Pillole di autodifesa digitale

come tutelare la propria riservatezza con un seminario bellissimo, pratico e indolore

Cryptoparty

CIOTOFLOW

** Ciotoflow ** - http://flow.ciotoni.net -

- Mercoledì 18.00 ca aula p2

CryptoParty

- Gran parte delle informazioni sulla nostra vita passa attraverso un computer (chat, mail, etc)
- I nostri dati passano per decine di dispositivi (potenzialmente malevoli) prima di arrivare a destinazione
- Facilità di analisi, immagazzinamento, e intercettazione dei nostri dati (quasi sempre sensibili)
- Molto spesso accettiamo nelle policy superficialmente che la destinazione analizzi,utilizzi e venda! i nostri dati

CryptoParty

- Gran parte delle informazioni sulla nostra vita passa attraverso un computer (chat, mail, etc)
- I nostri dati passano per decine di dispositivi (potenzialmente malevoli) prima di arrivare a destinazione
- Facilità di analisi, immagazzinamento, e intercettazione dei nostri dati (quasi sempre sensibili)
- Molto spesso accettiamo nelle policy superficialmente che la destinazione analizzi,utilizzi e venda! i nostri dati

CryptoParty

- Gran parte delle informazioni sulla nostra vita passa attraverso un computer (chat, mail, etc)
- I nostri dati passano per decine di dispositivi (potenzialmente malevoli) prima di arrivare a destinazione
- Facilità di analisi, immagazzinamento, e intercettazione dei nostri dati (quasi sempre sensibili)
- Molto spesso accettiamo nelle policy superficialmente che la destinazione analizzi,utilizzi e venda! i nostri dati

CryptoParty

- Gran parte delle informazioni sulla nostra vita passa attraverso un computer (chat, mail, etc)
- I nostri dati passano per decine di dispositivi (potenzialmente malevoli) prima di arrivare a destinazione
- Facilità di analisi, immagazzinamento, e intercettazione dei nostri dati (quasi sempre sensibili)
- Molto spesso accettiamo nelle policy superficialmente che la destinazione analizzi,utilizzi e venda! i nostri dati

Cryptoparty

- gli strumenti non sono solo per pochi nerd eletti
- più pratica possibile
- banchetti per approfondimenti/sperimentazioni/installazioni
- domande/risposte

Cryptoparty

- gli strumenti non sono solo per pochi nerd eletti
- più pratica possibile
- banchetti per approfondimenti/sperimentazioni/installazioni
- domande/risposte

Cryptoparty

- gli strumenti non sono solo per pochi nerd eletti
- più pratica possibile
- banchetti per approfondimenti/sperimentazioni/installazioni
- domande/risposte

Cryptoparty

- gli strumenti non sono solo per pochi nerd eletti
- più pratica possibile
- banchetti per approfondimenti/sperimentazioni/installazioni
- domande/risposte

Di cosa parleremo

Crittografia

Rendere illeggibile il contenuto di un informazione a chi non è autorizzato

cryptoparty!!

Crittografia

Rendere illeggibile il contenuto di un informazione a chi non è autorizzato

`cryptoparty!!`

Crittografia

Rendere illeggibile il contenuto di un informazione a chi non è autorizzato

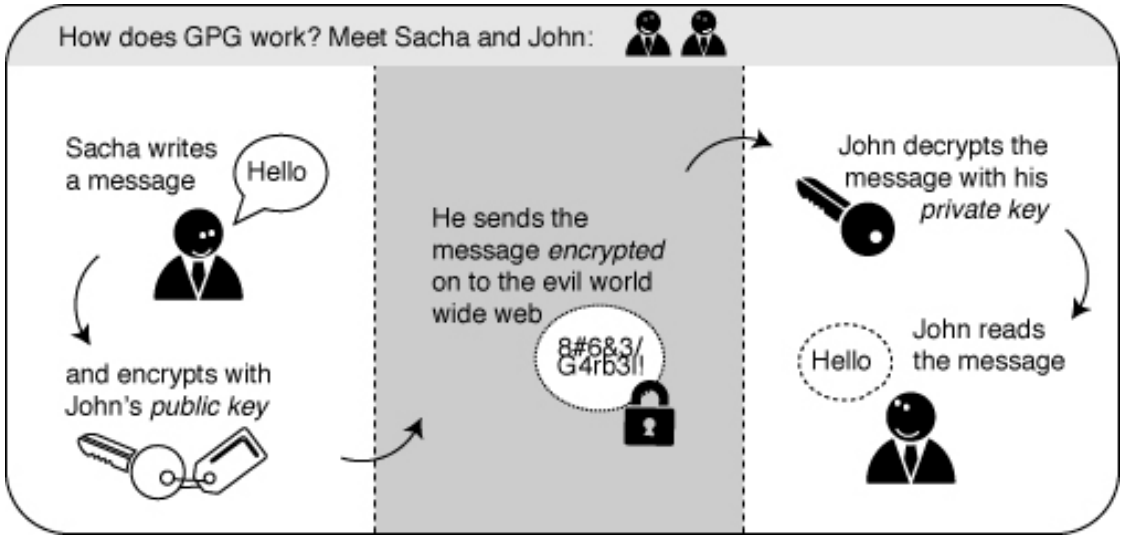
```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.12 (GNU/Linux)

hQIOA7vElRJR89J3EAf/VKtmXc6FnWmAre225nRN8NZRvJM1UZ0
57/Uy0xkiqOGv2nsg5e41eGHBx2qZoIMkSBKgVU1o4I+XwalZVb
Jpk4R/1Blj5ExaqkXJqjBwf5ZlO1gNXpYDmM+gyFrWB2mk9ZVNP
O/J9r3qySYrrw9k2L5QzJytAuvIZwmddqryUyaUemSzLMPV6eGP

P9+waOzlS6YZyKNQAPjWthhxiLDziTV178tUIQITEw==
=OEvO
-----END PGP MESSAGE-----
```

Coppia chiavi!

- !Coppia di chiavi! -
  - Coppia di file su un computer
  - Una pubblica e una privata

Coppia chiavi!

- !Coppia di chiavi! -
  - Coppia di file su un computer
  - Una pubblica e una privata



- Se qualcuno vuole inviarmi informazioni cifrate ha bisogno della mia chiave pubblica
- Se voglio inviare informazioni cifrate ho bisogno della sua chiave pubblica

Diffusione delle chiavi pubbliche

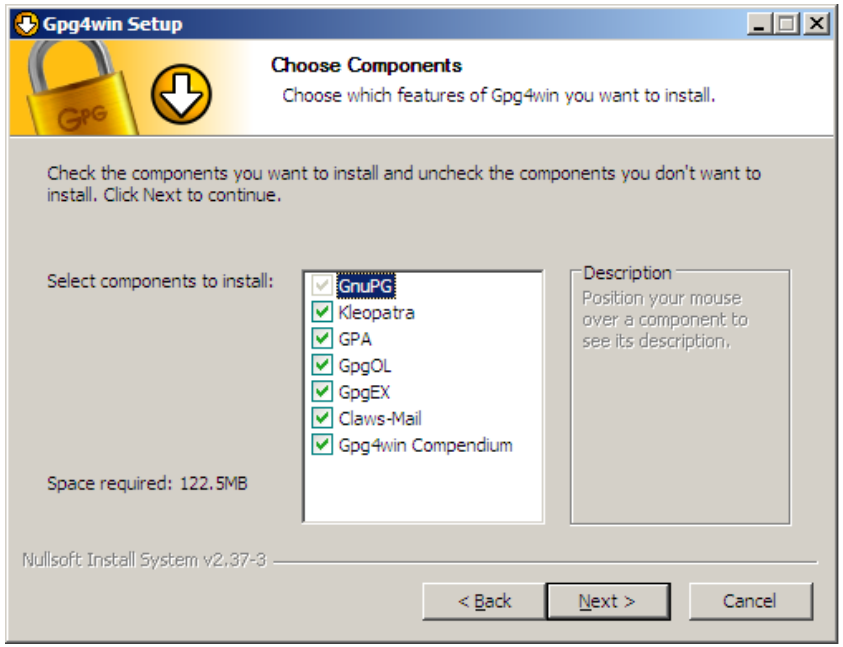
Quindi basta distribuire le chiavi pubbliche
Come??

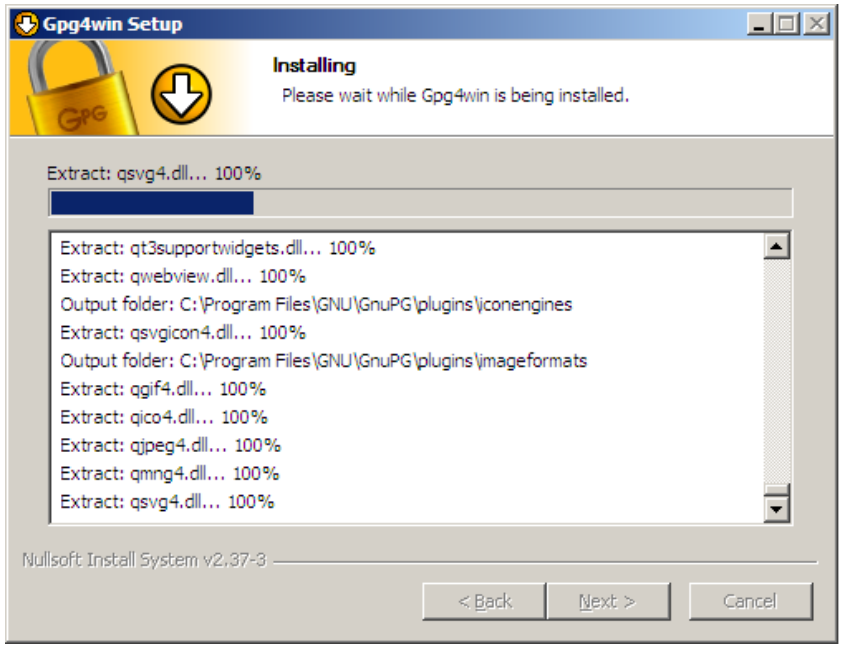
- Fisicamente (es. chiavette usb)
- Per email
- Archivi online dedicati allo scopo (key server)
- Alcuni programmi (es. pidgin+otr) si occupano trasparentemente della diffusione della chiave pubblica

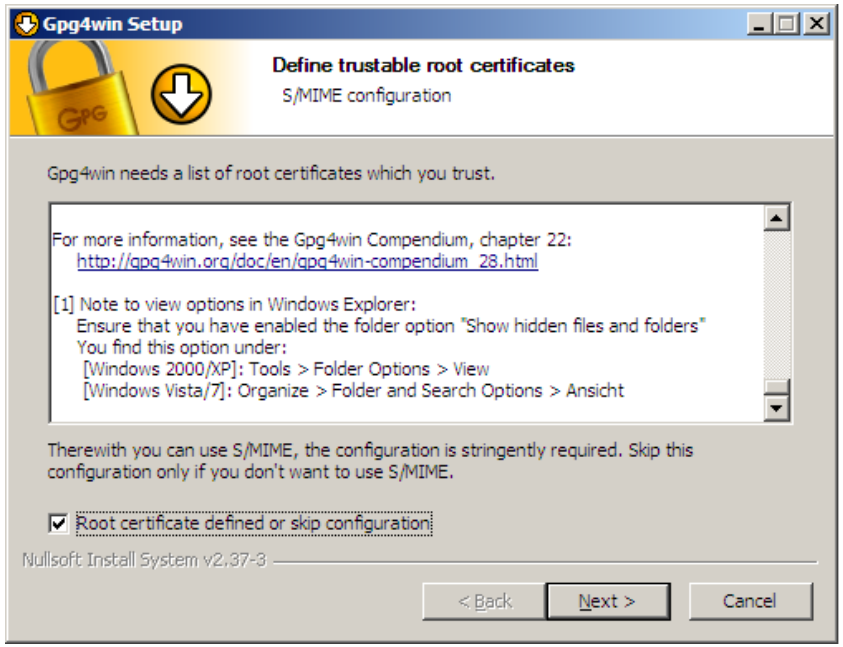
Di cosa parleremo

GPG4WIN

http://gpg4win.org/

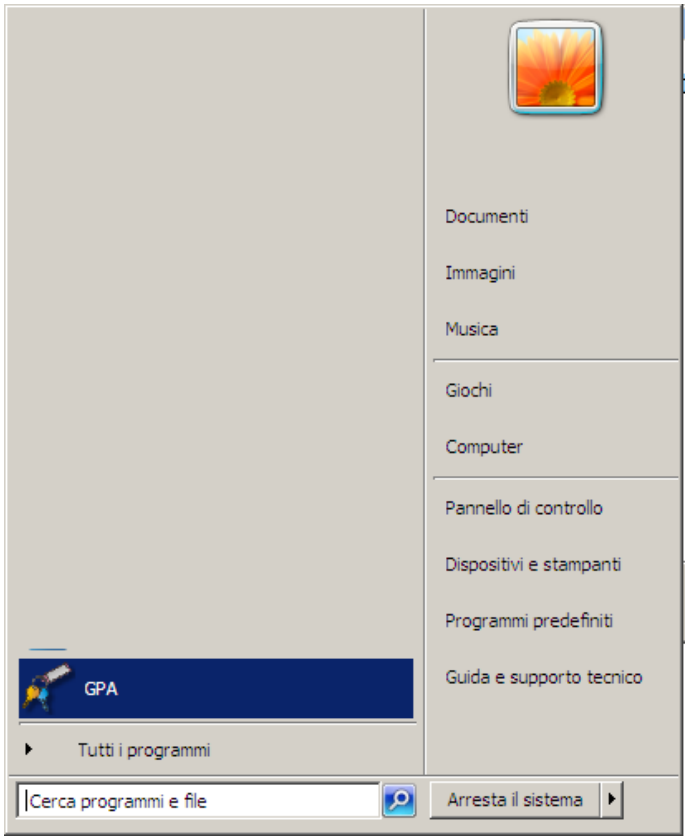

Gpg4win Setup
Choose Components
Choose which features of Gpg4win you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
GnuPG
Kleopatra
GPA
GpgOL
GpgEX
Claws-Mail
Gpg4win Compendium
Description
Position your mouse over a component to see its description.
Space required: 122.5MB
Nullsoft Install System v2.37-3
< Back
Next >
Cancel


Gpg4win Setup
Installing
Please wait while Gpg4win is being installed.
Extract: qsvg4.dll... 100%
Extract: qt3supportwidgets.dll... 100%
Extract: qwebview.dll... 100%
Output folder: C:\Program Files\GNU\GnuPG\plugins\iconengines
Extract: qsvgicon4.dll... 100%
Output folder: C:\Program Files\GNU\GnuPG\plugins\imageformats
Extract: qgif4.dll... 100%
Extract: qico4.dll... 100%
Extract: qjpeg4.dll... 100%
Extract: qmng4.dll... 100%
Extract: qsvg4.dll... 100%
Nullsoft Install System v2.37-3
< Back
Next >
Cancel

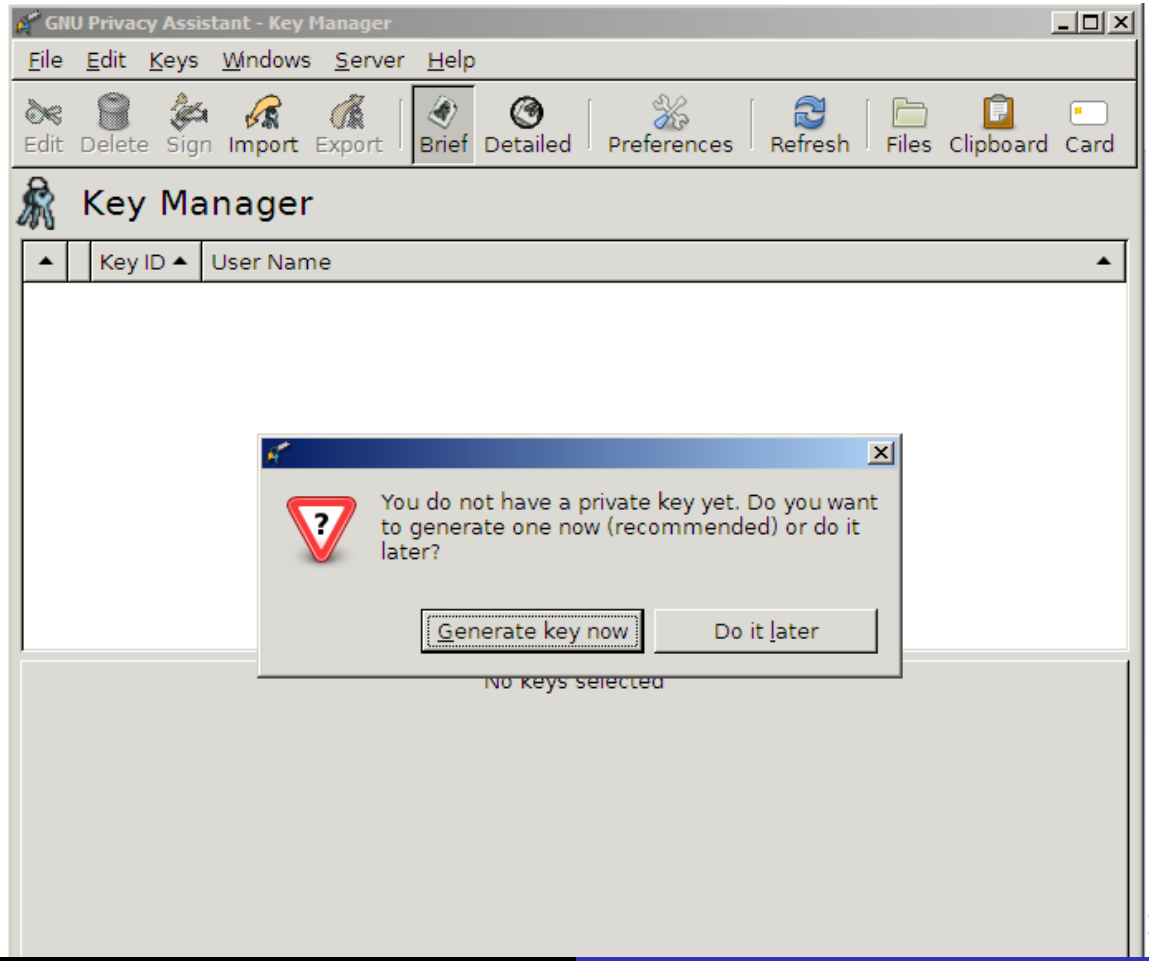

Gpg4win Setup
Define trustable root certificates
S/MIME configuration
Gpg4win needs a list of root certificates which you trust.
For more information, see the Gpg4win Compendium, chapter 22:
http://gpg4win.org/doc/en/gpg4win-compendium_28.html
[1] Note to view options in Windows Explorer:
Ensure that you have enabled the folder option "Show hidden files and folders"
You find this option under:
[Windows 2000/XP]: Tools > Folder Options > View
[Windows Vista/7]: Organize > Folder and Search Options > Ansicht
Therewith you can use S/MIME, the configuration is stringently required. Skip this configuration only if you don't want to use S/MIME.
Root certificate defined or skip configuration
Nullsoft Install System v2.37-3
< Back
Next >
Cancel


Gpg4win Setup
GPG4WIN
Completing the Gpg4win Setup Wizard
Gpg4win has been installed on your computer.
Click Finish to close this wizard.
Show the README file
Click here for the project's homepage
< Back
Finish
Cancel

Manager delle chiavi

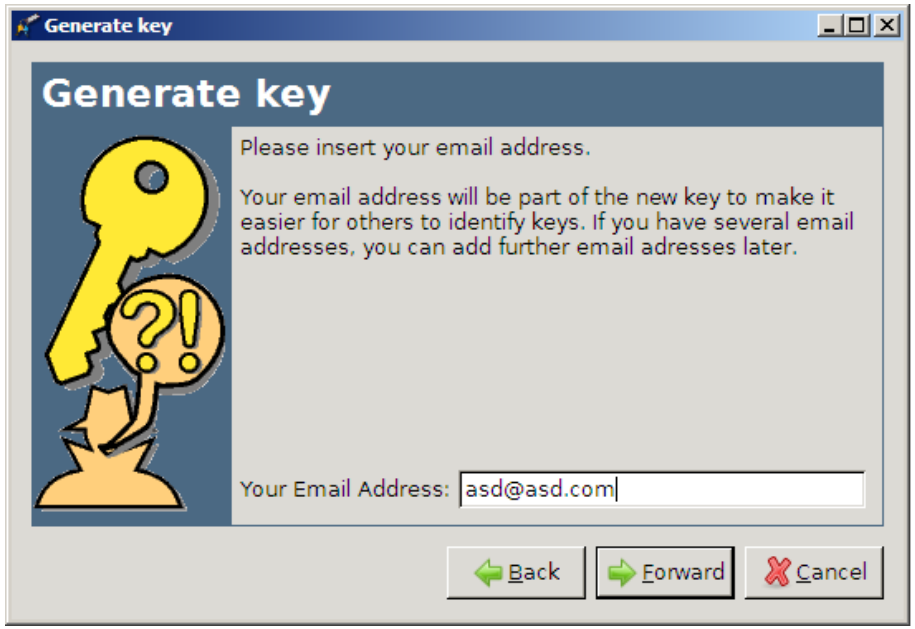


CREARE UNA NUOVA COPPIA DI CHIAVI



CREARE UNA NUOVA COPPIA DI CHIAVI

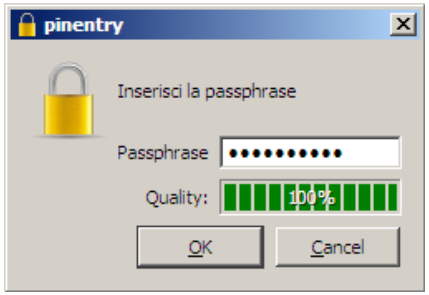
CREARE UNA NUOVA COPPIA DI CHIAVI



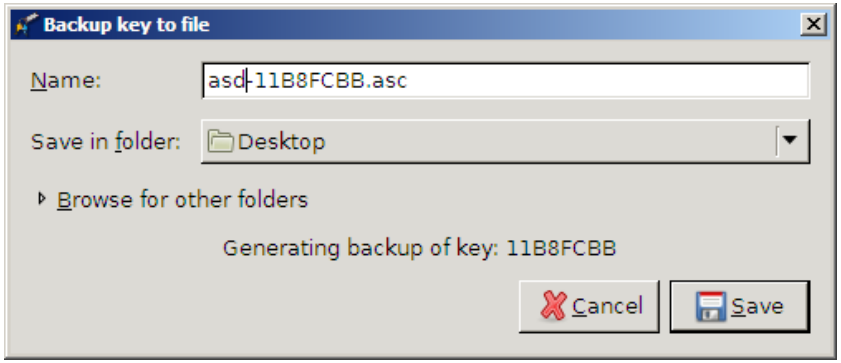
CREARE UNA NUOVA COPPIA DI CHIAVI

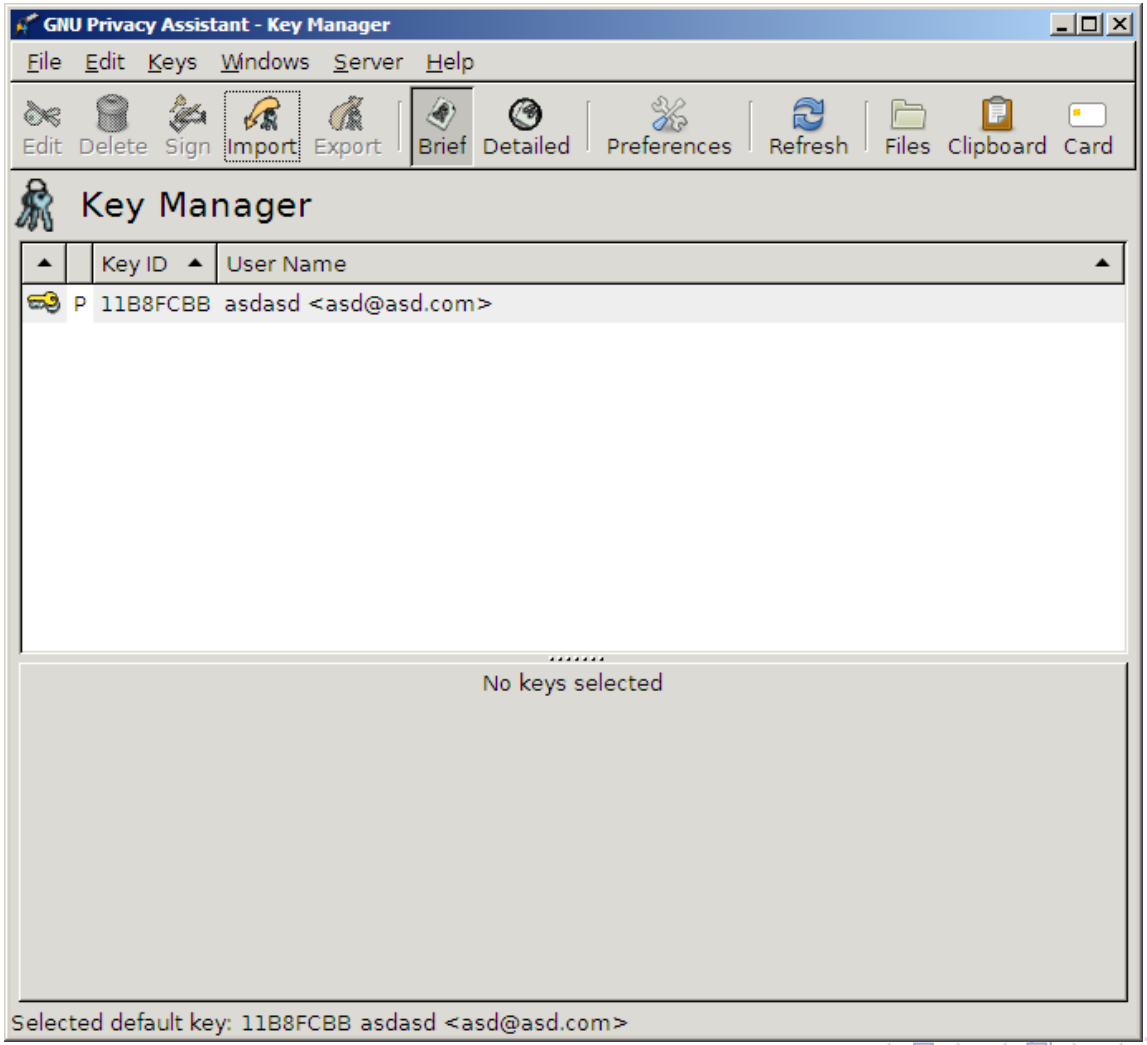
CREARE UNA NUOVA COPPIA DI CHIAVI

Proteggere la chiave privata con una parola d'ordine

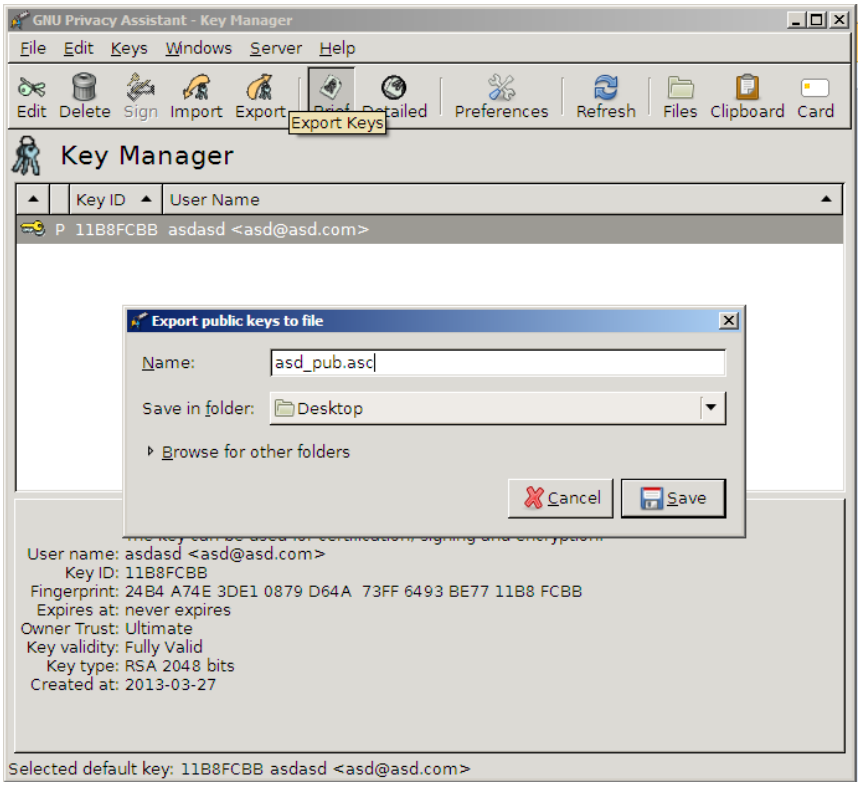


CREARE UNA COPIA DI BACKUP DELLA PROPRIA CHIAVE

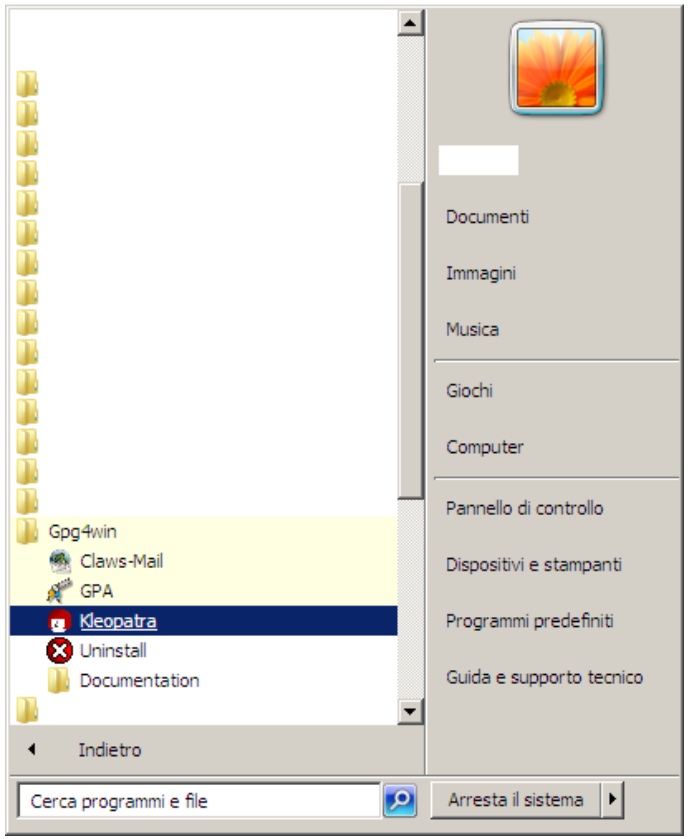



GNU Privacy Assistant - Key Manager
File Edit Keys Windows Server Help
Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card
Key Manager
Key ID
User Name
P 11B8FCBB asdasd <asd@asd.com>
No keys selected
Selected default key: 11B8FCBB asdasd <asd@asd.com>

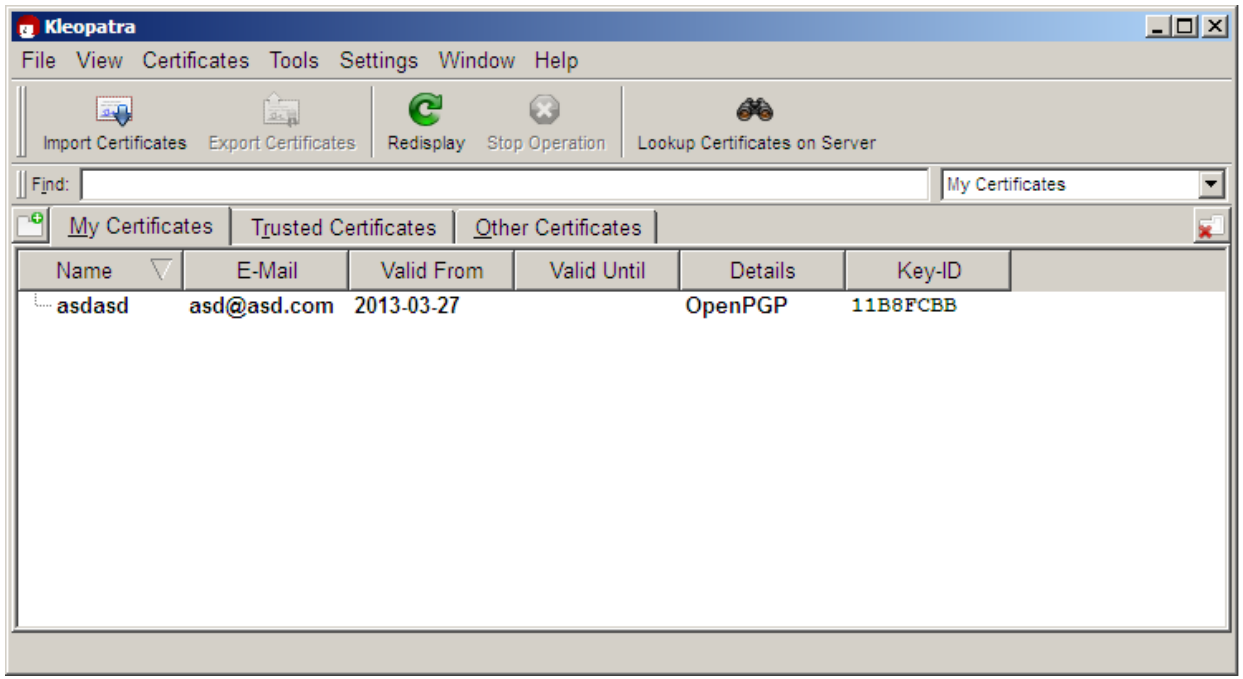
ESPORTARE CHIAVE PUBBLICA SU FILE



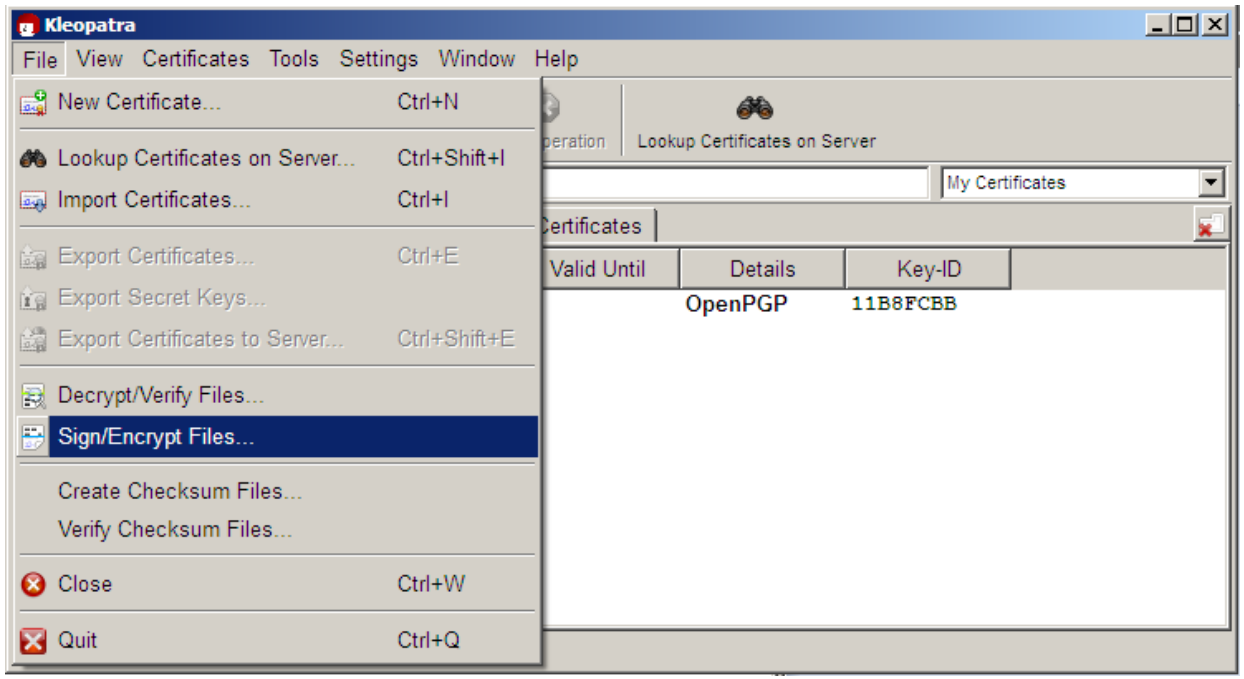
USARE KLEOPATRA PER CIFRARE FILE



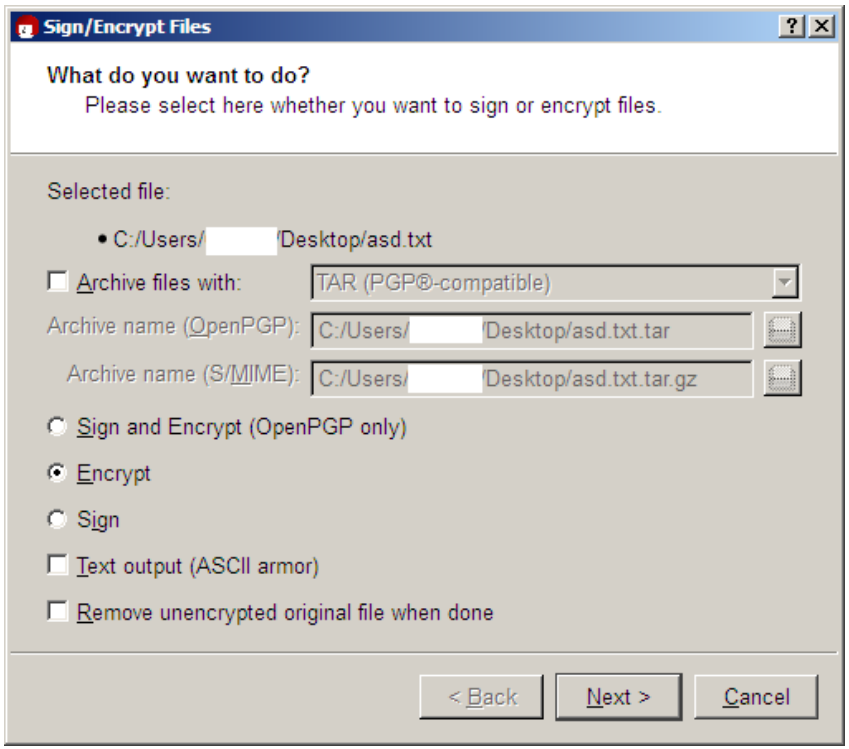
USARE KLEOPATRA PER CIFRARE FILE



USARE KLEOPATRA PER CIFRARE FILE

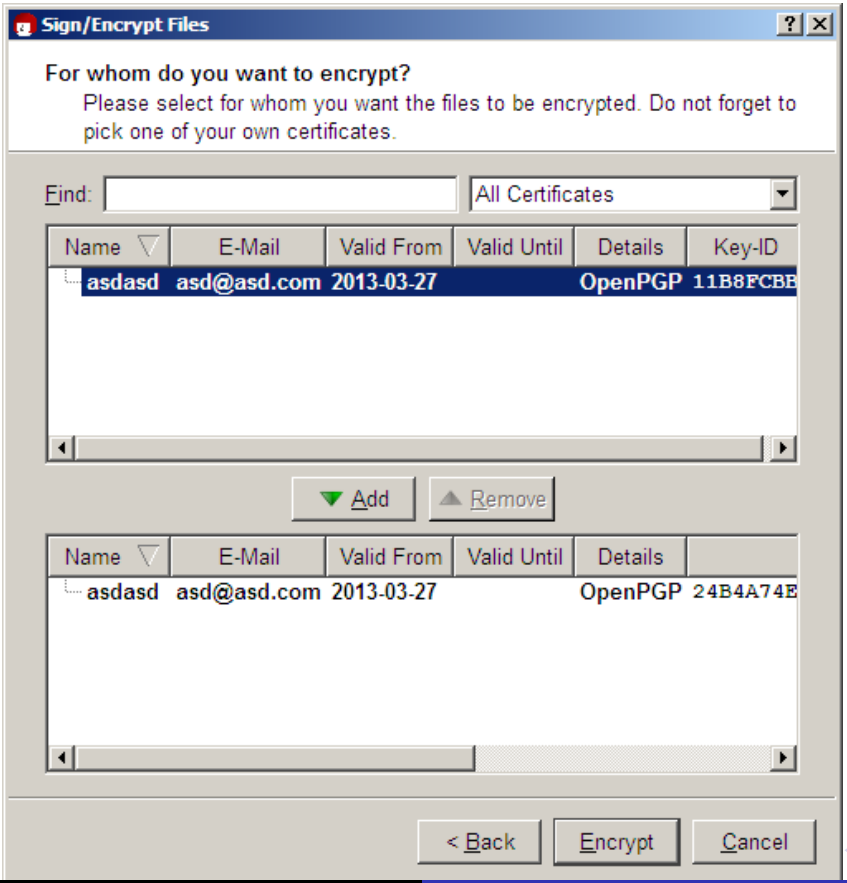


USARE KLEOPATRA PER CIFRARE FILE

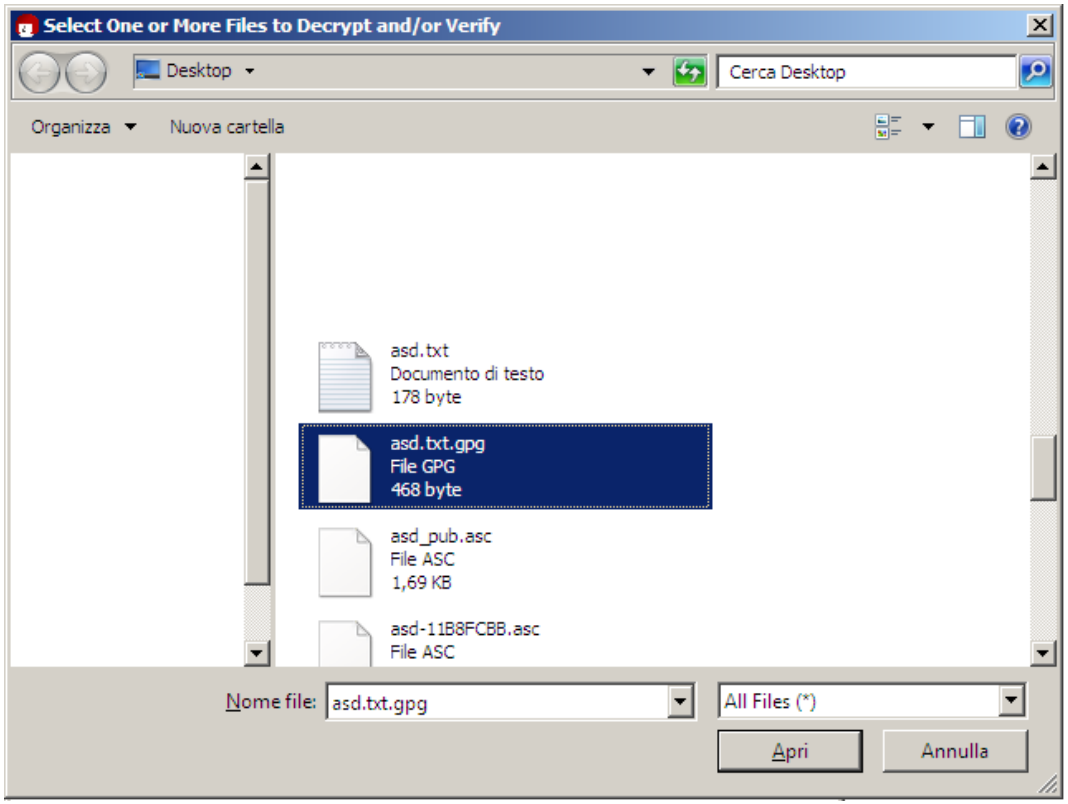


USARE KLEOPATRA PER CIFRARE FILE

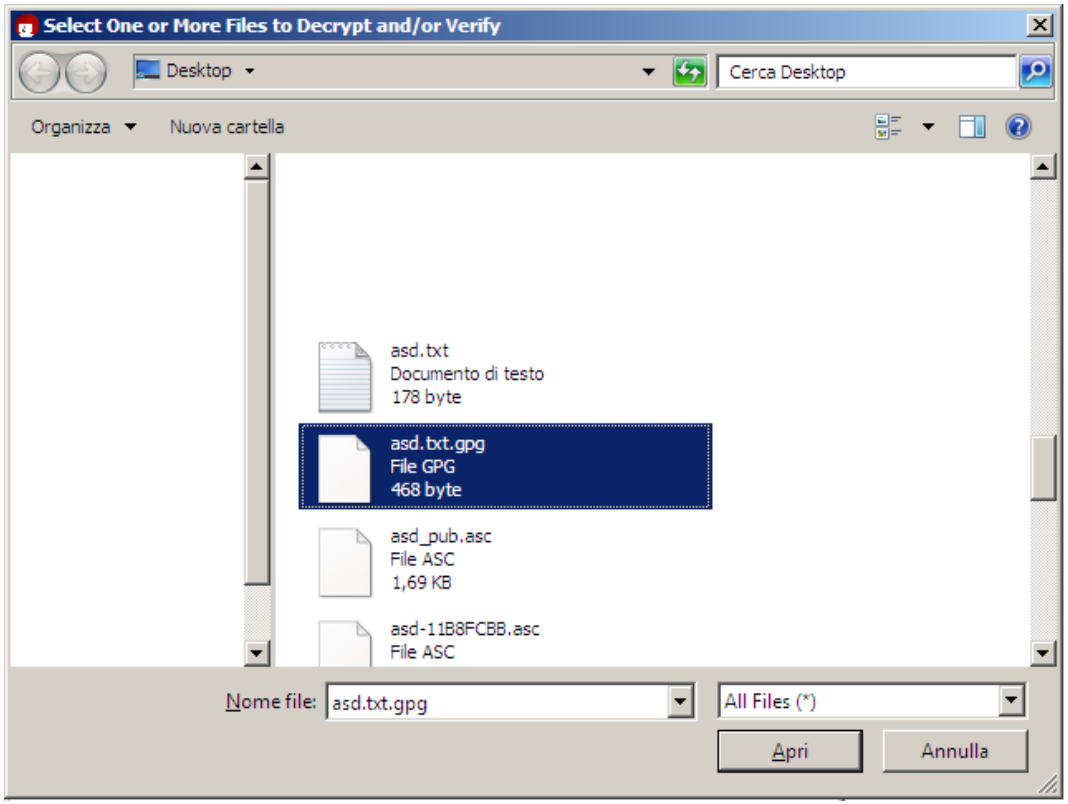
Per chi vogliamo cifrare il file???



USARE KLEOPATRA PER CIFRARE FILE



USARE KLEOPATRA PER CIFRARE FILE



Mail

Thunderbird

- Programma (client) per leggere la posta non dal browser
- Strumenti integrati per cifrare le email
- Permette di leggere le email anche offline

Mail

Thunderbird

- Programma (client) per leggere la posta non dal browser
- Strumenti integrati per cifrare le email
- Permette di leggere le email anche offline

Mail

Thunderbird

- Programma (client) per leggere la posta non dal browser
- Strumenti integrati per cifrare le email
- Permette di leggere le email anche offline

ENIGMAIL

Enigmail

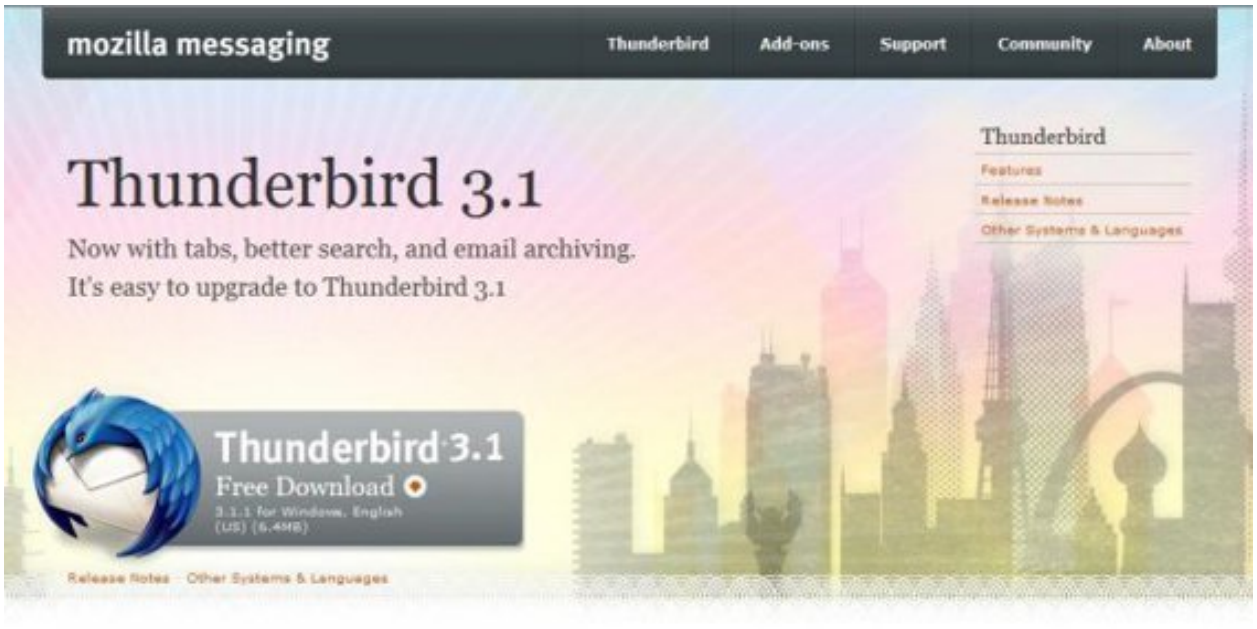
- estensione di Thunderbird per rendere facile e indolore la cifratura delle nostre mail
- gestisce chiavi, cifratura e firma delle nostre email

ENIGMAIL

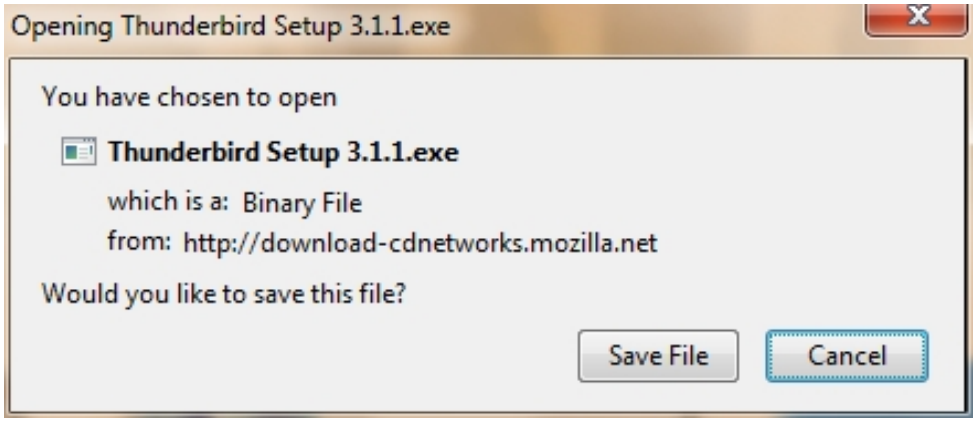
Enigmail

- estensione di Thunderbird per rendere facile e indolore la cifratura delle nostre mail
- gestisce chiavi, cifratura e firma delle nostre email

Installare Thunderbird

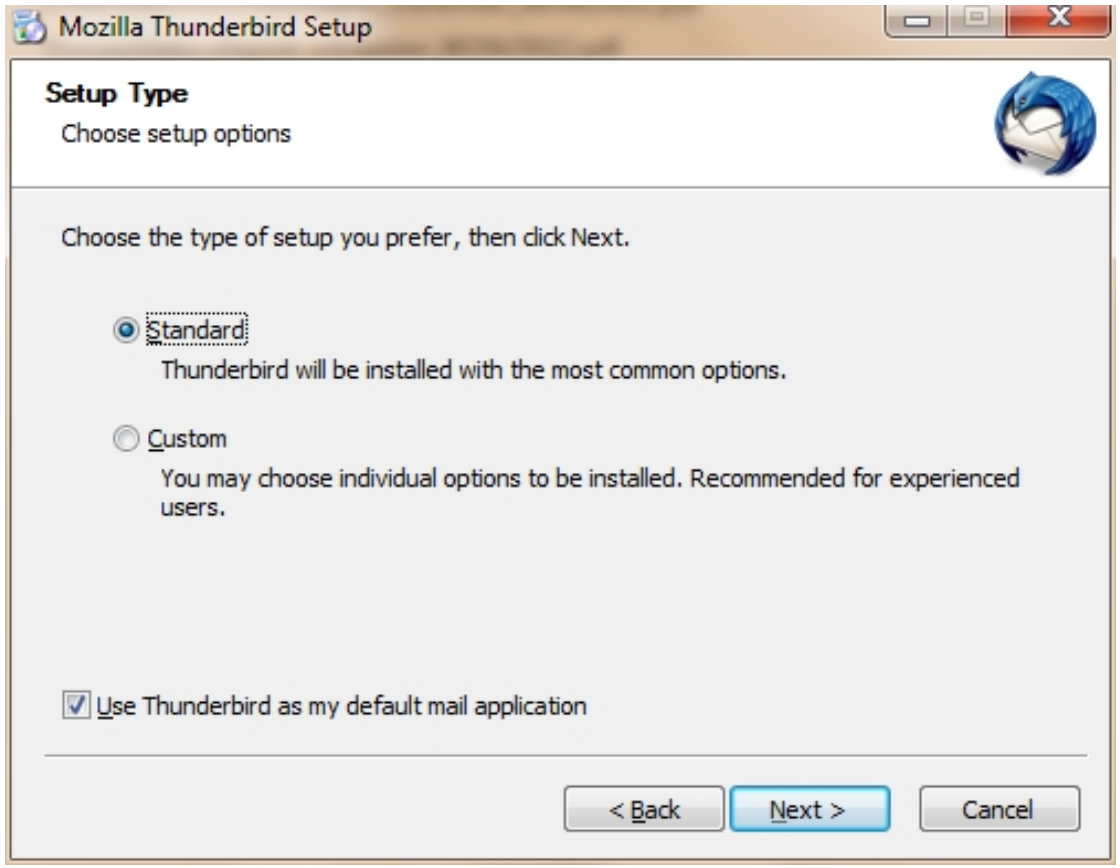


Installare Thunderbird

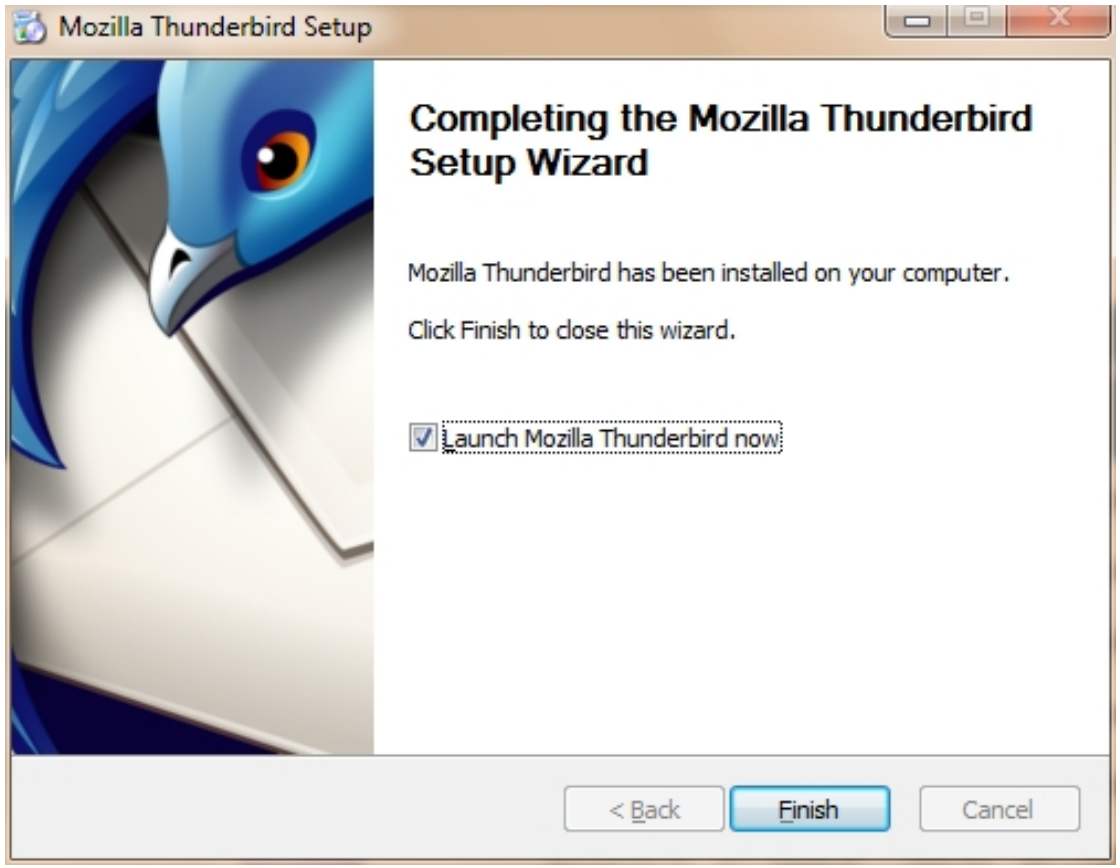


Installare Thunderbird

Installare Thunderbird

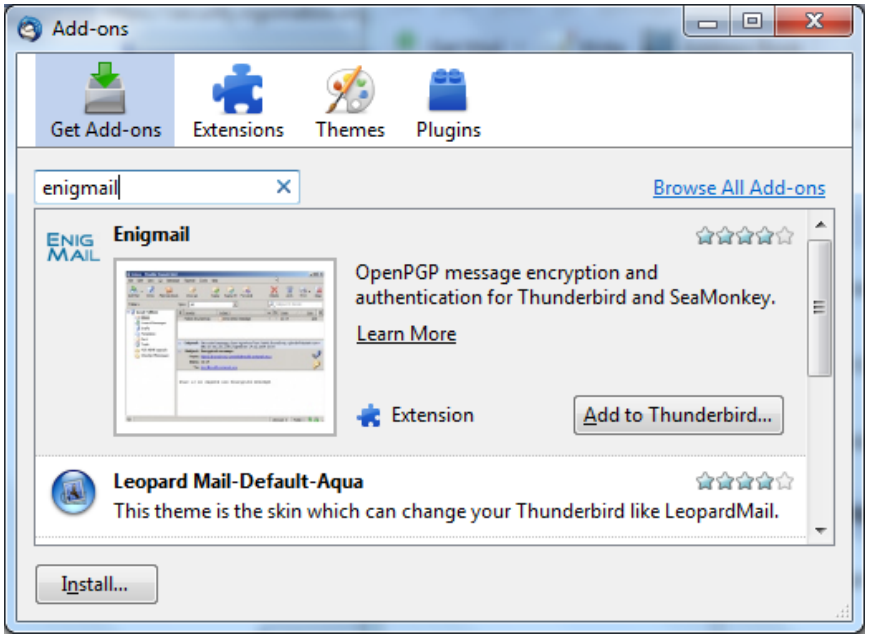


Installare Thunderbird

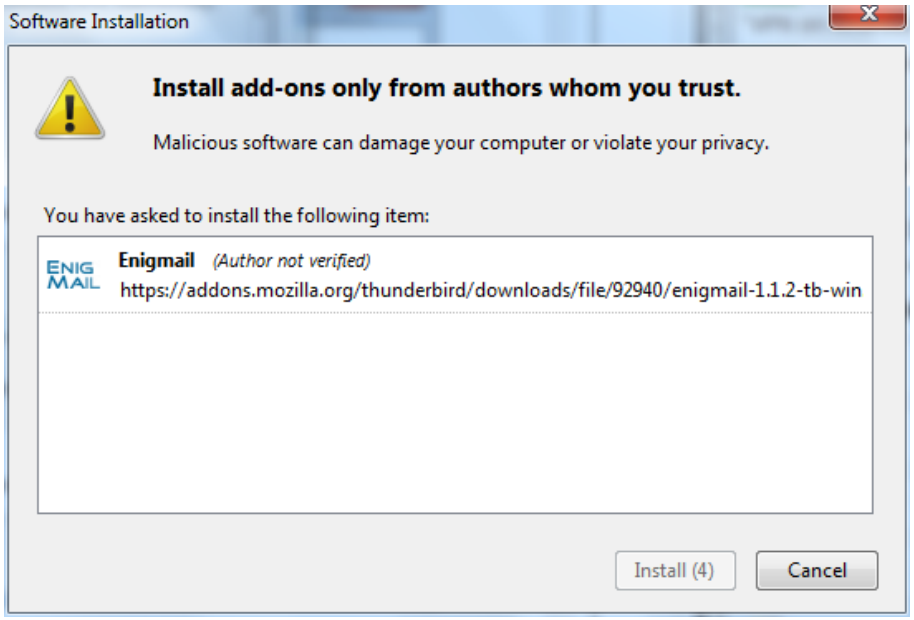


Installare Enigmail

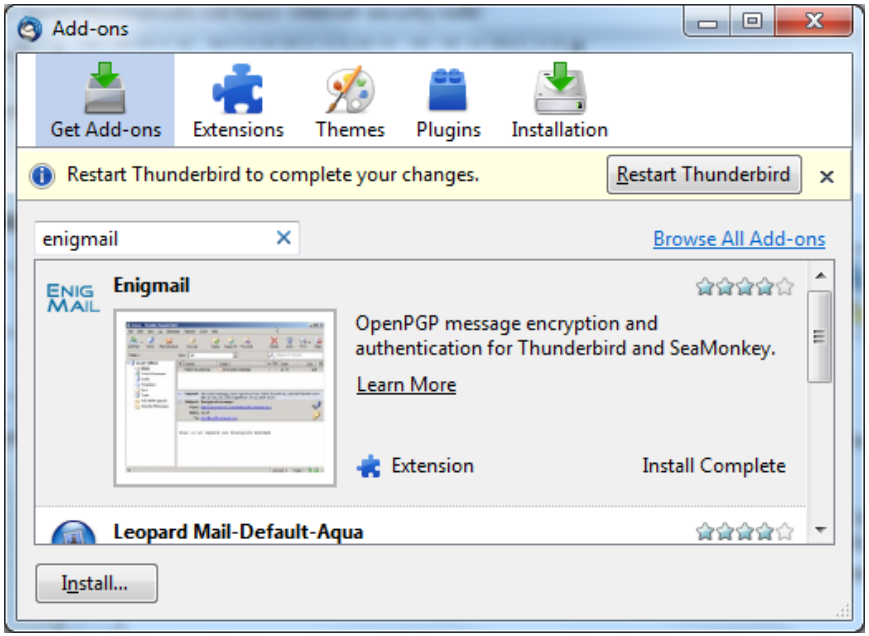
Enigmail



Installare Enigmail



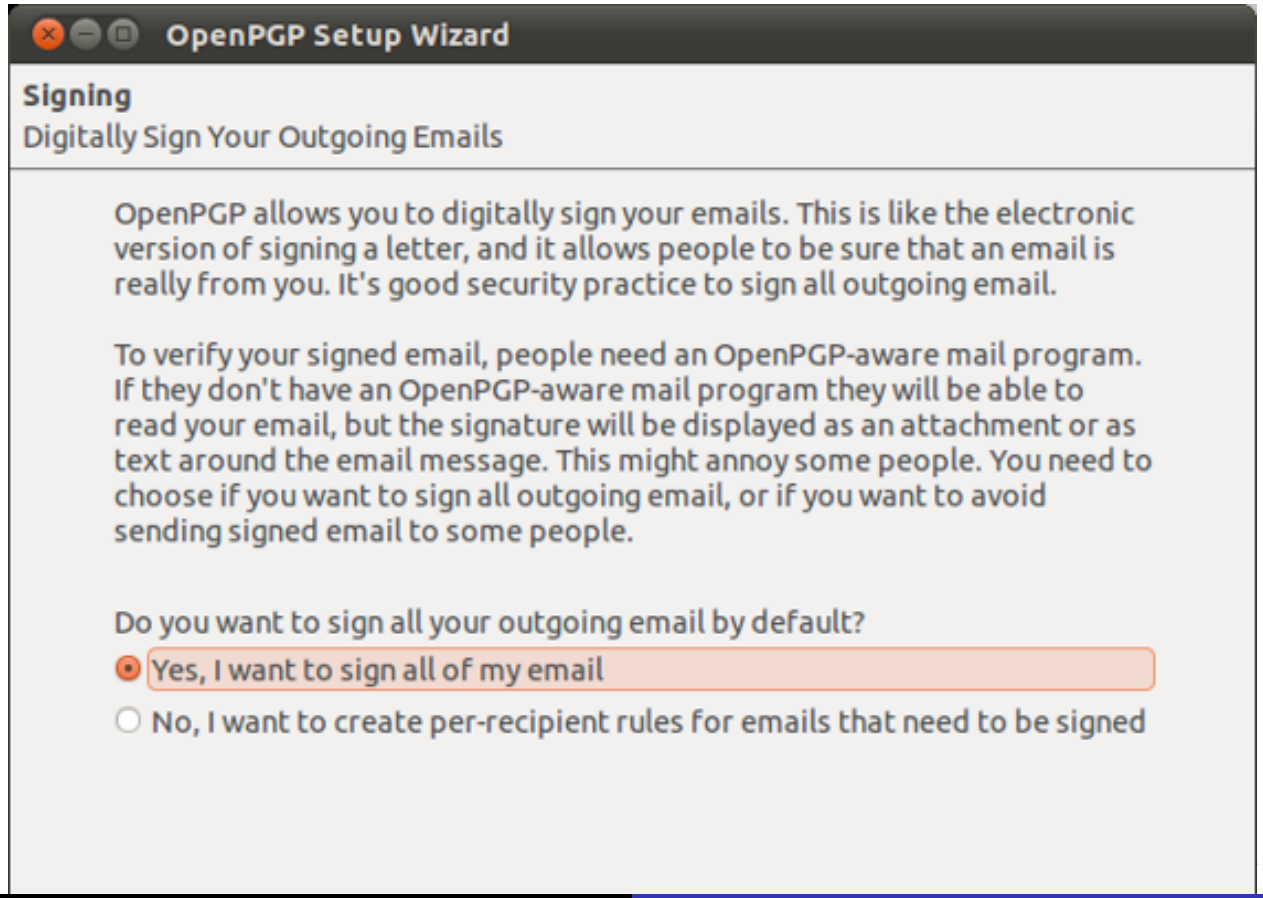
Installare Enigmail



Configurare Enigmail

Configurare Enigmail

Vuoi firmare tutte le email???



Configurare Enigmail

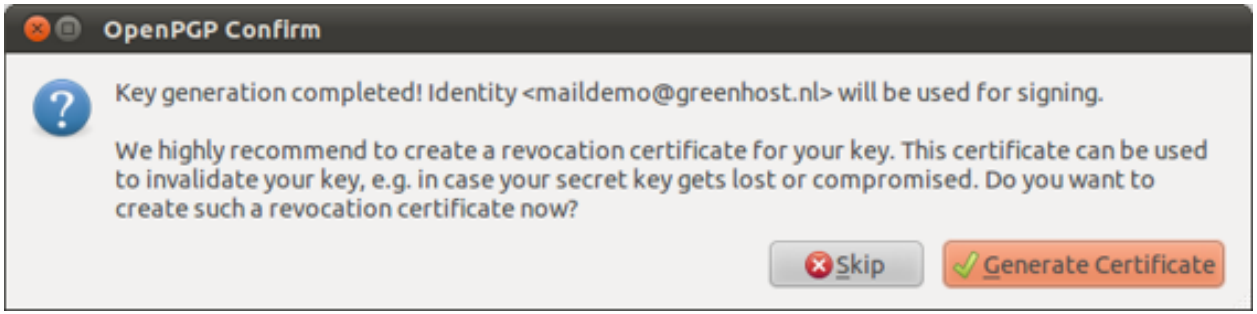
Vuoi cifrare tutte le email???

Configurare Enigmail

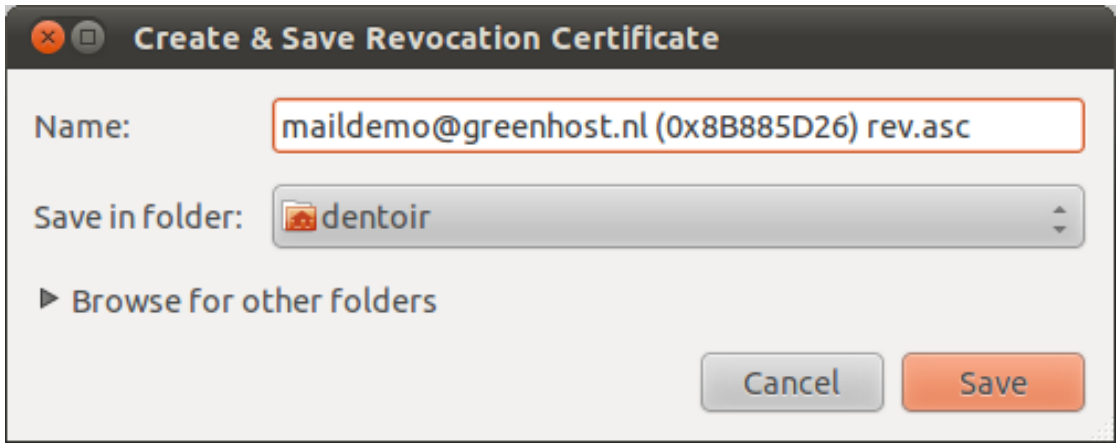
Configurare Enigmail

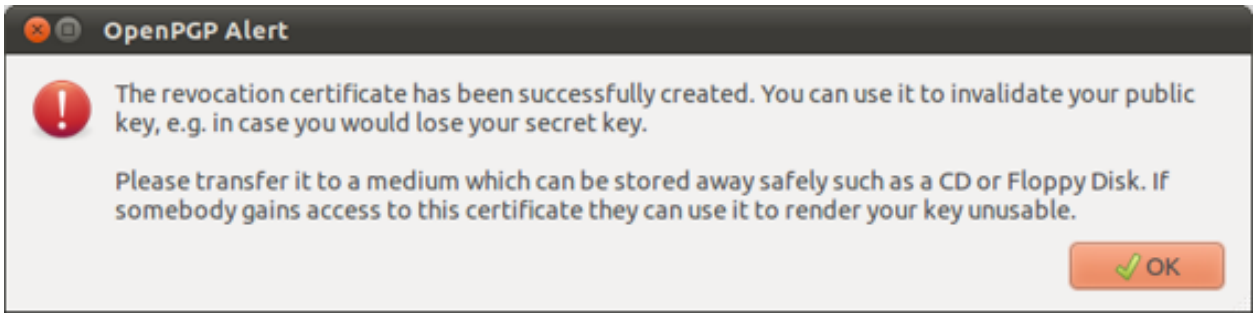
Configurare Enigmail

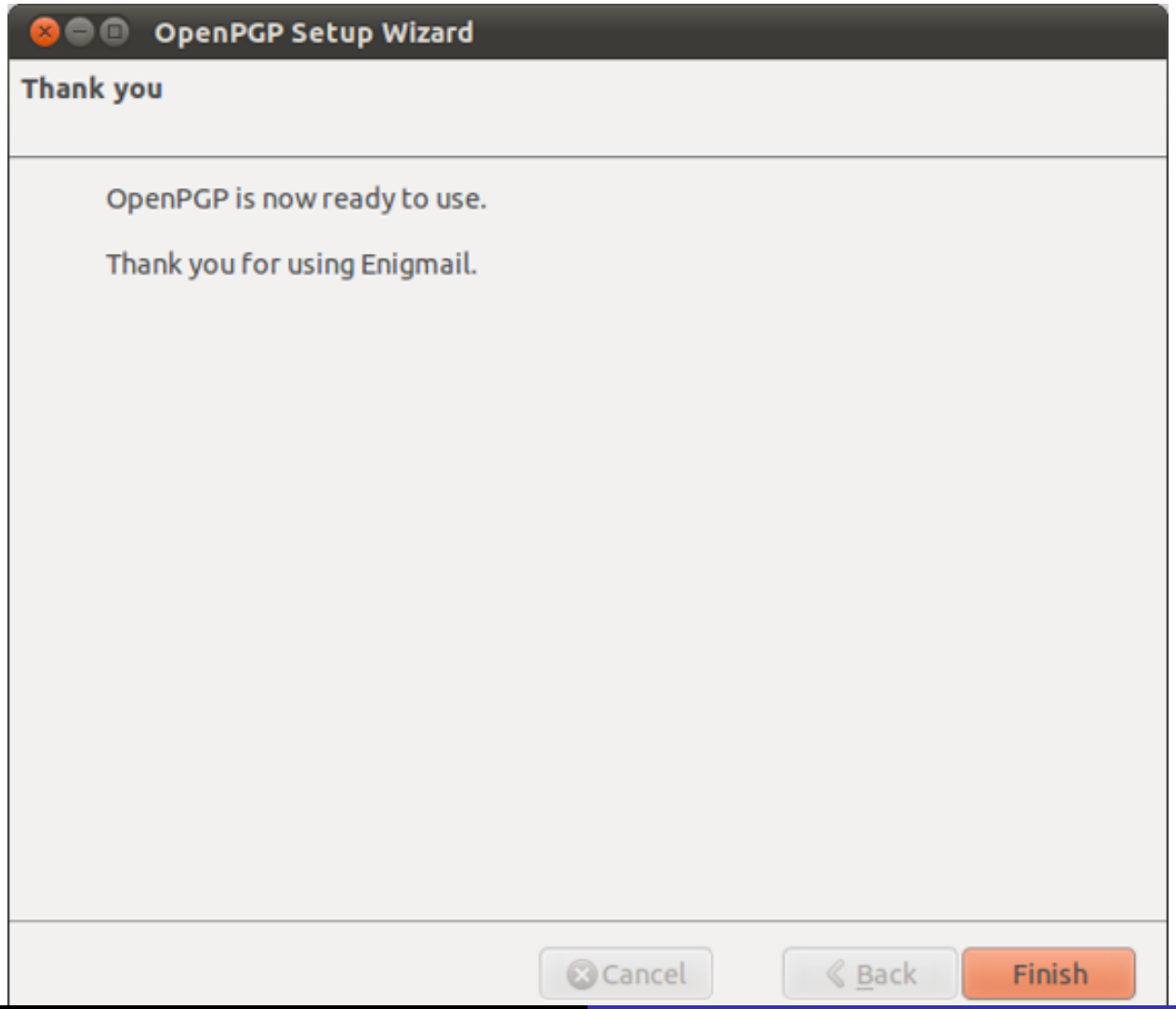
Configurare Enigmail



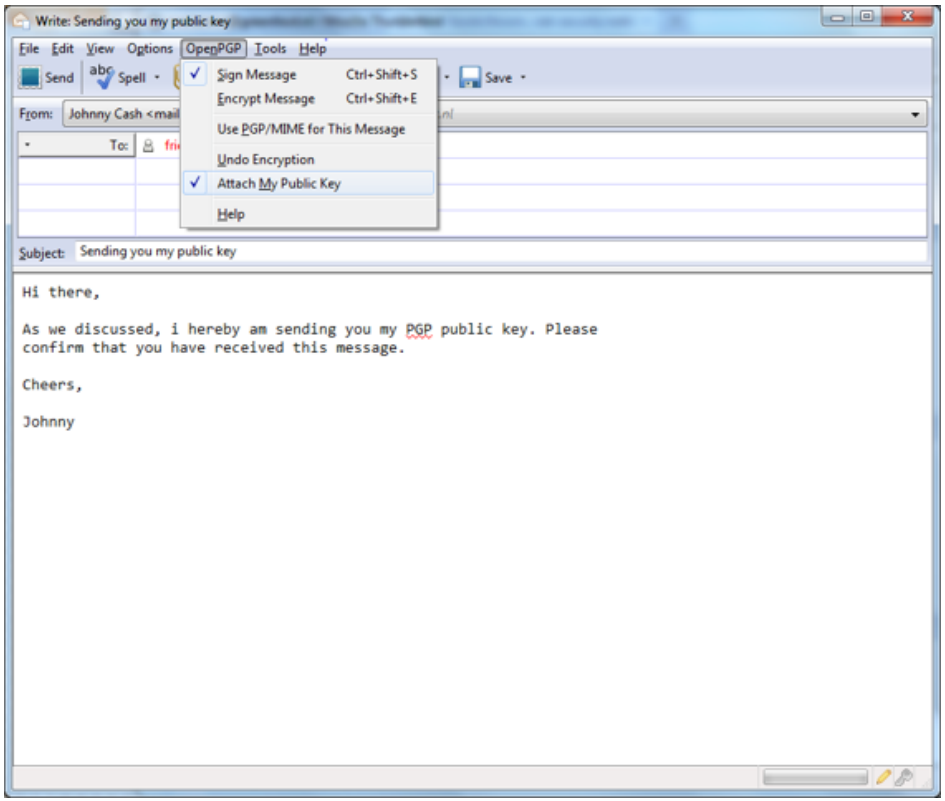
Configurare Enigmail



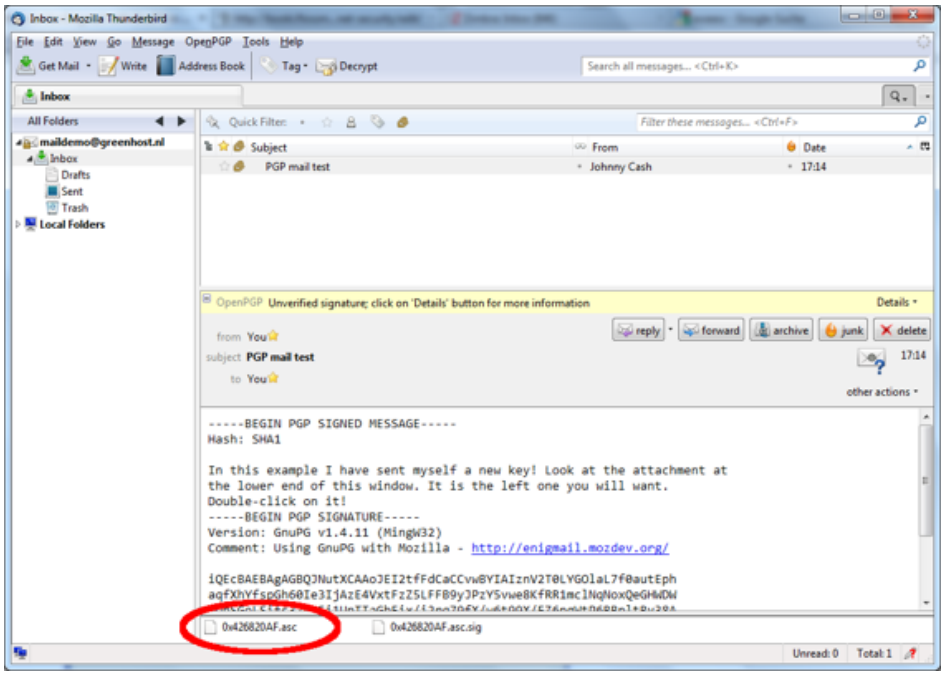

OpenPGP Alert
The revocation certificate has been successfully created. You can use it to invalidate your public key, e.g. in case you would lose your secret key.
Please transfer it to a medium which can be stored away safely such as a CD or Floppy Disk. If somebody gains access to this certificate they can use it to render your key unusable.
OK


OpenPGP Setup Wizard
Thank you
OpenPGP is now ready to use.
Thank you for using Enigmail.
Cancel
Back
Finish

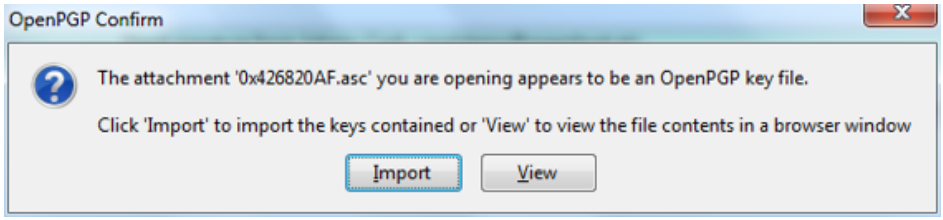
Spedire la chiave pubblica



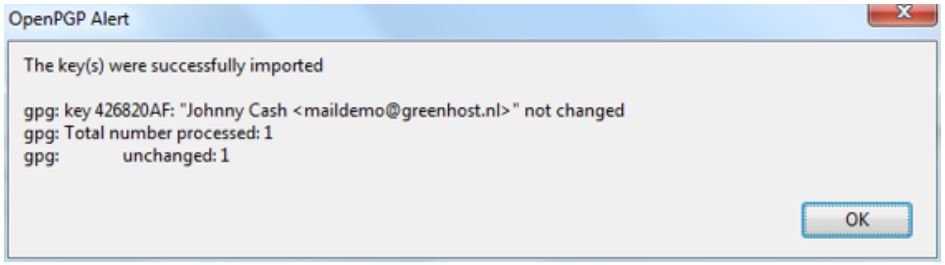
Ricevere e importare una chiave pubblica



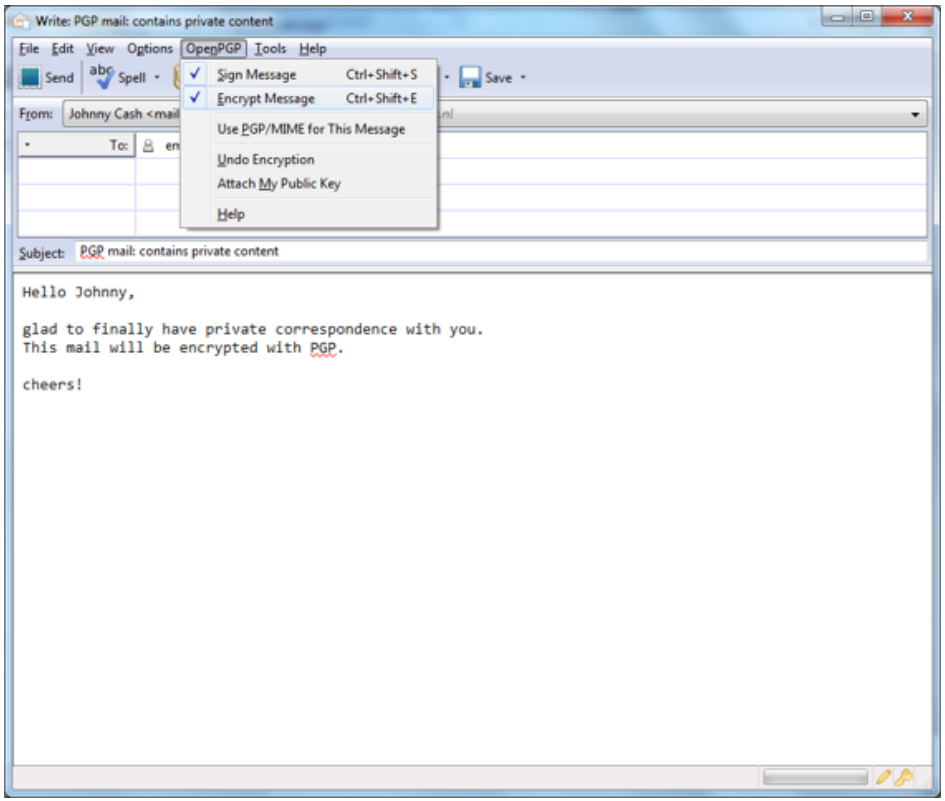
Ricevere e importare una chiave pubblica



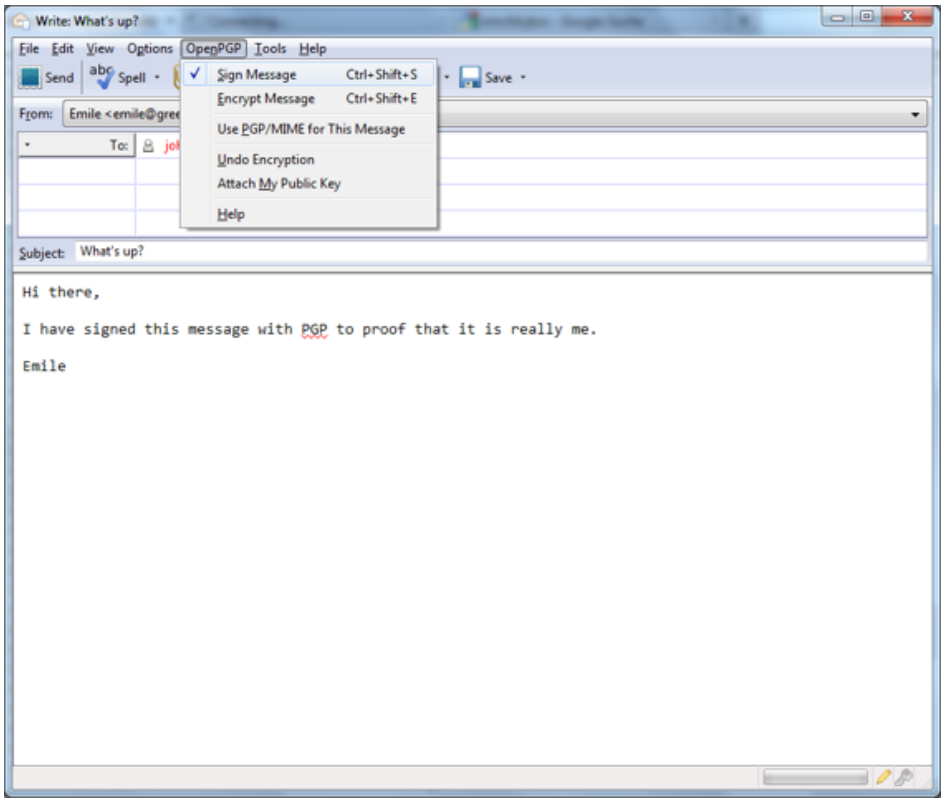
Ricevere e importare una chiave pubblica



Spedire un email cifrata



Spedire un email firmata



PIDGIN

Pidgin

- Client di messaggistica multiprotocollo - multiaccount (gmail, facebook, ICQ) - Multipiattaforma (va bene anche per winzozz)

OTR

OTR “off-the-record”

- Ci permette di avere delle conversazioni private
- Si basa sul paradigma della cifratura a chiave pubblica

OTR

OTR “off-the-record”

- Ci permette di avere delle conversazioni private
- Si basa sul paradigma della cifratura a chiave pubblica

PIDGIN-OTR

Pidgin + OTR

- Pidgin può essere facilmente esteso per utilizzare OTR
- OTR su tutti i protocolli supportati da pidgin
- Diffusione delle chiavi pubbliche “automatica”

PIDGIN-OTR

Pidgin + OTR

- Pidgin può essere facilmente esteso per utilizzare OTR
- OTR su tutti i protocolli supportati da pidgin
- Diffusione delle chiavi pubbliche “automatica”

PIDGIN-OTR

Pidgin + OTR

- Pidgin può essere facilmente esteso per utilizzare OTR
- OTR su tutti i protocolli supportati da pidgin
- Diffusione delle chiavi pubbliche “automatica”

PIDGIN-OTR

Pidgin + OTR

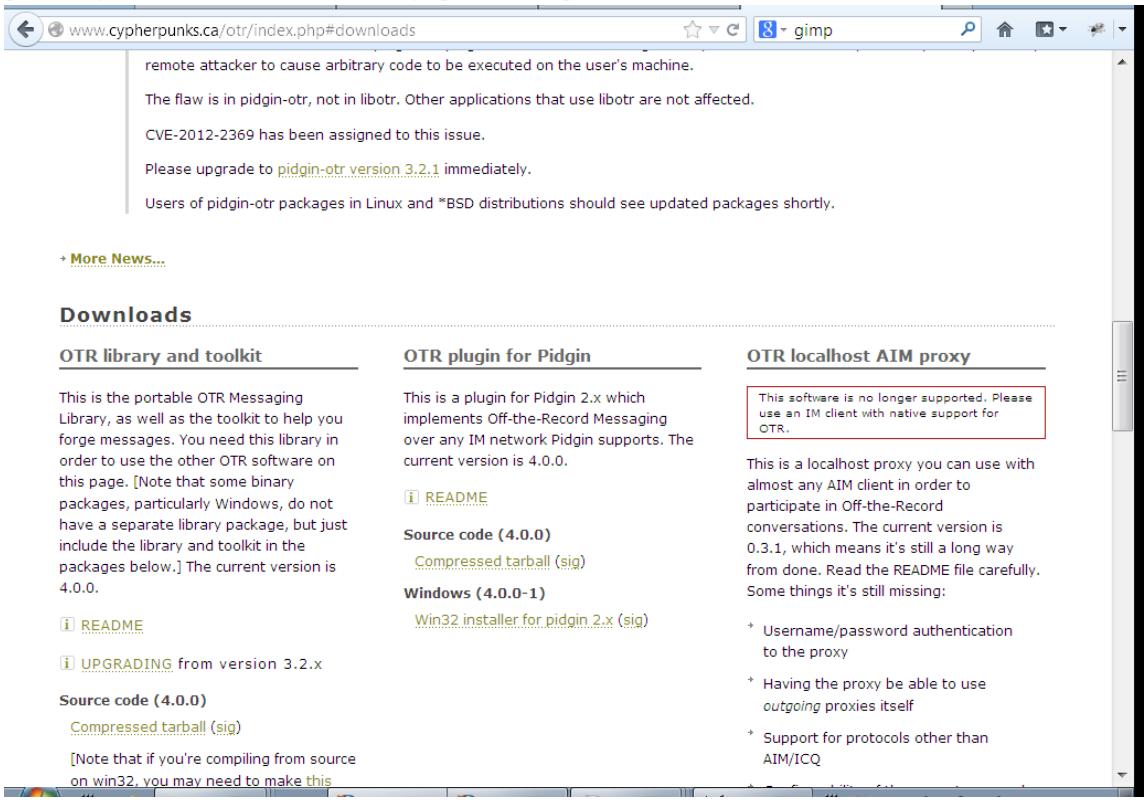
- Pidgin può essere facilmente esteso per utilizzare OTR
- OTR su tutti i protocolli supportati da pidgin
- Diffusione delle chiavi pubbliche “automatica”

Installazione/Configurazione

Winz:
pidgin: www.pidgin.im

Installazione/Configurazione

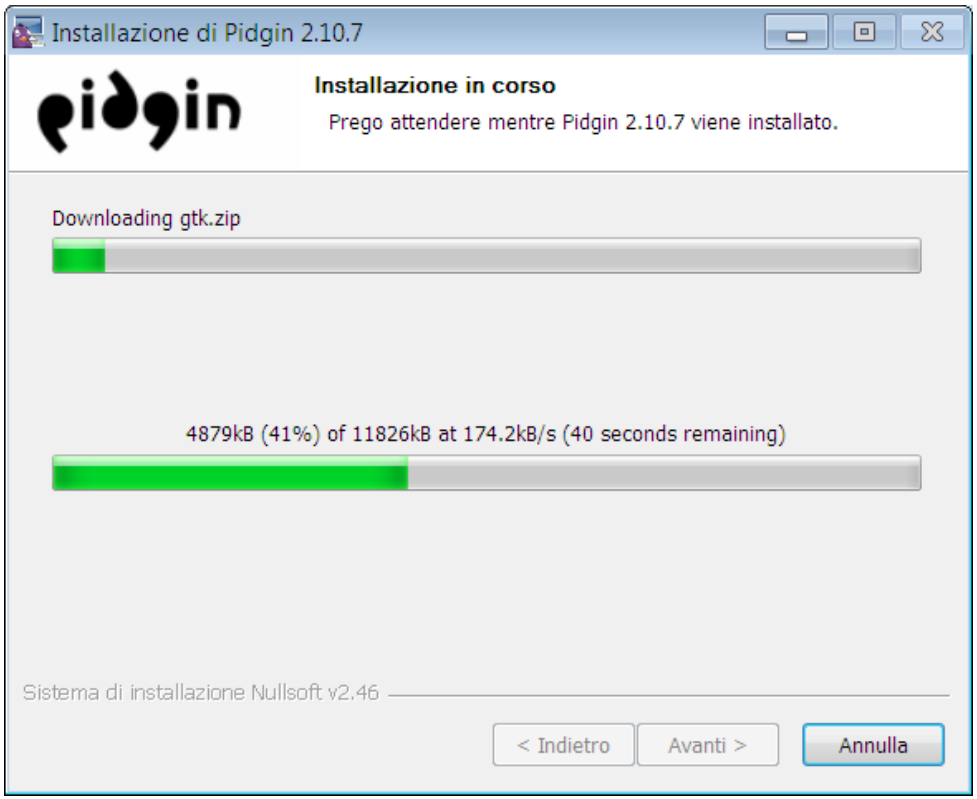
Winz:
pidgin-otr: otr.cypherpunks.ca -> win32_installer



Installazione/Configurazione

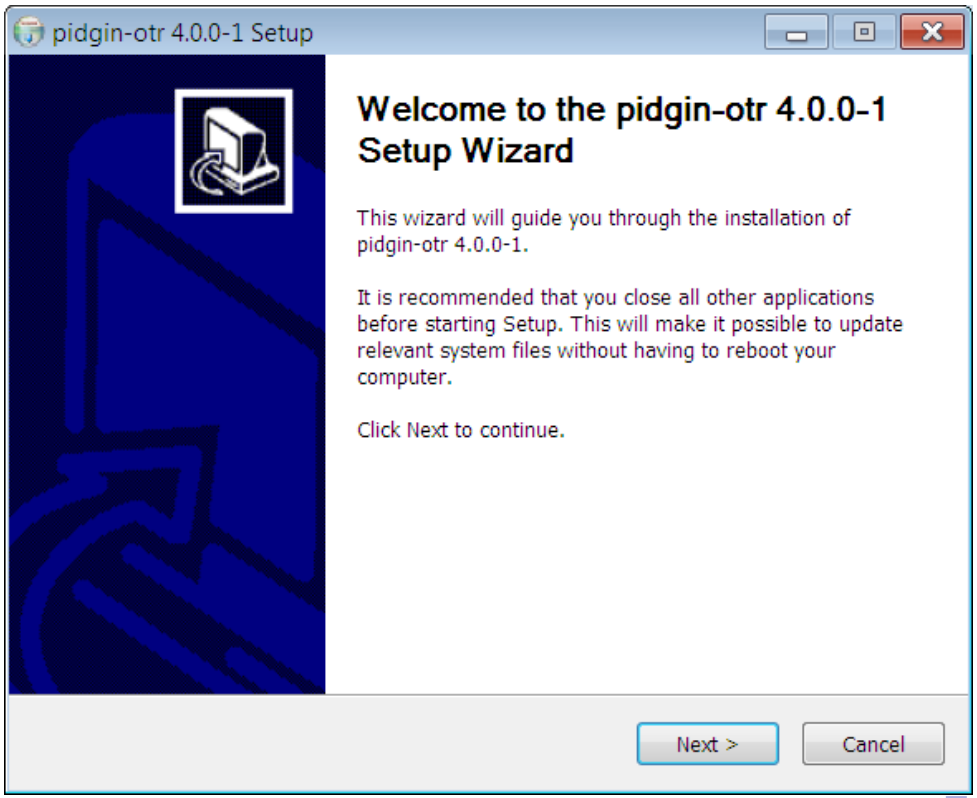
GNU/Linux:
ppp Utilizzare il gestore di pacchetti della propria distribuzione

Installazione/Configurazione



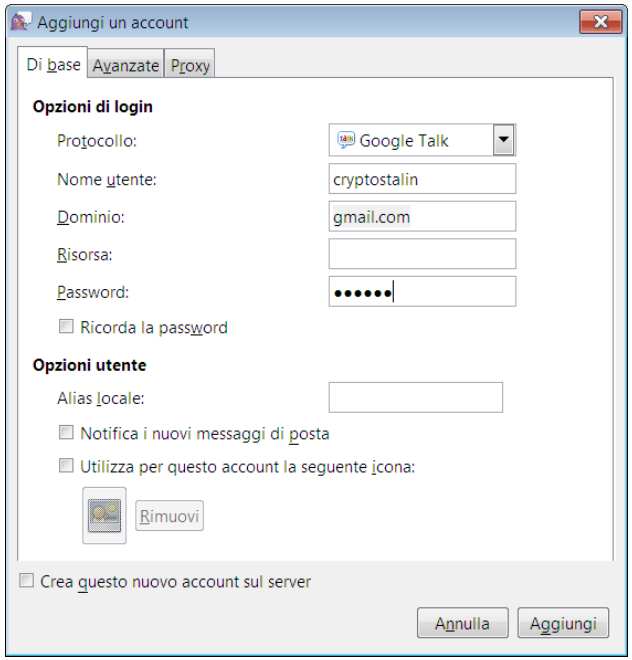
Installazione/Configurazione

Installare pidgin-otr



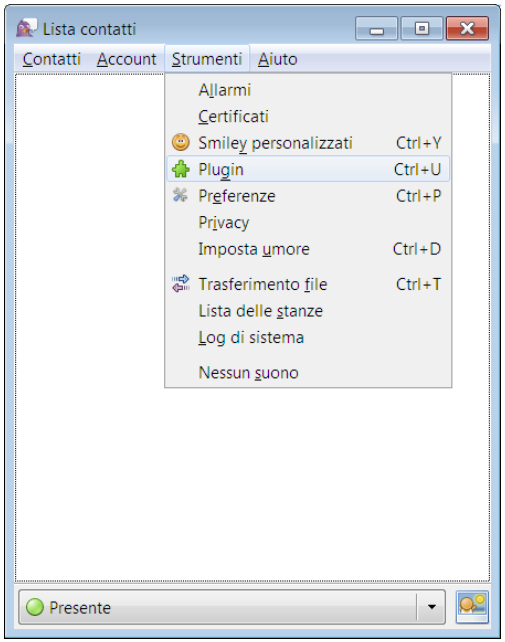
Installazione/Configurazione

Configurare un account su gmail

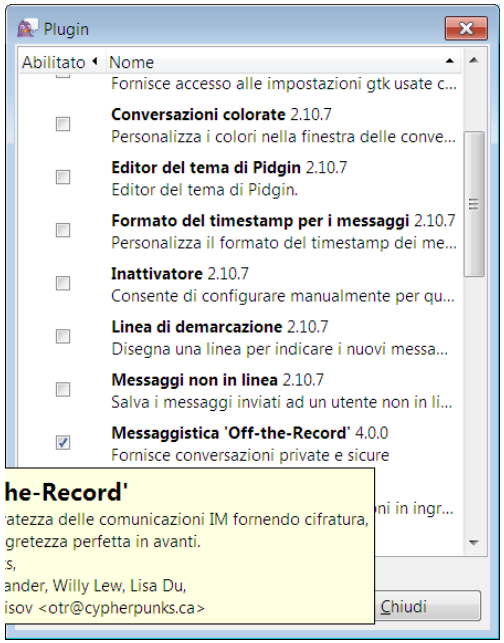


Installazione/Configurazione

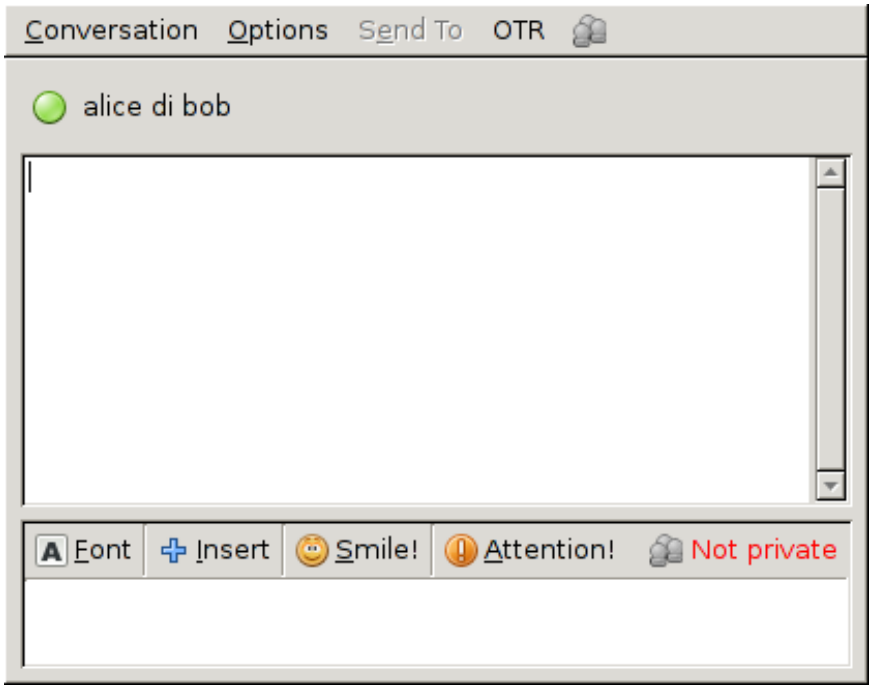
Abilitazione del plugin



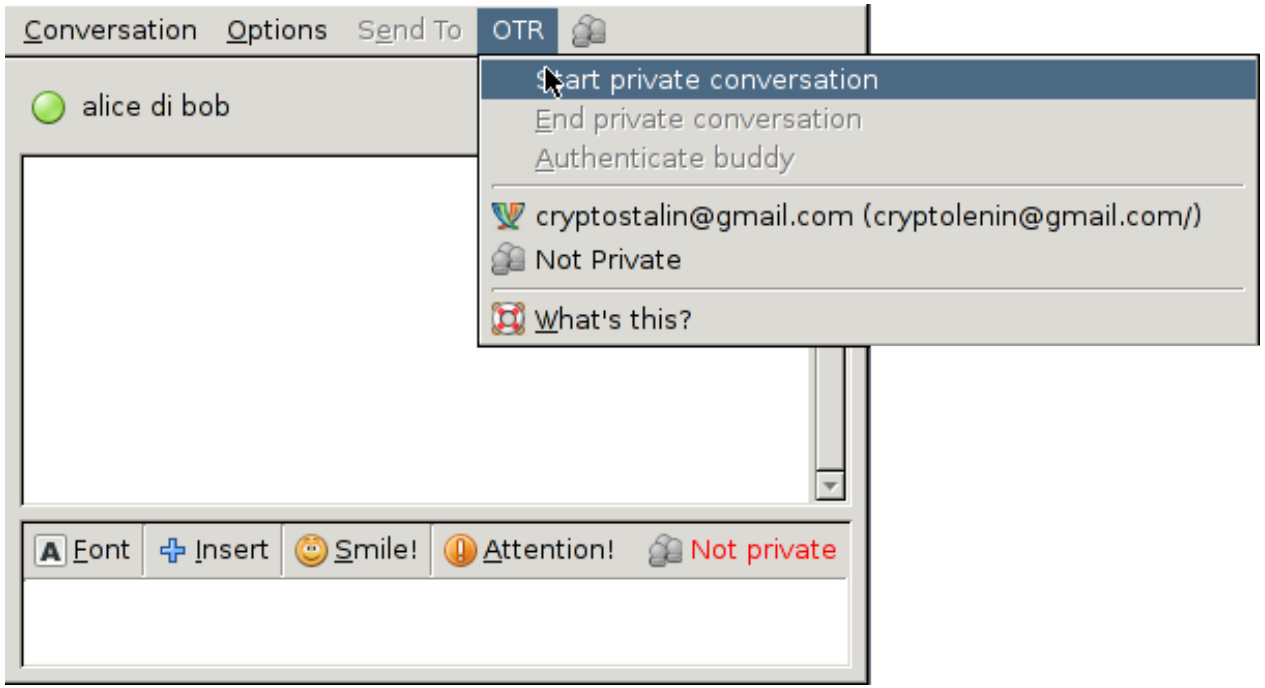
Installazione/Configurazione



Chat NON privata



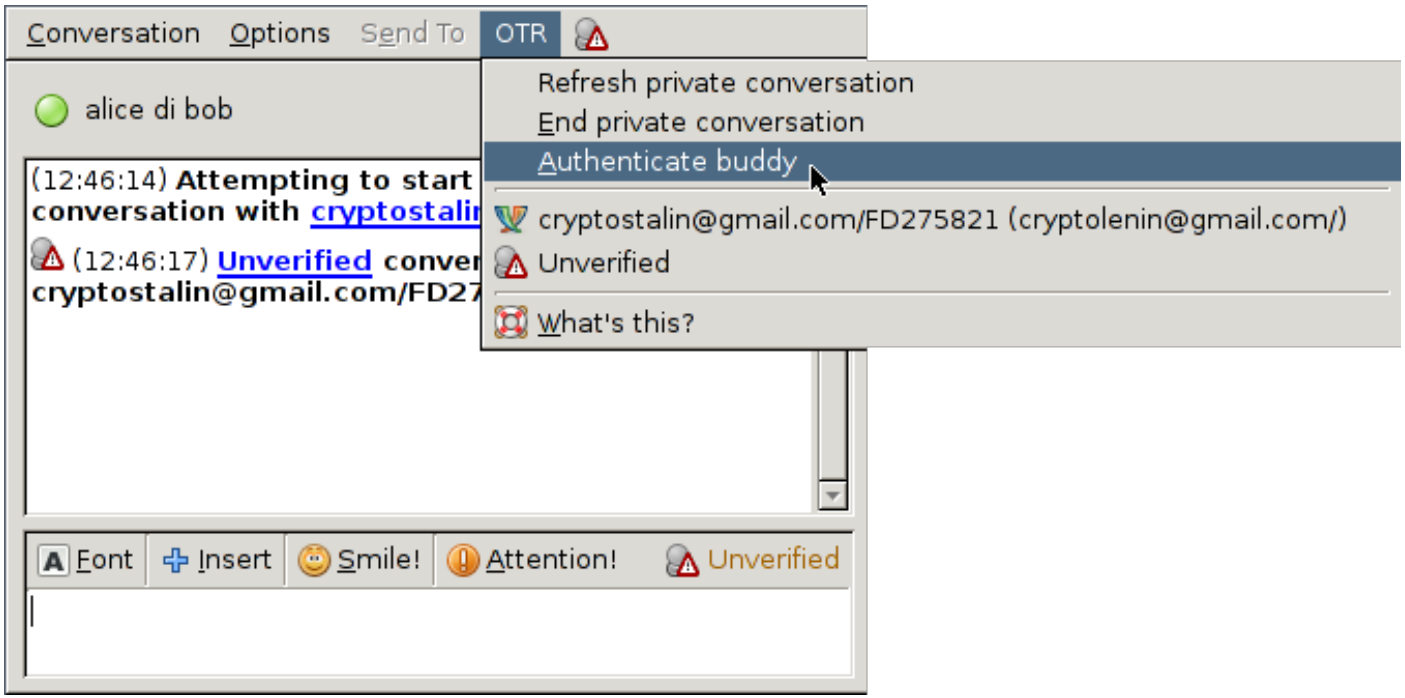
INIZIARE UNA CHAT PRIVATA



CHAT NON VERIFICATA

AUTENTICARE UN CONTATTO

La prima volta autenticate i vostri contatti!



AUTENTICAZIONE

Autenticazione con domanda segretissima

AUTENTICAZIONE

Autenticazione con password segretissima

AUTENTICAZIONE

Autenticazione con verifica manuale delle fingerprint (numeri unici per ogni chiave!)

CHAT PRIVATA

bla bla privato

Perche'???

- Tracciamento pubblicitario, profilazione
- Tutela della libertà di espressione
- Divulgazione sicura di informazioni che potrebbero metterci in pericolo
- Riservatezza
- Aggiramento della censura (es: PirateBay, Iran, China)

Perche'???

- Tracciamento pubblicitario, profilazione
- Tutela della libertà di espressione
- Divulgazione sicura di informazioni che potrebbero metterci in pericolo
- Riservatezza
- Aggiramento della censura (es: PirateBay, Iran, China)

Perche'???

- Tracciamento pubblicitario, profilazione
- Tutela della libertà di espressione
- Divulgazione sicura di informazioni che potrebbero metterci in pericolo
- Riservatezza
- Aggiramento della censura (es: PirateBay, Iran, China)

Perche'???

- Tracciamento pubblicitario, profilazione
- Tutela della libertà di espressione
- Divulgazione sicura di informazioni che potrebbero metterci in pericolo
- Riservatezza
- Aggiramento della censura (es: PirateBay, Iran, China)

Perche'???

- Tracciamento pubblicitario, profilazione
- Tutela della libertà di espressione
- Divulgazione sicura di informazioni che potrebbero metterci in pericolo
- Riservatezza
- Aggiramento della censura (es: PirateBay, Iran, China)

Browser

- Lascia un sacco di informazioni su chi siamo
- Se configurato male è molto ad-friendly
- Banchetti per configurazione più sicura e anonima di firefox

TOR

Tor:

- Invece di raggiungere direttamente un sito veniamo “rimbalzati” tra vari computer della rete TOR
- I computer che ci rimbalzano non possono sapere la nostra reale destinazione, nè la nostra reale provenienza

TOR

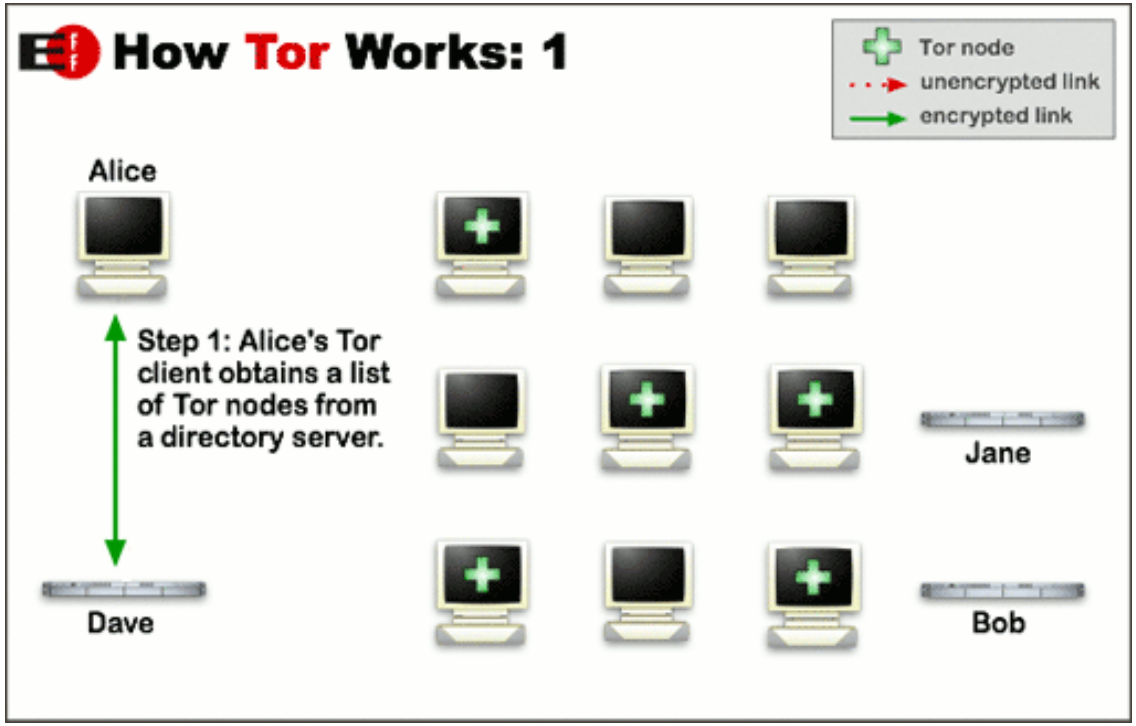
Tor:

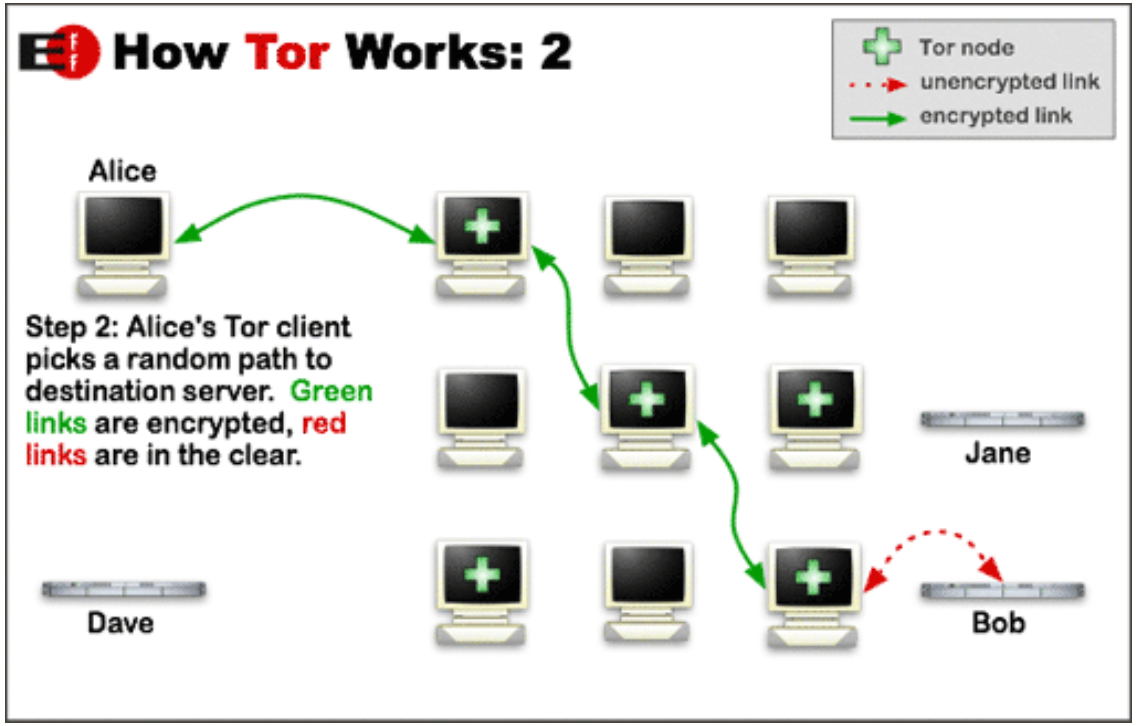
- Invece di raggiungere direttamente un sito veniamo “rimbalzati” tra vari computer della rete TOR
- I computer che ci rimbalzano non possono sapere la nostra reale destinazione, nè la nostra reale provenienza

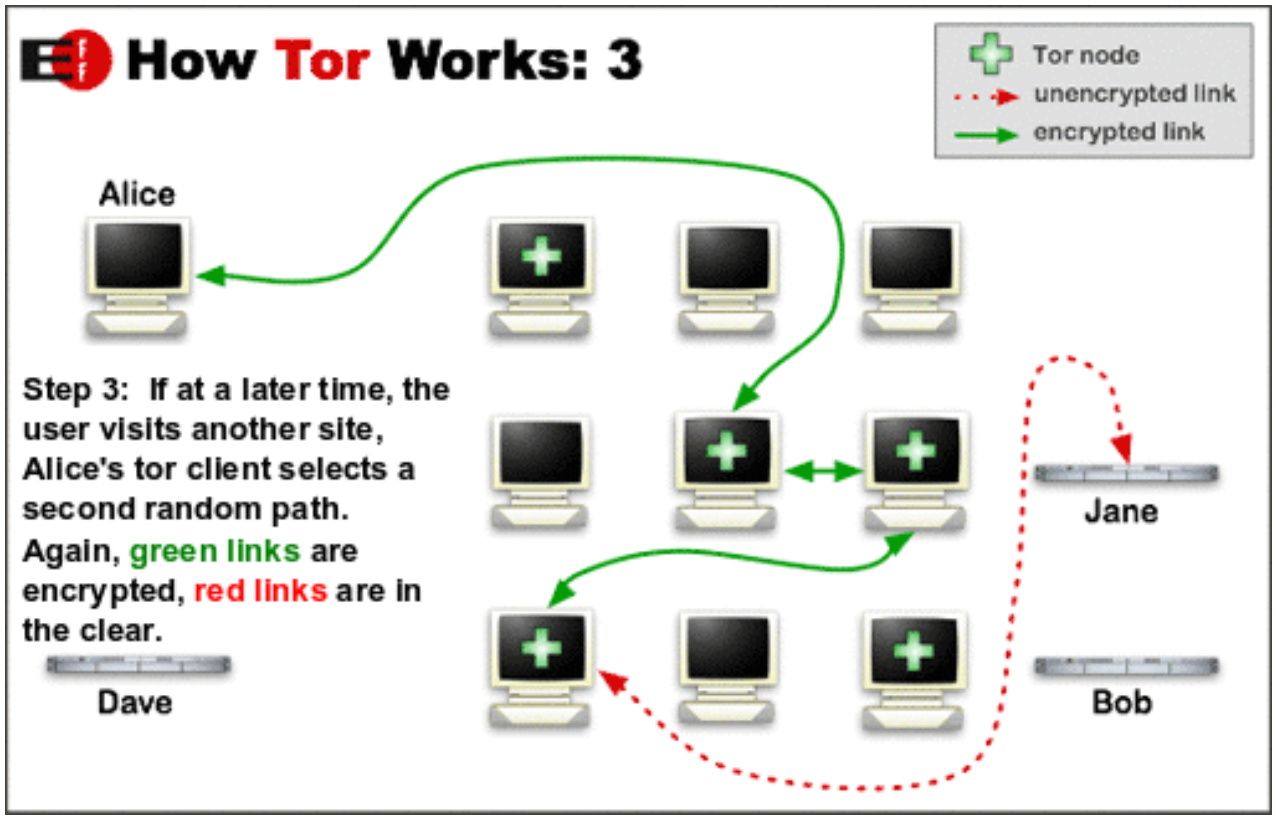
TOR

Tor:

- Invece di raggiungere direttamente un sito veniamo “rimbalzati” tra vari computer della rete TOR
- I computer che ci rimbalzano non possono sapere la nostra reale destinazione, nè la nostra reale provenienza


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob


How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Dave
Jane
Bob

Niente paura: Tor Bundle

Tor bundle

- realizzata per rendere più accessibile e sicuro l'utilizzo della rete TOR
- basata su firefox (Free software, multipiattaforma)

Niente paura: Tor Bundle

Tor bundle

- realizzata per rendere più accessibile e sicuro l'utilizzo della rete TOR
- basata su firefox (Free software, multipiattaforma)

Niente paura: Tor Bundle

Tor bundle

- realizzata per rendere più accessibile e sicuro l'utilizzo della rete TOR
- basata su firefox (Free software, multipiattaforma)

CIFRATURA FILE

Perche'???

- Furti
- Sequestri
- Manomissioni

CIFRATURA FILE

Metodi

- cifrare solo file sensibili
  - scomodo per molti file
  - non nasconde il nome, la dimensione, il numero di file, e altre informazioni
- contenitori cifrati
- cifratura totale del sistema (LUKS)

CIFRATURA FILE

Metodi

- cifrare solo file sensibili
  - scomodo per molti file
  - non nasconde il nome, la dimensione, il numero di file, e altre informazioni
- contenitori cifrati
- cifratura totale del sistema (LUKS)

CIFRATURA FILE

Metodi

- cifrare solo file sensibili
  - scomodo per molti file
  - non nasconde il nome, la dimensione, il numero di file, e altre informazioni
- contenitori cifrati
- cifratura totale del sistema (LUKS)

CIFRATURA FILE

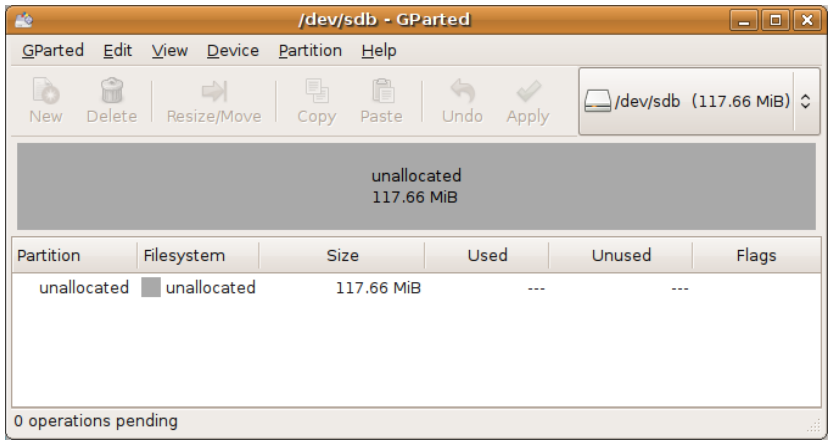
Metodi

- cifrare solo file sensibili
  - scomodo per molti file
  - non nasconde il nome, la dimensione, il numero di file, e altre informazioni
- contenitori cifrati
- cifratura totale del sistema (LUKS)

- Nella fase di installazione alcuni sistemi GNU Linux facilitano molto
- Luks + dm crypt (facile in fase di installazione)

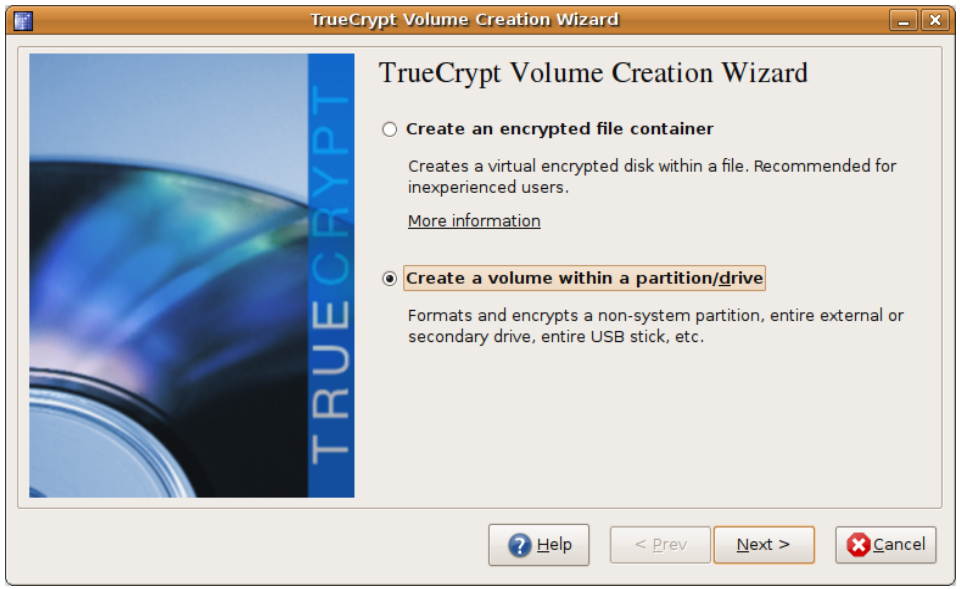
TRUECRYPT

Creiamo la partizione da cifrare nel nostro device (tipo una pennetta usb) con gparted



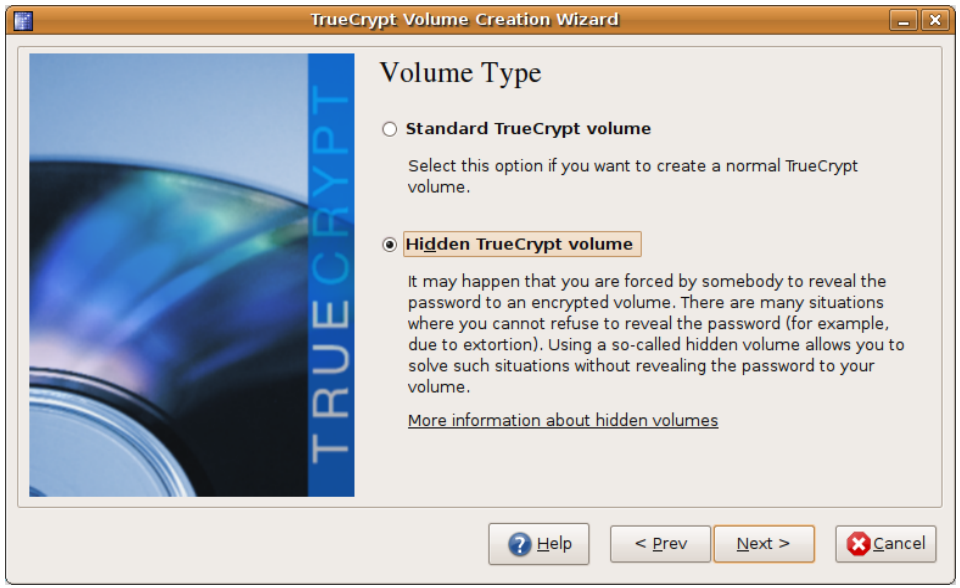
TRUECRYPT

Selezioniamo di creare una partizione cifrata



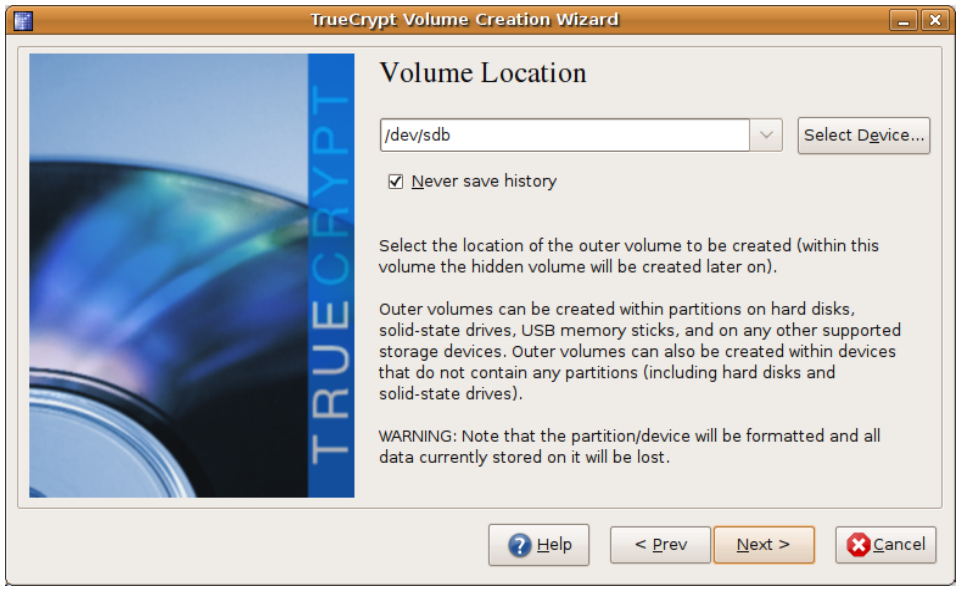
TRUECRYPT

Scegliamo di creare un volume nascosto



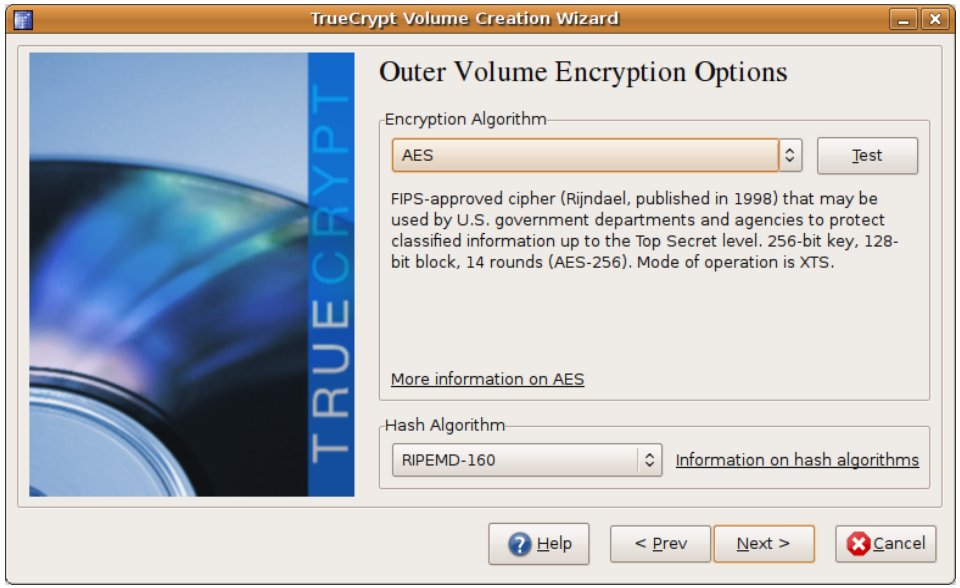
TRUECRYPT

Specifichiamo il device del nostro supporto (nel nostro caso la pennetta e' vista come /dev/sdb) ATTENZIONE: Assicuriamoci di non sbagliare il nome del device



TRUECRYPT

Scegliamo l'algoritmo con cui cifreremo il contenitore del nostro volume nascosto. AES va bene come scelta di default.

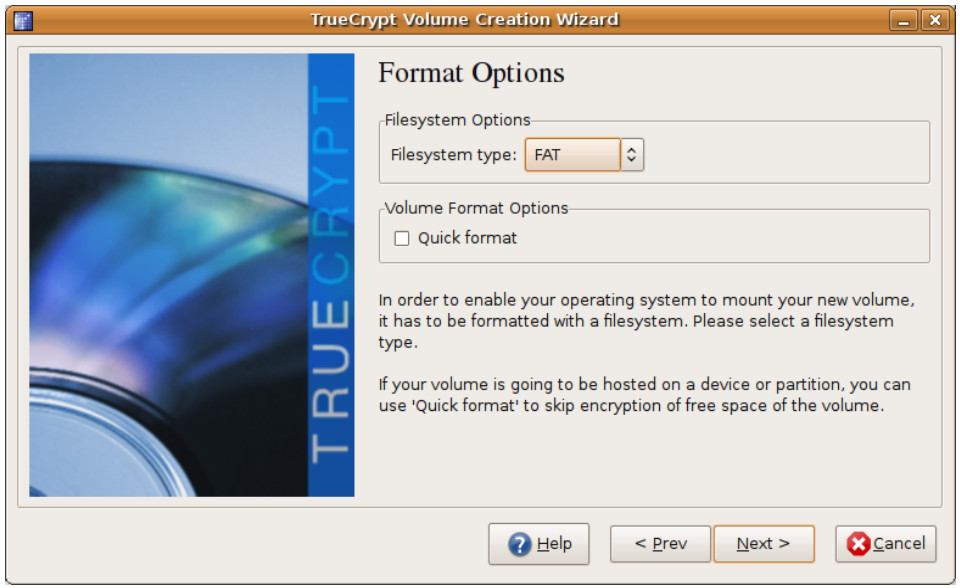


TRUECRYPT

Impostiamo una password per aprire il contenitore del volume nascosto.

TRUECRYPT

Scegliamo il filesystem per la nostra partizione

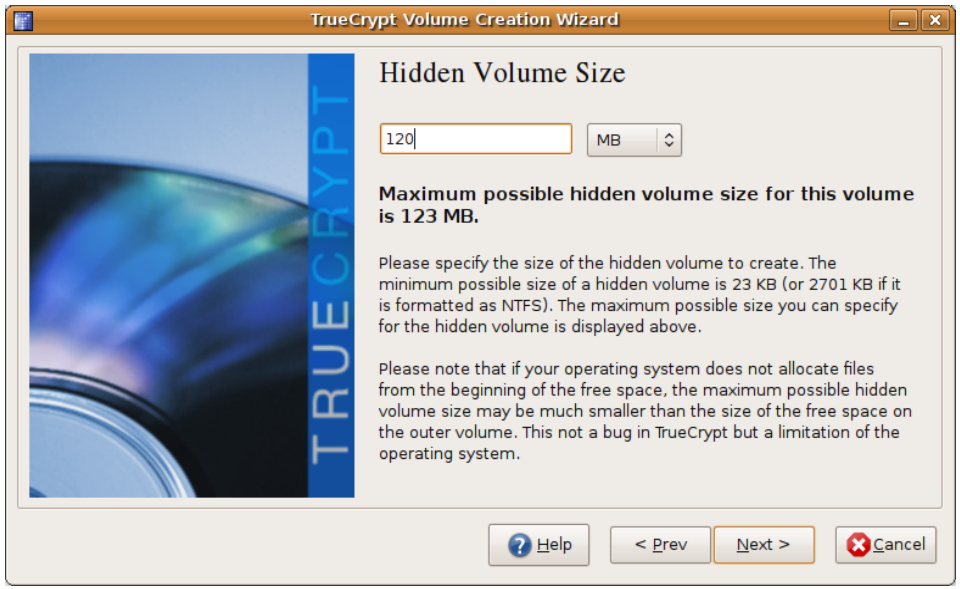


TRUECRYPT

Adesso copiamo dei files nel contenitore. ATTENZIONE: I files copiati qui non dovranno essere dati sensibili e non dovremo copiare nuovi files altrimenti rischiamo di sovrascrivere il contenitore nascosto sottostante.

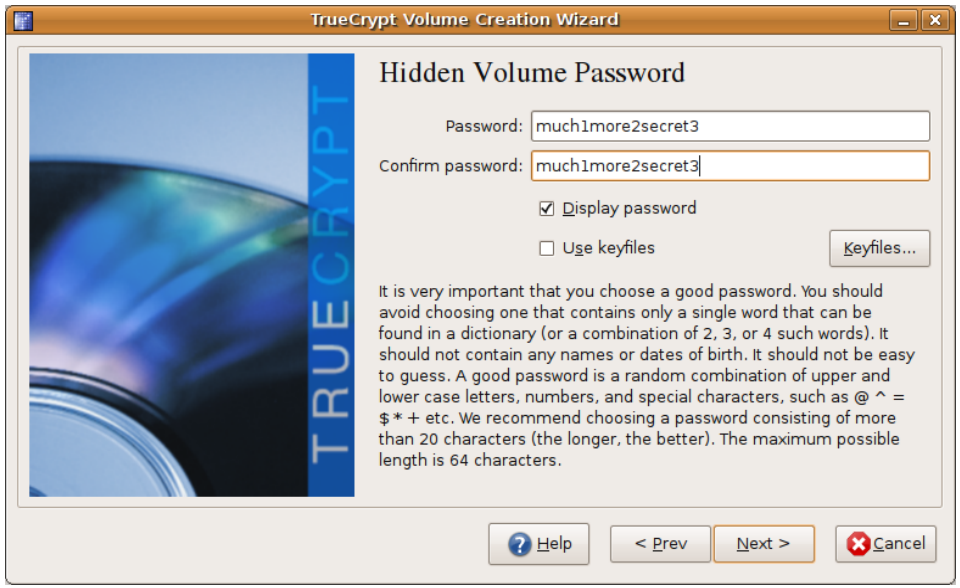
TRUECRYPT

Scegliamo la dimensione della partizione nascosta.
ATTENZIONE: la dimensione non potra' essere maggiore/uguale alla dimensione del contenitore.



TRUECRYPT

Scegliamo la password con la quale aprire la partizione nascosta: ATTENZIONE: la password dovra' essere ROBUSTA e DIVERSA dalla password del contenitore creato prima.



Sicurezza assoluta non esiste

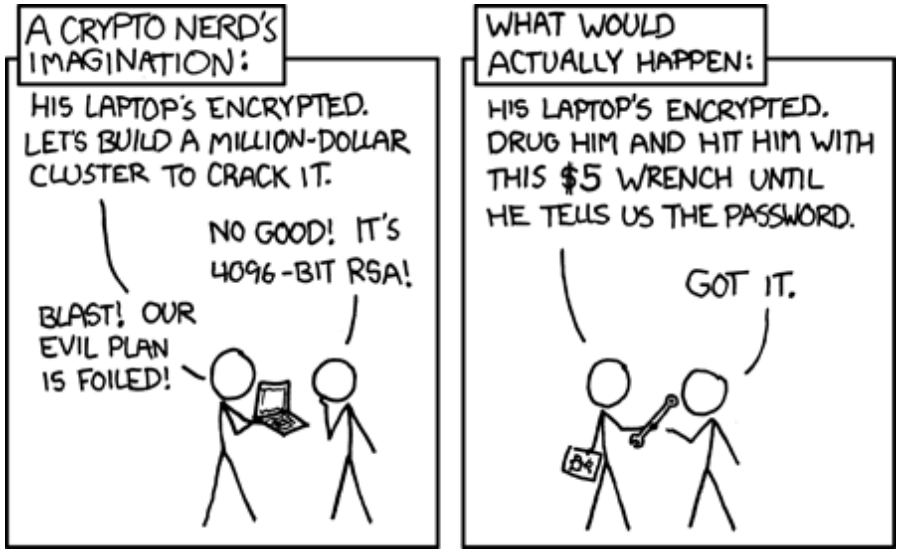
- Questi strumenti sono “sicuri” MA:
  - Il nostro computer è un’insime di molti software, e tutti questi potrebbero essere utilizzati per aggirare la sicurezza
  - I programmi sono scritti da esseri umani, errori nel software sono utilizzati per aggirare la sicurezza

Sicurezza assoluta non esiste

- Questi strumenti sono “sicuri” MA:
  - Il nostro computer è un’insime di molti software, e tutti questi potrebbero essere utilizzati per aggirare la sicurezza
  - I programmi sono scritti da esseri umani, errori nel software sono utilizzati per aggirare la sicurezza

Sicurezza assoluta non esiste

- Questi strumenti sono “sicuri” MA:
  - Il nostro computer è un’insime di molti software, e tutti questi potrebbero essere utilizzati per aggirare la sicurezza
  - I programmi sono scritti da esseri umani, errori nel software sono utilizzati per aggirare la sicurezza


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Allora che si fa??

- Importanza dell'utilizzo di software libero
- codice aperto == controllato dalla comunità