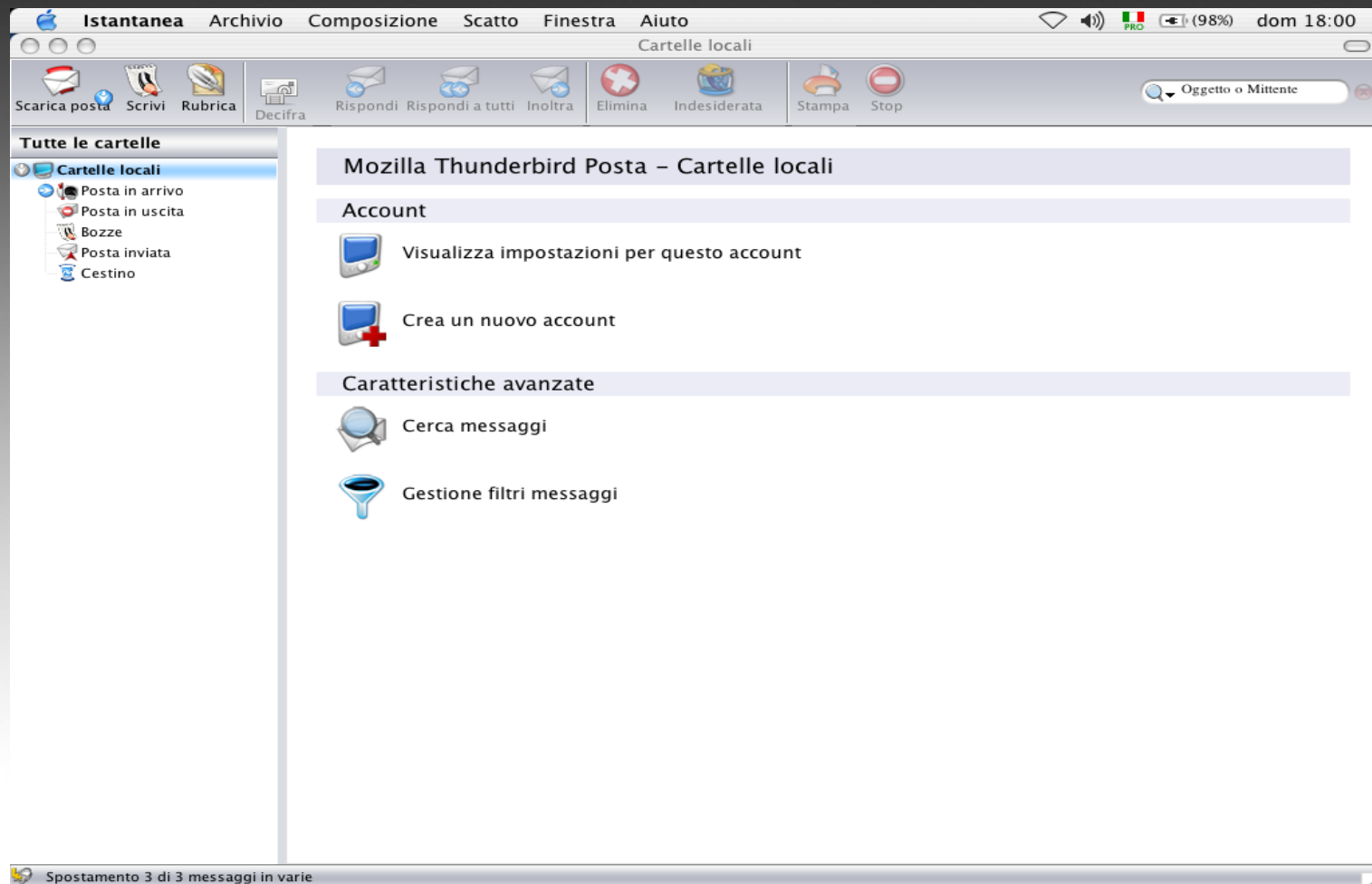
Supporto al GnuPG fornito
con l'estensione Enigmail

Enigmail permette la
gestione completa delle chiavi:

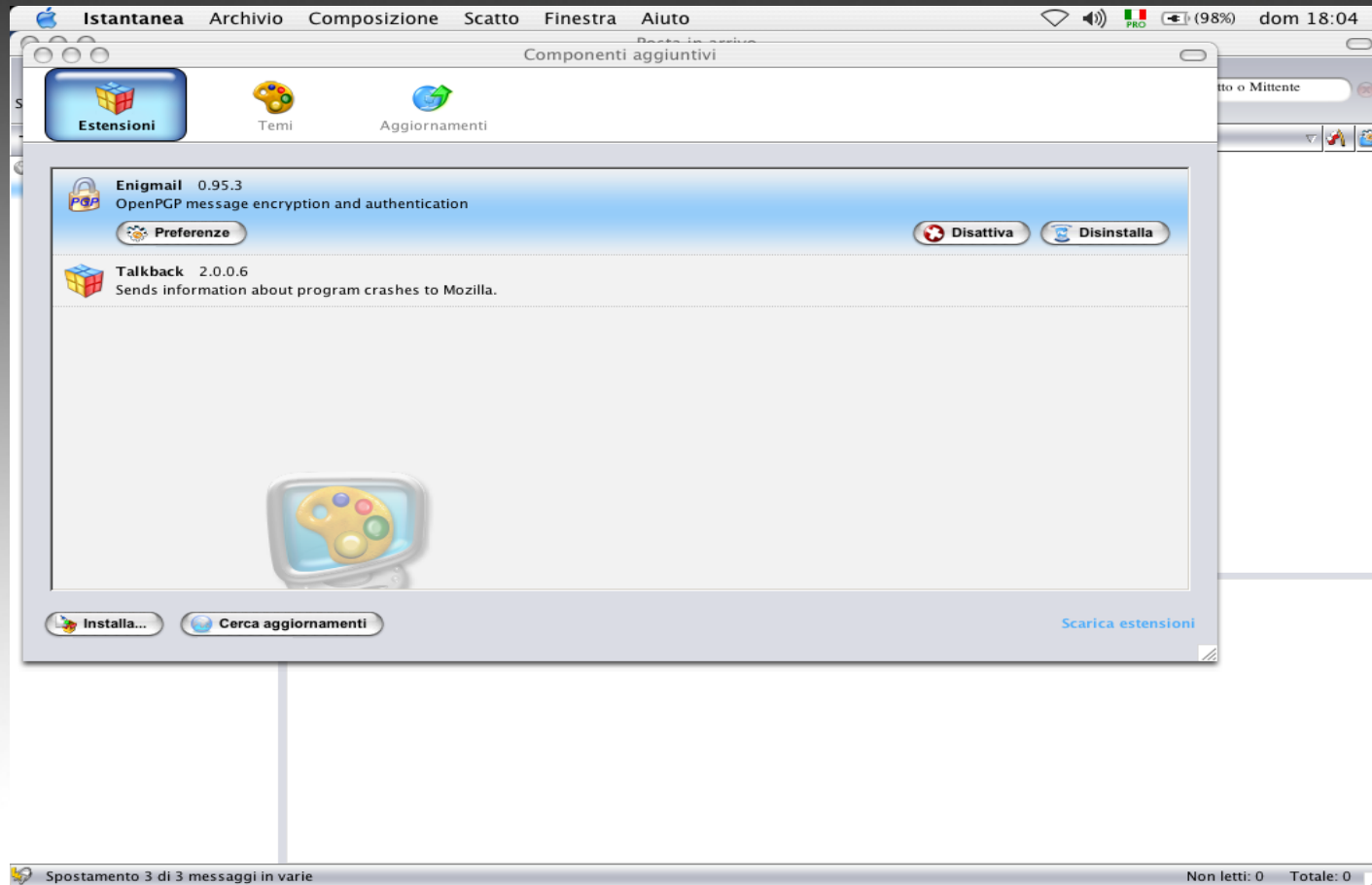
- cifratura
- firma
- creazione



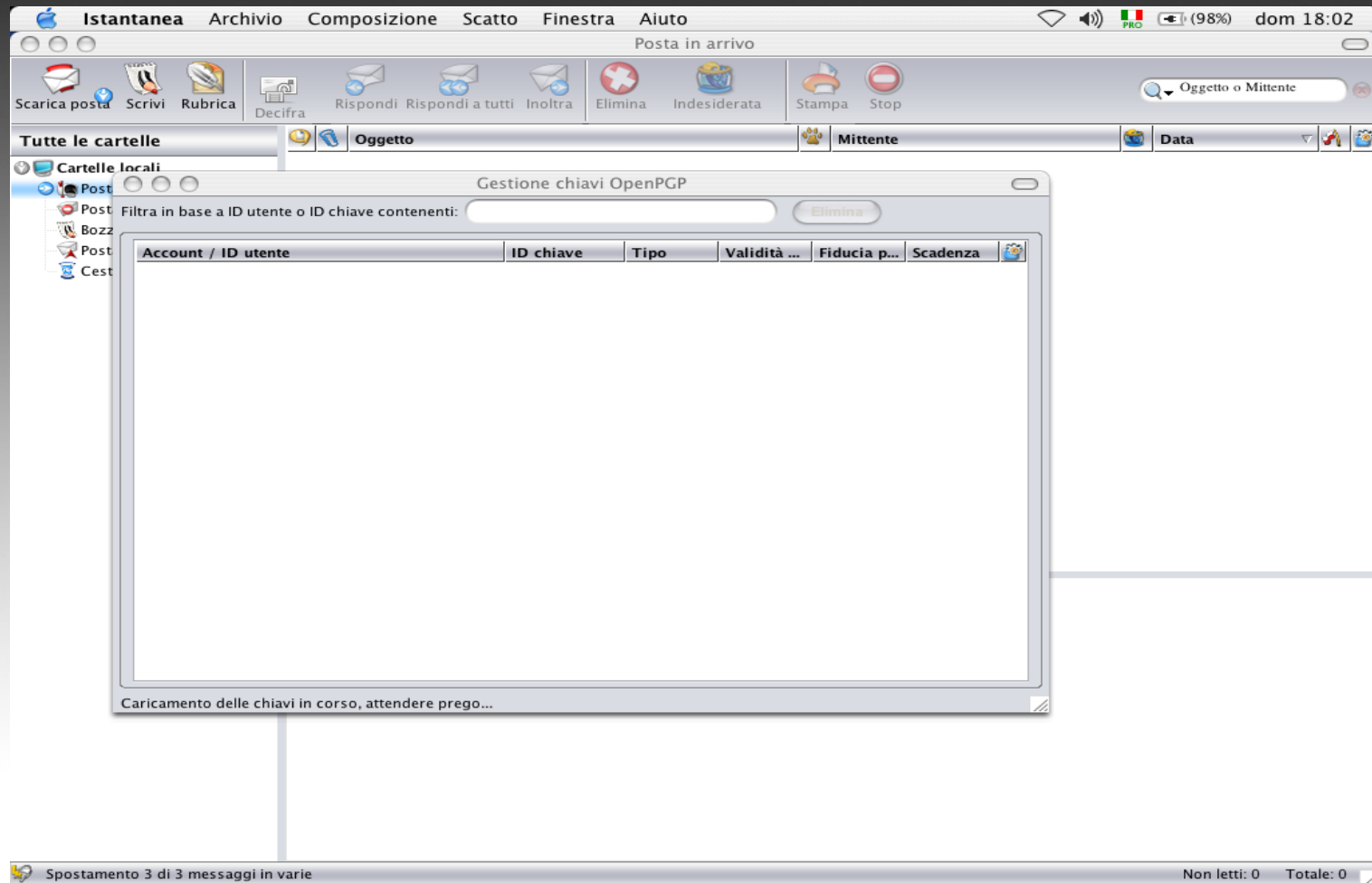
MOCA 2008



MOCA 2008



MOCA 2008



MOCA 2008

Generate OpenPGP Key

Account / User ID

☒ Use generated key for the selected identity

☐ No passphrase

Passphrase Passphrase (repeat)

Comment

Key expiry **Advanced**

Key expires in years ☐ Key does not expire

Key Generation Console

NOTE: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.



M O C A 2008

Mutt

Client testuale molto diffuso in tutte le distribuzioni Unix con supporto al GnuPG

Permette:

- cifratura della posta
- verifica della firma

```
1:Exit  -:PrevPg <Space>:NextPg v:View Attachm. d:Del r:Reply j:Next ?:Help
624 Aug 03 T Martinez ( 37) Loans with tiny points are here now
625 0 Jul 01 R. Jackson ( 123) Loans with tiny rates are here now
626 Aug 05 Benjamin E. Mag ( 50) Long time no hear
627 May 17 Krista Aaron ( 44) long time no see....
628 0 Jun 03 Josiah House ( 35) Looking for a hot date tonight, tomorrow, or next week?
629 Jul 03 Brigitte I. Hay ( 63) Looking for a N.ew H.ome?
630 May 17 Joe Burns ( 58) Looking for you
631 Jun 01 Save in a poor ( 145) Low Rate Consolidation Mortgage Loan
632 + Jul 02 Igiel@virtualig ( 2) LowCost SoftWare OnCD
-- Mutt: Mail/junk/spam [Msgs:950 Old:142 10M] --- (subject/date) --- (66%)
Date: Mon, 17 May 2004 03:40:09 +0100
From: Krista Aaron <Christinefeminine@highstream.com>
Subject: long time no see....

[-- Autoview using /usr/bin/elinks -force-html -dump '/tmp/mutt.html' --]
My name is Jen and I'm new to this dating thing. I've checked out your profile
you put up and it's interesting. => I just want to get to know you a little
better if you don't mind, come check my profile out at:

www.livejen.com/chat.html

I also got a webcam so we can make it interesting, anyways hope you get back to
me.
bye :)

gxsnkxxgnduvy.jwyceudc.jobxs
zcozccrociesbehgbpow
rnxlfu.jnqpblipdkgwyyqofracsz
xmqaubxsb.jrppoibvlpfhqowldtp
bixhghvrxtqgfeocofzycb
hugzffaffulsklpzhfrxbtt
btpztlfotqmmoaiwlosqv
-- 627/950: Krista Aaron long time no see.... --- (69%)
Key is not bound. Press '?' for help.
```



MOCA 2008

<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>

