E-privacy 2008

Progetto Winston Smith
http://pws.winstonsmith.info

La privacy e le comunicazioni digitali

Daniele Masini

daniele@winstonsmith.info

http://vandali.org/DanieleMasini

Agenda

- La privacy
- La posta elettronica
- Protezione delle informazioni
  - Steganografia e crittografia
- GNU Privacy Guard
- La posta elettronica cifrata
- La gestione delle chiavi
- Comunicazioni anonime

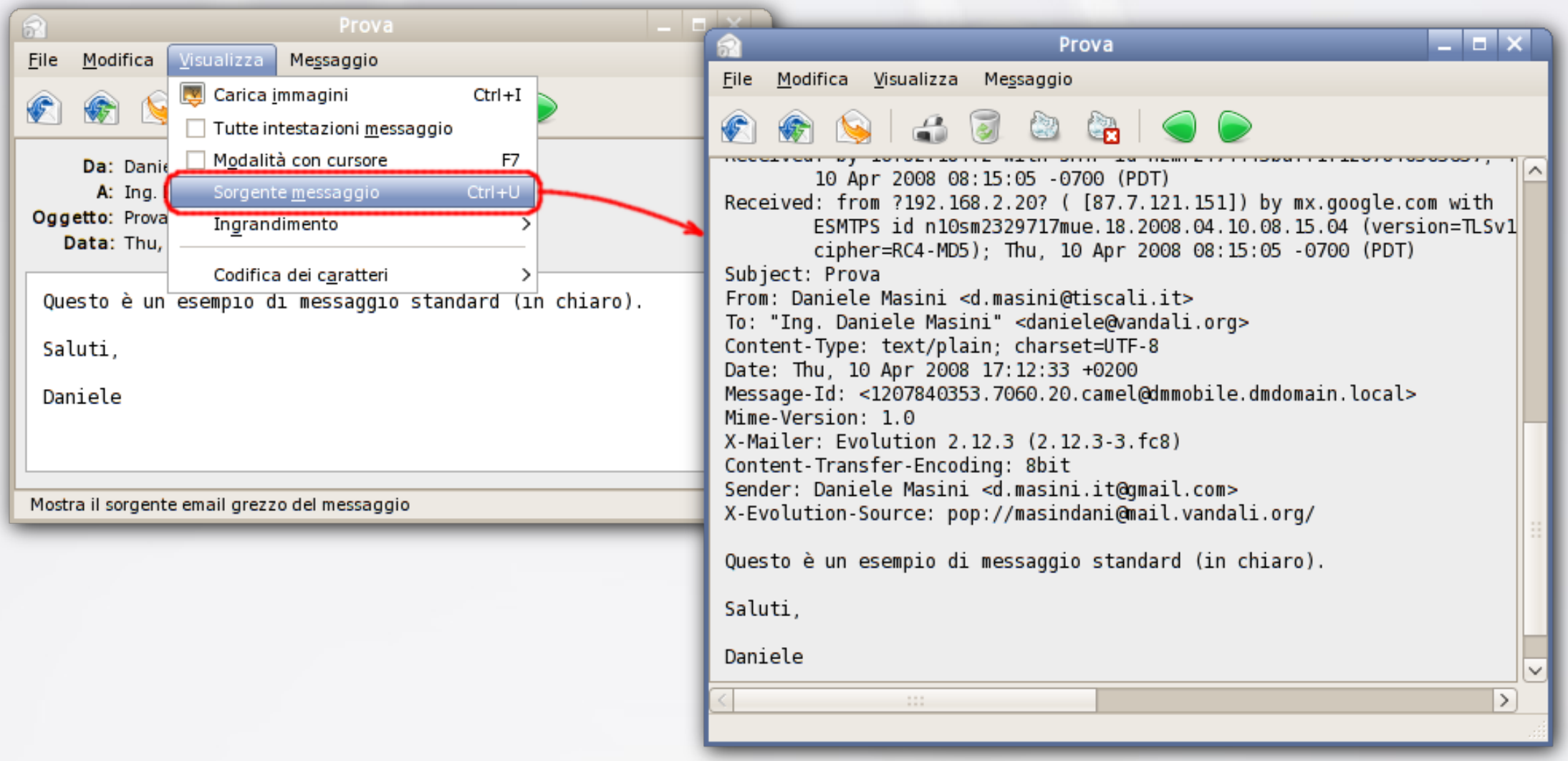
Privacy

Diritto alla *riservatezza* delle proprie informazioni e comunicazioni personali

Posta elettronica

- Utilizza protocolli generalmente in chiaro (POP, SMTP, IMAP)
- I messaggi di posta elettronica non sono gli analoghi delle lettere in busta chiusa, ma qualcosa di molto simile alle cartoline postali: nessuna riservatezza del messaggio 
- È possibile inviare e-mail fingendo di essere qualcun altro 

Posta elettronica



Posta elettronica

È possibile ottenere la riservatezza delle comunicazioni elettroniche via e-mail?

Protezione delle informazioni

- Meccanismi di protezione delle informazioni (occultamento)
  - Steganografia (informazione nascosta)
  - Crittografia (informazione non nascosta)

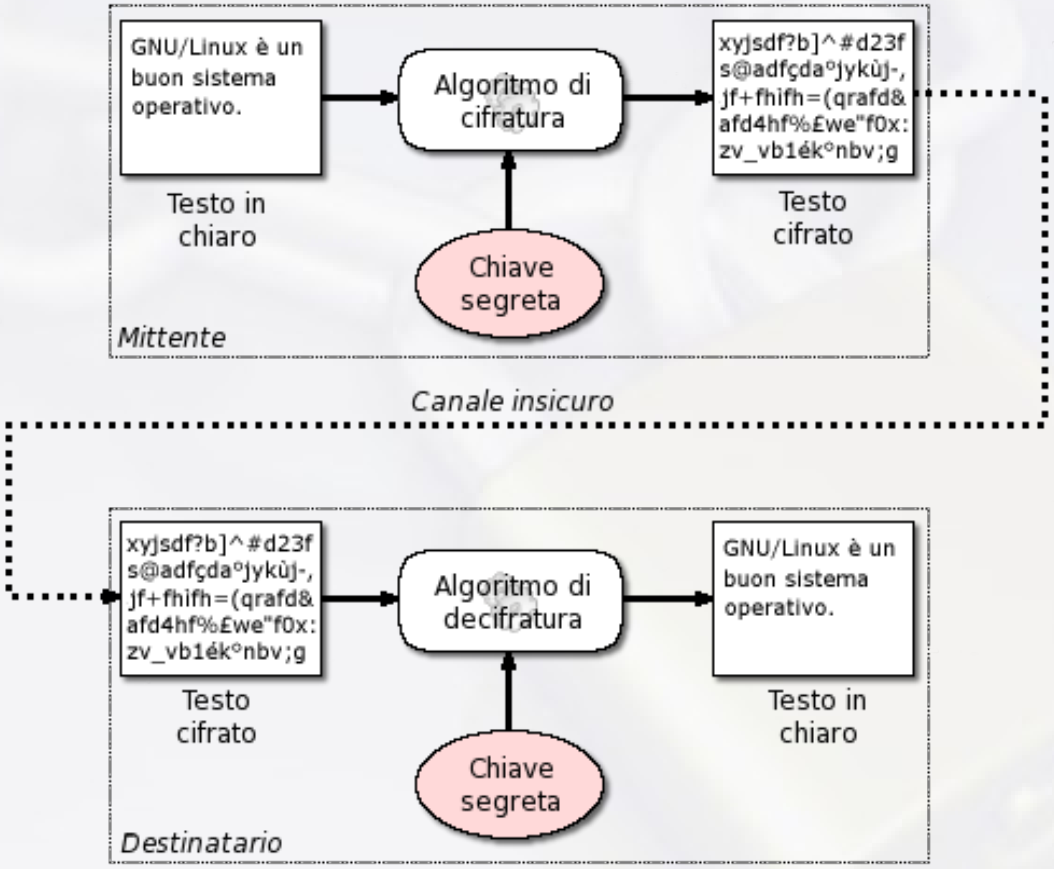
Protezione delle informazioni

- crittografia a *chiave simmetrica*
  - una sola chiave per cifrare e decifrare
- crittografia a *chiave asimmetrica*
  - una coppia di chiavi: una chiave *pubblica* ed una *privata*
  - non è possibile ricavare una delle due chiavi conoscendone l'altra
  - ciò che viene cifrato con una delle due chiavi può essere decifrato solo conoscendo l'altra
- funzioni hash
  - la ciratura one-way
- firma elettronica
  - garanzia dell'autenticità e della paternità dei documenti

Crittografia

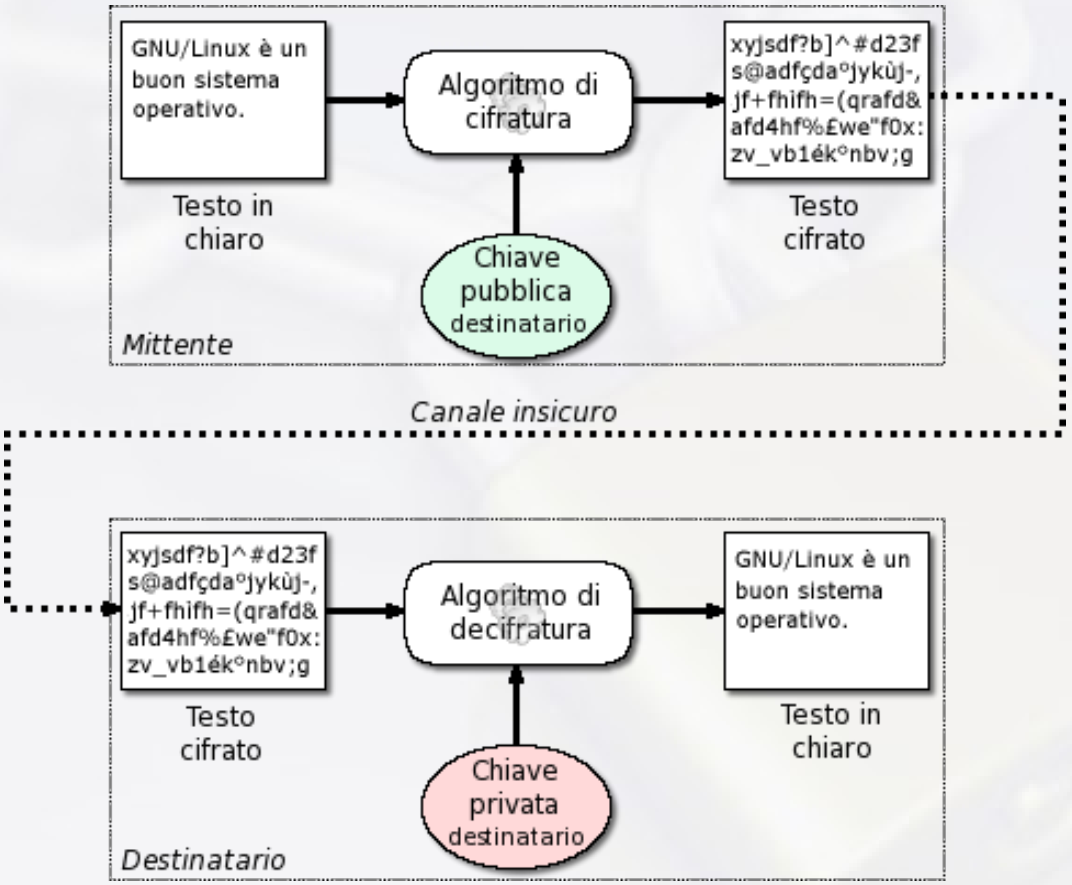
- Principio di Kerchkoffs: *un crittosistema deve essere sicuro anche se il suo funzionamento è di pubblico dominio, con l'eccezione della chiave*
  - Gli algoritmi di cifratura sono *pubblici*
  - La chiave è *segreta*
- Sicurezza del sistema di cifratura
  - Lunghezza della chiave
  - Dominio e scelta della chiave (attacchi per dizionario, per forza bruta)

Crittografia



Cifratura e decifratura con *chiave simmetrica*

Crittografia

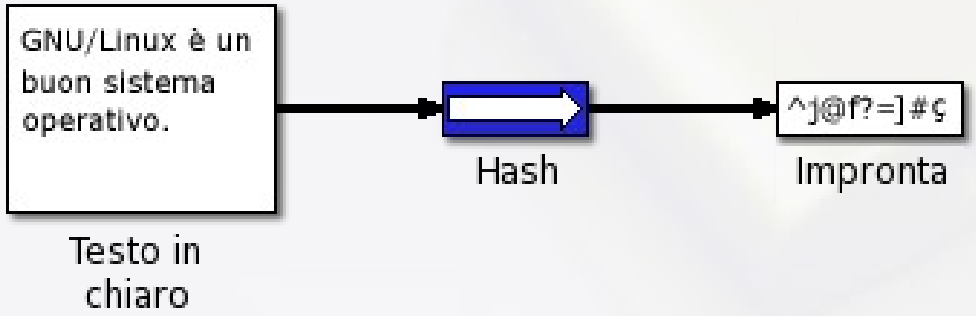


Cifratura e decifratura con *chiave asimmetrica*

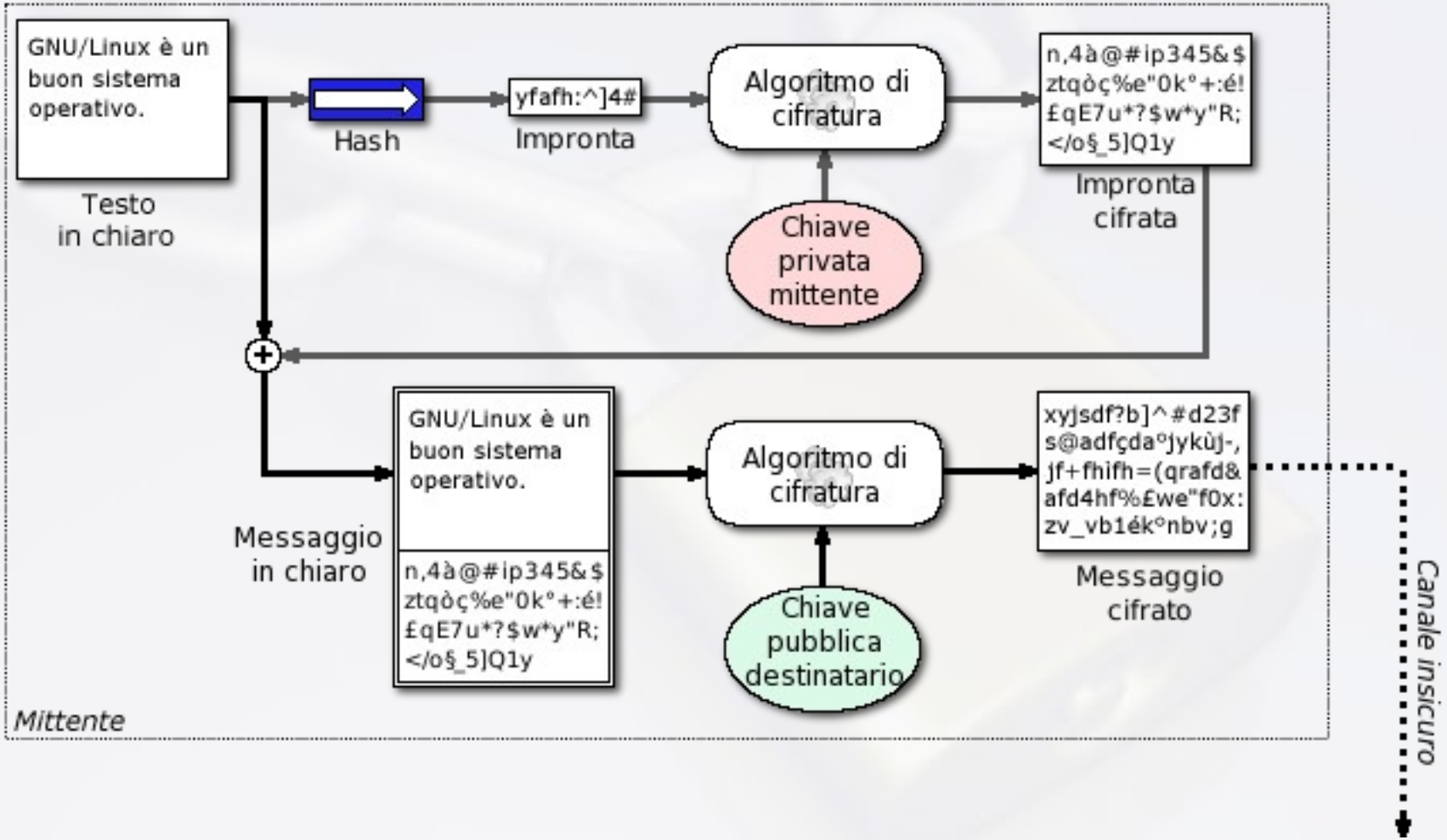
Protezione delle informazioni

Funzioni hash

- Cifratura *one-way*, creazione dell'**impronta** (*digest*)
- Nessuna chiave
- Algoritmi: MD5, SHA, RIPEMD, ...

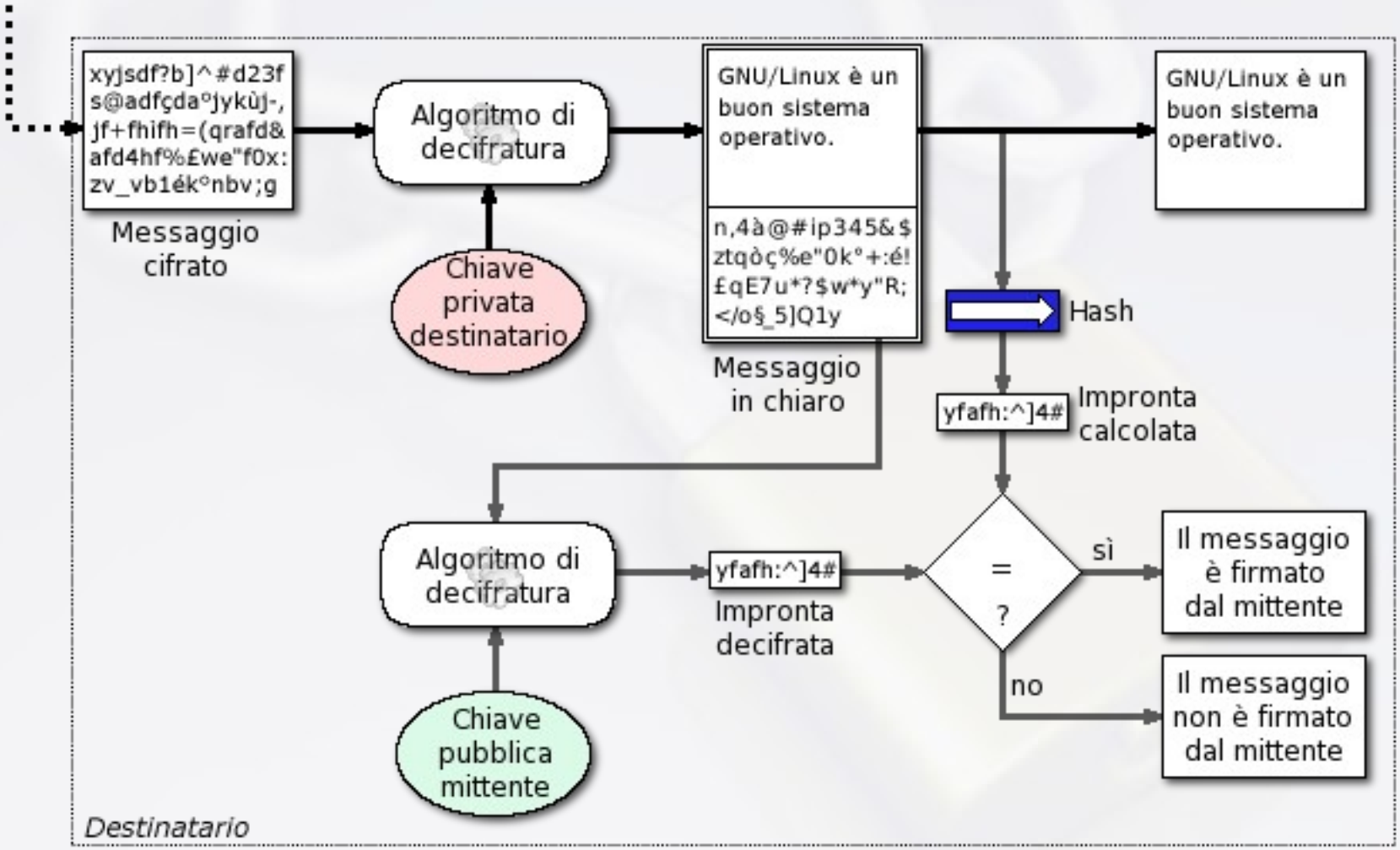


Protezione delle informazioni



Cifratura con *firma elettronica*

Protezione delle informazioni



Decifratura con *firma elettronica*

GNU Privacy Guard

- Implementazione del protocollo OpenPGP (RFC 2440) con algoritmi liberi
- Gestione di *chiavi asimmetriche*
  - Generazione chiavi
  - Impostazione della fiducia (web of trust)

- Cifratura delle informazioni
- Decifratura delle informazioni
- Firma delle informazioni
- Verifica della firma apposta alle informazioni

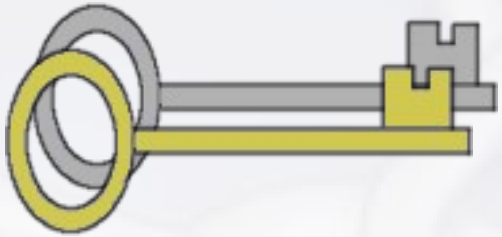
GnuPG – Caratteristiche

- Keyring (portachiavi)

pubblico privato

- ID (identificativo univoco di una keypair)
  - Es. 4E72B64D
- Compatibile con PGP (vers. 2.0+)

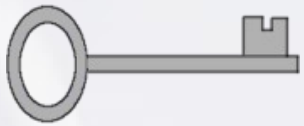
Generazione chiavi



`gpg --key-gen`

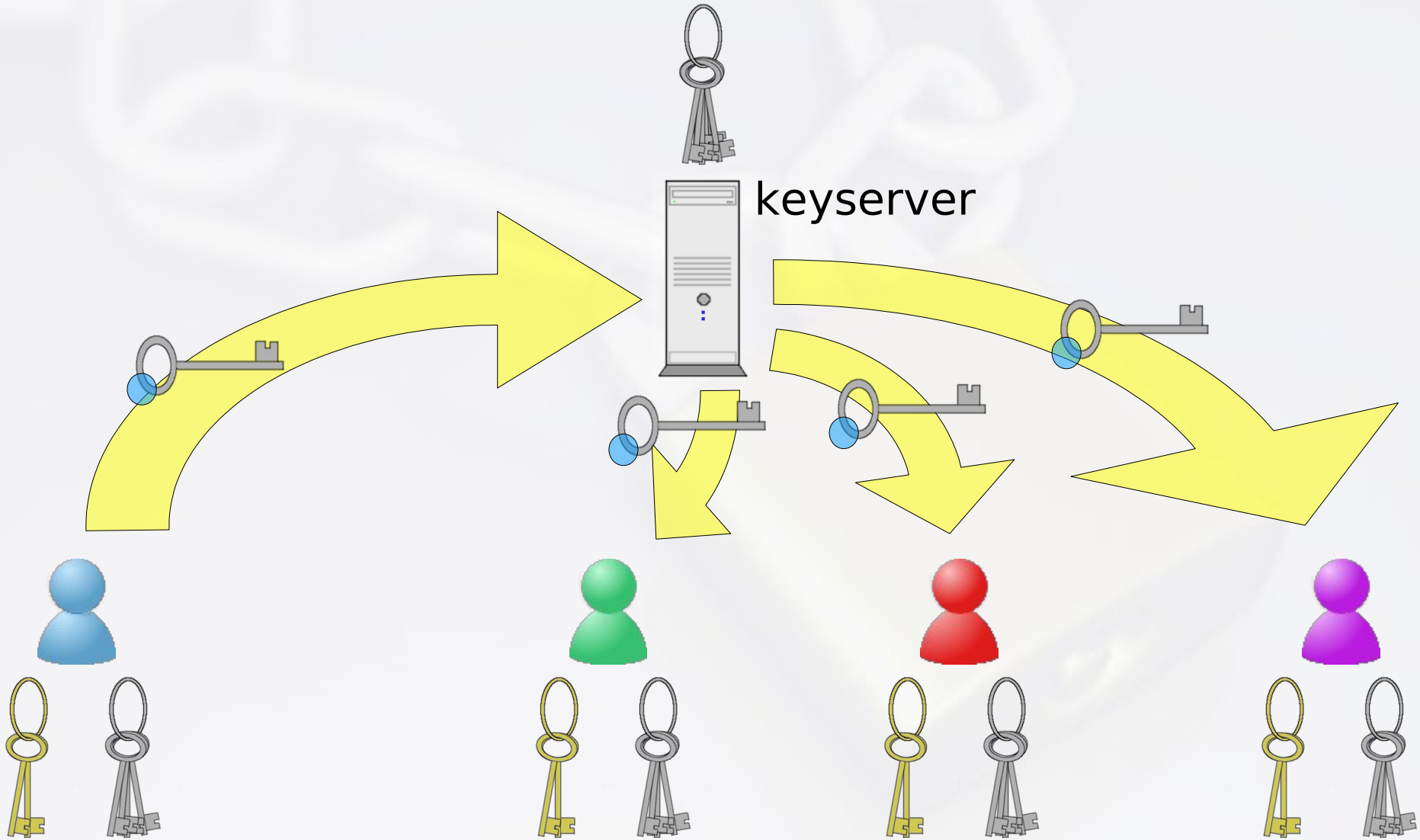
- Tipi di chiavi (solo firma o anche cifratura)
- Lunghezza della keypair
- Durata della keypair
- Nome e cognome del proprietario e relativo indirizzo di posta elettronica
- Passphrase (per la protezione della chiave privata)

Esempio di chiave pubblica



```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.1 (GNU/Linux)
mQGiBEHYH/YRBACLSzoi7Gq9dQMno2FyM7+GjzZI03ZfYmG++SzkFFR1WOU+t/X5
wViwQzUTAmO6kPIG0XklnjDNF3ECOCzcnecpoaiKVwaSL6O3Rg6WQ5CjWt1IUK1H
DJVNgM1wp3d1ul4+LULtThr+LsYAUnMsxiiWXJyCjrsKn36XMyr4xQCuNwCg7S9J
2QqlsHxdc6LL+5JRNmJ1G+kD+wQ1incMF/bU6V466SzMhSCgB2Zi1rgyNlm9ekay
A8rp7Jdeh8RaQztarJ319YA6Xt4u316ybYd3FQnOFwkKFbBjejkUJEYn/yYnmCFb
BLVdpjfe+HqdmKa0euIY0WEQ/DAoe2WFf1TtSqBY2AA0nLw+gHWbsWCW93SC5GNR
tEjBA/kBbO8cftKa0BVgYLa9t+jKSrC14JEykCEANOiiYoNHRj4//gLYKGLqOQch
2F/8KevAQOpe8mbRyAtTbMH7pvlvSsr+afXIHUZyFn+Fvtn6D6g4JQfHFNRvObpA
NTxzhs3/glPDXXCxAwUM2p0BuQ2HW4xNvo8kaFrydLjuMlsSnrQuRGFuaWVsZSBN
YXNpbmkgKGRhbmllbGUpIDxkLm1hc2luaUB0aXNjYWxpLml0PohkBBMRAgAkBQJB
2B/2AhsDBQkB4TOABgsJCAcDAgMVAgMDFgIBAh4BAheAAAoJEJmWtfONJngnk8QA
nin354A3dflHOm8YGiB5hPixdQbAAJ9j/ozLxt4R6w8xF3pYU68bSNZ3x7kBDQRB
2B/+EAQAozAzheLYsbl0XRuaKAF8BQLDYgGg57y1FgLGTwsKWpOq8NPdVd4PsVjc
5a7hrwcxgwQrCu0iAndpqhh8V0TwgSC3C+TWKvk1Z/dd0jJHgg8JaKrEXxdUjff3
qO5uVWZnNbikEm8t8rmGQVhLbZZTkmjikJsaWkvztSsp6nkHjBcAAwUD/0kUya2w
XYGycEMwV+L+ayx7Ge3yKHAtYF5ddFtnKkzIJp8HKL+a0rcGE4Drc0ox6amEtZ+2
0T/7ZsgfS3r5Kt76HhcJMS7Oa6ZKFf7/GndblcQVsPwYkdoq735xJlybsT+lO+KJ
krLM0M3zyhbVRLeTaL/g+gLtFJFIgOlpXrbhiE8EGBECAA8FAkHYH/4CGwwFCQHh
M4AACgkQmZa1840meCfh6gCeKJJ2tFyuewjGMPYEBCNB1bN3JIMAn1vlN1qmCZno
pg7P25fcOUfX5a4Q
=VDWE
-----END PGP PUBLIC KEY BLOCK-----
```

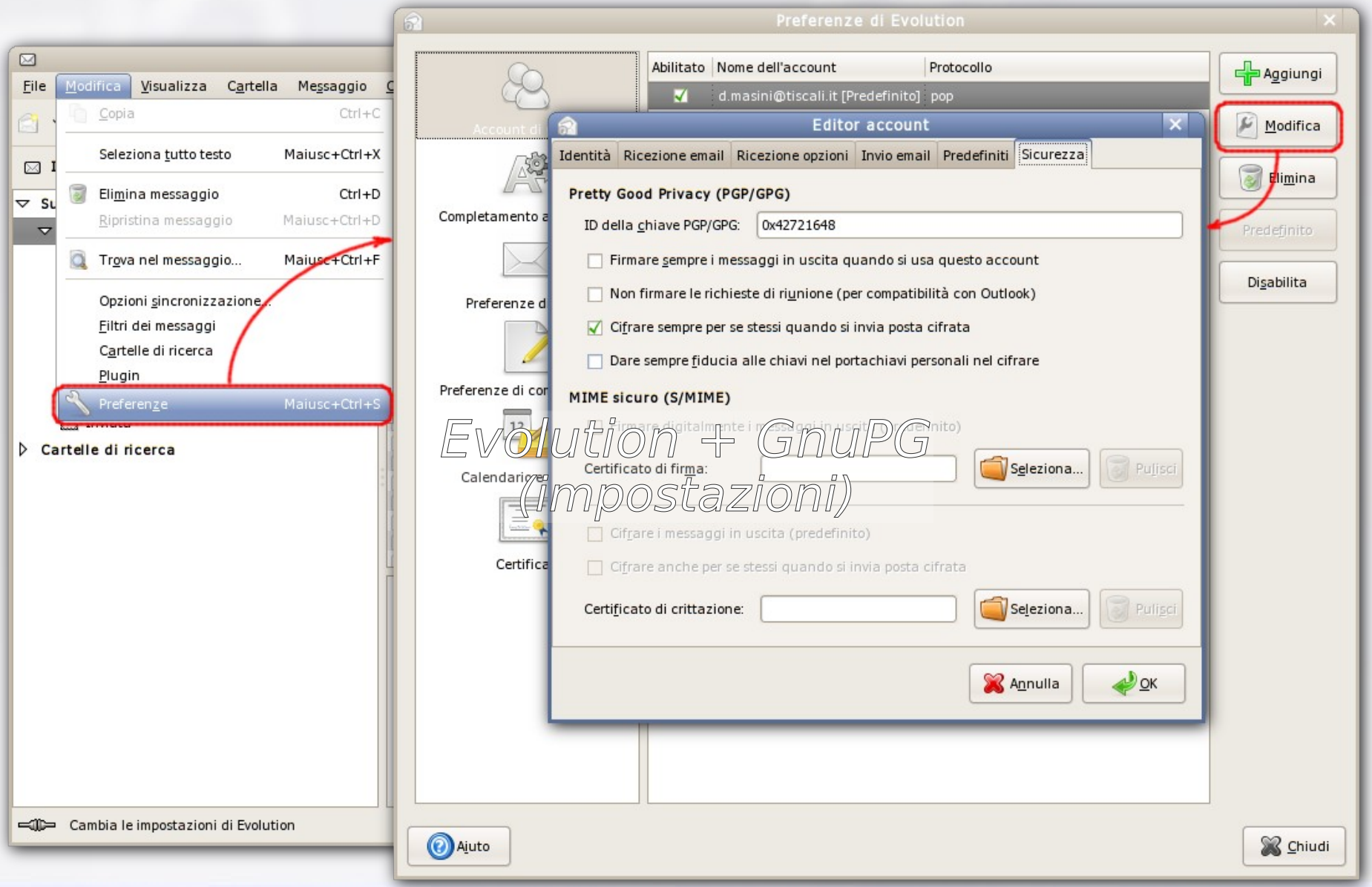
Pubblicazione della chiave



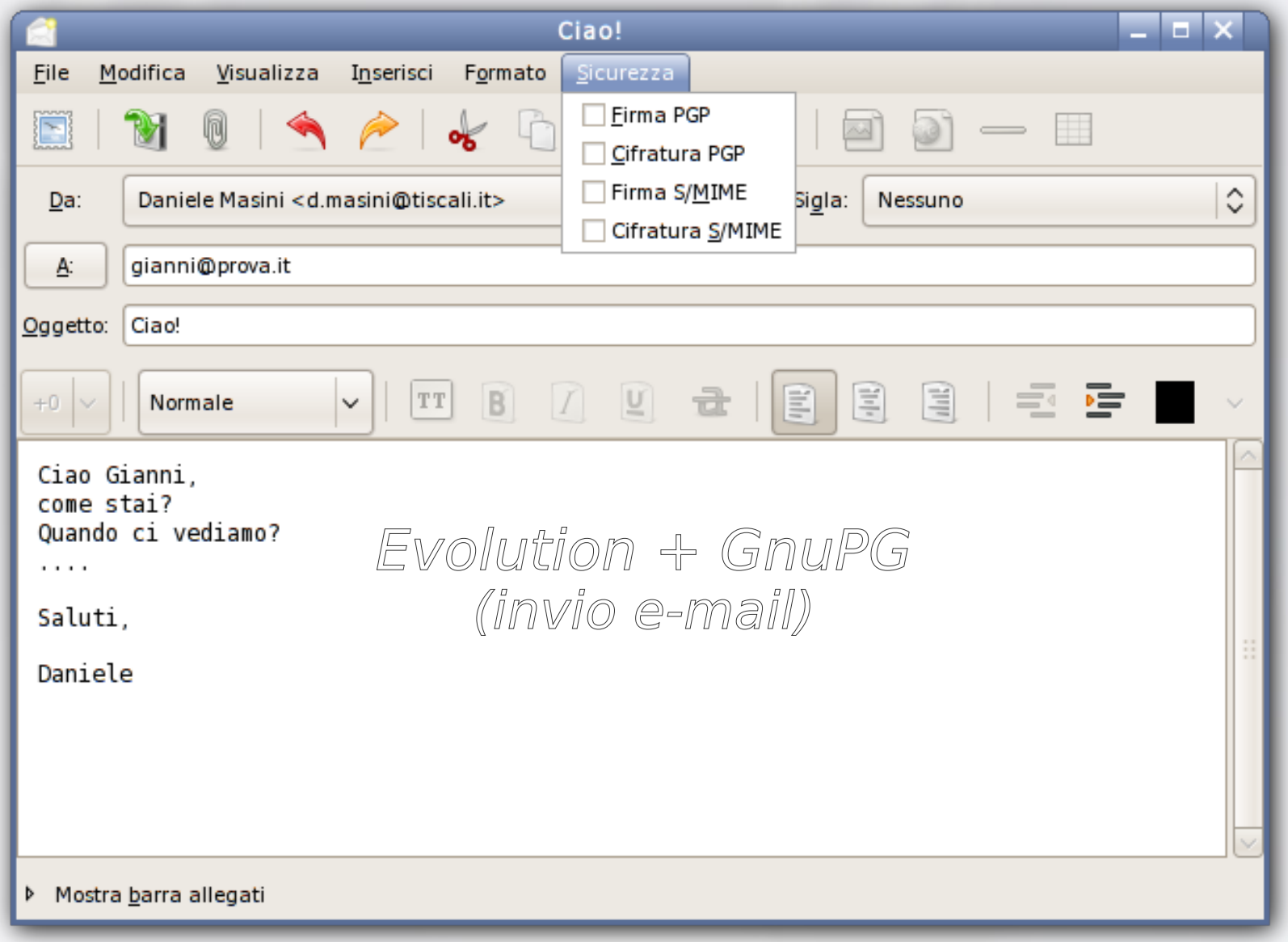
Posta elettronica cifrata

- È possibile utilizzare i meccanismi crittografici (GnuPG) in maniera automatica con la posta elettronica: le e-mail divengono così analoghe alle lettere in busta chiusa 
- Per mezzo della firma elettronica si certifica di essere l'autore del messaggio e si garantisce che il messaggio ricevuto non è stato alterato 

Posta elettronica cifrata

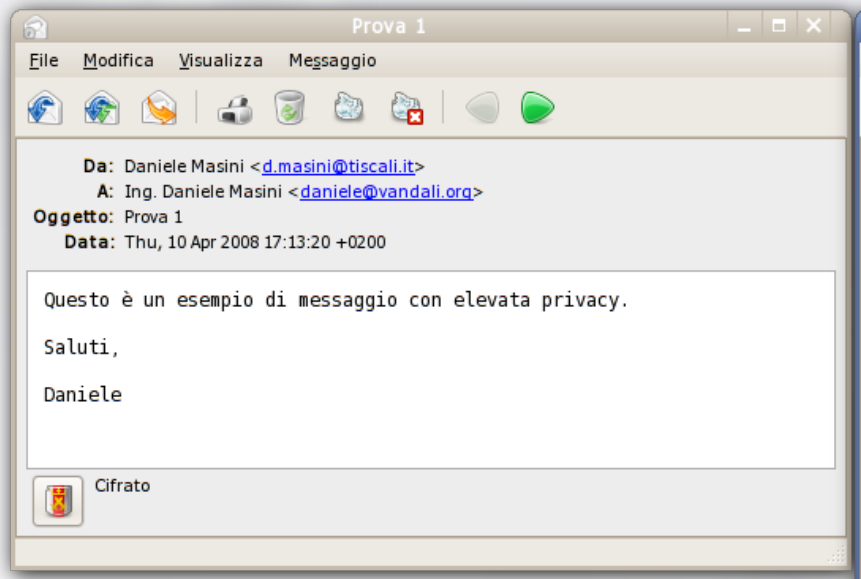


Posta elettronica cifrata



Evolution + GnuPG
(invio e-mail)

Posta elettronica cifrata

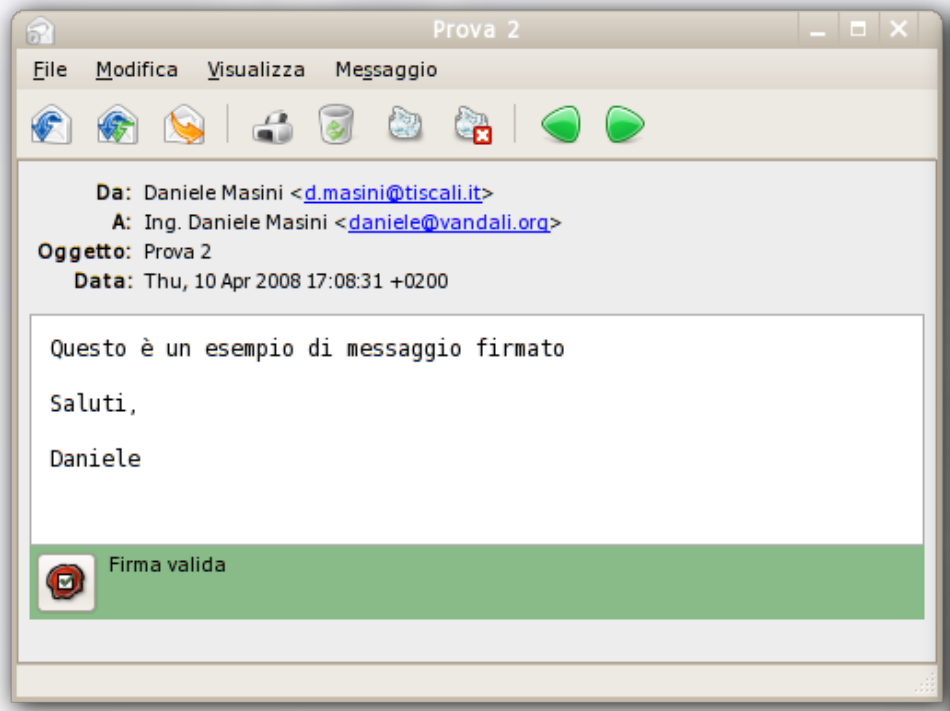


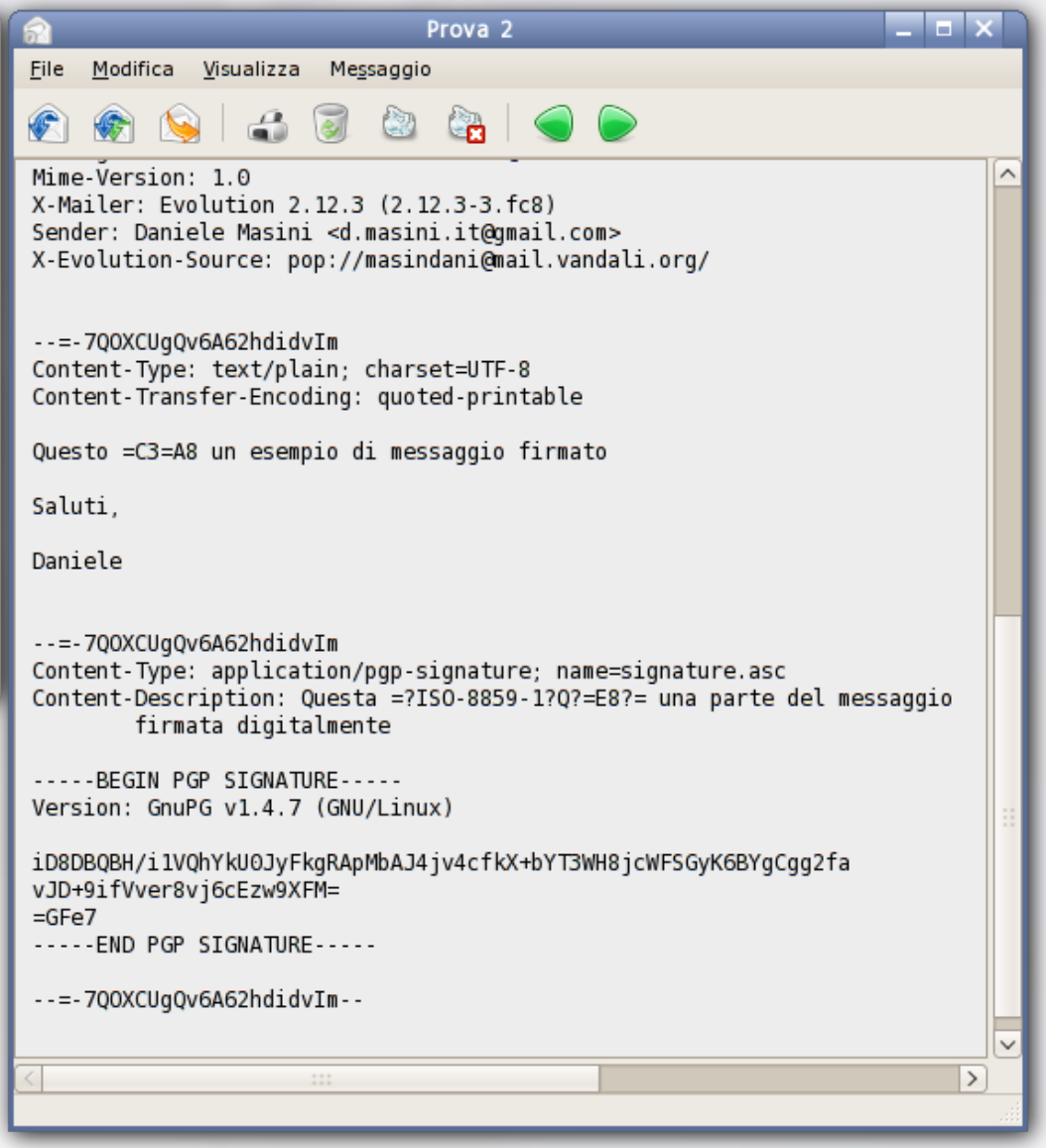
Evolution + GnuPG
(e-mail cifrata)

Posta elettronica cifrata

Evolution + GnuPG
(richiesta passphrase)

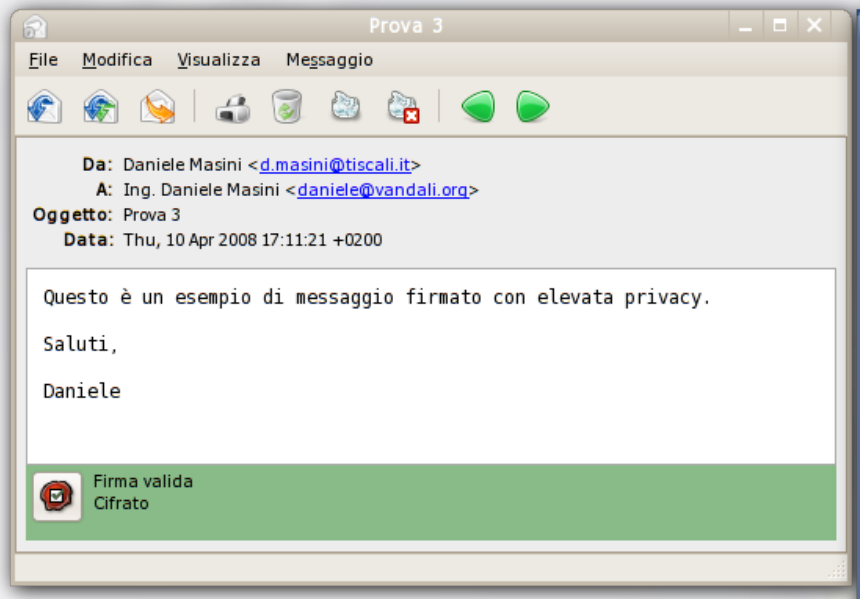
Posta elettronica cifrata





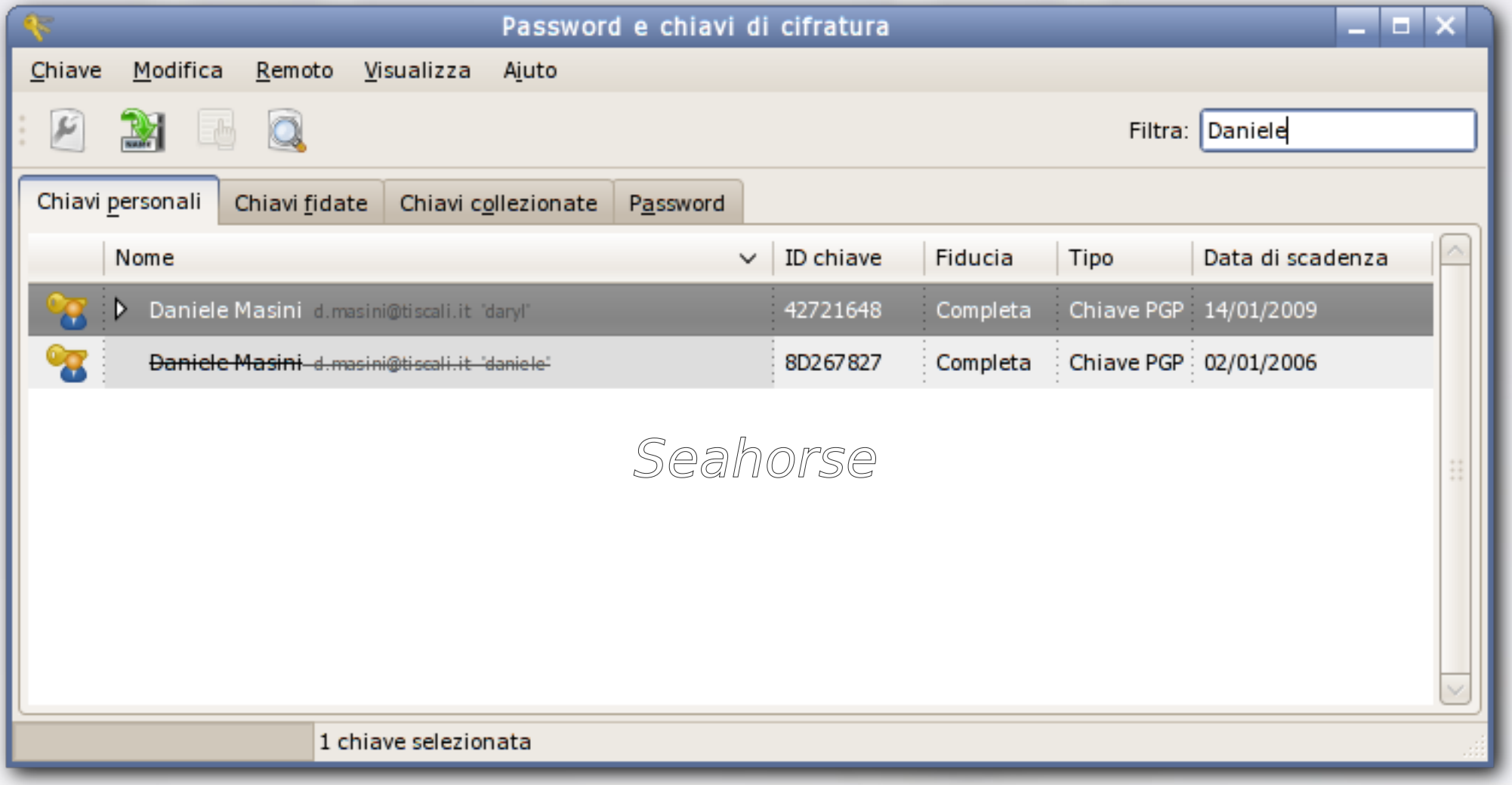
Evolution + GnuPG
(e-mail firmata)

Posta elettronica cifrata

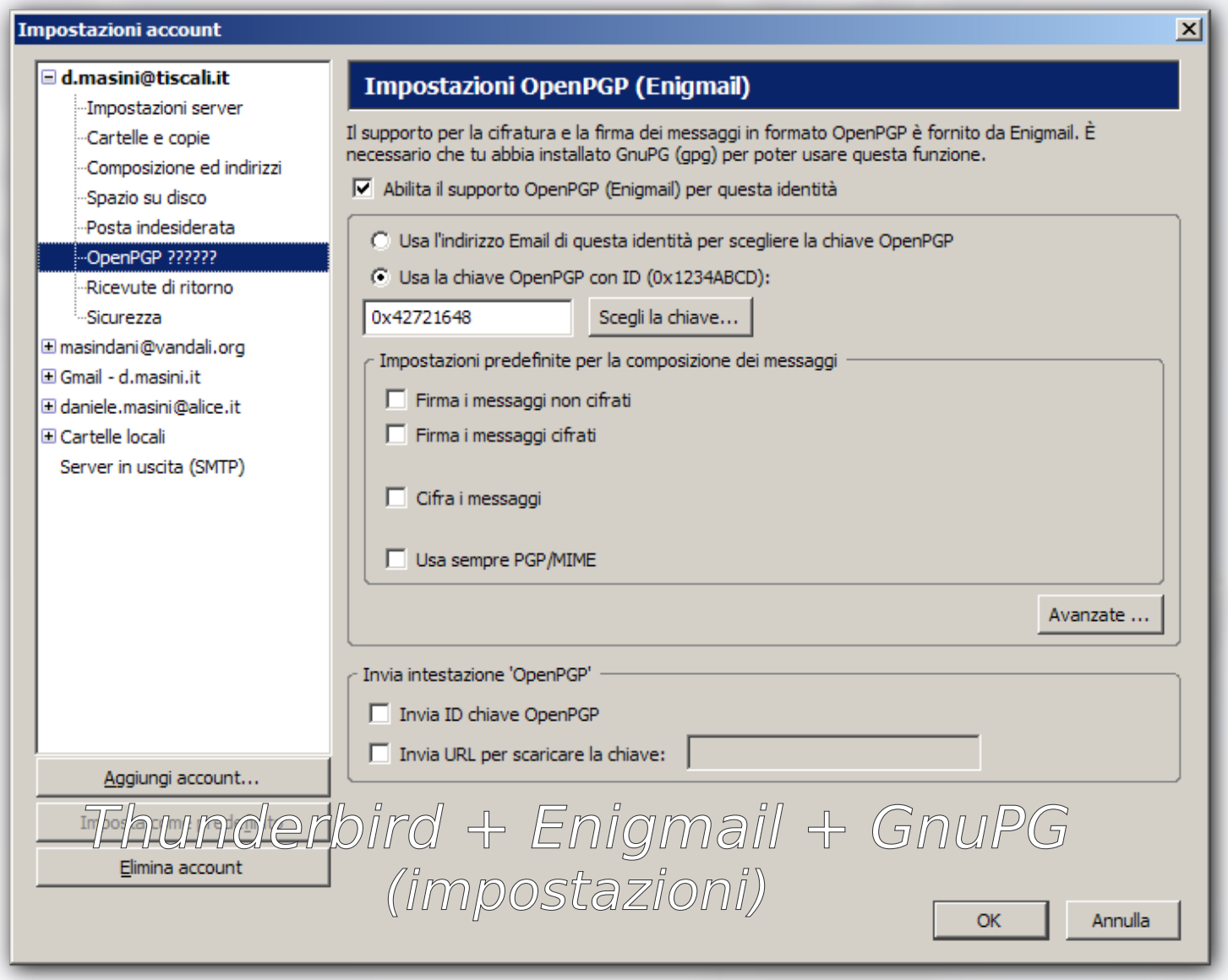


Evolution + GnuPG
(e-mail firmata e cifrata)

Gestione delle chiavi

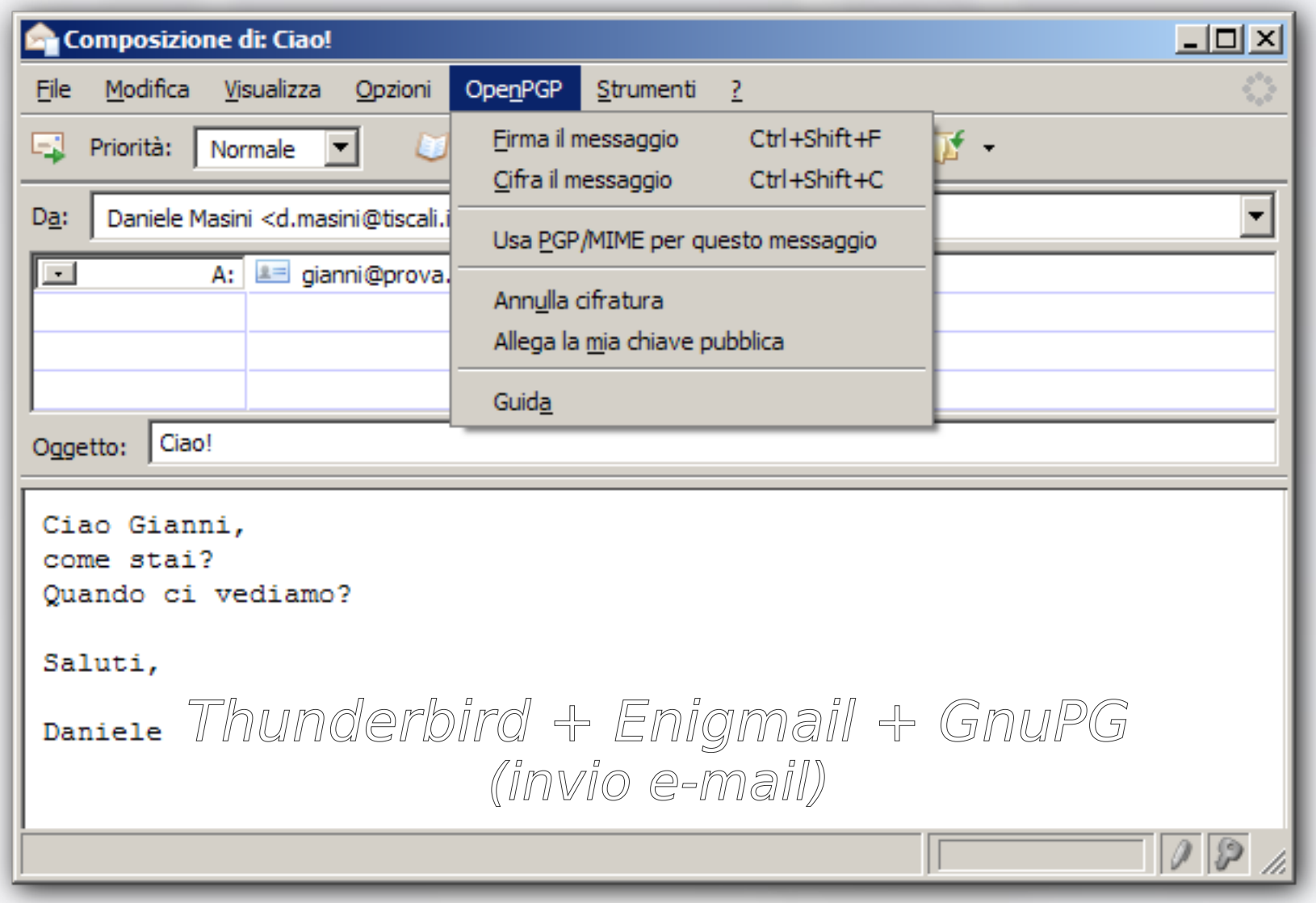


Posta elettronica cifrata

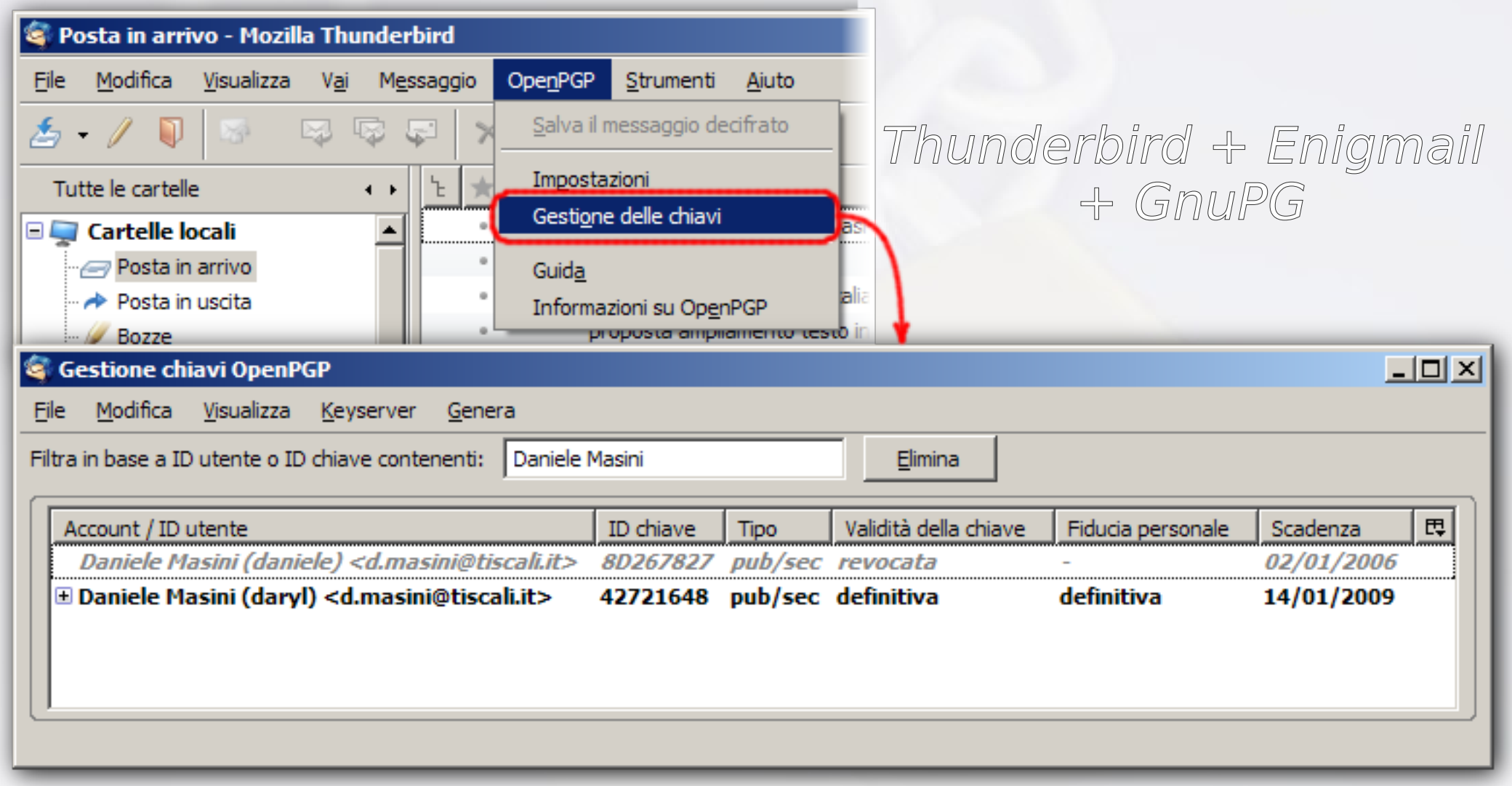


Thunderbird + Enigmail + GnuPG (impostazioni)

Posta elettronica cifrata



Gestione delle chiavi



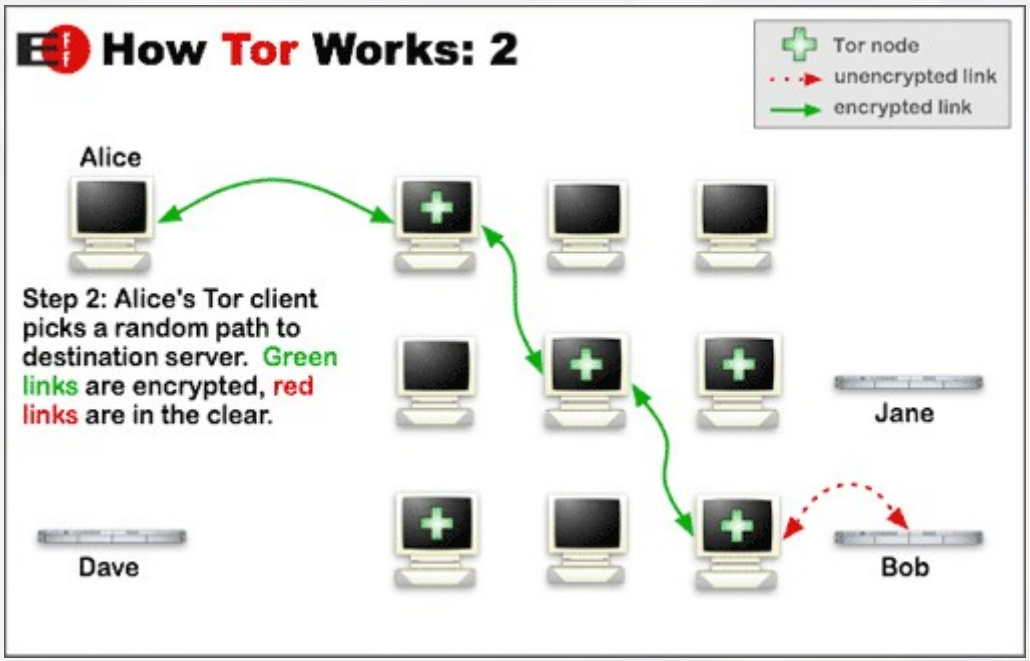
Thunderbird + Enigmail + GnuPG

La fiducia nelle chiavi

- Come essere sicuri dell'effettivo proprietario di una chiave pubblica, ovvero, la chiave che riporta il nome di Mario Rossi appartiene effettivamente a Mario Rossi?
- Fingerprint (consegnato brevi manu direttamente dal proprietario)
  - Es. `444A 193A 28C2 2A99 1966 B2A5 4216 2453 4272 1648`
- Key sign party
- Firma della chiave (certificato digitale)

Comunicazioni anonime

- TOR (http://www.torproject.org)



- Mixminion (http://mixminion.net)

Link utili

Steganografia
http://it.wikipedia.org/wiki/Steganografia

Crittografia
http://it.wikipedia.org/wiki/Crittografia

GNU Privacy Guard
http://www.gnupg.org/

GNU Privacy Handbook
http://www.gnupg.org/gph/en/manual.html
http://www.gnupg.org/gph/en/manual.pdf

Seahorse
http://www.gnome.org/projects/seahorse

GNU Privacy Assistant
http://wald.intevation.org/projects/gpa

Enigmail
http://enigmail.mozdev.org/home/index.php

Certificato digitale
http://it.wikipedia.org/wiki/Certificato_digitale

E-mail crittografata – Tutorial
http://www.gxware.net/labs/public_docs/encryptmail.html
http://www.ismprofessional.net/pascucci/documenti/gpg

OpenPGP
http://www.openpgp.org/index.shtml

Security Awarness for teens
http://www.hackerhighschool.org/lessons/HHS_it9_Sicurezza_Posta.pdf

Key signing party HowTo
http://www.gnupg.org/howtos/it/keysigning_party.html

Selected Papers in Anonymity
http://freehaven.net/anonbib/topic.html

Ringrazio per l'attenzione

Domande?