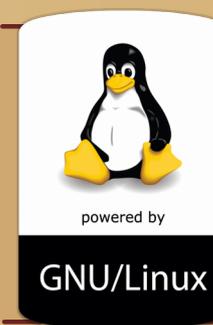


La Sicurezza

(Vista dal “pinguino” e non solo)



Seconda parte.

*“Percorso tra i vari aspetti della Sicurezza
(principalmente in GNU/Linux)”*



**ATTENZIONE
PINGUINO DA GUARDIA**



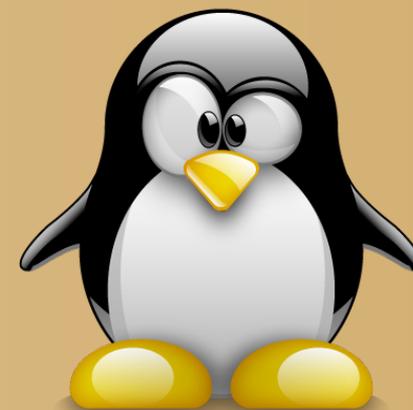
WARNING

Presentazione su
Sicurezza, Privacy,
Crittografia dei dati e
relativi strumenti nel
Mondo Opensource
by Gabriele Zappi

Martedì 16 e 30 Gennaio 2018 Ore 21
Laboratorio RiminiLUG
V.le Mantova, 6 Riccione

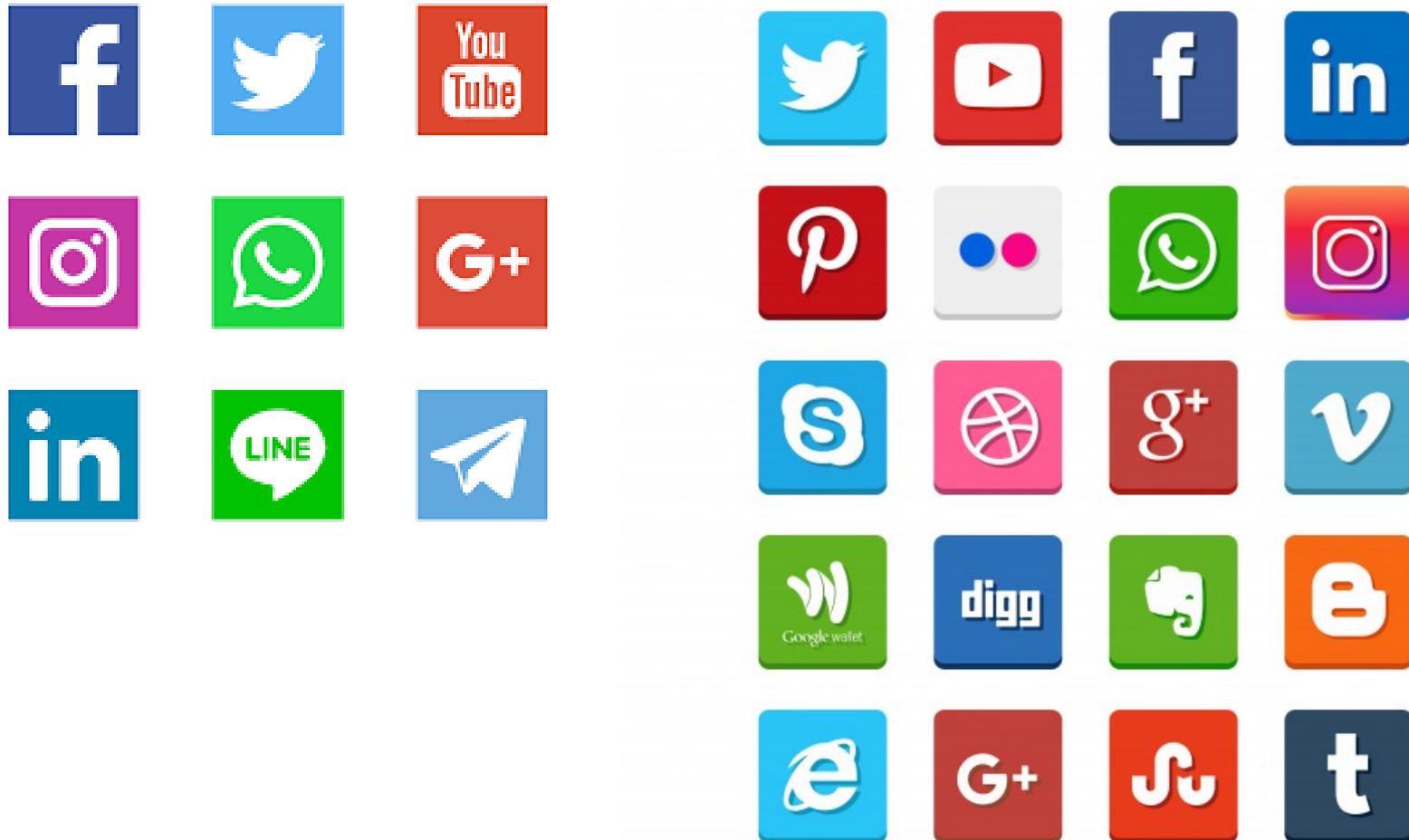
info su:
www.riminilug.it

associazione culturale per la promozione del software libero
RiminiLUG



Uso di Social

Limitare visibilità e-mail e dati sensibili



facebook



✎ Crea un post | 📁 Album con foto o video | 📺 Video in diretta



Stasera al #Riminilug, la 2a serata!!!

Foto/video | Registrati | Stato d'animo/attività | Tagga amici | GIF | Adesivo

Amici | Pubblica

Chi può vedere questo contenuto?

- Tutti**
Chiunque su Facebook e fuori Facebook
- Amici**
I tuoi amici su Facebook
- Amici tranne...**
Non mostrare ad alcuni amici
- Altro...

13 h

Gabriele Zappi "Gabolander" ▶ [Le mie cerchie](#)

Stamattina ho voglia di scherzare! #celhoconlinter !!



ANNULLA | PUBLICA POST

ATTENZIONE AL ...



Scelta delle password

La scelta delle password è molto importante.

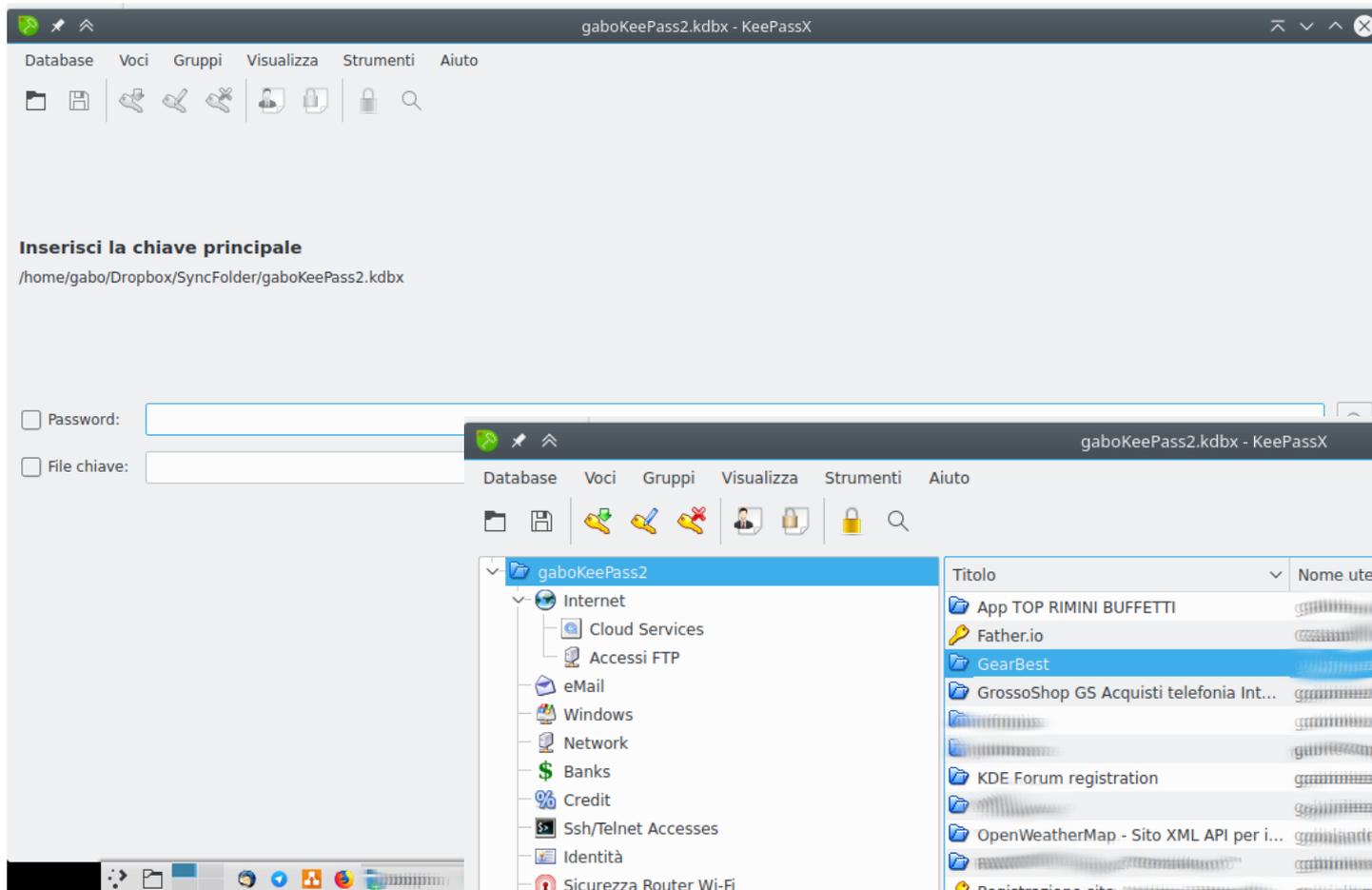
Occorre scegliere delle password che:

- 1) Non siano parole semplici o facilmente riconducibili alla propria persona (data di nascita, cognome, soprannome, ecc.)
- 2) Occorre evitare parole (anche composte) che si possono trovare nel dizionario, specie della propria lingua madre e del dizionario inglese (preferibilmente comprese nei dizionari di qualsiasi lingua)
- 3) Occorrerebbe evitare parole (anche composte) riconducibili a persone o cose che sono risapute far parte della vostra vita (e quindi potenzialmente violabili dagli algoritmi di “brute force”)
- 4) Mai utilizzare la stessa password per diversi servizi web!

Insomma, la password dovrebbe essere abbastanza complessa, ma che sia stata pensata con un meccanismo con cui sia facile per voi memorizzarla ... **MA QUANDO NON BASTA ...**

Il problema delle password.

Suggerimento: Usare un “password-safe” sicuro, pratico e versatile



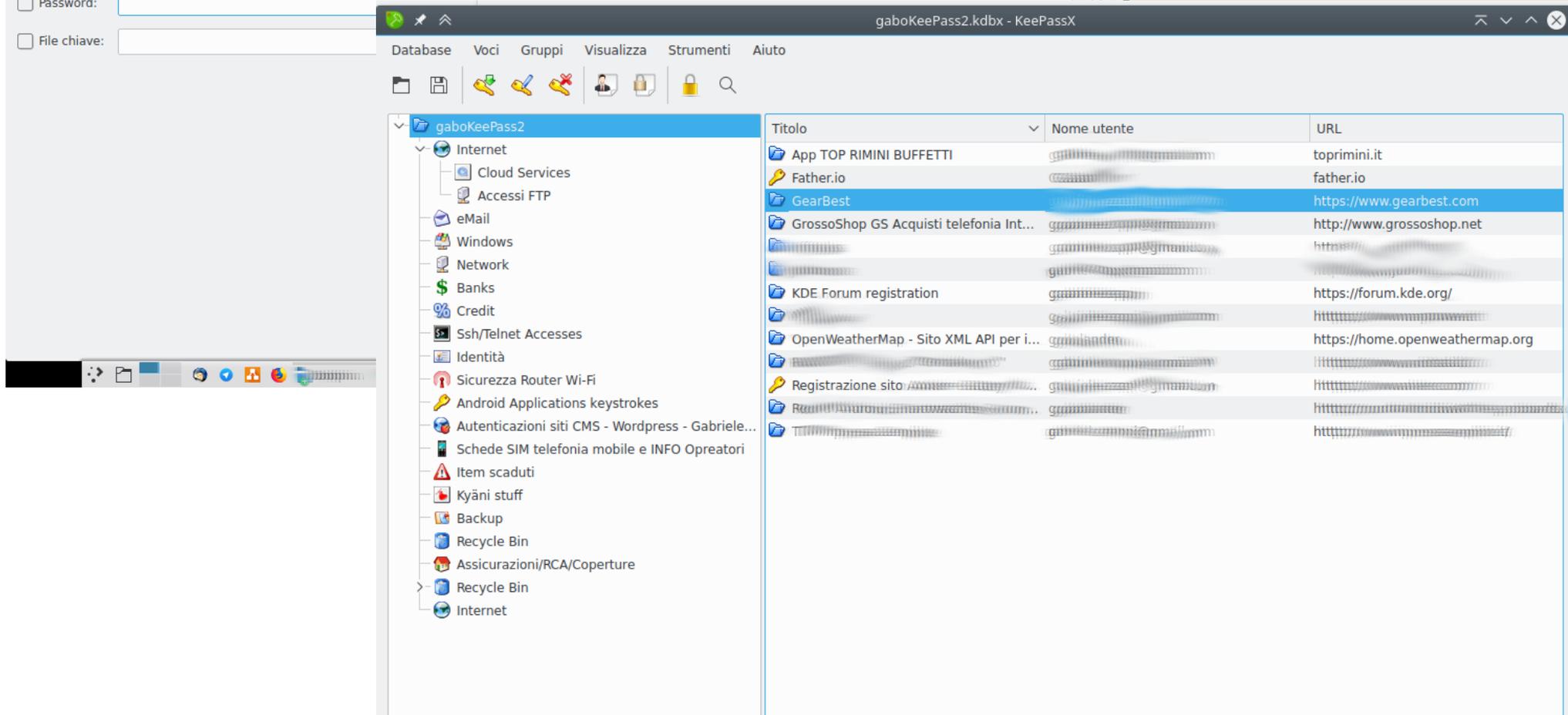
Keepass

Linux: KeePassX

Windows: KeePass2

Android: KeePassDroid

Etc ..



- gaboKeePass2
 - Internet
 - Cloud Services
 - Accessi FTP
 - eMail
 - Windows
 - Network
 - Banks
 - Credit
 - Ssh/Telnet
 - Identificatori
 - Sicurezza
 - Android
 - Autenticazione
 - Schedari
 - Item s
 - Kyāni
 - Backu
 - Recycl
 - Assicu
 - Recycl
 - Intern

Trova: fake

Gruppo corrente (Internet) Gruppo radice

| Gruppo | Titolo | Nome utente |
|----------|--|-------------|
| Internet | Account | |
| Internet | Sito Farlocco - Voce Fake dimostrativa | jonsnow |

gaboKeePass2.kdbx* - KeePassX

Database Voci Gruppi Visualizza Strumenti Aiuto

Internet > Sito Farlocco - Voce Fake dimostrativa > Modificare voce

Voce

- Avanzate
- Icona
- Auto-Type
- Proprietà
- Cronologia

Titolo: Sito Farlocco - Voce Fake dimostrativa

Nome utente: jonsnow

Password: ●●●●●●●●●●

Ripeti: ●●●●●●●●●●

URL: www.kinginthenorth.com

Scade: 22/01/18 15:58 ▼ Preimpostazioni ▼

Note: record dimostrativo

KeePassDroid

INFO IMPOSTAZIONI

Nome file del database di KeePass:
content://com.android.externalstorage...

Usa come database predefinito

Inserisci una password e/o file chiave per sbloccare il database:

Password



Listening for fingerprints

File chiave (opzionale)



OK

Mostra Password

KeePassDroid



gaboKeePass2



Android Applications keystrokes Gruppo

Assicurazioni/RCA/Coperture Gruppo

Autenticazioni siti CMS - Wordpress
Gabrielezappi.net - etc

Backup Gruppo

Banks Gruppo

Credit Gruppo

eMail Gruppo

Identità Gruppo

Internet Gruppo

Internet Gruppo

Item scaduti Gruppo

AGGIUNGI GRUPPO

AGGIUNGI VOCE

E-mail

Usare cautela con le e-mail di dubbia provenienza.

La posta elettronica, è lo strumento più utilizzato negli ultimi 10 anni come adescamento di persone su Internet, specie con il meccanismo del Phishing, al fine di trafugare informazioni e dati personali e/o sensibili.

Negli ultimi anni, è inoltre aumentata in maniera esponenziale la distribuzione via mail di virus e malware anche molto dannosi (come gli ultimi ransomware, cryptolocker, etc.), spesso senza allegare codice malevolo all'interno delle mail stesse, ma inserendo dei link a procedure appoggiate a server esterni, opportunamente formattati (in modo incomprensibile per buona parte degli utenti) per fare eseguire dagli stessi browser degli utenti, del codice arbitrario, al fine di danneggiarlo o di sottrargli informazioni sensibili.

29% Usato da 400,0 MB

gabriele.zappi@ Posta arrivata (599/302)

Muovi i messaggi selezionati nella cartella... Marca messaggi...

| Da | Oggetto | Data | Dimensione |
|-----------------------|---|------------------|------------|
| Apple | Il tuo ID Apple e stato utilizzato per... | 23-11-2017 14:52 | 12,1 KB |
| Gabriele Zappi | Re: estensione memoria posta elettronica... | 23-11-2017 14:45 | 7,6 KB |
| Gestione Abilitazioni | Fw: estensione memoria posta elettronica... | 23-11-2017 13:33 | 3,4 KB |
| xymon-rimini-no | Xymon [424245]... | 23-11-2017 12:49 | 1,4 KB |
| xymon-rimini-no | Xymon [103426]... | 23-11-2017 12:49 | 1,4 KB |

Il tuo ID Apple e stato utilizzato per accedere a iCloud da un browser web.

Data e ora: 23 novembre 2017, 12:32 PDT

Indirizzo IP , Luogo: 61.155.164.106, China - Shanghai

Se recentemente hai eseguito l'accesso a iCloud, puoi ignorare questa email.

Se recentemente non hai eseguito l'accesso a iCloud e ritieni che qualcun altro possa aver eseguito l'accesso al tuo account, clicca sul link seguente per riavviare il tuo ID Apple.

Cordiali saluti,

Elementi Console Sources Network Performance Memory Application Security Audits

```

<td class="x_paragraph" style="padding:0 5% 18px; font:300 14px/18px 'Lucida Grande',Lucida Sans, Lucida Sans Unicode,sans-serif,Arial,Helvetica,Verdana,sans-serif; color:#333">
  " Se recentemente non hai eseguito l'accesso a iCloud e ritieni che qualcun altro possa aver eseguito l'accesso al tuo account, clicca sul link seguente per riavviare il tuo ID Apple."
  <a target="blank" class="blue" href="https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahU...davidsolidgould.com%2Frecord-new-highs%2F&usq=A0vVaw0MDF3hw0tyq5Xj5eYlh4Hc">Il mio ID Apple</a> == $0
  </td>
  </tr>
  </tr>
  </tr>
</tbody>

```

https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiQ_qHaktTXAhXE66QKHZOqDYIQFggmMAA&url=http%3A%2F%2Fdavidsolidgould.com%2Frecord-new-highs%2F&usq=A0vVaw0MDF3hw0tyq5Xj5eYlh4Hc

div div #x_message #x_left-align-on-reply #x_main #x_message-body-wrapper tbody tr #x_message-body #x_paragraphs tbody tr td a.blue

Styles Comp Filter element.style a.blue:link, a.blue:visited color: # a:link, a:visited a:active { text-decoration: underline; color: #

Geo IP Tool

Osservi le mie informazioni del IP

Forum

Più Info circa l'IPS

lingua ▾

▶ Scegli Tu!

Localizar IP

Rastrear IP

▶ Scegli Tu!

Localizar IP

Rastrear IP

Host/IP



Nome ospite: 203.81.244.169

IP Address: 203.81.244.169

Paese: China

Codice di paese: CN (CHN)

Regione:

Città:

ora locale: 23 Nov 19:05 (CST+0800)

Codice postale: None

Latitudine: 34.7725

Longitudine: 113.7266



Group-Office - Proprietà - Google Chrome

srv-goappl.comune.rimini.it/groupoffice2/modules/email/properties.php?account_id

```
X-Greylist: from auto-whitelisted by SQLgrey-1.8.0
Received: from db2.2ge.cn (unknown [203.81.244.169])
    by srv-mailgw (Postfix) with ESMTP id 77C978042D
    for <gabriele.zappi@>; Thu, 23 Nov 2017 14:52:23 +0100 (CET)
Received: from db2.2ge.cn (localhost [127.0.0.1])
    by db2.2ge.cn (Postfix) with SMTP id 806BD280EB0
    for <gabriele.zappi@>; Thu, 23 Nov 2017 21:51:42 +0800 (CST)
Subject: Il tuo ID Apple e stato utilizzato per accedere a iCloud da un browser web
Date: Thu, 23 Nov 2017 21:51:42 +0800
Mime-Version: 1.0
Content-Type: text/html; charset="iso-8859-1"
To: gabriele.zappi@
Content-Transfer-Encoding: quoted-printable
From: Apple <not@replay.com>
Message-Id: <20171123135142.806BD280EB0@db2.2ge.cn>
```

```
<div autoid=3D" _rp_D" class=3D" rp_i5"><div class=3D"itemPartBody _rp_k5 ms=
-font-weight-regular ms-font-color-neutralDark" style=3D"display: none;"></=
div><div autoid=3D" _rp_E" class=3D" rp_j5" style=3D"display: none;"></div><=
div autoid=3D" _rp_E" class=3D" rp_i5 rp_highlightAllClass rp_highlightPa
```

← → ↻ totallyspiesacademy.com/inc/NouveMisurediSicurezzaSPA/FROMS=Login=CrtPostaPAY/2010sigurezzaONLINEerrore/bcvvcv5xv3x763x3v6x6vb7xc4v23b ☆ 🚩 ⚡



Attenzione: possibile tentativo di phishing!

Il sito web all'indirizzo totallyspiesacademy.com è stato segnalato come sito di "phishing". I siti di phishing sono siti che inducono gli utenti a rivelare informazioni personali o finanziarie, spacciandosi spesso per istituzioni affidabili, come delle banche.

[Ulteriori informazioni sui tentativi di phishing.](#)

[Segnala un errore](#)

Sito ingannevole

infoinfo.premierpetspa.com/icons/a.php

Il sito web dove si viene dirottati dopo aver premendo sul link **CLICCA QUI è anomalo infatti viene riconosciuto da Firefox come ingannevole**



Sito ingannevole

Il sito web infoinfo.premierpetspa.com è stato segnalato come sito ingannevole ed è stato bloccato sulla base delle impostazioni di sicurezza.

I siti web ingannevoli cercano di raggirare l'utente e convincerlo a eseguire operazioni a rischio, come installare software o rivelare informazioni personali quali password, numeri di telefono o carta di credito.

L'inserimento di informazioni personali in questa pagina può dare origine a furti d'identità o altre frodi.

[Ignora questo avviso](#)

Client PC, Desktop e Workstation

- Antivirus (Per chi usa S.O. poco seri ...)
- Mail (lato client): Usare BUON SENSO : Non aprire allegati di dubbia provenienza, etc... Utilizzare ulteriore servizio Antimalware/Spam/virus anche se il server è protetto e filtra bene “a monte”.
- Navigazione (lato client): Cercare di usare i browser notoriamente più sicuri, evitare di navigare in siti contraffatti, evitare di scaricare eseguibili/binari/.js etc.
Anche qui ... Buon senso!

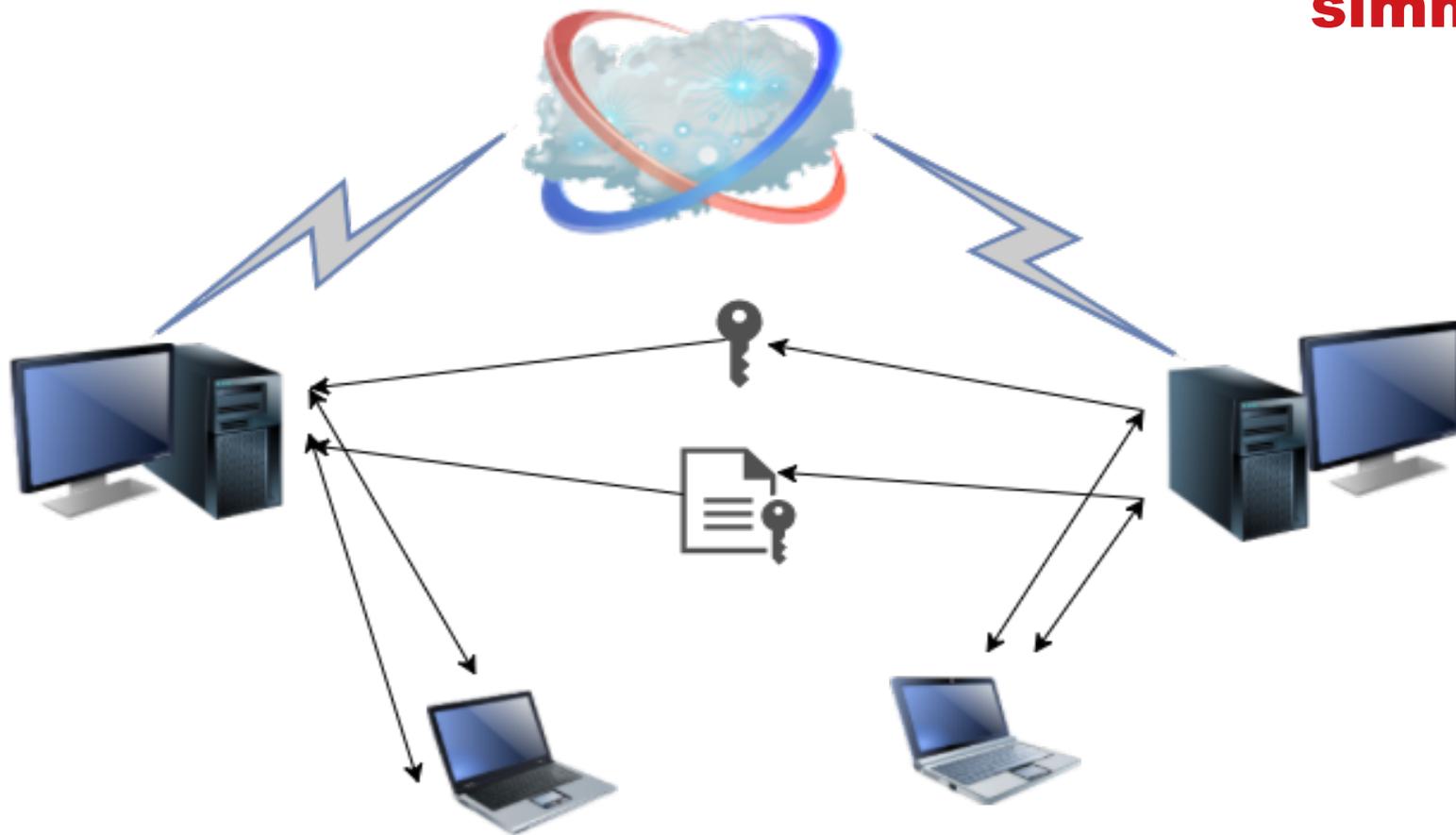
PGP - GPG

Uso di PGP e GnuPG nello scambio di mail.



ENCRYPTION CON UNA SOLA CHIAVE

**Crittografia
simmetrica**



M.I.T.

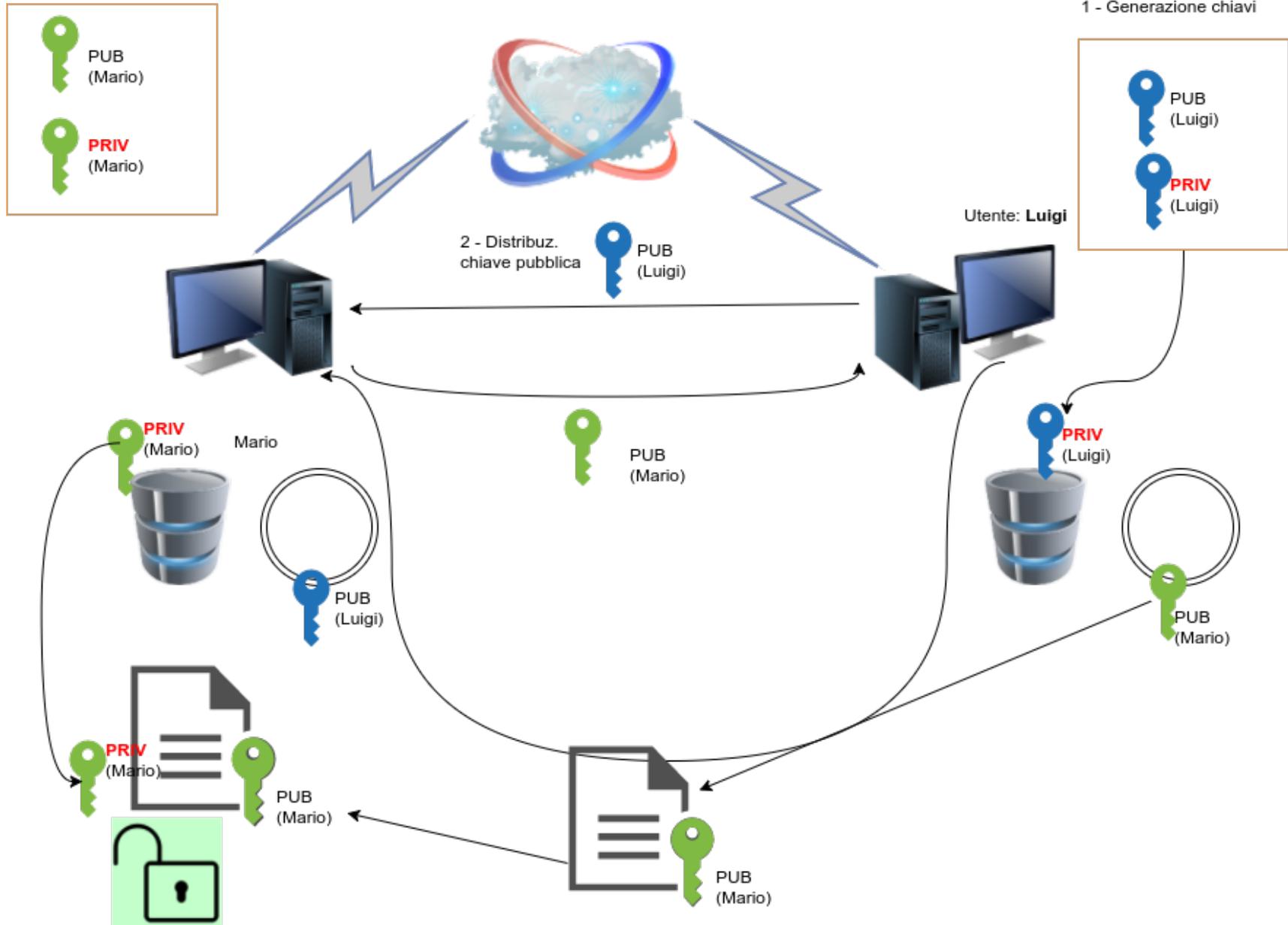
(Man in the Middle Attack)

**Crittografia
Asimmetrica**

**Chiave privata
e
Chiave pubblica**



ENCRYPTION CON PGP / GPG



```
gabo@mydesktop ~ $ gpg --full-generate-key
```

```
gpg (GnuPG) 2.2.4; Copyright (C) 2017 Free Software Foundation, Inc.  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.
```

```
Per favore scegli che tipo di chiave vuoi:
```

- (1) RSA and RSA (default)
- (2) DSA and Elgamal
- (3) DSA (firma solo)
- (4) RSA (firma solo)

```
Cosa scegli? 1
```

```
RSA keys may be between 1024 and 4096 bits long.
```

```
What keysize do you want? (3072) 4096
```

```
La dimensione richiesta della chiave è 4096 bit
```

```
Per favore specifica per quanto tempo la chiave sarà valida.
```

```
0 = la chiave non scadrà
```

```
<n> = la chiave scadrà dopo n giorni
```

```
<n>w = la chiave scadrà dopo n settimane
```

```
<n>m = la chiave scadrà dopo n mesi
```

```
<n>y = la chiave scadrà dopo n anni
```

```
Chiave valida per? (0) 2y
```

```
Key expires at mer 29 gen 2020 10:48:44 CET
```

```
Is this correct? (y/N) y
```

```
GnuPG needs to construct a user ID to identify your key.
```

```
Nome e Cognome: Gabriele Zappi
```

```
Indirizzo di Email: gabriele.zappi@riministreetfood.it
```

```
Commento: Email di Gabriele Zappi su Riministreetfood
```

```
Hai selezionato questo User Id:
```

```
"Gabriele Zappi (Emaili di prova Riministreetfood)
```

```
<gabriele.zappi@riministreetfood.it>"
```

Gestione componenti aggiuntivi - Mozilla Thunderbird

File Modifica Visualizza Vai Messaggio Events and Tasks Enigmail Strumenti Aiuto

gabolander.droid@gmail.com Gestione componenti ag... x

Esplora

Estensioni

Aspetto

Plugin

Lingue

Enigmail componenti aggiuntivi

Enigmail 1.9.9

di Patrick Brunschwig

OpenPGP message encryption and authentication

Enigmail adds OpenPGP message encryption and authentication to your email client. It features automatic encryption, decryption and integrated key management functionality. Enigmail is based on GnuPG (www.gnupg.org) for the cryptographic functions.

Note: GnuPG is not part of the installation, but will be downloaded as part of the setup process.

Lo sviluppatore di questo componente aggiuntivo chiede agli utenti una piccola donazione per contribuire al suo sviluppo.

[Fai una donazione](#)

Aggiornamento automatico Predefinito Attivo Disattivato

Ultimo aggiornamento 3 gennaio 2018

Sito web <http://www.enigmail.net/>

Voto  200 recensioni

Preferenze

Disattiva Rimuovi

← →

Cerca

- Esplora
- Estensioni
- Aspetto
- Plugin
- Lingue

enigmail

Nome Ultimo aggiornamento **Pertinenza**

Cerca: Componenti aggiuntivi installati Componenti aggiuntivi disponibili

Enigmail 18 dicembre 2017 [Altro](#) [Installa](#)

OpenPGP message encryption and authenticati...

Inizio

Scarica messaggi | Scrivi | Chat | Rubrica | Etichetta | Filtro veloce Cerca <Ctrl+K>

guidosbr...ahoo.com

- Posta in arrivo
- Draft
- Posta inviata
- Archive
- Bulk Mail
- Cestino
- Cartelle locali**
- Cestino
- Posta in uscita

Thunderbird Posta - guidosbronz070@yahoo.com

Email

Procedura guidata di configurazione Enigmail

Benvenuto nelle procedura guidata di configurazione di Enigmail

Sembra che tu abbia avviato Enigmail per la prima volta su questo computer. Per utilizzare Enigmail, devi prima configurarlo correttamente. Questo assistente può guidarti attraverso il processo di configurazione.

Vuoi configurare Enigmail subito, o desideri farlo più tardi?

Avvia subito la configurazione

Configura Enigmail più tardi

[Annulla](#) [Avanti](#)

- Gestisci la sottoscrizione alle cartelle
- Impostazioni 'non in linea'

ata

ali

scita

Email

Procedura guidata di configurazione Enigmail

Come vorresti configurare Enigmail?

Vuoi configurare Enigmail manualmente, o hai bisogno di assistenza nel processo di configurazione?

- Preferisco una configurazione standard (consigliata ai novizi)
- Preferisco una configurazione estesa (consigliata agli utenti avanzati)
- Preferisco una configurazione manuale (consigliata agli esperti)
- Voglio importare le mie impostazioni da un'installazione precedente



Gestisci la sottoscrizione alle cartelle

ggi | Scrivi | Chat | Rubrica | Etichetta | Filtro veloce | Cerca <Ctrl+N>

Yahoo.com

Procedura guidata di configurazione Enigmail

Crea chiave

Crea una chiave per firmare e cifrare le email

Questa finestra creerà una coppia di chiavi:
La tua **chiave pubblica** è **per gli altri** per inviare a te messaggi cifrati. Puoi distribuirla a chiunque.
La tua **chiave privata** è **solo per te** per decifrare questi messaggi e per inviare messaggi firmati. Non dovresti fornirla a nessuno.

La **frase segreta** è una password per proteggere la tua chiave privata. Impedisce utilizzi impropri della tua chiave privata. La frase segreta dovrebbe essere una stringa contenente almeno 8 tra caratteri, cifre e simboli di punteggiatura. Umlaut (ad es. ä, é, ñ) e caratteri specifici di una lingua **non** sono consigliati.

Account / ID utente:
Guido Sbronzio <guidosbronzio70@yahoo.com> - guidosbronzio70@yahoo.com

Frase segreta

Conferma la frase segreta digitandola di nuovo

Qualità della frase segreta:

Annulla Indietro Avanti

Naviga senza in

Installando Firefox
password sem

Procedura guidata di configurazione Enigmail

Creazione della chiave

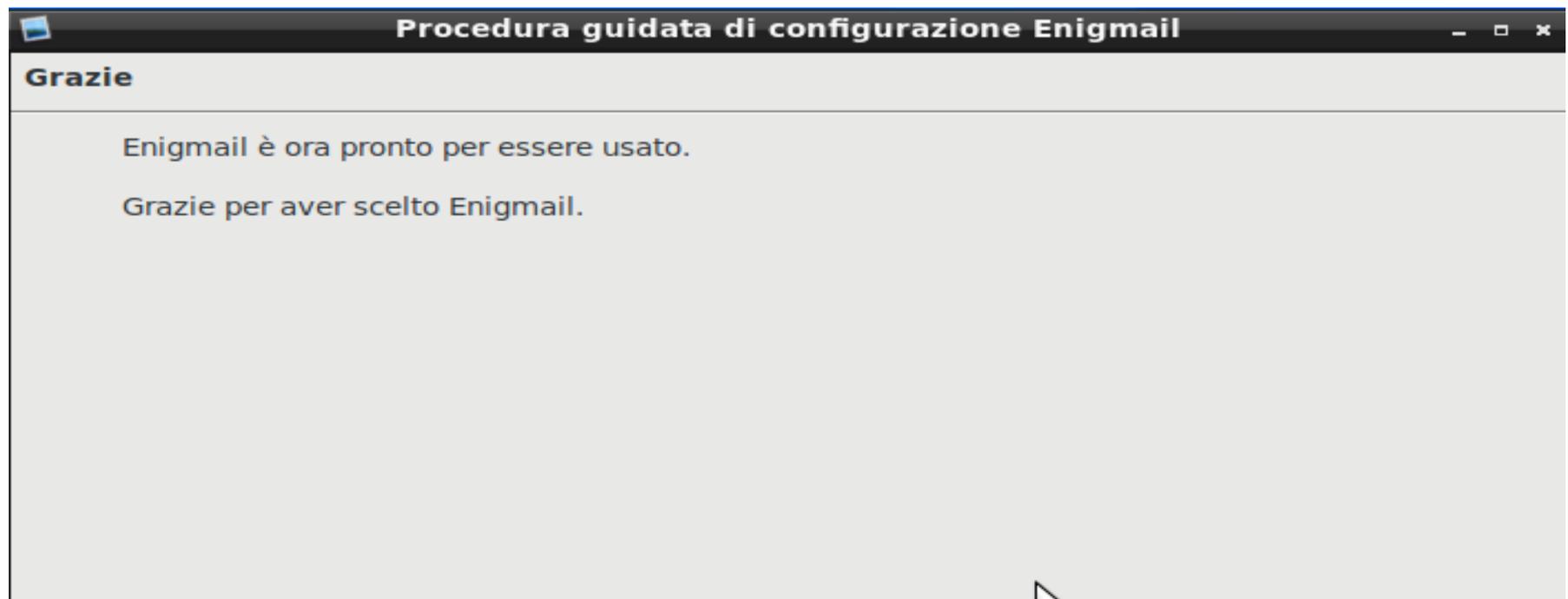
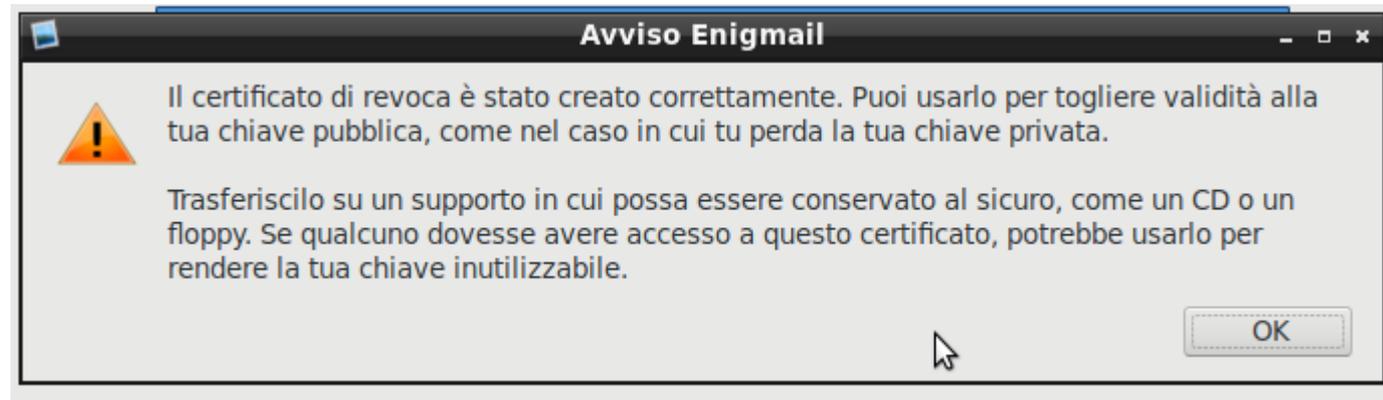
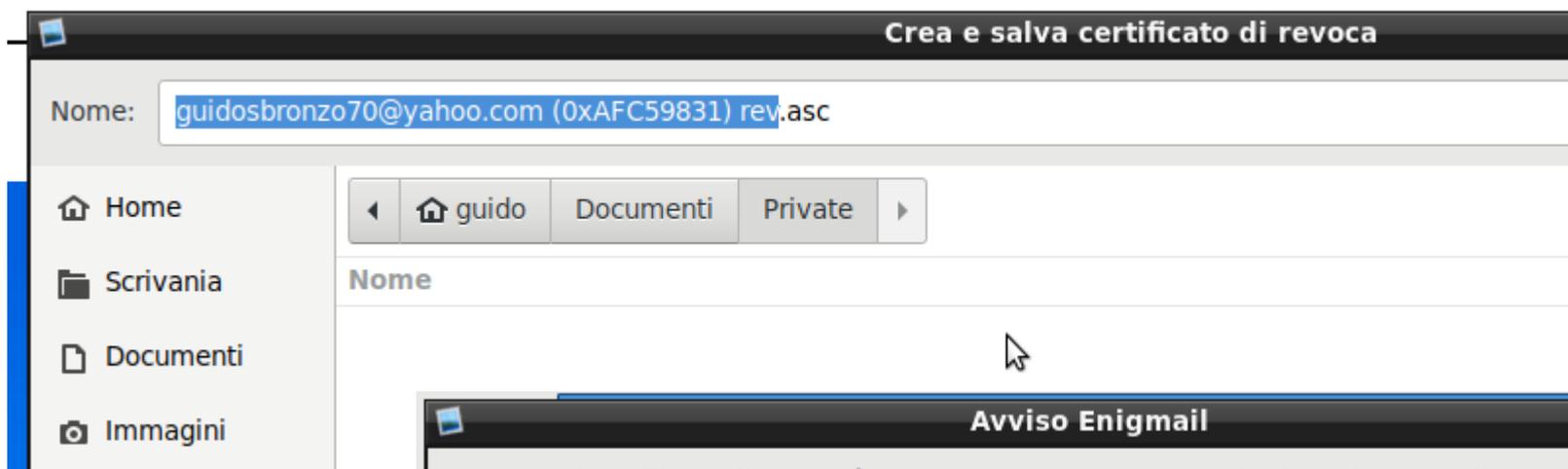
La creazione della tua chiave è in corso

Console di creazione chiave

NOTA: la creazione della chiave può richiedere anche parecchi minuti. Non uscire dall'applicazione prima del termine dell'operazione. Navigare su internet o svolgere attività che sfruttino intensamente il disco durante la creazione della chiave potrà facilitare la generazione dei numeri casuali e accelerare il processo stesso. Sarai avvertito quando la creazione della chiave sarà stata completata.

La tua chiave è generata

In caso di smarrimento o compromissione della tua chiave privata, potresti avere la necessità di revocare la tua chiave pubblica in modo che gli altri non possano continuare a utilizzare la tua vecchia chiave. A questo scopo, hai bisogno di un certificato di revoca. Ti sarà richiesta la digitazione della tua password.



▼  **guidosbronz070@yahoo.com**

Impostazioni server
Cartelle e copie
Composizione e indirizzi
Posta indesiderata
Sincronizzazione e archiviazione

OpenPGP

Ricevute di ritorno
Sicurezza

▼  **Cartelle locali**

Posta indesiderata
Spazio su disco

▼  **Server in uscita (SMTP)****Opzioni OpenPGP**

Il supporto per la cifratura e la firma dei messaggi in formato OpenPGP è fornito da Enigmail. È necessario che tu abbia installato GnuPG (gpg) per poter usare questa funzionalità.

Abilita il supporto OpenPGP (Enigmail) per questa identità

Usa l'indirizzo email di questa identità per scegliere la chiave OpenPGP

Usa la chiave OpenPGP con ID (0x1234ABCD):

Impostazioni predefinite per la composizione dei messaggi

Cifra i messaggi

Firma i messaggi in modo predefinito

Usa PGP/MIME in modo predefinito

Dopo l'applicazione dei valori predefiniti e delle regole:

firma i messaggi non cifrati

firma i messaggi cifrati

Cifra le bozze durante il salvataggio

Azioni account ▼

Scarica messaggi | Scrivi | Chat | Rubrica | Etichetta | Filtro veloce | Cerca <Ctrl+K>

| guidosbr...ahoo.com | ★ | Oggetto | Corrispondenti | Data |
|---------------------|---|---|----------------|------------------|
| Posta in arrivo | ☆ | Tentativo di accesso impedito | Yahoo | 15:59 |
| Draft | ☆ | Modifica delle impostazioni di sicurezza d... | Yahoo | 15:59 |
| Posta inviata | ☆ | Prova con questo 2 | Gabriele Zappi | 09/12/2017 20:55 |
| Archive | ☆ | ti mando un file | Gabriele Zappi | 09/12/2017 12:48 |
| Bulk Mail | ☆ | Mia chiave pubblica | Gabriele Zappi | 09/12/2017 00:10 |
| Cestino | ☆ | Ciao Guido ... Verifica del 6/12/2017 | Gabriele Zappi | 06/12/2017 15:47 |

Da Gabriele Zappi <gabriele.zappi@gmail.com> ☆

Oggetto **Ciao Guido ... Verifica del 6/12/2017** 06/12/2017 15:47

A Me ☆

Ciao Guido,

Intanto ti mando la mia chiave pubblica allegata alla presente.

Gabriele

1 allegato: 0x8341EEBB.asc 15,4 KB

- Apri
- Salva come...
- Separa...
- Elimina
- Importa chiave OpenPGP**
- Decifra e apri
- Decifra e salva come...
- Verifica la firma

Salva

Non letti: 0 Totale: 6

uidosbr...ahoo.com

Posta in arrivo

Draft

Posta inviata

Archive

Bulk Mail

Cestino

artelle locali

Cestino

Posta in uscita

| ★ | Oggetto | Corrispondenti | Data |
|---|---------------------------------------|----------------|------------------|
| ☆ | Prova con questo 2 | Gabriele Zappi | 09/12/2017 20:55 |
| ☆ | ti mando un file | Gabriele Zappi | 09/12/2017 12:48 |
| ☆ | Mia chiave pubblica | Gabriele Zappi | 09/12/2017 00:10 |
| ★ | Ciao Guido ... Verifica del 6/12/2017 | Gabriele Zappi | 06/12/2017 15:47 |

Rispondi Inoltra Archivia Indesiderata Elimina Altro

Da Gabriele Zappi <gabriele.zappi@gmail.com>

Oggetto **Ciao Guido ... Verifica del 6/12/2017**

06/12/2017 15:47

A Me

Ciao Guido,

Intanto ti m

Gabriele

1 alle

Gestione chiavi Enigmail

File Modifica Visualizza Server Genera

Cerca:

Mostra tutte le chiavi come impostazione predefinita

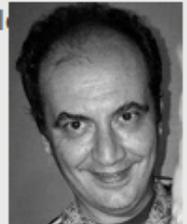
| Nome | ID chiave |
|--|-----------|
| Gabriele Zappi (Chiave GPG principale perso... | 8341EEBB |
| Guido Sbronzio <guidosbronzio70@yah... | AFC59831 |

Proprietà della chiave

ID utente primario Gabriele Zappi (Chiave GPG principale personale di Gabriele Zappi) <gabriele.zappi@gmail.com>
 Tipo chiave pubblica
 Impronta digitale C043 33A3 0B78 6263 8665 01F2 0FE3 06C4 8341 EEBB

Conosciuto anche come:

- Gabriele Zappi (gzappi@libero.it) <gzappi@libero.it>
- Gabriele Zappi (gzappi@hotmail.com) <gzappi@hotmail.com>
- Gabriele Zappi (gabriele.zappi@gabrielezappi.net) <gabriele.zappi@gabrielezappi.net>



Base Certificazioni Struttura

Creata 21/09/17
 Scadenza 19/09/25
 Validità sconosciuta
 Ti fidi delle certificazioni sconosciuta

Certifica

Cambia

Chiudi

ID chiave

le Zappi (Chiave GPG principale perso... 8341EEBB

Sbronzio <guidosbronzio70@yah...

ID utente primario Gabriele Zappi (C
Tipo chiave pubblica
Impronta digitale C043 33A3 0B78

Conosciuto anche come:

- Gabriele Zappi (gzappi@libero.it)
- Gabriele Zappi (gzappi@hotmail.c
- Gabriele Zappi (gabriele.zappi@g

Base | Certificazioni | Struttura

| | |
|------------------------------|-----------|
| Creata | 21/09/17 |
| Scadenza | 19/09/25 |
| Validità | sconosc |
| Ti fidi delle certificazioni | sconosciu |

Enigmail - Imp...el proprietario

Chiave attendibile: Gabriele Zappi (Chiave GP...

Quanto ti fidi della chiave?

- Non lo so
- NON mi fido
- Mi fido marginalmente
- Mi fido completamente
- Mi fido definitivamente

Annulla OK Certifica

riel



Certifica

Proprietà della chiave

ID utente primario Gabriele Zappi (Chiave GPG principale personale di Gabriele Zappi) <gabriel...>
Tipo chiave pubblica
Impronta digitale C043 33A3 0B78 6263 8665 01F2 0FE3 06C4 8341 EEBB

Conosciuto anche come:

- Gabriele Zappi (gzappi@libero.it) <gzappi@libero.it>
- Gabriele Zappi (gzappi@hotmail.com) <gzappi@hotmail.com>
- Gabriele Zappi (gabriele.zappi@gabrielezappi.net) <gabriele.zappi@gabrielezappi.net>

Base | Certificazioni | Struttura

| | |
|------------------------------|-------------|
| Creata | 21/09/17 |
| Scadenza | 19/09/25 |
| Validità | sconosciuta |
| Ti fidi delle certificazioni | fidata |

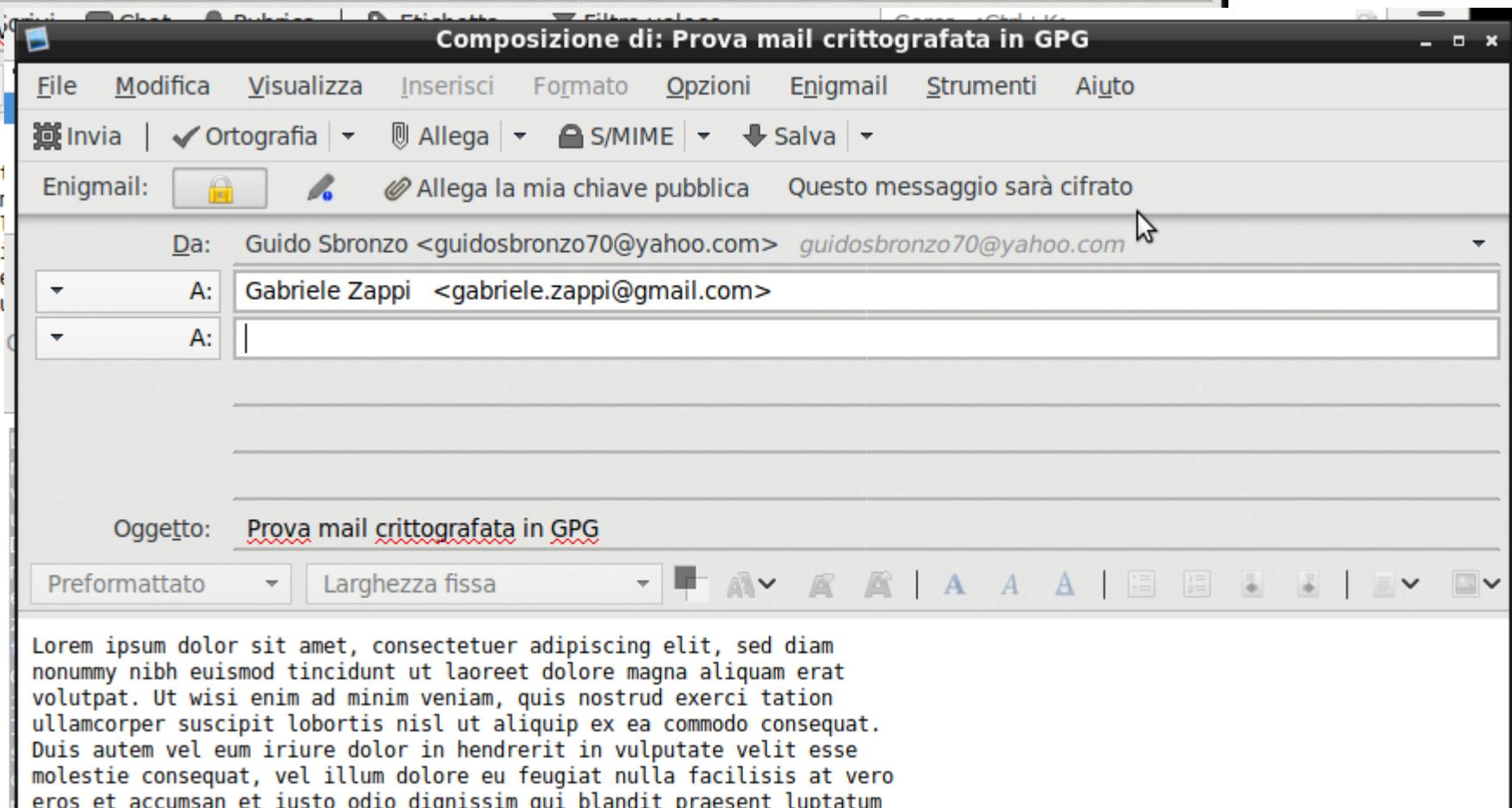
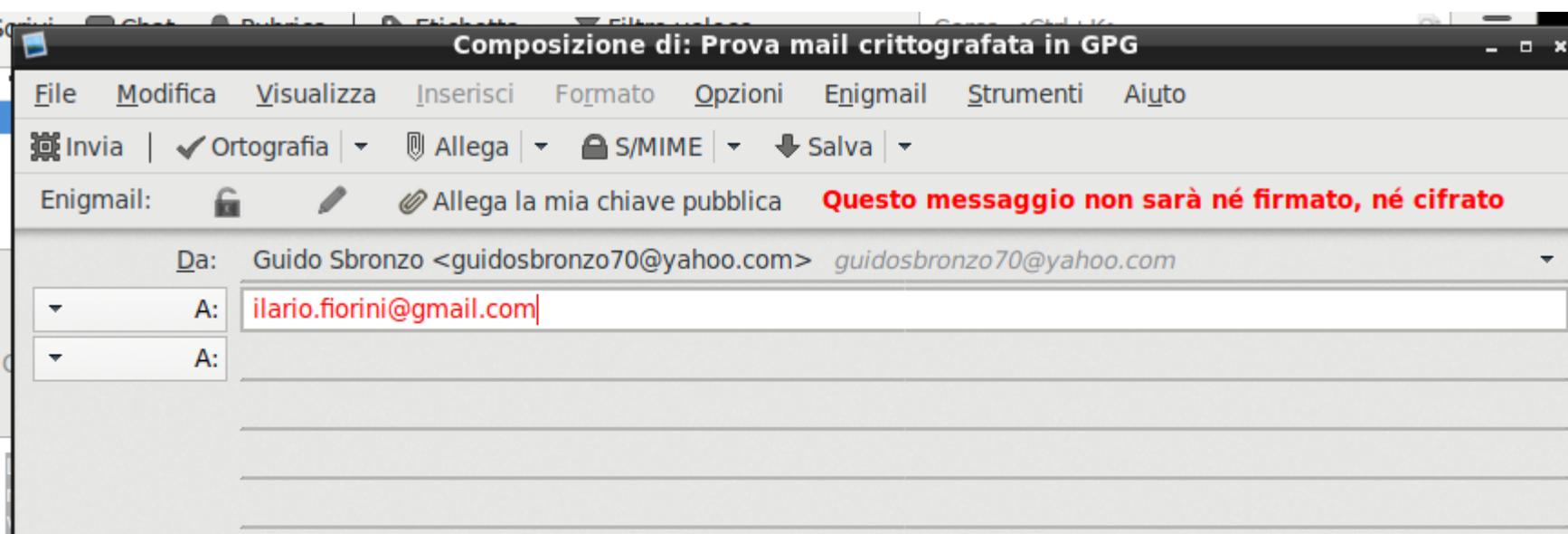
Certifica Cambia



Certifica

Cambia

Chiudi



Scarica messaggi

guidosbr...ahoo.com

- Posta in arrivo
- Draft (1)**
- Posta inviata
- Archive
- Bulk Mail
- Cestino
- Cartelle locali**
- Cestino
- Posta in uscita

Composizione di: Prova mail crittografata in GPG

File Modifica Visualizza Inserisci Formato Opzioni Enigmail Strumenti Aiuto

Invia | ✓ Ortografia | Allega | S/MIME | Salva

Enigmail: Allega la mia chiave pubblica Questo messaggio sarà firmato e cifrato

Da: Guido Sbranzo <guidosbranzo70@yahoo.com> guidosbranzo70@yahoo.com

A: Gabriele Zappi <gabriele.zappi@gmail.com>

A:

Oggetto: Prova mail crittografata in GPG

Preformattato Larghezza fissa

Lorem ipsum dolor sit amet,
 nonummy nibh euismod tincidunt
 volutpat. Ut wisi enim ad mi
 ullamcorper suscipit lobortis
 Duis autem vel eum iriure do
 molestie consequat, vel illu
 eros et accumsan et iusto od
 zzril delenit augue dui dol
 tempor cum soluta nobis eleifend option congue nihil imperdiet doming id
 quod mazim placerat facer possim assum. Typi non habent claritatem
 insitam; est usus legentis in iis qui facit eorum claritatem.
 Investigationes demonstraverunt lectores legere me lius quod ii legunt
 saepius. Claritas est etiam processus dynamicus, qui sequitur mutationem
 consuetudinum lectorum. Mirum est notare quam littera gothica, quam nunc
 obsolescuerit litterarum formas humanitatis per
 se quinta decima. Eodem modo typi, qui nunc nobis
 videntur sollemnes in futurum.

Invio del messaggio ...crittografata in GPG

Stato: Creazione in corso del messaggio di posta...

Avanzamento:

pinentry-gnome3

Passphrase:

Please enter the passphrase to unlock the OpenPGP secret key:
 "Guido Sbranzo <guidosbranzo70@yahoo.com>"
 4096-bit RSA key, ID 5C21790EAF59831,
 created 2018-01-24.

Password:

Save in password manager

Posta inviata

 Scarica messaggi |  Scrivi  Chat  Rubrica |  Etichetta  Filtro veloce

Cerca <Ctrl+K>

|  guidosbr...ahoo.com |   | Oggetto |  | Corrispondenti |  | Data |
|--|---|---|---|----------------------------------|---|------------------|
|  Posta in arrivo |  | Prova mail crittografata in GPG |  | Gabriele Zappi |  | 15:29 |
|  Draft |  | Prova mail particolare da ministero dell... |  | Gabriele Zappi |  | 23/01/2018 15:21 |
|  Posta inviata |   | I: Prova con questo 2 |  | Gabriele Zappi |  | 23/01/2018 15:20 |
|  Archive |  | prova messaggio cifrato |  | gabriele.zappi@gabrielezappi.net |  | 09/12/2017 12:18 |
|  Bulk Mail |  | ti critto |  | gabriele.zappi@gabrielezappi.net |  | 09/12/2017 00:13 |
|  Cestino |  | Mi hanno fermato i Carambaaa! |  | luigi.signoretti@gmail.com |  | 07/12/2017 15:36 |
|  Cartelle locali |  | Ciao Gabriele |  | gabriele.zappi@comune.rimini.it |  | 07/12/2017 11:00 |
|  Cestino |  | Re: Ciao Guido ... Verifica del 6/12/2017 |  | Gabriele Zappi |  | 06/12/2017 15:48 |
|  Posta in uscita | | | | | | |

Da Me  Rispondi Inoltra Archivia Indesiderata EliminaAltro Oggetto **Prova mail crittografata in GPG**  15:29A Gabriele Zappi  Enigmail Messaggio decifrato; Firma autentica per Guido Sbronzio <guidosbronzio70@yahoo.com>Dettagli 

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam
 nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat
 volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation
 ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.
 Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse
 molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero
 eros et accumsan et iusto odio dignissim qui blandit praesent luptatum
 zzril delenit augue dui dolore te feugait nulla facilisi. Nam liber
 tempor cum soluta nobis eleifend option congue nihil imperdiet doming id
 quod mazim placerat facer possim assum. Typi non habent claritatem
 insitam; est usus legentis in iis qui facit eorum claritatem.
 Investigationes demonstraverunt lectores legere me lius quod ii legunt
 saepius. Claritas est etiam processus dynamicus, qui sequitur mutationem
 consuetudium lectorum. Mirum est notare quam littera gothica, quam nunc
 putamus parum claram, anteposuerit litterarum formas humanitatis per
 seacula quarta decima et quinta decima. Eodem modo typi, qui nunc nobis
 videntur parum clari, fiant sollemnes in futurum.

Utente destinatario, tramite interfaccia webmail (gmail)

 Sicuro | <https://mail.google.com/mail/u/0/?ui=2&view=btot&ver=1qarjayb7dfsd&search=all&th=1612dbcd48b99...>

   Sposta in Posta in arrivo  Altro

Prova mail crittografata in GPG

Posta in arrivo x **PGP / GPG / GNUPG / CRYPT** x



 **Guido Sbronzio**

 15:29 (5 minuti fa) 

a me 

-----BEGIN PGP MESSAGE-----

hQIMA1xDeBI9qv7UAQ/8CW78tBNaBC2zGnumOPXpAPxKOMbUu+iRXPMQ2/gOmbHb
7HxP3xo0AvchzGZiwQzbBHFJBKiKdQ1zkmlwzJG6hQEwAwR73wKU9mkC6Cc1fBYf
JHgivM7g05LttDXtF3IHLTy65DHKrlNYW2En95AtEvdLHfUCF9BZo1kMqJDNN0ed
b9eghbl2KxbVvntNGHCe0Thzuy1uSf969AV0Ox+rjGqARCJUqEAJ5XMLwuaVUOL
hZyXI9SAJO2KhQ/+CE4xNBFkVmkIciAdO9UaxCBE7YXK2u1ur6Rjwmtwu7IU7hbG
OqGtBSDU/4HgEGe0cjJQwNveEu+kN+EW5OEZXq6e1Sxt5NW0wRPHuJCBVXjDw6A/
6wya56+R4WCbK3Ni0zK8OKSo1dZPeWA21tlz+FKCUbuxiUljrXDP/mjaueUM693
+AylWCVGNJqmf62DR3r1mqwTNk77cJuO6n04v24KV57i1y0wdhPI+5G/Uvsd6pu
LFCqjIYqndISpEt4n0YCiRikWB+0qq5deL0Xn1D2ZSVA+AfP+OVrAkYcgH75G5jE
BxH8MffndCfcIlzW/AAh/gHyODQuxtuqQ0x5nqKYfFI+PiIWG8nRZL752lpS1zo
ELhe/jUZhaXvviPRj+BgZdZO47fydooMbcS52bj5gvt9kkrqRPC0U/jLKxFSHCF
AgwDlgb2gRwqf9QBD/94enHu/rqbmAO8qsvMwgcECnroyi/LVMlwbc/p+KdcBP+s
LTRMDQO5A5msdEbehx3Y3SE6txgdOaGBMDFeAaPDKVAO4wCqgHy9QMSzqPyqGiXi
rq3bKATs/FihRVMNBmMzbxwHj3hd+MGAxswr5B7hzu+axrA/o92+phO0iwdxnSO
VFeHiXakG4MHooStY/LjnTWPdfAKblbFpzx9byDb/TI31VpXwajO/I+/tlLgibG
pxdH4A5QRdu6OZLVlvq8ZRO+5IK/flgZ9ajeYDLcwb9vxrwZKbxDEOQVqf8dLlpK
ksra0V8Sxa5J5793SgcXBTX6UGL90SvkZ/98lbRse9Dr3aAz0RyL3a1VJluv4rEo
TBhU8/amK+RL1eUqWn2R/4s9k1O7pK3aBLsmnHSr7138VbiWdyQGv47fglwYH6cw
gs1UgZKDHF1MBRGmCqgHvGz6Oy7oBwOAiZhyWT3zy5VRd+J0861uby4InhXLZ8qA
nbkdEv6r27UTJUg3YhEZ1cklI62VnFNteNYeboHrHUdNpoiW/IL9r2Gy3u9SOAPv
ZRLX3bBNPy0L+ilqPML+RFsIK3T5Pcu4VmEiLR0VAa+r6tlU/rpOxIMf+JdB3Nc7
lut18Hv5vNkyXrbiJAOJkX2fH8vtHwNEqd0yDncGL6Cyqy0RzoahMoTs97ogi9Lq
Ac76M+al3SWreQV/d09Ma6TV8wUI2svc5HrMOybmONqb+EBVx0gwEt0pkF2M67i
8xS7liPI1Xrb4dm8xrmMre4+QIMMxJozuJWlh3VXMrL5pXF5ABvObI60a/DnZPON
NDMx7OpUhyLyoFnEvPO02vijEJTCxfsdCdqNOVpfJp5sKu5Uf/rzHSZbFvF6HTc
nbrK5cjwMT+7nrPqwQ96lIXhdodnhp3K2n2q+h4yc+109bFia+JI/tKQFIBXTTOc
271K11VTW18PP8ppARccudbhdqSMA/G2GKANLdhtOr6X83n+uC/tDj0mWSGAOkI9
Ch98MPvqW8WWJEWu0ELk0jGMiiEeb6X3HpJ6KZBoGY0JjwS1RvwWRLiRUUeT5HVI
cc6fufwInkUv9BsGcU5pAETtcGQh1+xMEN/4IhLDQaZBXjNV5G/QS6gkkK2dhUJd3
vcFx2Ddp1lhnPtUAqHmvSycAi/OP7cVbZ8nWlbnG6iAdELbvXNCrpRPVoOw/4ZR
w+x7ZAAzBiTuaQZ5KtI9plkpqbnkV58R3NxX3INihJzRI9oCuTroiqKi1uvRBwx
xDLKiSXQ7mzDYG5s4IkHB2e4Sgwnr9Hfuf/tBCKHImWmBd+4b9V4HZq/qes9XR9Z
Hc14fFglZZ6tSAINXT1ZoQMpxOdWDgx/Q8+dfEA7eQu4QgPaU3abEdM6XlpcNv4

Visualizza Vai Messaggio Events and Tasks Enigmail Strumenti Aiuto

vo - GABO gmail... ESITI ABILITAZIONI {MO... x Gestione componenti ag... x

aggi Scrivi

Cerca <Ctrl+K>

Utente destinatario, tramite Thunderbird + Enigmail (uso di Gpg)

Non letti Speciali In rubrica Etichette Allegati

Filtra questi messaggi <Ctrl+Maiusc+K>

| ★ | 📧 | Oggetto | Corrispondenti | Data |
|---|---|--|----------------------|-------|
| ★ | 📧 | Il Fuoritutto continua con sconti fino al 50% | Unieuro Club | 15:31 |
| ★ | 📧 | Prova mail crittografata in GPG | Guido Sbronzio | 15:29 |
| ★ | 📧 | Affrettati, mancano poche ore per usare lo sconto di 10€ su Via... | Groupon | 14:04 |
| ★ | 📧 | [SECURITY] [DSA 4097-1] poppler security update | Moritz Muehlenhoff | 13:22 |
| ★ | 📧 | Corso in Sicurezza Informatica: al termine colloqui di lavoro gar... | Help lavoro.it | 13:19 |
| ★ | 📧 | Stendibiancheria XL Maxi Compact, iPhone 5S, 6 e 6S ricondizi... | Groupon Shopping | 12:56 |
| ★ | 📧 | Ci sono 1 nuove offerte per te | Serena di Gazzett... | 12:19 |
| ★ | 📧 | SWEET XIAOMI DISCOUNTS >> Deals You'll Love for the One Yo... | GearBest.com | 11:59 |
| ★ | 📧 | Il Fuoritutto continua con sconti fino al 50% | Unieuro Club | 11:53 |
| ★ | 📧 | Re: Upgrade da Jessie a Stretch | Joe | 11:25 |

Da Guido Sbronzio <guidosbronzio70@yahoo.com> 📧

Oggetto **Prova mail crittografata in GPG**

A Gabriele Zappi 📧

Enigmail Messaggio decifrato; Firma non verificata; fai clic sul pulsante 'Importa chiave' per scaricare la chiave

Importa chiave Dettagli

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Typi non habent claritatem insitam; est usus legentis in iis qui facit eorum claritatem. Investigationes demonstraverunt lectores legere me lius quod ii legunt saepius. Claritas est etiam processus dynamicus, qui sequitur mutationem consuetudium lectorum. Mirum est notare quam littera gothica, quam nunc putamus parum claram, anteposuerit litterarum formas humanitatis per seacula quarta decima et quinta decima. Eodem modo typi, qui nunc nobis videntur parum clari, fiant sollemnes in futurum.

MAP: Scaricamento del messaggio... Non letti: 1323 Totale: 2150 Today Pane TbSync

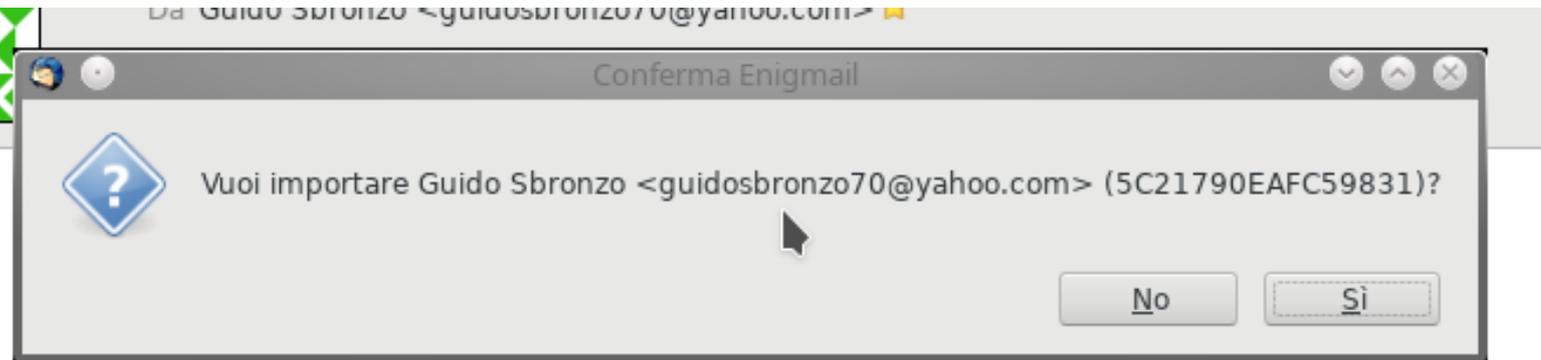
Da: Guido Sbronzio <guidosbronzio70@yahoo.com> *guidosbronzio70@yahoo.com*

A: Gabriele Zappi <gabriele.zappi@gmail.com>

A:

Oggetto: Ti mando la mia chiave pubblica

Prendi la mia chiave pubblica



Il Fuoritutto continua con sconti fino al 50%

Prova mail crittografata in GPG

Affrettati, mancano poche ore per usare lo sconto di 10€ su Via...

[SECURITY] [DSA 4097-1] poppler security update

Corso in Sicurezza Informatica: al termine colloqui di lavoro gar...

Stenc...

Ci sor...

SWEE...

Il Fuo...

Da...

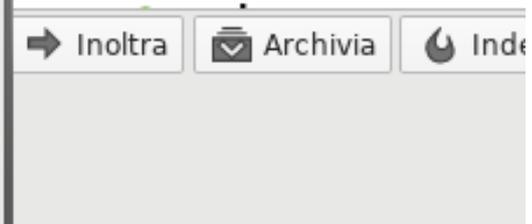
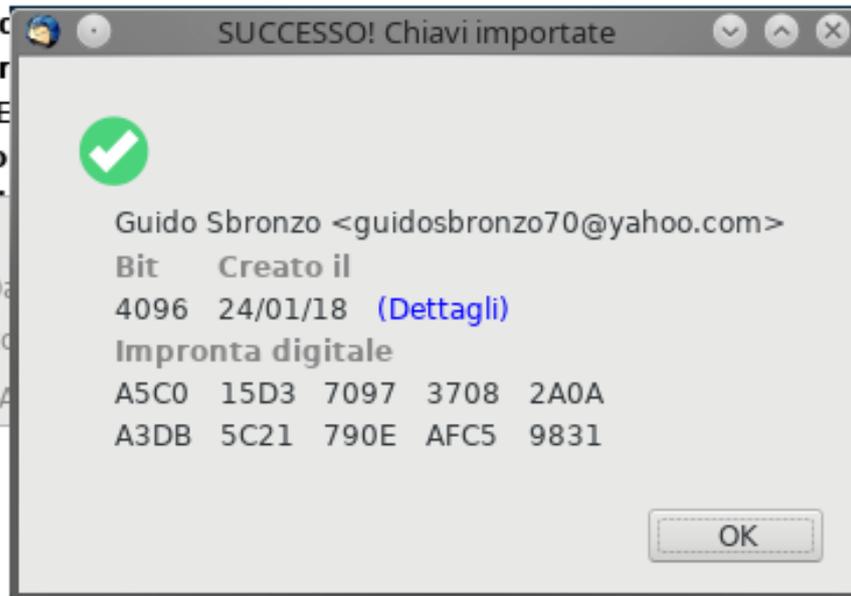
Dggetto...

Da...

Dggetto...

A...

- Unieuro Club
- Guido Sbronzò
- Groupon
- Moritz Muehlenho
- Helplavoro.it
- Groupon Shopping
- Serena di Gazzett.
- GearBest.com
- Unieuro Club



- pi@a...acantho.net (v1)
- pi@comune.rimini.it
- rrivo (323)
- viati
- 359)
- 155)
- es (111)
- erata
- ata
- iderata
- orse
- ilitazioni
- e e Report (809)
- gmail.com (v1096)
- MAP
- rrivo (18222)
- a

| Non letti | Speciali | In rubrica | Etichette | Allegati | Corrispondenti | Data |
|-----------|----------|------------|-----------|----------|----------------------|-------|
| ★ | | | | | Guido Sbronzio | 15:43 |
| ★ | | | | | Unieuro Club | 15:31 |
| ★ | | | | | Guido Sbronzio | 15:29 |
| ★ | | | | | Groupon | 14:04 |
| ★ | | | | | Moritz Muehlenhoff | 13:22 |
| ★ | | | | | Helplavoro.it | 13:19 |
| ★ | | | | | Groupon Shopping | 12:56 |
| ★ | | | | | Serena di Gazzett... | 12:19 |
| ★ | | | | | GearBest.com | 11:59 |
| ★ | | | | | Unieuro Club | 11:53 |

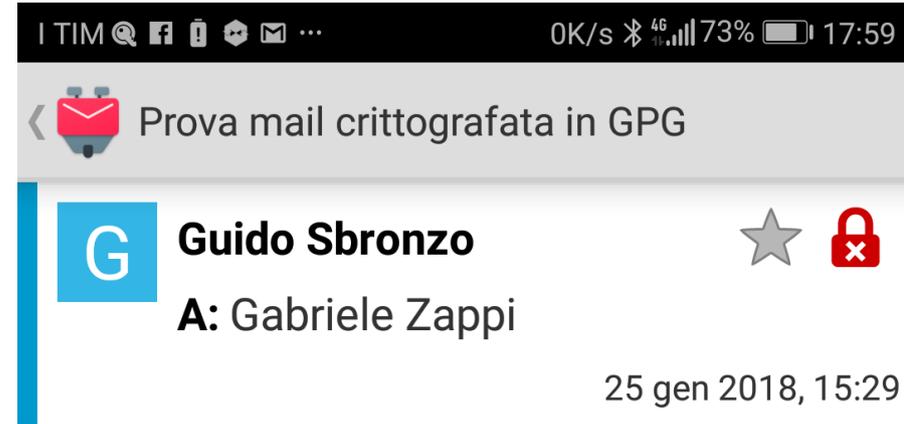
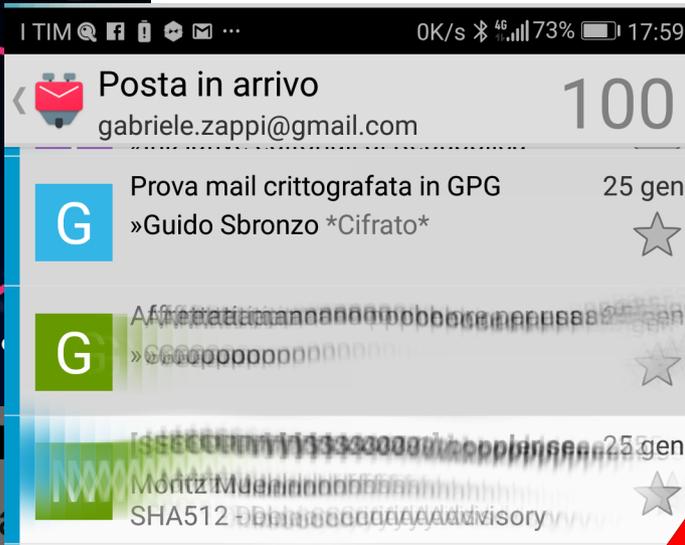
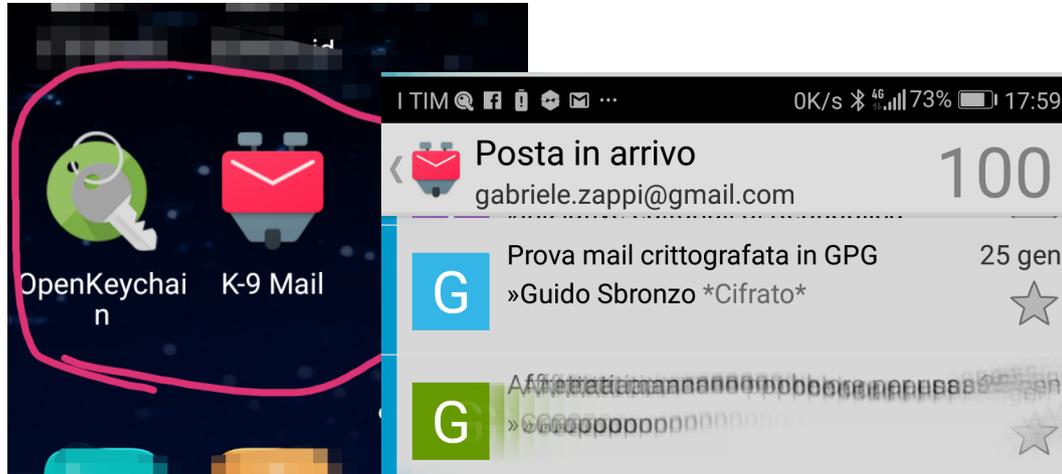

Rispondi Inoltra Archivia Indesiderata Elimina Altro

Da Guido Sbronzio <guidosbronzio70@yahoo.com> ★
 Oggetto **Prova mail crittografata in GPG**
 A Gabriele Zappi ★

Enigmail Messaggio decifrato; SENZA FIDUCIA Firma autentica per Guido Sbronzio <guidosbronzio70@yahoo.com> Dettagli

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam
 nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat
 volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation
 ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.
 Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse
 molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero
 eros et accumsan et iusto odio dignissim qui blandit praesent luptatum
 zzril delenit augue duis dolore te feugait nulla facilisi. Nam liber
 tempor cum soluta nobis eleifend option congue nihil imperdiet doming id
 quod mazim placerat facer possim assum. Typi non habent claritatem
 insitam; est usus legentis in iis qui facit eorum claritatem.
 Investigationes demonstraverunt lectores legere me lius quod ii legunt
 saepius. Claritas est etiam processus dynamicus, qui sequitur mutationem
 consuetudium lectorum. Mirum est notare quam littera gothica, quam nunc
 putamus parum claram, anteposuerit litterarum formas humanitatis per
 saecula quarta decima et quinta decima. Eodem modo typi, qui nunc nobis
 videntur parum clari, fiant sollemnes in futurum.

E in mobilità (Android) ?



Questo messaggio è cifrato

Questo messaggio è stato cifrato con OpenPGP.
Per leggerlo, devi installare e configurare un'applicazione compatibile con OpenPGP.

Scegli applicazione OpenPGP

Questo messaggio è cifrato

Applicazione OpenPGP

Nessuno

OpenKeychain

Inserisci la password per
'Gabriele Zappi'

.....

Remember until
cleared

ANNULLA SBLOCCA

I TIM 26B/s 65% 21:09

Inserisci la password per
'Gabriele Zappi'

.....

fino allo spegnimento dello schermo
per un'ora
per una giornata
until cleared

I TIM 0K/s 4G 73% 18:00

Prova mail crittografata in GPG



Guido Sbronzio

A: Gabriele Zappi



25 gen 2018, 15:29

Lorem ipsum dolor sit amet, consectetur
adipiscing elit, sed diam
nonummy nibh euismod tincidunt ut laoreet
dolore magna aliquam erat
volutpat. Ut wisi enim ad minim veniam, quis
nostrud exerci tation
ullamcorper suscipit lobortis nisl ut aliquip ex ea
commodo consequat.
Duis autem vel eum iriure dolor in hendrerit in
vulputate velit esse
molestie consequat, vel illum dolore eu feugiat
nulla facilisis at vero
eros et accumsan et iusto odio dignissim qui
blandit praesent luptatum
zzril delenit augue duis dolore te feugait nulla
facilisi. Nam liber
tempor cum soluta nobis eleifend option congue
nihil imperdiet doming id
quod mazim placerat facer possim assum. Typi
non habent claritatem
insitam; est usus legentis in iis qui facit eorum
claritatem



Le Mie Chiavi

3 chiavi

Gabriele Zappi
gabriele.zappi@gmail.com

G

Gabriele Zappi
gabriele.zappi@comune.rimini.it

S

Samuele Battarra
battarsa@email.it



Gabriele Zappi

Mia chiave



Healthy
No key issues found.

Pubblicato
Last checked: 12 nov 2017

Identità

gabriele.zappi@gmail.com
Gabriele Zappi
Chiave GPG principale personale di Gabriele Zappi

gzappi@libero.it
Gabriele Zappi
gzappi@libero.it



OpenKeychain

- Chiavi
- Codifica/Decodifica
- Apps
- Backup/Ripristina
- Secure Wifi Transfer
- Impostazioni
- Aiuto

Server (Linux)

- CLAMAV (+definizioni UNOFFICIAL)
SE SERVER MAIL:
- Amavis + Clamav + Blocco eseguibili e altre estensioni dannose
Privacy – Limitazione SPAM:
- (Greylisting) – Spamassassin - RBL

Uso di strumenti di crittografia, in storage locali.

- Gpg
- Veracrypt (truecrypt), CipherShed
- Encfs – cryFS
- Luks container (dm-crypt)

Uso di strumenti di crittografia, in Cloud pubblici.

- Proteggere i file più “sensibili” con crittografia (anche con gpg)
- Utilizzo delle tecniche di crittografia più adatte ai cloud (EncFS, CryFS, ..)

GPG

Lo stesso GPG può essere utilizzato come strumento di cifratura / decifratura sui singoli file, sia in modalità simmetrica, che asimmetrica.

ESEMPI PRATICI

Terminale

```
File Modifica Visualizza Cerca Terminale Aiuto
gabo@gabolaptop7 ~/.local/share/nautilus/scripts $ ls
pgp-out unpgg-out
gabo@gabolaptop7 ~/.local/share/nautilus/scripts $ cat pgp-out
#!/bin/bash
[ -z "$1" ] && { echo "missing parameter"; exit 1; }
pgp -c "$1"
gabo@gabolaptop7 ~/.local/share/nautilus/scripts $ cat unpgg-out
#!/bin/bash
[ -z "$1" ] && { echo "missing parameter"; exit 1; }
pgp -o "${1%.*}" -d "$1"
gabo@gabolaptop7 ~/.local/share/nautilus/scripts $
```

Android Sessioni

Get personalized job matches now

started  stackoverflow JOBS

Home test gpg arc1

| Nome | Dimensione |
|-------------|------------|
| aaa.mp3 | 3,4 MB |
| canzone.mp3 | 3,4 MB |

Recenti Home Documenti Immagini Musica

3 Please note the newer version of software is available

 **Passphrase:**
Inserisci la passphrase

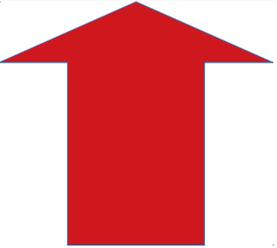
Password:

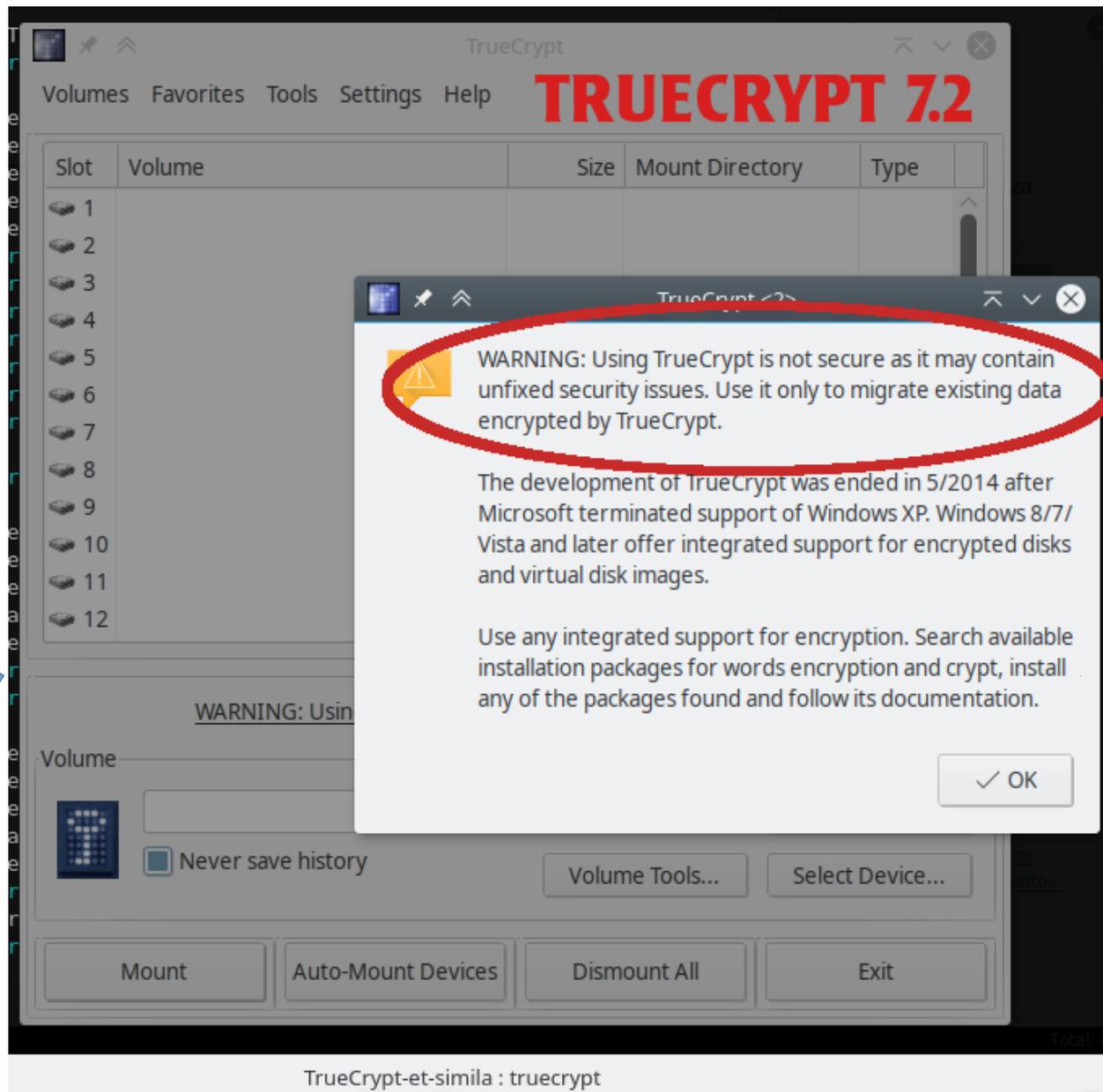
Save in password manager

Cancel OK

Home test gpg arc1

| Nome |
|-----------------|
| aaa.mp3 |
| canzone.mp3 |
| canzone.mp3.gpg |





Nato nel 2004, e sviluppo terminato nel 2014....

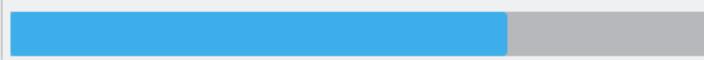
VeraCrypt

CipherShed

Volume Format

Random Pool: 4C33BC33456DB66D01CF1CF80E... Show
 Header Key: E126FC417F0803351A8C21ADB0...
 Master Key: 6FD883877CA563D49247FB7454...

Randomness Collected From Mouse Movements



Abort

Done Speed Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.



Volumes Favorites Tools Settings Help

| Slot | Volume | Size | Mount Directory | Type |
|------|--------|------|-----------------|------|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |
| 11 | | | | |
| 12 | | | | |

Volume

Never save history

paper-gtk-th
seafile
Telegram
Telegram De
TrueCrypt-et
Filtro:
6 file (29,4 MiB)

TrueCrypt-et-simila : bash

~/Scaricati/TrueCrypt-et-simila \$ 1

Enter password for "/home/gabo/test/archivioveracrypt.vc"

Password:

Use PIM

Cache passwords and keyfiles in memory

Display password

Use keyfiles

PKCS-5 PRF: Autodetection TrueCrypt Mode

veracrypt-1.21-setup-con... 2.8 MiB 09/07/17 11:10

veracrypt-1.21-setup-gui... 4.2 MiB 09/07/17 11:08

truecrypt-7.2-setup-x64 1.6 MiB 27/05/14 18:52

Filtro:

file (29,4 MiB)

VeraCrypt

Volumes Favorites Tools Settings Help

| Slot | Volume | Size | Mount Directory | Type |
|------|--------|------|-----------------|------|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |
| 11 | | | | |
| 12 | | | | |

Volume

Never save history

45,9 GiB / 142 GiB

TrueCrypt-et-simila : bash — Konsole
veracrypt1 — Dolphin

Trova Anteprima Dividi Terminale Rinom

/media/veracrypt1/

| Nome | Dimensioni | Modificato |
|----------------------------|------------|----------------|
| Materiale | 21 elem... | 20/01/18 13:53 |
| BiosPSW-cryptofs-Screen... | 38 elem... | 09/01/18 17:37 |
| Grub | 4 eleme... | 05/12/17 19:09 |
| LaSicurezzaLinux-1p (Co... | 18,1 MiB | 16/01/18 20:39 |
| LaSicurezzaLinux-1p.odp | 18,1 MiB | 16/01/18 10:25 |
| LaSicurezzaLinux-1p (Co... | 17,8 MiB | 15/01/18 22:50 |

Filtro:

3 cartelle, 3 file (53,9 MiB)

VeraCrypt

Volumes Favorites Tools Settings Help

| Slot | Volume | Size | Mount Directory | Type |
|------|------------------------------------|--------|-------------------|--------|
| 1 | /home/gabo/test/archivioveracry... | 5,0 GB | /media/veracrypt1 | Normal |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |
| 11 | | | | |
| 12 | | | | |

Create Volume Volume Properties... Wipe Cache

Volume

 /home/gabo/test/archivioveracrypt.vc

Never save history

```
1 gabo gabo 3626 gen
1 gabo gabo 487888 gen
2 gabo gabo 4096 gen
1 gabo gabo 50744 gen
1 gabo gabo 13460 gen
1 gabo gabo 1152 gen
1 gabo gabo 5835 gen
1 gabo gabo 483200 gen
1 gabo gabo 490 gen
1 gabo gabo 7419 gen
```

CipherShed

Volumes Favorites Tools Settings Help

CipherShed

Enter password for "/h...archiviocipher

Password:

Cache passwords and keyfiles in r

Display password

Use keyfiles

Key

```
laptop7 ~/Scaricati/TrueCrypt
on.cpp FavoriteVolu
on.d FavoriteVolu
on.h FavoriteVolu
on.o Forms
GraphicUserI
GraphicUserI
GraphicUserI
GraphicUserI
Hotkey.cpp
Hotkey.h
LanguageStr
LanguageStr
LanguageStr
LanguageStr
laptop7 ~/Scaricati/TrueCrypt
```

Main : ciphershed

CipherShed

ciphershed1 — Dolphin

Nome

- Juve-Gabo-
- ROD
- ClockSkin

Filtro:

3 cartelle

ciphershed1 — Dolphin

Volumes Favorites Tools Settings Help

| Slot | Volume | Size | Mount Directory |
|------|------------------------------------|---------|--------------------|
| 1 | /home/gabo/test/archiviociphers... | 1023 MB | /media/ciphershed1 |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 1. | | | |
| 1. | | | |
| 1. | | | |

Create Volume Volume Properties... Wipe C

Volume

/home/gabo/test/archiviociphershed.c

Never save history

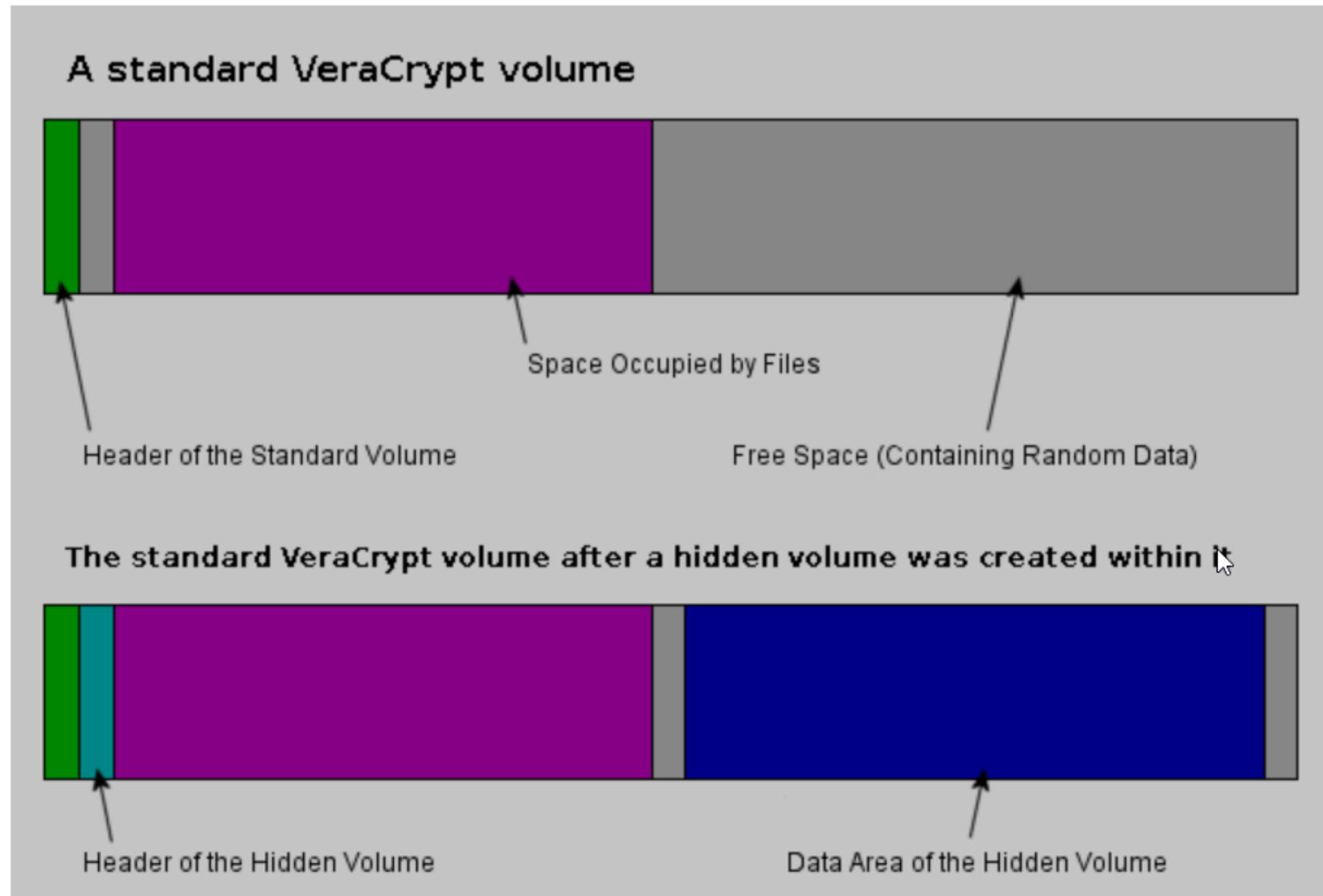
Volume Tools... Select D

Dismount Auto-Mount Devices Dismount All

Hidden Volume

Plausible Deniability

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.



The layout of a standard VeraCrypt volume before and after a hidden volume was created within it.

EncFS / CryFS

ESEMPI PRATICI

| | Volume Path | Mount Point Path | File System | Mode |
|---|-----------------------------|-------------------------------|-------------|------|
| 1 | /home/comune/Dropbox/EncCRY | /home/comune/.SiriKali/EncCRY | cryfs | rw |
| 2 | /home/comune/Dropbox/EncFS | /home/comune/.SiriKali/EncFS | encfs | rw |

SiriKali

Alphin

Trova Terminale

EncCRY

| | Dimensione | M |
|---------------------------|------------|---|
| ziaFiat.pdf | 5,5 MiB | 0 |
| MechanicalCode-Riattiv... | 733,3 KiB | 0 |
| ziaConvenz-Fiat.pdf | 5,9 MiB | 0 |

Certificato-Garan Fiat.pdf

Create Volume Mount Volume Refresh Favorites Menu

home

- backups
- comune
 - ~
 - 3CimeCertsUpdate
 - Android
 - AndroidStudioProjects
 - apktool
 - Audio
 - backups
 - Biblioteca di calibre
 - bin
 - blender_projects
 - c
 - com.fgol.HungrySharkEvolut
 - cpp
 - crypt
 - decrypted
 - Desktop
 - dlang
 - Documenti
 - Downloads

17 file (28,4 MiB)

40,1 MiB

40,4 GiB liberi

Version Info

"sirikali" Installed Version Is : 1.3.2.
Latest Version Is : 1.3.2.

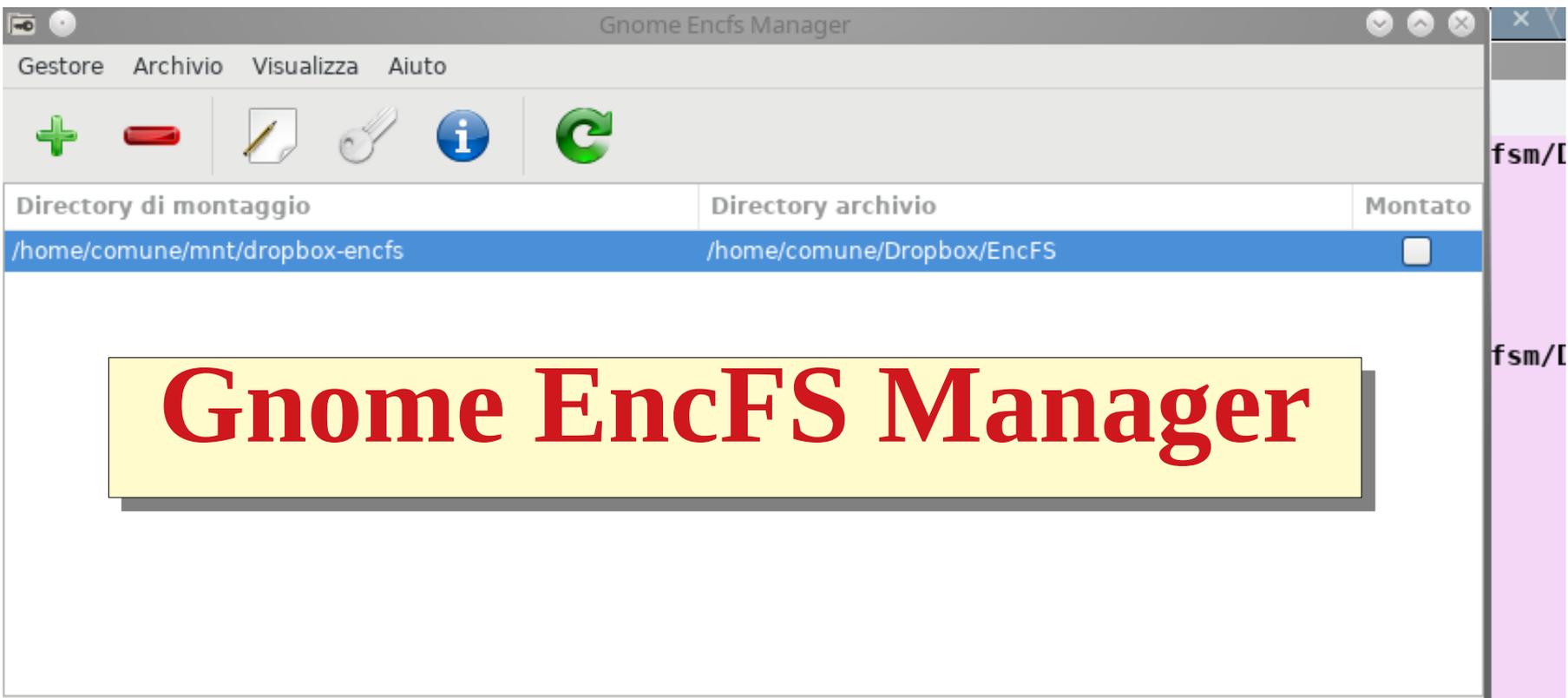
"cryfs" Installed Version Is : 0.9.8.
Latest Version Is : 0.9.8.

"gocryptfs" Installed Version Is : N/A.
Latest Version Is : N/A.

"securefs" Installed Version Is : N/A.
Latest Version Is : N/A.

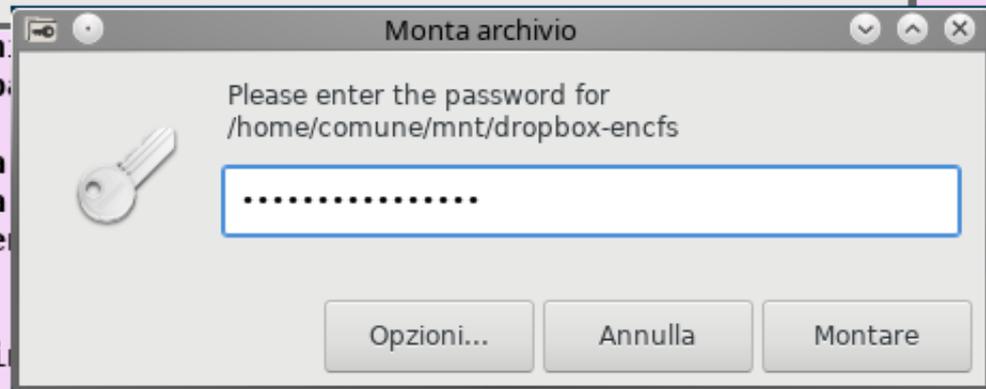
"encfs" Installed Version Is : 1.9.2.
Latest Version Is : 1.9.2.

Ok



 Puoi riordinare gli oggetti tramite drag and drop

```
E necessario scaricare 220 kB di arch.  
Dopo quest'operazione, verranno occup.  
Continuare? [S/n] S  
Scaricamento di:1 http://mi.mirror.ga  
Scaricamento di:2 http://mi.mirror.ga  
Scaricamento di:3 http://download.ope  
[186 kB]  
Recuperati 220 kB in 0s (885 kB/s)  
Selezionato il pacchetto libnotify-bi  
(Lettura del database: 615116 file
```



EncFS MP

HOME DOWNLOAD NEWS DOCS - WINDOWS DOCS - OS X

WELCOME TO THE ENCF SMP PROJECT HOMEPAGE

This is the homepage of EncFS MP, a program to mount EncFS folders on Windows and OS X.

Features of EncFSMP:

Aggiungi ad Accesso rapido Copia Incolla Copia percorso Incolla collegamento Sposta in Copia in Elimina Rinomina

Appunti Organizza

Questo PC > DB-EncFS (X:)

- torrents
- Txt
- ubuntu
- Videos
- webogram-master
- WinApps
- www
- XCF

Nome

- AWS
- Documenti
- ggg
- LG D605 Cris
- Scansioni
- 20150106_152312-EFFECTS.jpg
- 20150106_152726.jpg
- 20150106_170430_001.jpg
- 20150106_170612.jpg
- 20150106_170930_001.jpg
- 20161017_160454.jpg
- loremipsum.txt
- tim.sql.bz2
- tim_db.tar.xz

EncFS MP

File Tools Options Help

Create new EncFS Open existing EncFS

Mounts

| Mounted | Name | EncFS path | Drive |
|---------|----------|-----------------------|-------|
| Yes | DB-EncFS | D:\Gabo\Dropbox\EncFS | X: |

Unmount Remove Edit

Browse Show Info Change password

EncFS MP (Win)

About EncFS MP x64

EncFS MP x64 0.11.1

© 2017 Roman Hiestand

Mount EncFS folders - multiplatform style.

Built with: GCC 4.7.1

Linked with:

- wxWidgets 3.1.0
- EncFS 1.7.4
- OpenSSL 1.0.2l 25 May 2017
- boost 1.64.0

Pismo File Mount version found: pfm.1.0.0.190

Icon © by Oxygen

OK

| Metodo \ Target. | Adatto uso STORAGE LOCALE | Adatto uso CLOUD |
|---|---|---|
| GpG on single file Altri tools "file-based" cryptography |  |  |
| GpG on directory |  |  |
| Truecrypt derivatives (Veracrypt, CipherShed) |  |  |
| EncFS - CryFS |  |   |
| LUKS/dm-crypt |  |  |

Un ringraziamento a Roberto Gamberini, per aver dato l'idea di questa presentazione

Fine dell'intervento.

Domande? Curiosità?

A close-up photograph of a woman with brown hair and bangs, smiling warmly. She is holding a white rectangular card in front of her face, which partially obscures her eyes. The card contains contact information for Gabriele Zappi.

gabriele zappi

gabriele.zappi@gmail.com