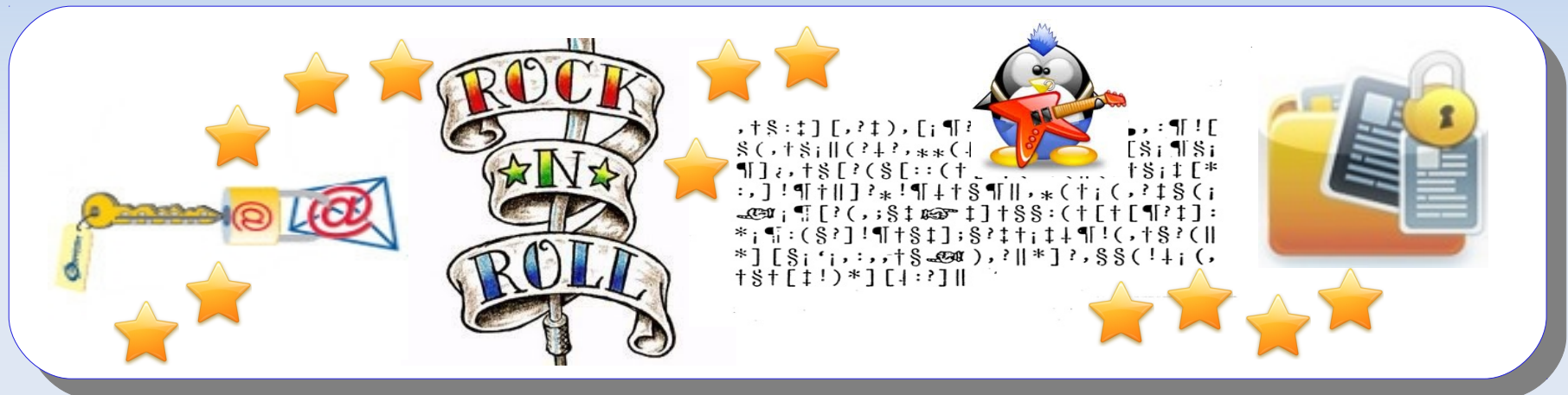






- rapida panoramica dello standard *OpenPGP* e della sua libera implementazione *GnuPG*
- semplice introduzione alla *crittografia asimmetrica*
- overview su alcuni *strumenti OpenSource* da utilizzare per una gestione più sicura e riservata nello scambio di *messaggistica ed e-mail*

## PGP e Zimmermann

<http://philzimmermann.com/>



- Phil crea PGP nel 1991, libero per uso non commerciale (*sorgenti disponibili*)
- la condanna per "esportazione di armi senza apposita licenza" (1993)
- problemi con brevetti (*RSA/RSADSI*)
- PGP diventa commerciale (1996 - *Viacrypt e PGP Inc.*)
- PGP Inc. acquisita dalla NA Inc.
- PGP Corp. (2002)
- Symantec (2010)

## OpenPGP

<http://www.openpgp.org/>



- deriva originariamente da *PGP*  
creato da *Phil Zimmermann*  
nel 1991
- definito dall'*IETF* nel 1997 (*RFC 2440* del 98)
- Aggiornato da *RFC 4880*  
(*novembre 2007*)
- standard Internet per  
l'interoperabilità dei messaggi  
protetti tramite  
*crittografia asimmetrica*

## GnuPG

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



- rilasciato sotto licenza *GNU GPL* (1999)
- completamente compatibile con *OpenPGP*  
(sotenuto dal governo tedesco)
- disponibile praticamente per tutti i SO  
(2000 porting su Win, sotto la spinta del Ministero dell'Economia e Tecnologia della Germania Federale)
- interfaccia a riga di comando (CUI)
- non usa algoritmi brevettati  
(DSA, RSA, 3DES, AES, Blowfish)
- supporta l'uso delle smartcard

## Crittografia asimmetrica

Ad ogni attore coinvolto è associata una coppia di chiavi:

- la *chiave pubblica*, che deve essere distribuita, serve a cifrare un documento destinato alla persona che possiede la relativa chiave privata
- la *chiave privata*, personale e segreta, utilizzata per decodificare un documento cifrato con la chiave pubblica

[fonte: Wikipedia]

## Crittografia asimmetrica [...]

**ES** - *Analogia postale*, in cui il mittente è Alice ed il destinatario Bob, i *lucchetti* fanno le veci delle *chiavi pubbliche* e le *chiavi* recitano la parte delle *chiavi private*:

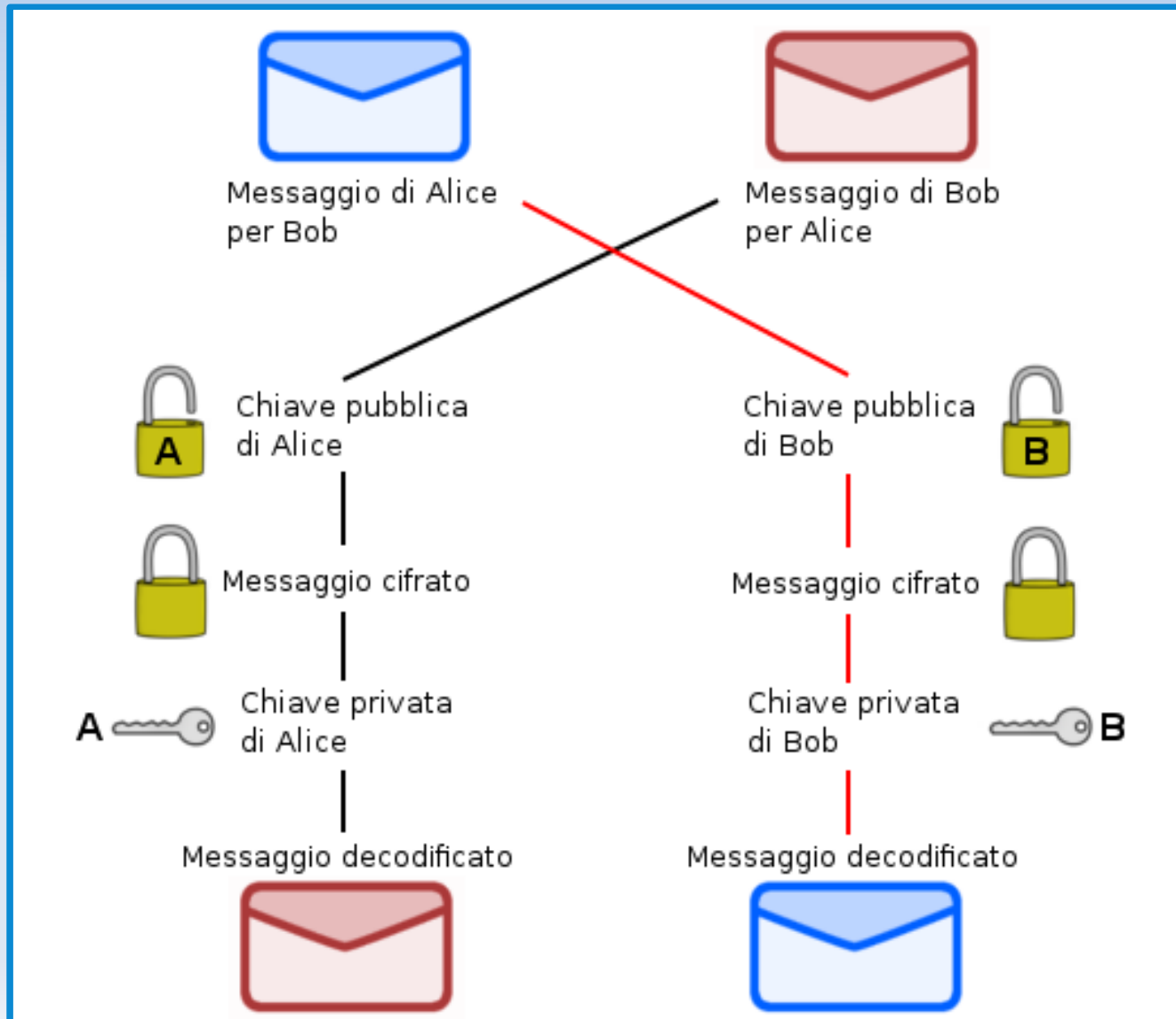
1. Alice chiede a Bob di spedirle il suo lucchetto, già aperto. La chiave dello stesso verrà però gelosamente conservata da Bob.

2. Alice riceve il lucchetto e, con esso, chiude il pacco e lo spedisce a Bob.

3. Bob riceve il pacco e può aprirlo con la chiave di cui è l'unico proprietario.

## Crittografia asimmetrica [...]

*[fonte: Wikipedia]*



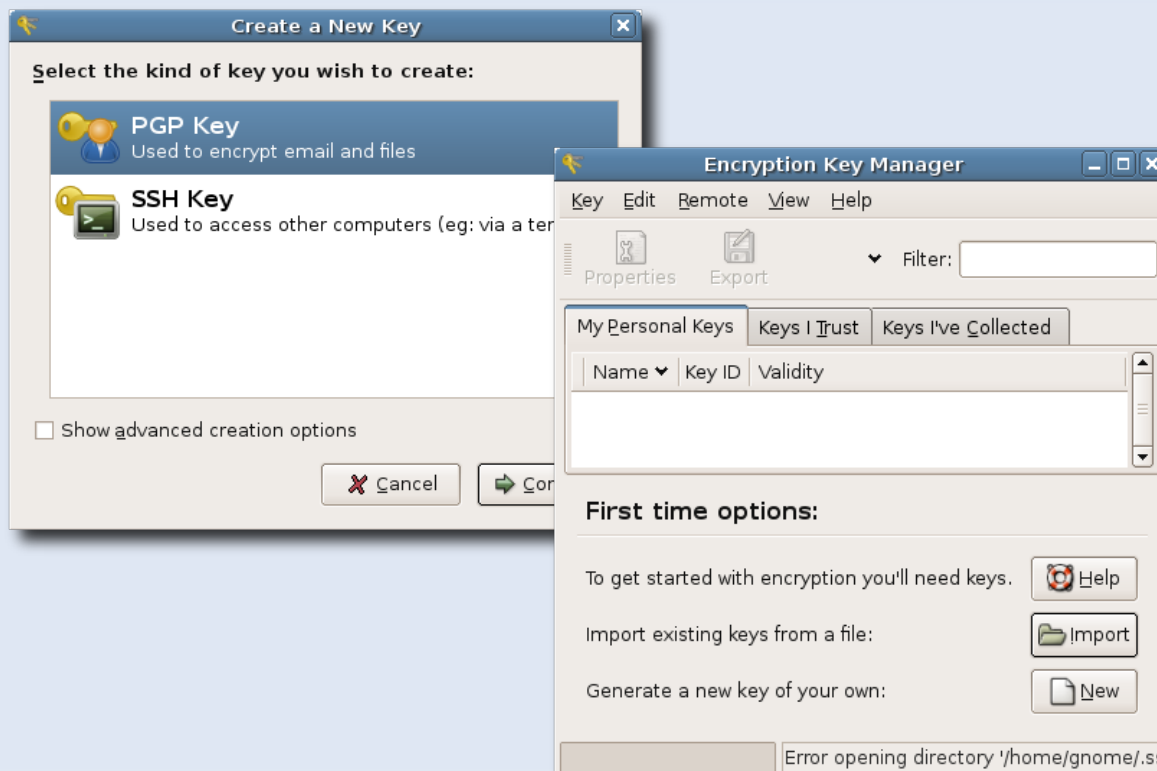


SCOPI - OpenPGP - GnuPG - CRYPTO - **TOOLS**

## Seahorse

<http://projects.gnome.org/seahorse/index.html>

- interfaccia grafica per la gestione delle chiavi per *GNOME*

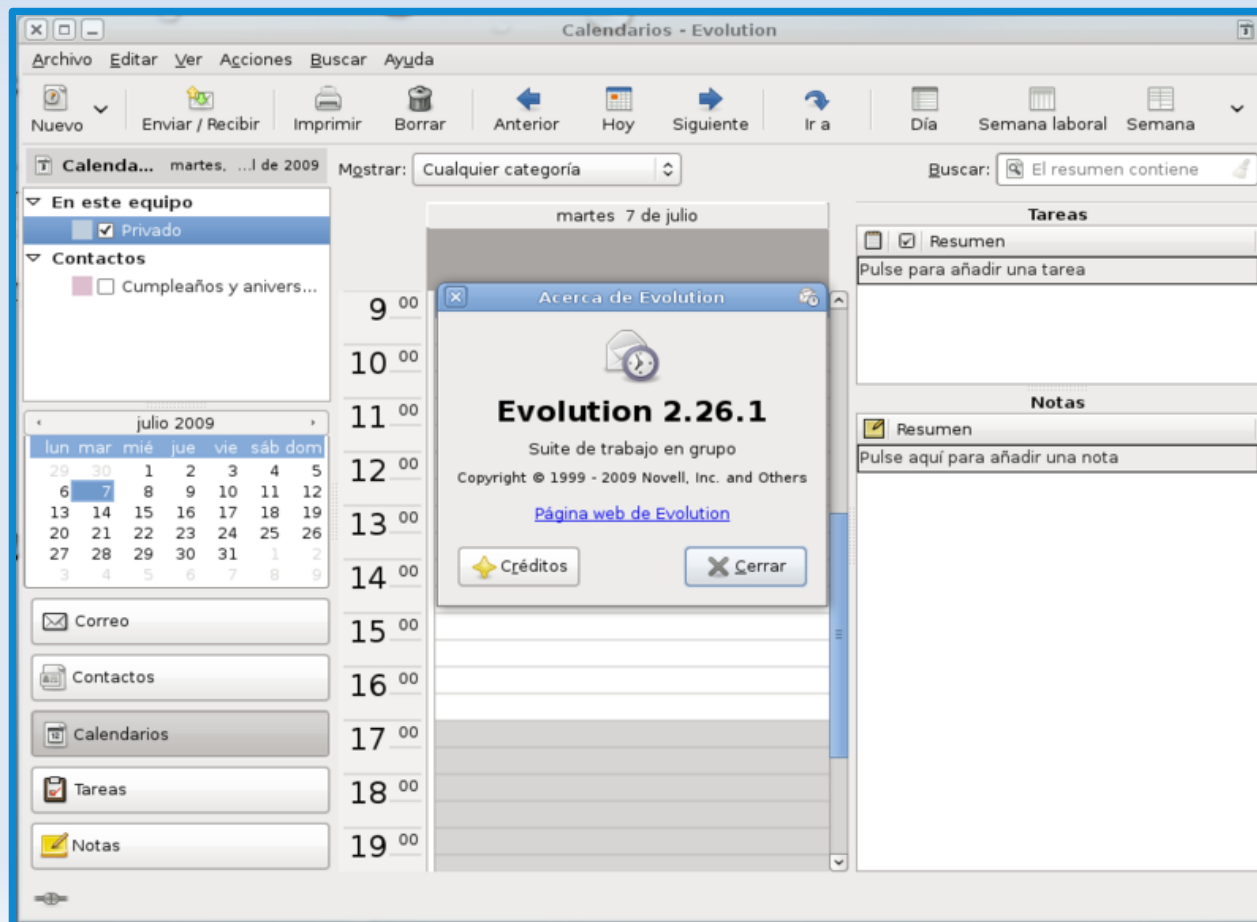


SCOPI - OpenPGP - GnuPG - CRYPTO - **TOOLS**

# Evolution

<http://projects.gnome.org/evolution/>

- client e-mail per *GNOME*

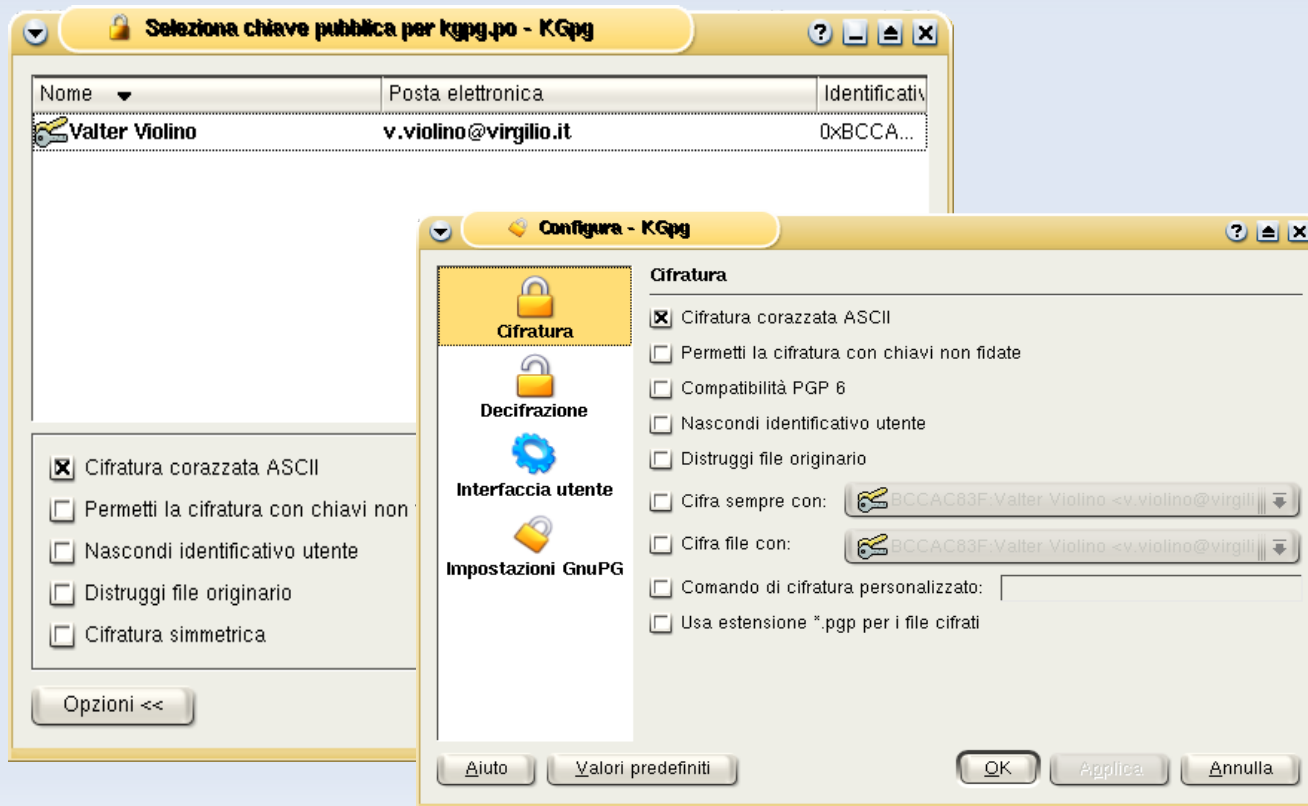


## KGpg

<http://utils.kde.org/projects/kgpg/>



- interfaccia grafica per la gestione delle chiavi per *KDE*

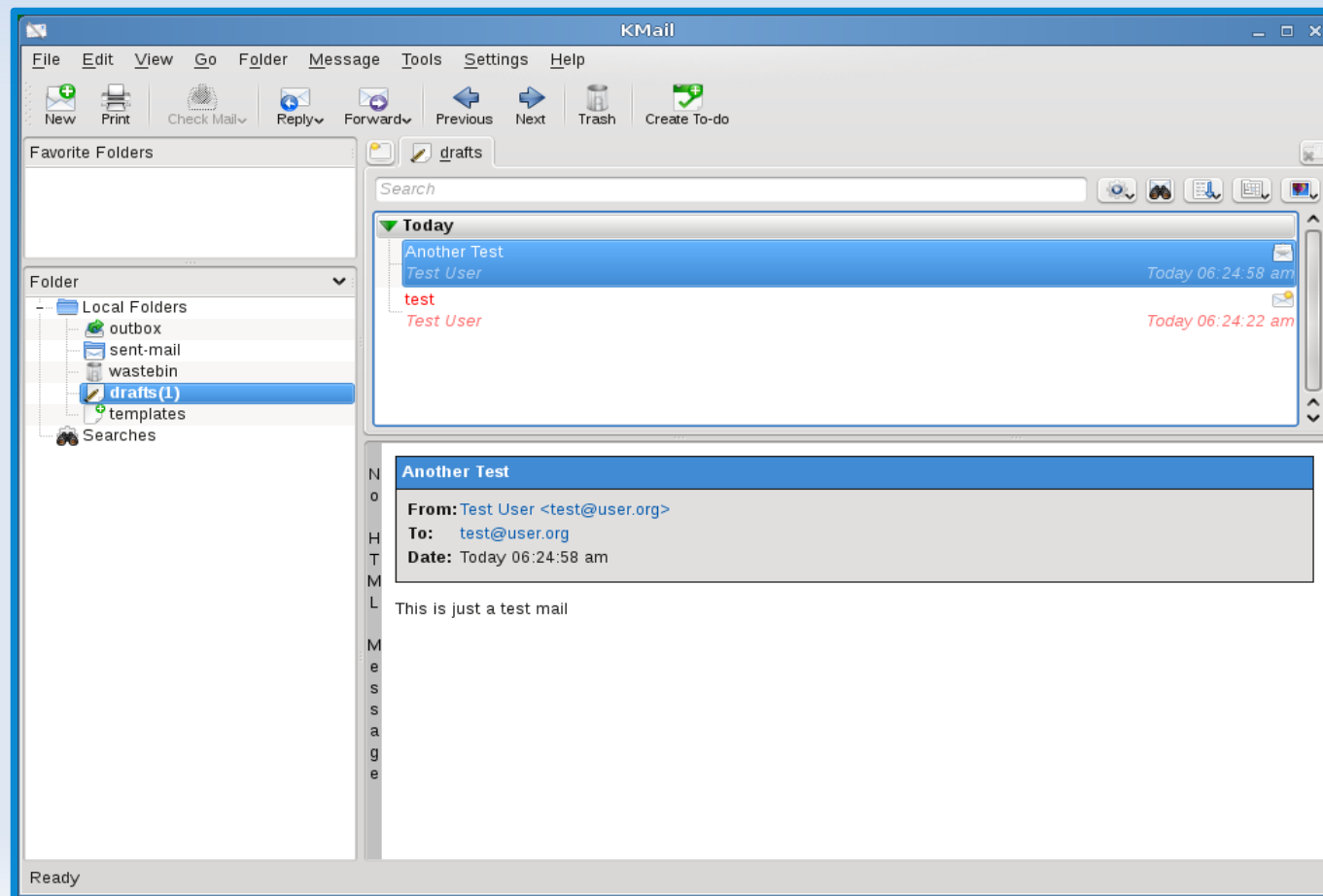


SCOPI - OpenPGP - GnuPG - CRYPTO - **TOOLS**

# KMail

<http://userbase.kde.org/KMail>

- client e-mail per *KDE*



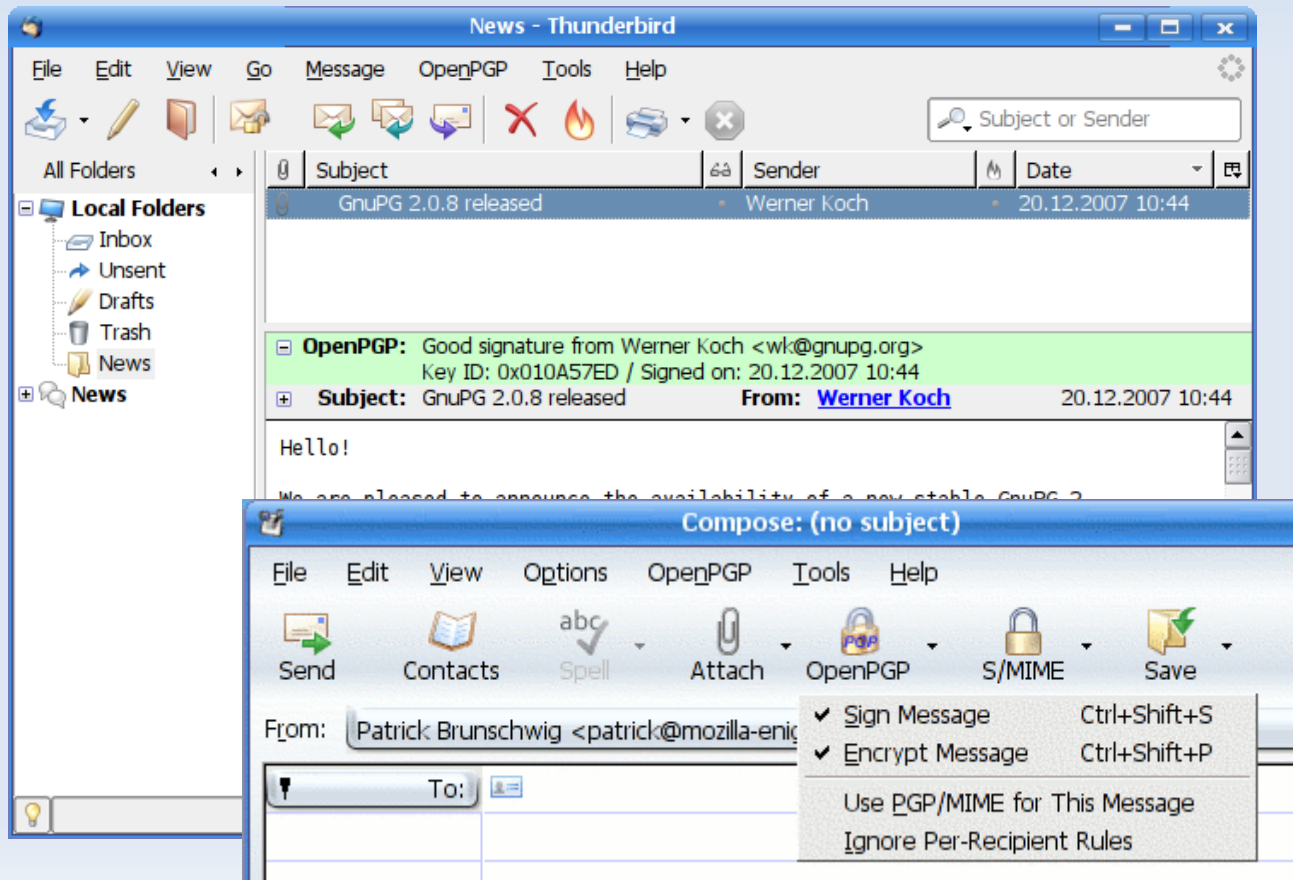
SCOPI - OpenPGP - GnuPG - CRYPTO - **TOOLS**

# Enigmail

<http://enigmail.mozdev.org/home/index.php.html>

**ENIGMAIL**

- plug-in per il client e-mail *Mozilla Thunderbird*



SCOPI - OpenPGP - GnuPG - CRYPTO - **TOOLS**

## Gpg4win

<http://www.gpg4win.org/>



- **pacchetto per Windows**  
(tutti gli elementi sono sotto GNU GPL e licenze libere)

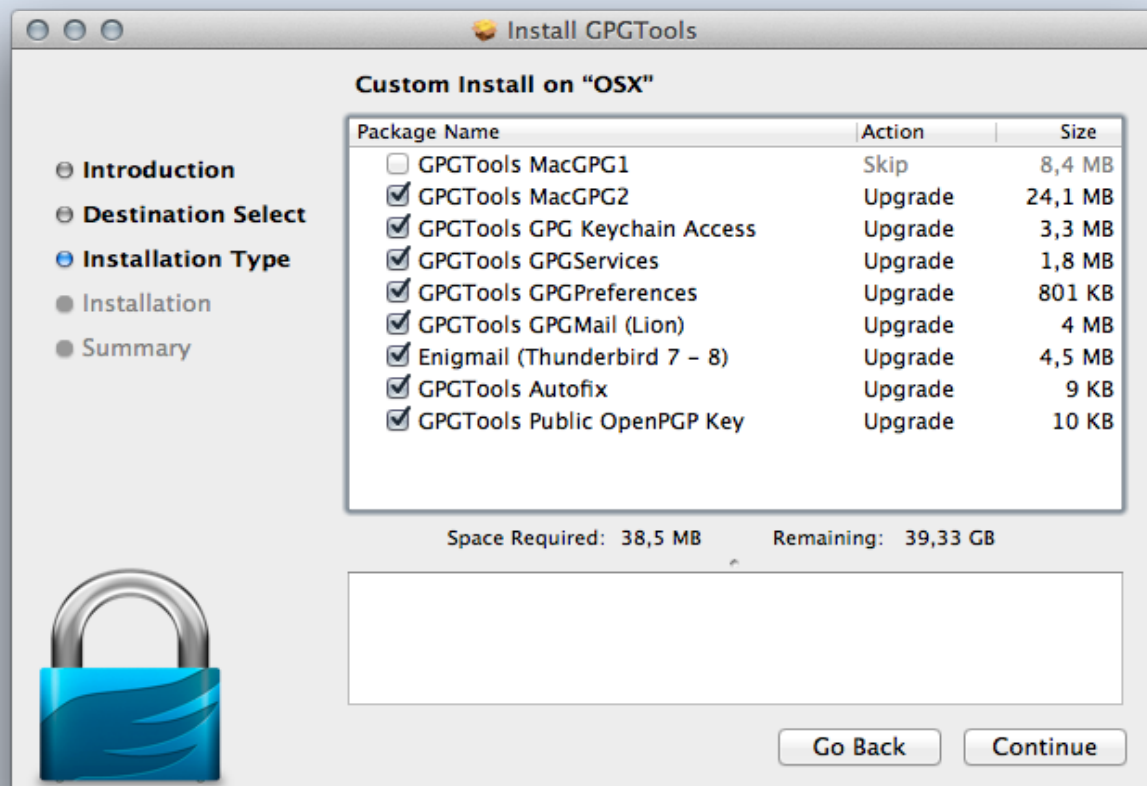


SCOPI - OpenPGP - GnuPG - CRYPTO - **TOOLS**

## GPGTools (MacGPG)

<http://www.gpgtools.org/>

- pacchetto per OS X





<http://carnialug.net>





**THANKS !**



[manuel.cacitti@carnialug.net](mailto:manuel.cacitti@carnialug.net)