Primer Numero

ADVERTENCIA

Un dels primers preceptes de la seguretat informàtica es que no hi ha res 100% segur. Aquest document conté una serie de recomanacions pensades per a que usuaris inexperts puguin adquirir una serie de coneixements per a que les seves conversacions a través de la xarxa siguin més segures i més difícilment interceptables.
Tot hi això, si estem utilitzant algun **sistema operatiu intervingut,** ja sigui per algun keylogger (programa que enregistra les pulsacions del teclat) o troià, com per alguna **mala configuració de l'equip** (geolocalització activada entre d'altres) o per alguna **mala *praxis*** (com introduir dades personals o falles humanes de seguretat [com dir les contrasenyes]) faran que aquestes mesures de seguretat no serveixin de res.
Per tant, aquest document, es basarà sobretot en **donar conceptes bàsics sobre com encriptar la informació i amagar-nos per Internet.** Sempre d'una forma molt bàsica i a nivell d'usuari.

INDICE----------

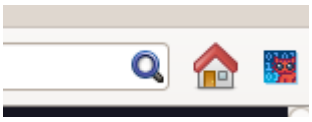
Cryptocat

Cryptocat és una aplicació web de codi obert de moment només disponible per Chrome, Mozilla, opera i Safari.
Cryptocat, que encara està en fase de desenvolupament, permet obrir sessions de xat on la informació viatja encriptada entre els usuaris amb una clau única.

Per instal·lar-ho accediu a aquesta pàgina:
https://crypto.cat/

Vídeo explicatiu del seu funcionament (per inexperts):
http://www.youtube.com/watch?v=bSjT-_y5Ioo

Com obrir una conversació?
Al instal·lar-ho us apareixerà un icona com aquest a la part superior dreta.
Al fer-hi click accedireu a l'aplicació:



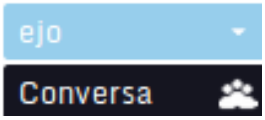
Per **crear** una conversa s'escriu el nom de la conversa a crear i el nom d'usuari.
Per **accedir** a una conversa creada s'ha de ficar simplement el nom de la conversa on es vol accedir i un nom d'usuari.

Un cop la conversa es creada, per a que la informació no la pugui veure ningú més, s'ha d'accedir a la conversació privada. Per això s'ha de fer click al nom

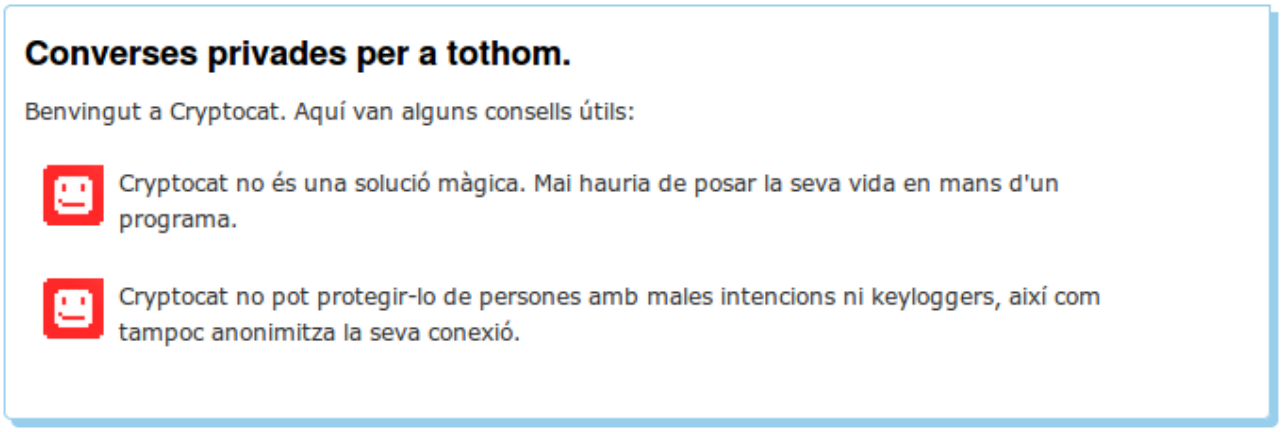
de la persona amb la que es vulgui mantenir el xat en privat.

Conversa per a tots els usuaris

Conversa privada



Aquí es veu com el nom d'usuari queda marcat i en la part superior quan estas en la conversació privada.
Fixeu-vos en les recomanacions que dona cryptocat:



NOTA: En el següent enllaç podem veure com xifrar les nostres conversacions de xat amb Pidgin i OTR. Amb aquest software podem configurar la nostra conta de Facebook o Gmail. De totes maneres, l'altre persona ha de usar el mateix mètode per a que la comunicació sigui realment encriptada
http://rafael.bonifaz.ec/blog/2013/03/chat-encriptado-con-pidgin-y-otr/

Claus PGP

Introducció:

PGP es un acrònim de Pretty Good Privacy. Es un sistema de xifrat consistent en un parell de claus (una pública i una privada) que permeten encriptar un arxiu o un text.

El funcionament es el següent: cada usuari te un parell de claus, una **pública** que mostrarà a tothom, i una **privada** que només coneixerà ell.

Quan algú vol enviar un missatge a l'usuari A, encripta la informació amb la clau pública de A.
L'usuari A rep la informació encriptada amb la seva clau pública que només pot ser desencriptada amb la seva clau privada (que només coneix ell).

Aquesta es la teoria del funcionament de les claus PGP que són molt útils en casos com, per exemple, enviar un correu electrònic sense que es sàpiga el que s'ha escrit.
Per altra banda les claus PGP també serveixen per signar correus i verificar la identitat d'aquell que l'envia.

Atenció: s'ha d'afegir que si no es té guardada la clau privada en un entorn segur, la encriptació no es segura. Això es degut ja que qualsevol que tingui la vostra clau privada podria desencriptar els vostres correus, per tant es igual d'important, per a que el medi sigui segur, de quina manera emmagatzemeu la vostra clau privada.

Hi ha diverses maneres d'aconseguir i gestionar les claus PGP:

- GPG (software)
- Generadors de claus online: http://www.igolder.com/pgp/generate-key/
- Extensions del explorador com: http://www.mailvelope.com/
- A través de gestors de correus com thunderbird
- Altres ...

Per encriptar arxius via PGP:

- Sobre Windows GnuPGK o GPGShell
- Sobre Linux Seahorse (interfície gràfica) (+ info)

Una de les formes més clàssiques d'encriptar el correu és a partir del gestor Thunderbird i del seu complement Enigmail que és la que utilitzarem aquí. Tot hi això, qualsevol de les formes dalt esmentades pot ser vàlida, ara comentarem per sobre algunes d'elles:

- Mailvelope: funciona com una extensió de l'explorador per a que puguis gestionar, crear i utilitzar parells de claus PGP. Força senzill de fer servir.

- Seahorse: ens permet encriptar arxius amb PGP fàcilment des de submenús a l'explorador i l'escriptori. Tot i que la encriptació d'arxius amb PGP és prou interessant, no és la més segura. És preferible utilitzar altre software com Truecrypt.

Instal·lació i configuració de thunderbird i enigmail:

Necessitarem el programa thunderbird i una extensió anomenada enigmail.
Per instal·lar thunderbird podem seguir els passos explicats als següents llocs:

- Ubuntu
- Debian
- Windows (per instal·lar enigmail i GnuPGP a Windows seguir aquest enllaç)

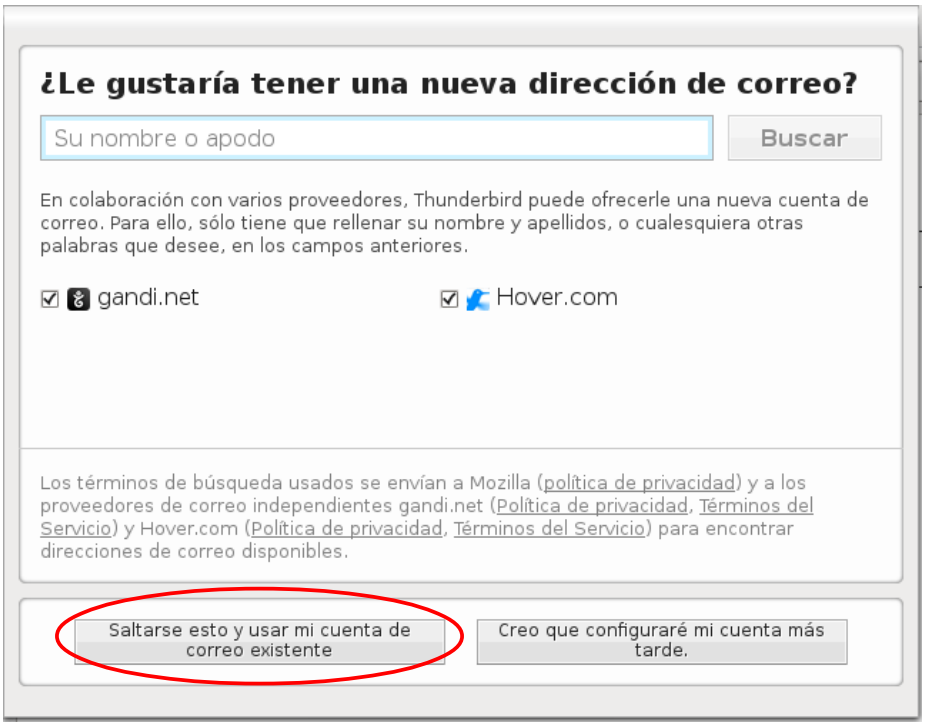
O simplement, per a Ubuntu executar:

```
sudo apt-get install thunderbird enigmail thunderbird-l10n-es-ar
```

I per a Debian:

```
sudo apt-get install icedove enigmail icedove-l10n-es-ar
```

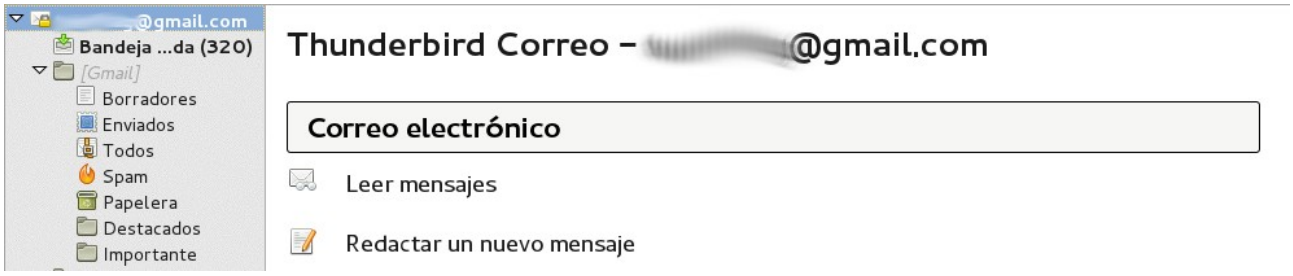
Un cop instal·lat executem el programa que iniciara un assistent:



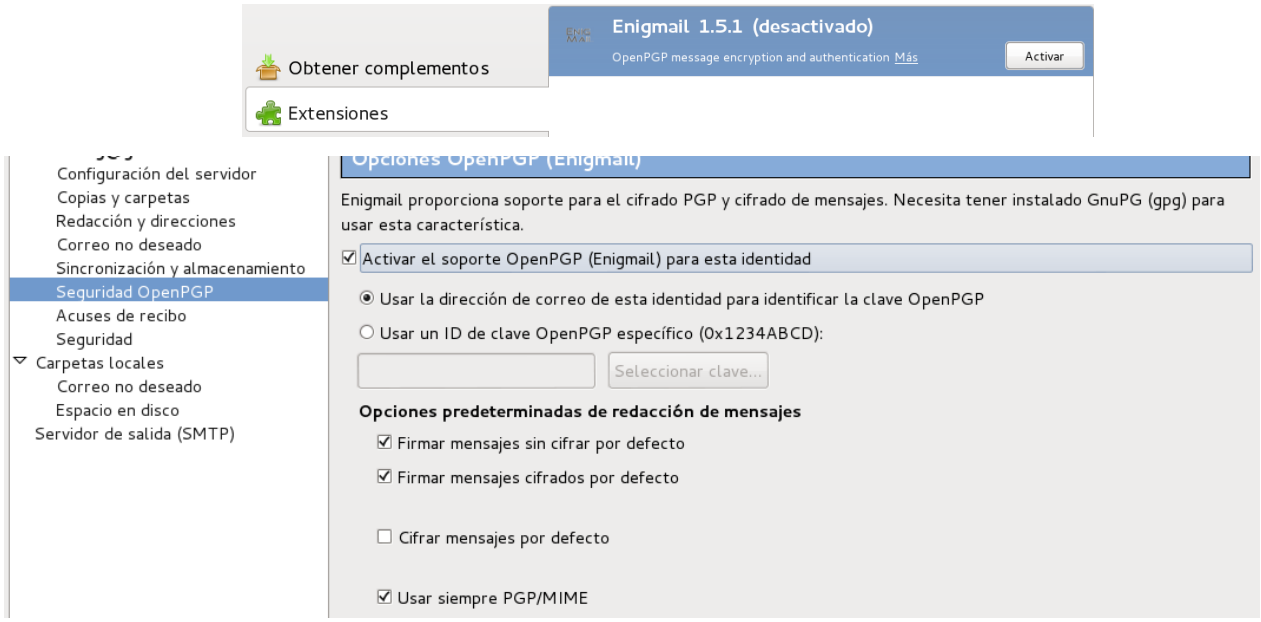
Seleccionarem la opció "*Saltarse esto y usar mi cuenta de correo*"

Posarem les nostres dades i la contrasenya del nostre correu, **cal remarcar que també accepta riseup:**

Un cop això ja tindrem configurat el Thunderbird per a que funcioni amb el nostre correu. Podrem escriure, veure els nostres missatges i carpetes etc...

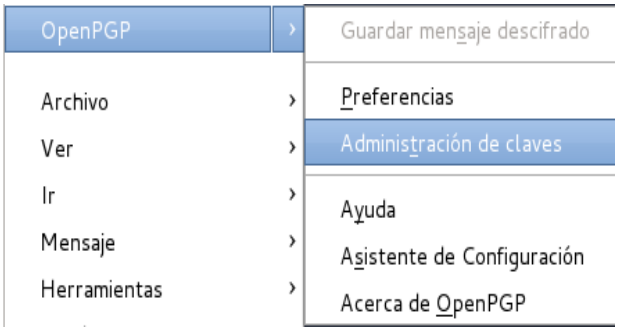


Anem al menú i seleccionem “complementos” per activar el enigmail.

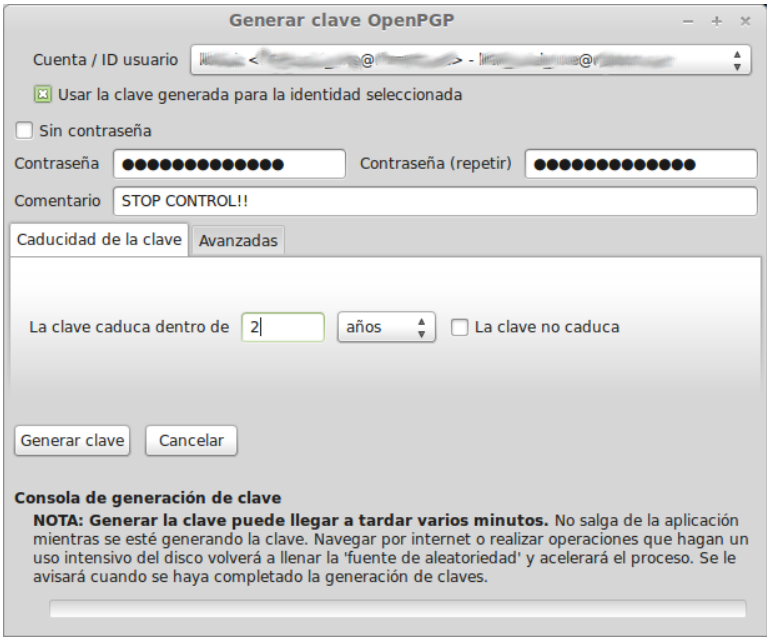


Reiniciem el Thunderbird i ja podrem utilitzar l'Enigmail. Primer, clicarem amb el botó dret a sobre del nostre correu i accedirem a la configuració de la conta. Allà anirem a la opció *seguridad Open PGP* i activarem la seguretat per la nostra conta:
Activant les opcions de firmar missatges s'afegira la nostra firma PGP a cada missatge que enviem. **Quan firmes un missatge estàs introduint una informació en el missatge que valida la teva identitat**, i assegura que el missatge ha sortit del remitent esperat. D'aquesta manera, si algú modifiques el teu missatge o intentes suplantar la teva identitat, es veuria reflexat en una firma digital errònia.

Ara tornarem a accedir al menú, on apareixerà una nova opció: Open PGP, l'obrirem i executarem l'administrador de claus.



Un cop obert en el menú superior accedirem a *Generar>Nuevo par de Claves.* Allí configurarem de la següent manera:



Seleccionarem la conta a la que volem associar la clau. On contrasenya ficarem una contrasenya que s'utilitzarà per la generació de la clau i que serà necessària per desencriptar els correus (recordem que les contrasenyes son més segures quan son alfanumèriques i mesclen majúscules, minúscules i símbols).
Les claus PGP poden tenir data de caducitat, això es bo i útil: imaginem-nos que una dels nostres parells de claus PGP queda en un disc dur antic que acaba en mans d'un desconegut, i decideix utilitzar-les, suplantant la nostra identitat. Al tenir data de caducitat, les claus van quedant inservibles amb el temps.
En el comentari es una petita informació que acompanyara les nostres claus

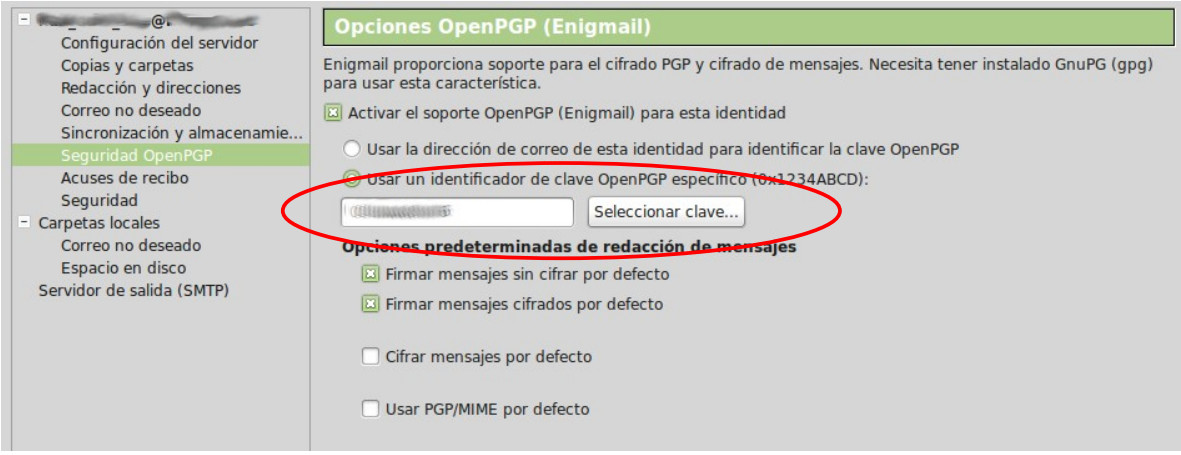
Anem a avançades i configurem el xifrat, augmentant la grandària de la clau al màxim, per augmentar la complexitat del xifrat .

Acceptem, ens demanarà confirmació i esperem.

S'han de fer complicats i increïbles càlculs per generar el parell de claus!! Haurem d'esperar una estona fins a que finalitzi.

Durant el procés ens demanarà si volem crear un certificat de revocació. Serveixen per a que els servidors de claus PGP (que emmagatzemen claus públiques d'usuaris, ja siguin privats o empreses o institucions, per a que siguin fàcils de localitzar), esborrin la clau emmagatzemada. La clau de revocació la podrem generar quan vulguem.

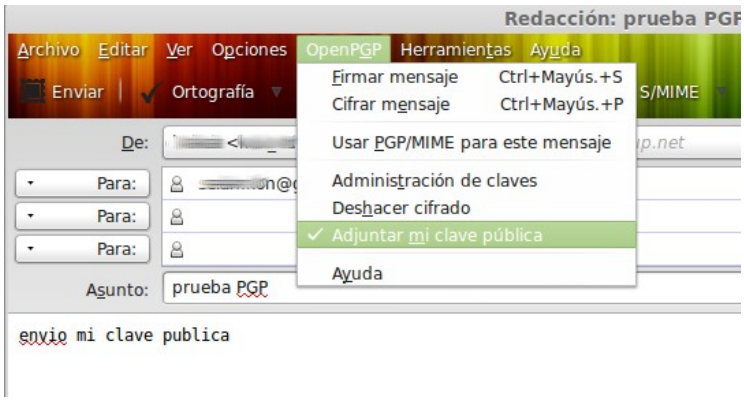
Un cop finalitzat podem comprovar que la clau s'ha associat a la nostra conta i ho configurarem de la següent manera:



Firmant i encriptant correus

==> Com firmar

Una vegada tenim la nostra clau l'hi hem de fer arribar a algú, per a que ens pugui enviar els correus encriptats. **La nostra clau es guarda en un arxiu, així que li podem passar per USB (o altres medis) o directament com a adjunt en un correu**, tal i com es mostra en la imatge de sota:



També podem modificar les opcions per xifrar o firmar el missatge:

- **Firmar el missatge**: s'adjunta, al final del missatge, la nostra clau PGP. Serveix per veure que el qui ha escrit el missatge som realment nosaltres.
- **Xifrar el missatge**: serveix per encriptar el missatge amb la clau pública del destinatari.

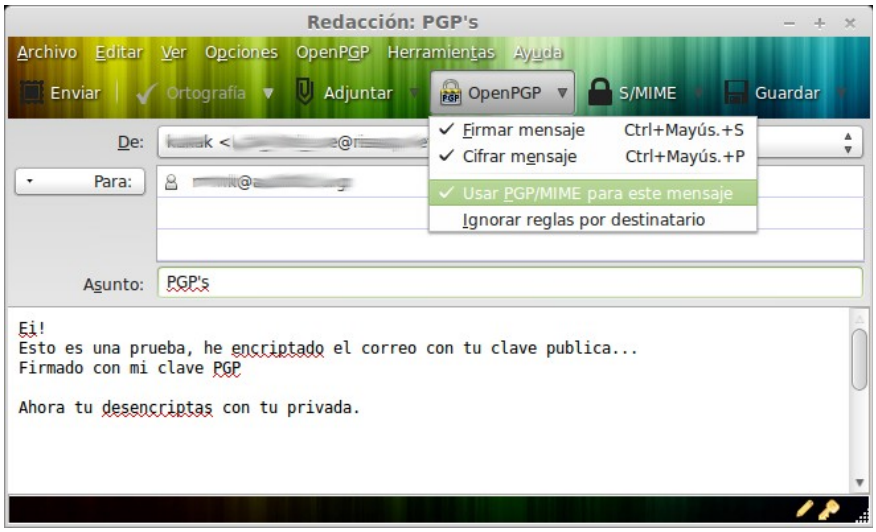
Com que encara no tenim la clau de ningú només el firmarem. El receptor rebrà un missatge de les següents característiques:

La part que es veu borrosa, es realment, la nostra signatura. **Quan firmem un correu estem afegint una marca de temps al correu, per tant si aquest fos modificat, no es podria verificar la signatura.**

Quan rebem un correu al que s'ha adjuntat una clau pública la podem descarregar en un arxiu i agregar-la al nostre administrador de claus, on seleccionem *“importar clau des d'un fitxer”,* quedant així agregada al nostre administrador.

==> Com encriptar

Una vegada disposem de la clau pública d'algú, ja podem enviar-li missatges encriptats que només ell podrà llegir. Per això anirem a redactar i seleccionarem tal i com es mostra a continuació:



Ja hem vist la diferencia entre xifrar i firmar. Podem comprovar que a la part inferior dreta es veuen dos icones, el llapis es per indicar que estem firmant, i la clau es per indicar que estem encriptant.
Automàticament encriptarem amb la clau pública associada al nostre contacte.

Quan ens arribi la resposta (encriptada amb la nostra clau pública) nosaltres veurem un missatge semblant al següent:

```
-----BEGIN PGP MESSAGE-----
Charset: UTF-8
Version: GnuPG v1.4.12 (GNU/Linux)
Comment: Using GnuPG with Icedove - http://www.enigmail.net/

hQIMA14GWQuB8a8/ARAAmaGRPufFAnv41Mqv0hRnVSl11AhUeshexmp7xoBC9Vji
Qy3e6M0mxVuvp7cVPcPeltUuUgl3jPMnnzbFSuzzexEYsHC7Ah4q9qyz6UBNLXtm
W6WgLuPPpJTHF8yd5fP1L/XQ/OHMWEkVmhLx2DHGomuYXF0INwxIqQDqsWSeONaU
gid2kbMYam6Xof/CkE+e8jKWOKTlhorB6FZTRdtwUsNktqysyhOVqIRTvDTyhTA1
IQ53aK0sRaoZOCCK2uM6RfKBDbBYKR55PAcDATWNYjZo7970EsN2RWWQjOKWKgxf
5GXxZuoALXx+ydgHyT5IIGZKEiL0N2SNDSyVgabUqqujr2j26v5ANXeFmK6p7Djt
IWaNEmit4XAfaF/Fqdbu+NYQyOkQvKpVxbsn07iUorp8ysISTOXVaqa4WIeKVbGO
5aa+souDwYjRUDEQqC02J4cShIdATSTZNeMF3HSSPS9+2gJBUBcjlRn+s33G9Sp3
n74pAJ34PQEIqats3ds/cbEDEB2JxdccrWKOVk4x+Esz7uMvHKCrTVroUx+wS7MT
avF043/vzuO1oV0tlXX/PEhWSCyscJRgnLFG8Mdmd1wPhGgArQifQsRMlPifonF5
LFwW/qIuRwwkMFMMj57gcDnx1zCEAx0WPWnXt/pZFFePuFLT6p3FqScb0uB70KaF
AQwDZwFh4bCWWlgBCAC+7nCJHVmq7QEeiPFdVtLAx9qgz4d1FIsGKoyzOVKCH9Ma
yfLpjU0G2OnoTUVgBhFAPzGN3YfZl/LmuvxduPZBWb6o1dqZvEe/lZHtW+GuJYNX
m2NdZ/pP9d1WCUQiiH3nFe7rM9ea3zynDFrFaUjPa/K1NLIuS3HEw3gmwQ58uzlf
DwSp9VvlwPFJLRjucd2MeTNGYgVablfOFikL1fzh1NhbP/BcTWeKaItMPv9StWoG
sSXWIEfVSZdJ/TvcVnl0zNnEuT1n4R35J9yQ/vq2UqxyNHSsUwEvVR+hb4C8m5va
naIUIGgnGtzSy5wX1vPAZFVx+lquuh2V588Z5maW0sDfARFf2zmxLjZSXGjRAfTw
HlbfJlEvtmPKxSrTAYzVhV31scn1Qu7WXuFl59TCYGsP851D+oCtc21xzM/+JSSR
4/WlxXZCnO22r8sDyIY+g05WZ680gTCu4eNp1GpMbX2KMOv8gBt3RCsETuxprtRv
ue0UUlrZP8tJ6V06sf2jlo2oeBQwVnB62m9hOmdjgiRZY7OAl2MyVwnQvRzzaI0C
VyKA4BqAHqTS7Ll9zKjb7EH6fEAyNIS0BQRj9iGZIc6FDohWdlRHtvCR3un7dwal
ZRWBeG/qGGlnCTg/ny4RiTUg7v0TUC/fTNSD1l62yOgYkj9hsgLCPjz7g1W1Kbum
ED3x6It6vHwMhYf6UKwBl5scCDBzXv4OZjnLcBL2QtTc2sOG85NypmY640QNyP05
KDpGq9ws4iMbAte/mJcrFXY/maOhVogZE/CoBmtijgSnTRq6b0Z53//DGMzs0Hus
KkNE53QdcLdA7/Pmg9AtWmvqCAzjXv2SqG3lxn7FydJ/AGjJ2Xz2RqjYqtvZIq7G
vo3n1LXS5rifXvJZfiJuIg==
=MVln
-----END PGP MESSAGE-----
```

Això no es res més que la resposta encriptada de forma màgica! Per desencriptar només haurem de fer clic al icona de desencriptar i **introduir la contrasenya que vam introduir per les nostres claus PGP.** D'aquesta manera podrem veure el missatge:

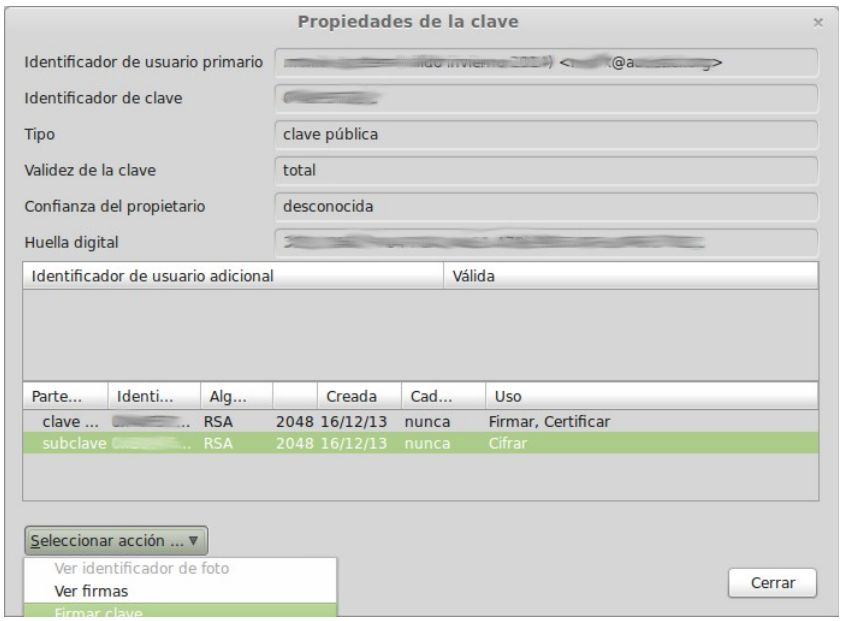
Exacto, a mi me pide mi calve privada que descodifica mi clave publica
con la que tu has encriptado el correo.

Salut!

On 18/12/13 23:56, [redacted] wrote:
> Ei!
> Esto es una prueba, he encriptado el correo con tu clave publica...
> Firmado con mi clave PGP
>
> Ahora tu desencriptas con tu privada.

==> Firmar claus alienes

També podem firmar la clau d'algú per verificar la seva identitat d'avant d'algú altre.
Per exemple, nosaltres tenim una relació de confiança amb dos persones, la Cospedal i en Puig, i sabem del cert que les seves claus son verídiques. Aleshores la Cospedal vol enviar-li un correu encriptat a en Puig, però no te la seva clau pública i no se'n refia de que la comunicació pugui ser interceptada, per tant si en Puig li envies la seva clau pogués ser modificada. Per això ens demana a nosaltres que l'hi enviem de forma segura la clau d'en Puig, ja que la nostra clau sap del cert quina és. Per això nosaltres anirem a l'administrador de claus, farem doble clic a la clau que volem firmar i sel·leccionarem la acció "*firmar clave*".



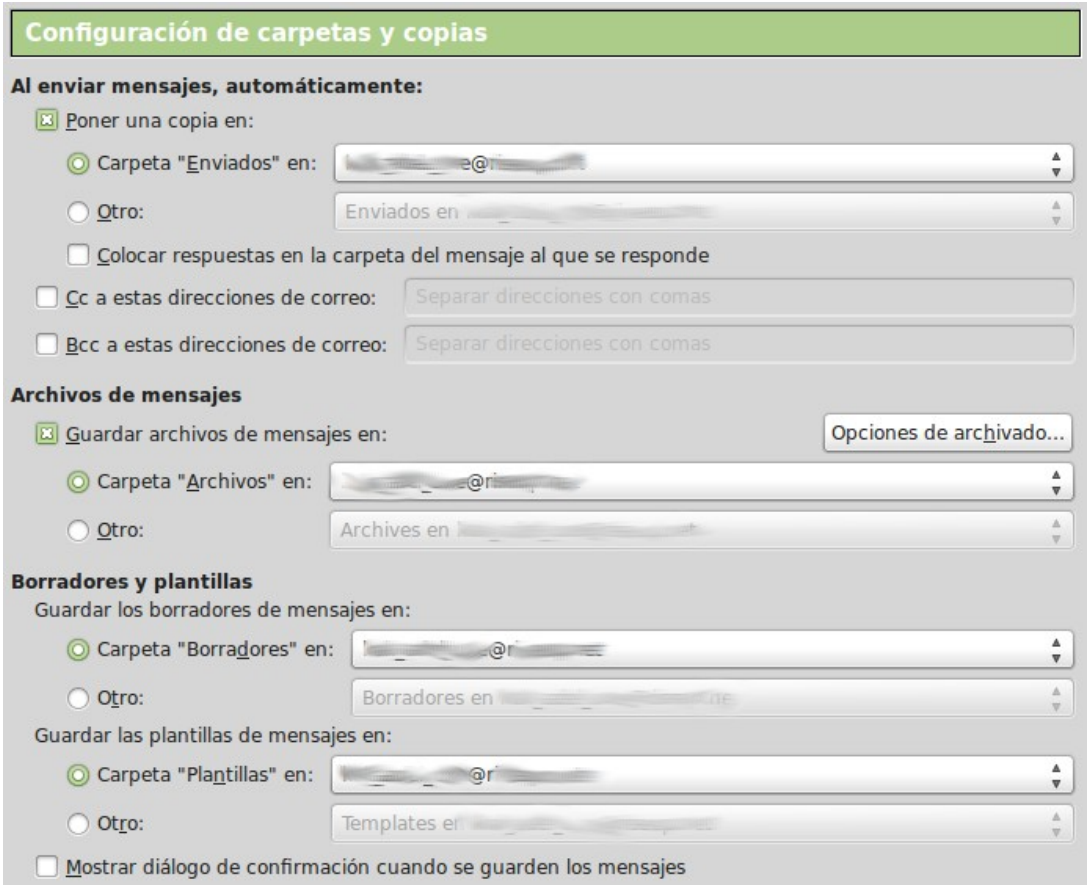
Ens apareixerà un formulari que acceptarem i ja tindrem la clau firmada i preparada per l'enviament. Quan redactem un correu, al menú "*OpenPGP*" podem seleccionar la opció "*adjuntar la clave pública*" per enviar-la.

Apunts de seguretat per a Thunderbird

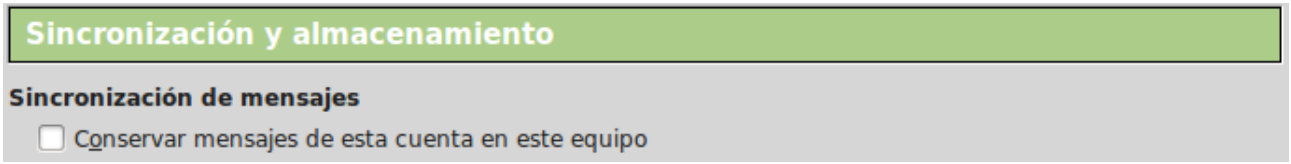
Una vegada ja disposem del nostre parell de claus i enviem correus signats i encriptats, encara podem millorar la seguretat del Thunderbird

==> Configuració

Per començar configurarem que no es guardin al disc dur del nostre ordinador els correus electrònics. A la configuració de la conta accedirem a:

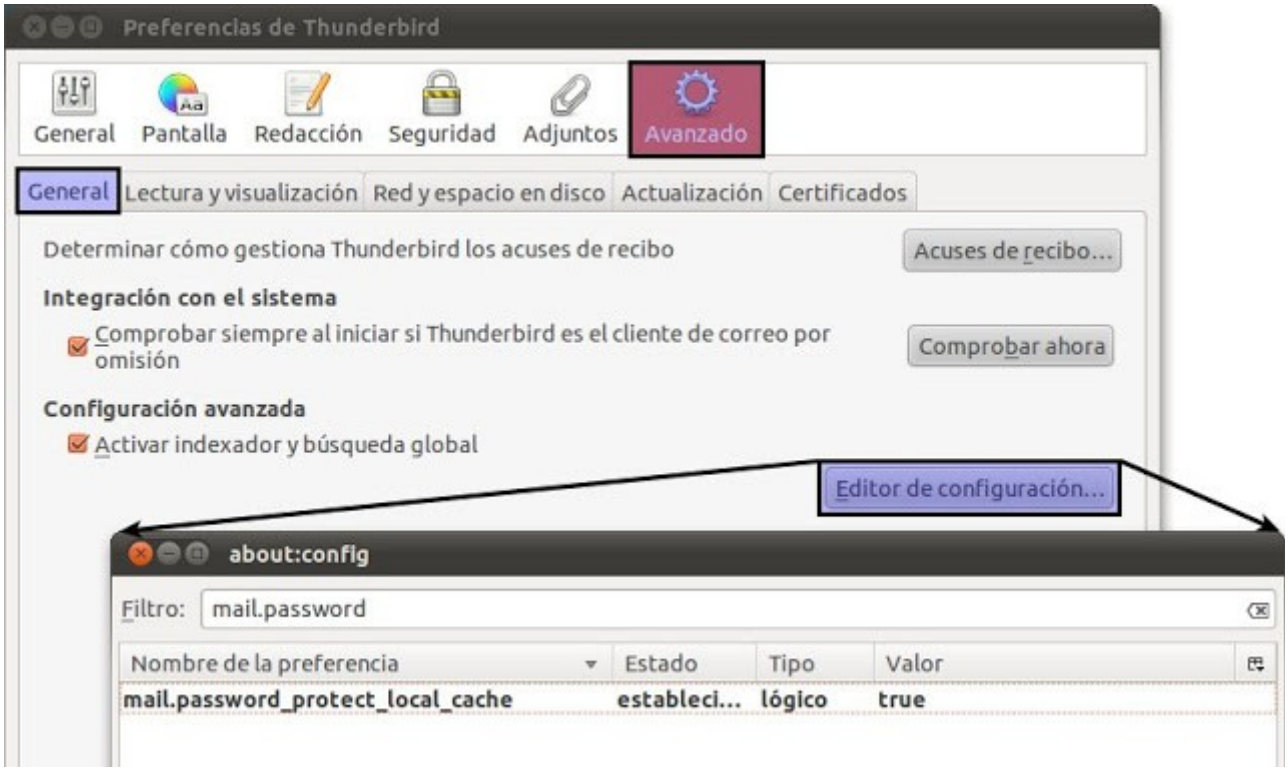


Configurant que tot es guardi al nostre correu electrònic.
I a “sincronización i almacenamiento” configurarem el següent:



També hi ha un petit problema a solucionar: **al obrir el Thunderbird, apareixen els missatges que ja havíem obert o que ja teníem descarregats a la memòria del programa**. Per a que no es puguin veure sense haver ficat la password primer crearem una contrasenya mestra de la següent manera, al menú de *preferencias*:

I seguidament *avanzado > general > editor de configuración* i cambiarem el valor de false a true.



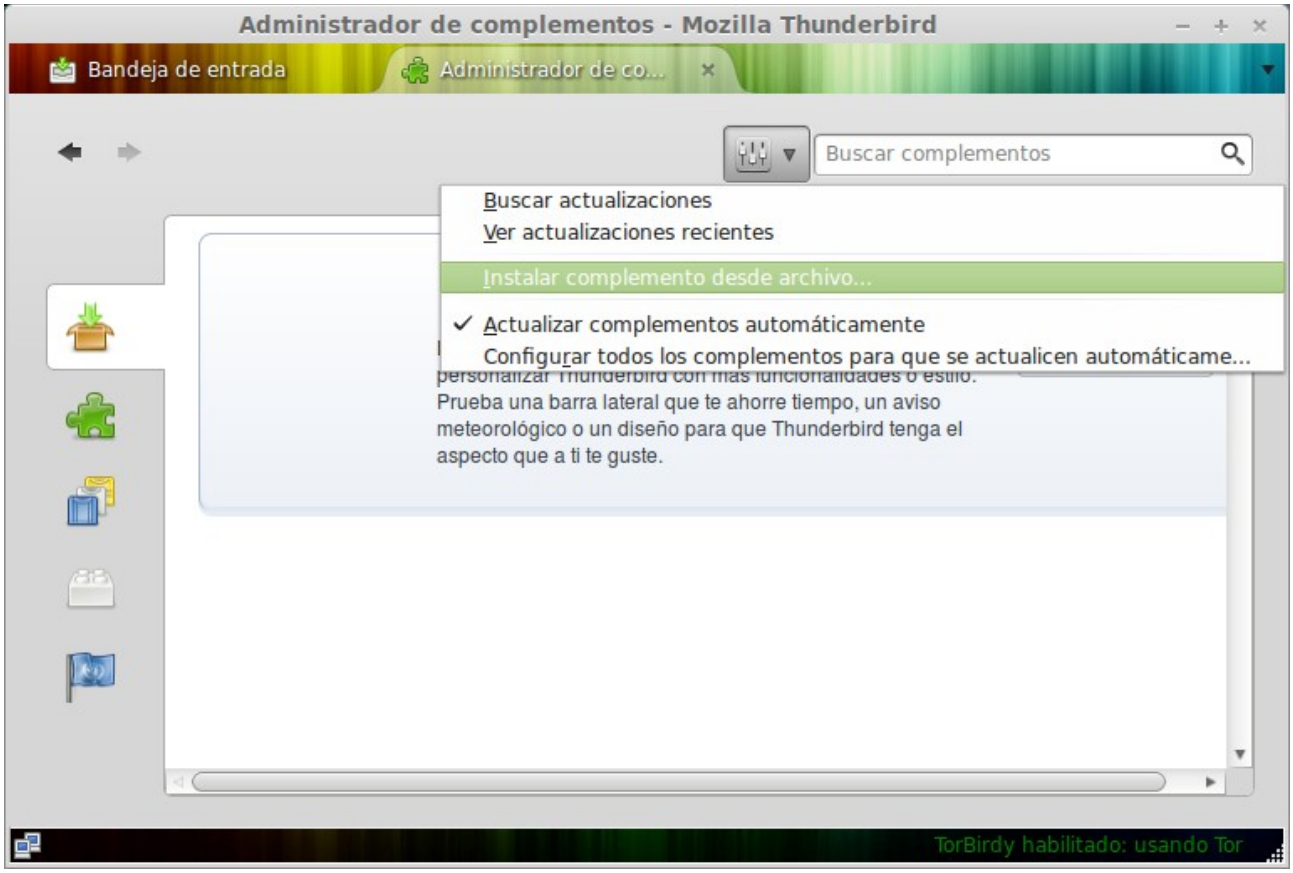
==> Navegació anònima

Hi ha diverses maneres de fer que Thunderbird amagui la nostra identitat a l'hora de connectar-se al servidor de correu preservant així el nostre anonimat. No explicarem cada una d'elles, ni profunditzarem en el funcionament, això ho deixarem per una futura entrega o per l'autoaprenentatge del lector.
Una de les maneres es fent la connexió a traves d'un **proxy**, això es podria configurar amb la extensió *FroxyProxy.* Però nosaltres no utilitzarem aquesta, hem escollit un altre mètode: **fer que tunderbird es connecti i navegui a través de la xarxa TOR.**

Per fer-ho haurem de descarregar l'extensió de la següent pàgina:

https://addons.mozilla.org/en-US/thunderbird/addon/torbirdy/

Aleshores seguirem les instruccions d'instal·lació: anirem als complements del thunderbird i seleccionarem la opció d'instal·lar complements des d'un arxiu tal i com es mostra en la imatge.



Haurem de reiniciar el Firefox per a que la instal·lació es finalitzi. De totes maneres, no navegara per TOR si el nostre ordinador no està preparat per a fer-ho, i per tant no descarregarà correus. Per a que TorBirdy funcioni correctament haurem de descarregar el *TorBroserBundle* de la següent pàgina:

https://www.torproject.org/

Quan el descarreguem, descomprimirem l'arxiu clicant amb el botó dret i seleccionant la opció *extraer aqui*. S'obrirà una carpeta on haureu de buscar l'arxiu *star-tor-broser*. Aleshores l'haureu d'executar.

Per a la gent que utilitzi linux, es molt provable que l'hi hagueu de donar permisos d'execució. En aquest cas, amb el botó dret *propiedades* > *permisos* i marcar la casella de permetre executar-se com un programa.

Un cop fet, una finestra com aquesta s'obrirà:

Això ens indica que ja estem connectats a TOR i que el TorBirdy funcionarà correctament.
En versions a partir de la 3.5 en tindrem prou amb mantenir obert el Firefox que s'obre.

NOTA sobre TOR: lo anteriorment explicat resulta molt útil quan no volem que se sàpiga qui està utilitzant el correu (per exemple en els casos de correus utilitzats col·lectivament), per això amaguem la nostra identitat.
Per saber més sobre com funciona TOR, i perquè amaga la nostra identitat i naveguem d'una forma més segura, es pot visitar el següent enllaç:

http://www.genbeta.com/seguridad/como-funciona-la-red-tor

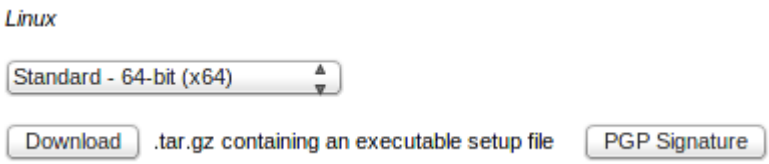
Truecrypt

Truecrypt es un software que utilitzem per encriptar arxius o inclús disc durs sencers. Això significa poder tenir arxius a l'ordinador sense perill de que ningú pugui veure-ho. Això es útil en molts àmbits, doneu-li a la imaginació: des de actes d'assemblees fins a vídeos picants. Encriptant-los els estem protegint de qualsevol persona que tingui accés al nostre ordinador (ja sigui de forma física o a través de malware).

Truecrypt s'ha guanyat molta fama ja que a resultat ser un programa impossible de hackejar (de moment), tenint als omnipresent USA en una constant recerca per trobar-l'hi alguna vulnerabilitat que li permeti desxifrar -lo.

Amb Truecrypt podem encriptar carpetes, USB, particions senceres i inclús particions ocultes. **Aquí veurem com encriptar i ocultar un volum ja que probablement es el que ens donara més seguretat**. Quan ocultem una partició encriptada, estem amagant la quantitat d'informació que conté i si existeix. Per tant, si volem encriptar i ocultar una carpeta de 100MB, a la carpeta contenidora no s'hi reflexarà aquesta grandària (per tant no hi ha manera de saber si realment existeix). Això es perillós, ja que **sense voler podem sobreescriure l'arxiu ocultat**, i perdre la informació. Per tant hem de calcular molt be la grandària que ha de tenir la carpeta.
Realitzarem tot el procés sota Linux.
Accedirem a la següent pàgina i seleccionarem el que més ens interessi en cada cas:

http://www.truecrypt.org/downloads

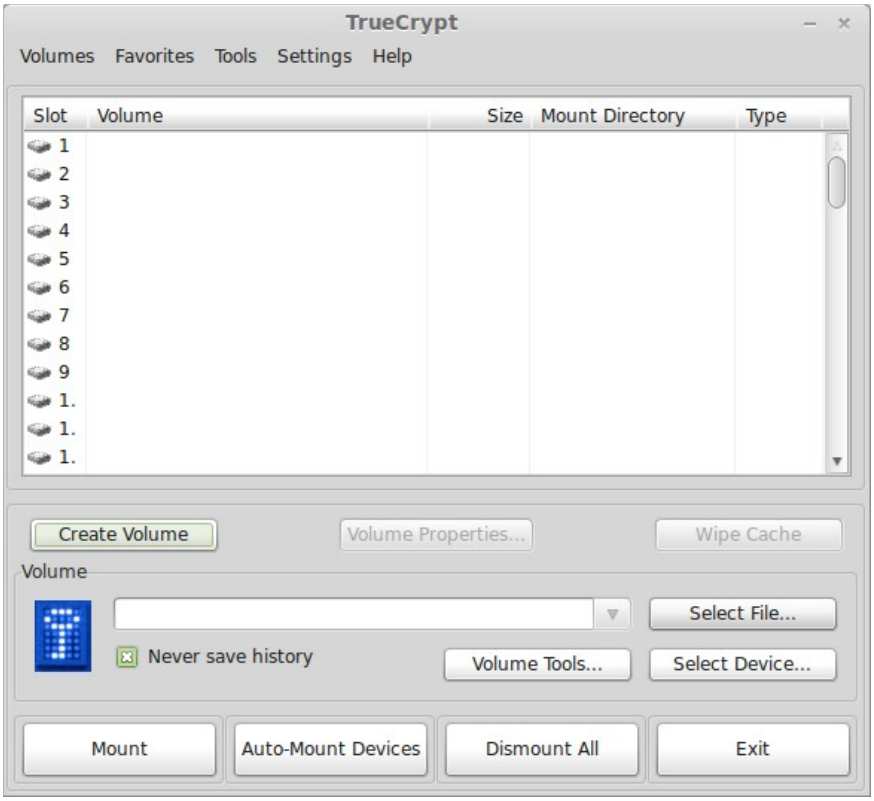


Una vegada descarregat, farem la descompressió de l'arxiu i l'hi donarem permisos d'execució (clic dret sobre l'arxiu, *propiedades > permisos > permitir ejecutar el archivo como un programa*). L'executarem i s'iniciarà la instal·lació: seleccionem instal·lar el programa i acceptem les condicions d'ús, ens demanarà la contrasenya d'administrador i llest!

Ara mostrarem el procés a seguir per crear un volum ocult.

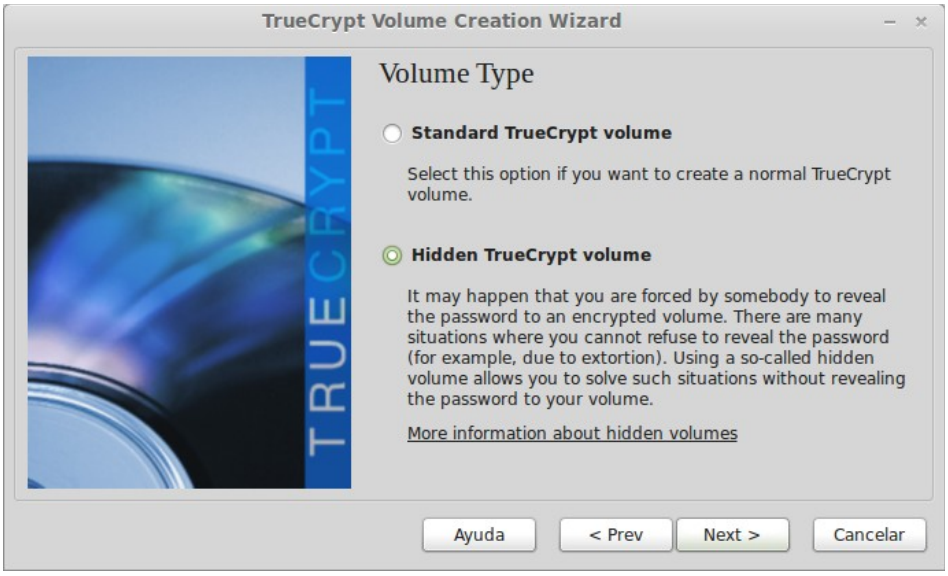
Creant un volum ocult

Quan creem un volum ocult estem creant-lo dins d'un volum encriptat. Per tant, **primer es crea un volum encriptat i després un volum ocult dins d'aquest.** Com ja s'ha comentat abans s'ha de tenir molt en compte l'espai que s'utilitzarà en els volums: si creem un volum encriptat de 10MB i un d'ocult de 5 MB tindrem un espai de 5MB per al volum comú (el no encriptat) i 5MB per l'ocult. Truecrypt no detecta per si sol la grandària del volum ocult (ni la seva existència), per tant si superéssim l'espai de 5MB del volum comú sobreescriuríem l'espai reservat pel volum ocult perdent així els nostres arxius. Obrirem el TrueCrypt:

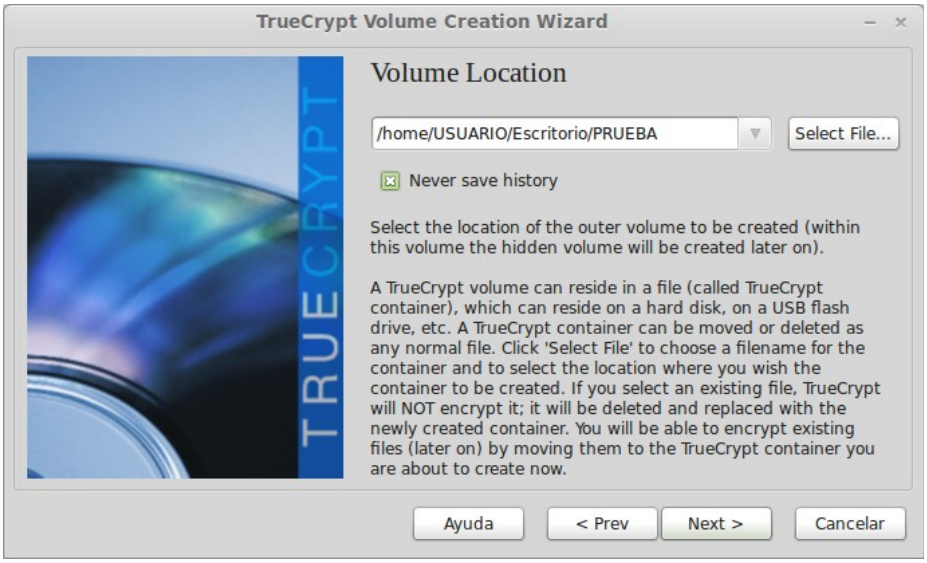


Seleccionarem "*Create Volume*" i després la primera opció:

Si haguéssim seleccionat la segona opció podríem encriptar una partició, o un USB. A la següent pantalla seleccionarem crear un volum ocult.



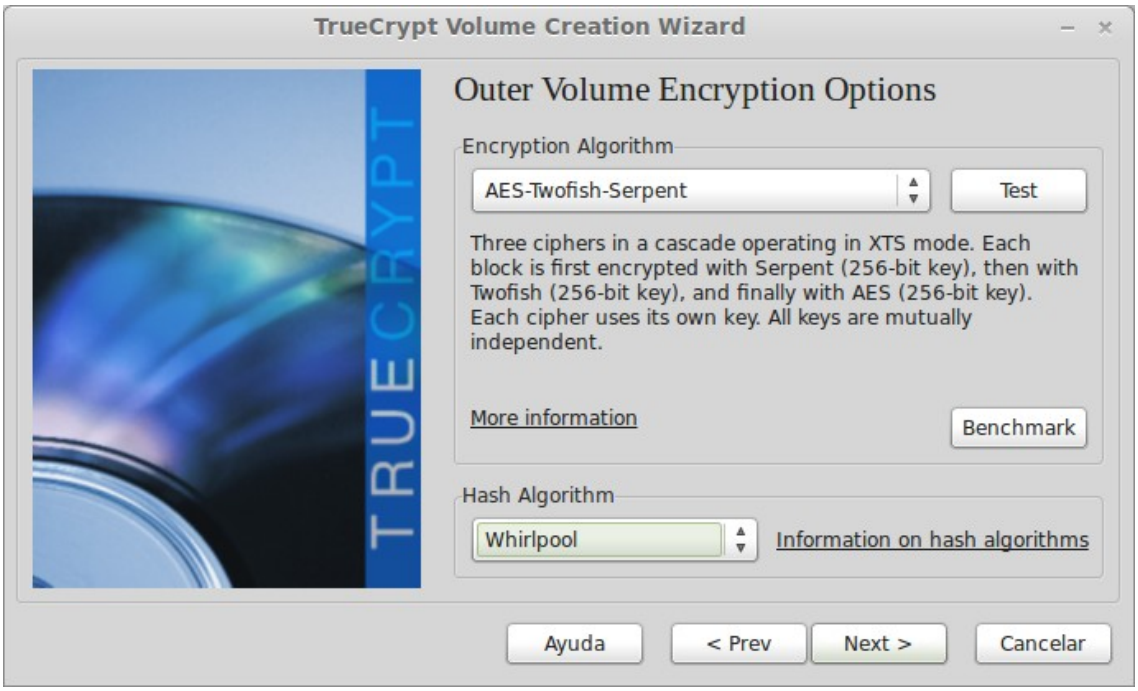
Ara ens demana el lloc on volem crear el contenidor, podem escriure la ruta o seleccionar-ho a través del botó.



Ara toca el pas més important i seleccionar l'algoritme amb el que voldrem encriptar els arxius. Segons he llegit en diverses fonts, el més segur es *"**AES-Twofish-Serpent**"* com a algoritme i el *"**Whirlpool**"* com a hash. No explicarem aqui que es cada cosa ja que a internet hi ha suficient informació. De totes maneres, suposadament, seleccionant nomes AES ja n'hi ha suficient.

Font:

http://superuser.com/questions/207831/which-truecrypt-algorithm-is-the-safest

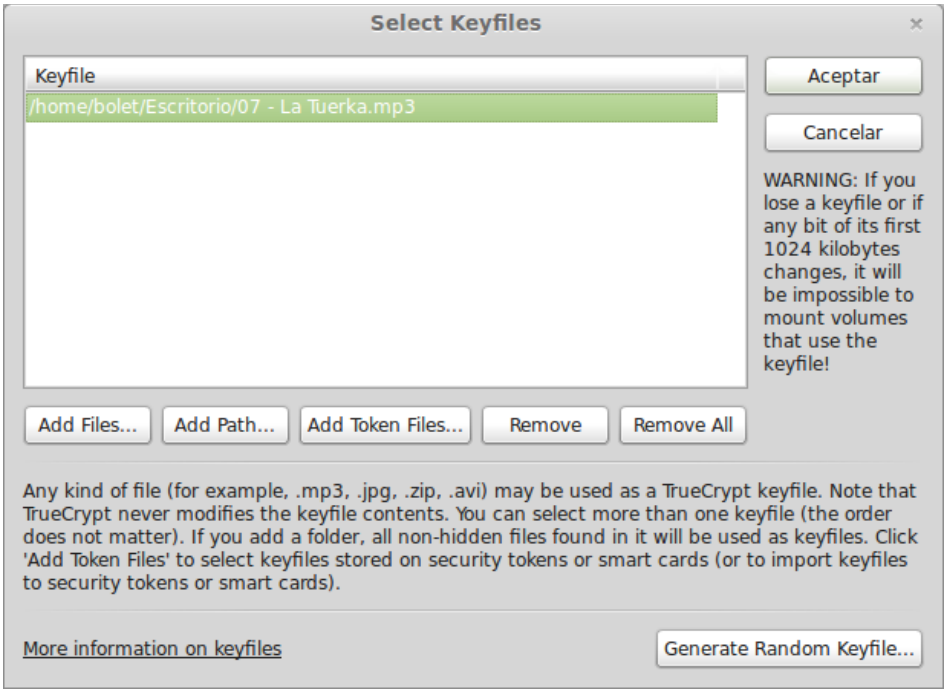


Un cop fet assignarem l'espai que volem encriptar.

Aleshores ens demanarà que introduïm una contrasenya per encriptar els arxius. Es molt important que la contrasenya sigui llarga i contingui caràcters alfa-numèrics i símbols. Quant més llarga sigui la contrasenya més difícil serà desencriptar-la. Segons la empresa de seguretat Kaspersky, una contrasenya de 6 caràcters alfabètics en minúscules es pot desencriptar en 10 minuts. En canvi, una contrasenya de 9 caràcters que contingui lletres, majúscules i minúscules, números i símbols, poden tardar fins a 44.530 anys. (font)
Un truc es substituir lletres per números i afegir els símbols en una frase que ens agradi, fàcil de recordar. Per exemple:

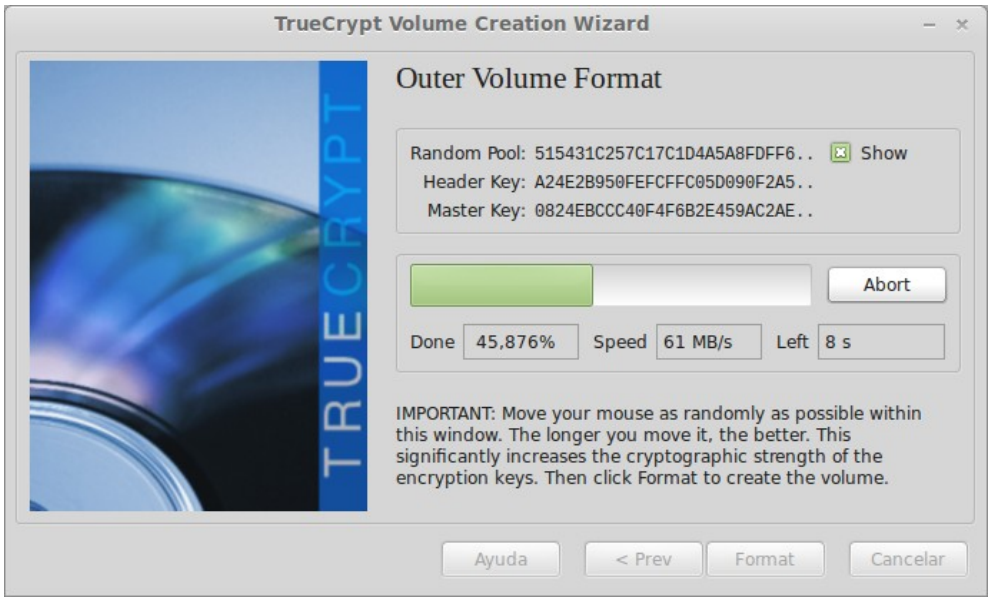
stop control --> !!St0p-C0ntr0L??

Per altra banda hi ha el tema dels *“key files”*. Aquests son arxius, que nosaltres utilitzem per encriptar el volum. Per tant per desencriptar-lo necessitarem exactament el mateix arxiu, per exemple una cançó.
Per seleccionar un, clicarem al botó *“keyFiles”* i amb *“add files”* afegim un a la llista, el seleccionem i acceptem.



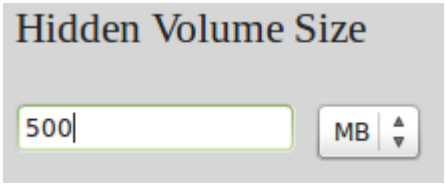
Quedant de la següent manera:

A la següent pantalla es crea un numero aleatori a partir del moviment del ratolí, que també s'utilitzarà a l'encriptació. Cliquem a format i esperem que es generi la encriptació.



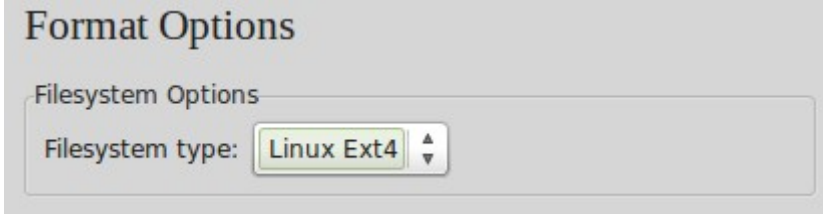
Finalment ens demana el password d'administrador de l'ordinador i munta el volum.

Ara es el moment en que es crea el volum ocult dins del volum encriptat. Tornem a passar per alguns dels passos fets anteriorment i quan ens demana la grandària del volum ocult hem de tenir en compte que ha de ser més petita que el volum contenidor:



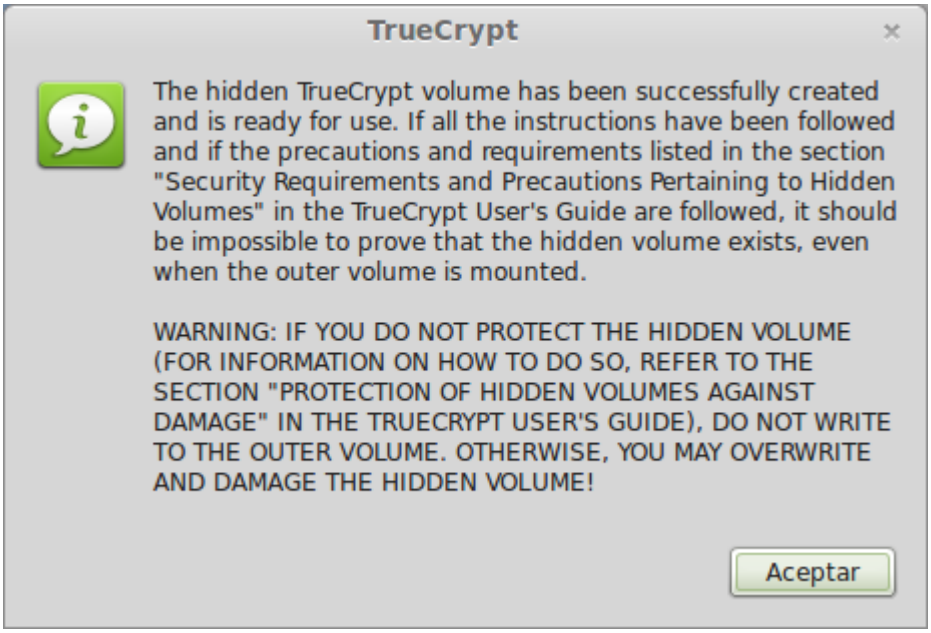
Ara ens torna a demanar una clau per desencriptar el volum ocult, que hauria de ser diferent al volum contenidor (el no ocult) per dificultar la obtenció de la contrasenya.

Seguidament ens demana en quin tipus de sistema de fitxers volem tenir formatat el volum. Si utilitzem Windows escollim FAT, si utilitzem Linux escollim Ext4 (que es el seu sistema de fitxers).



Seguidament ens pregunta si muntarem el volum en Linux únicament o ho també voldrem que sigui accessible des d'altres sistemes operatius. Aquí escollim la opció que mès ens convingui, en el nostre cas només Linux. Completarem les últimes passes i ja tindrem el volum creat.

Ens apareixerà una advertència en referencia al perill de revelar l'existència del volum ocult i al perill de sobreescriure el volum ocult (abans esmentat).



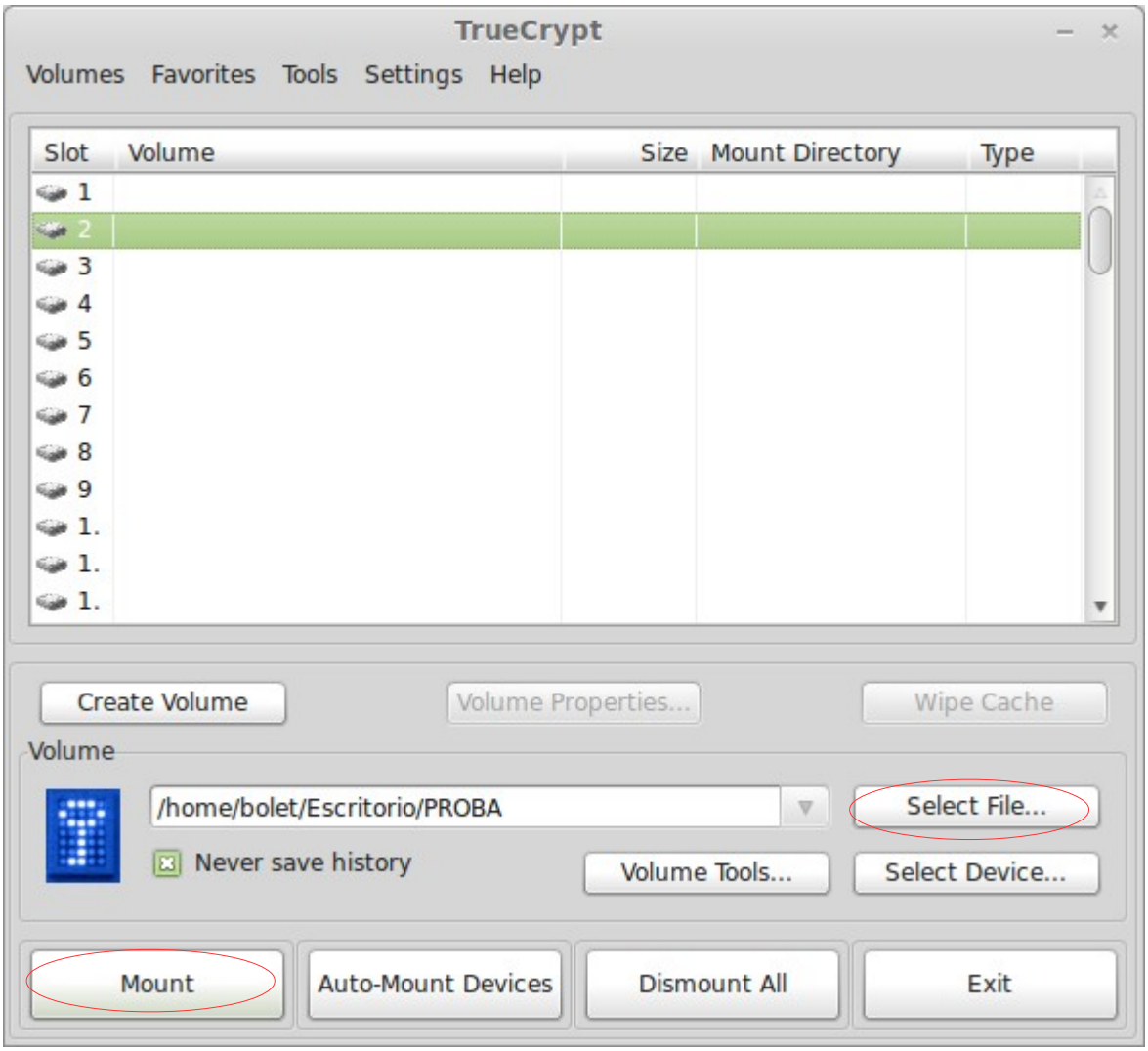
Ara ja tenim creat el nostre volum encriptat dins del qual hi ha un volum encriptat i ocult. Ara veurem com accedir-hi i com utilitzar-lo.

Es important que els contrasenyes siguin diferents entre el volum ocult i el volum encriptat, per a afegir-hi mes seguretat. Igual que els keyfiles.

Tenir la opció de no recordar els historials fa que cada vegada que vulguis muntar els arxius hagis d'escriure la contrasenya i escollir el keyfile corresponent, afegint més seguretat.

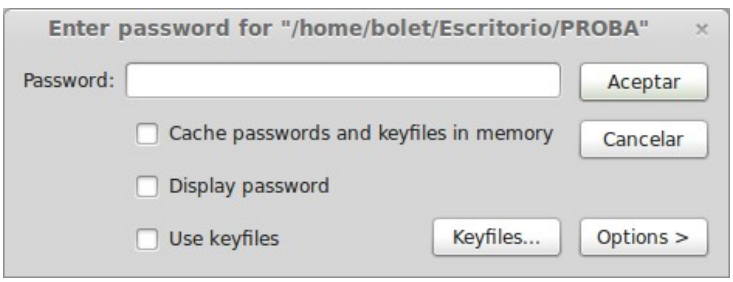
Usant el volum ocult

Per muntar el volum seleccionarem l'arxiu des de la pantalla principal del Truecrypt (amb el botó de "*select file*"). Recordem que aquest arxiu l'hem creat en el primer pas, quan hem creat el volum encriptat que conté el volum ocult. Després seleccionem en quina unitat ho volem muntar (les unitats son els números que apareixen amunt) i cliquem el botó de *"Mount"*.



Una vegada cliquem Mount sens obrirà la finestra en que ens demana la contrasenya (i keyfiles si els hem escollit) per desencriptar el volum. Aquí es important, **que si el que volem veure es el volum ocult, haurem d'escriure la contrasenya del volum ocult**.

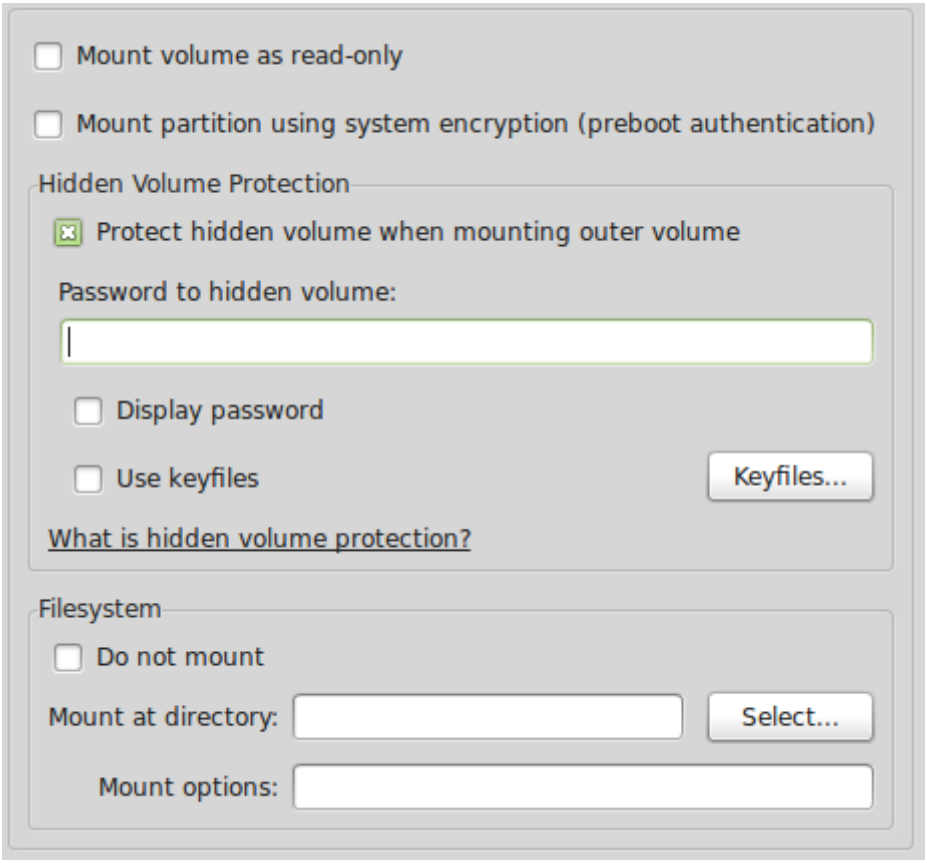
La pantalla mostra el següent aspecte:



O apareix *“password”* hi hem d'escriure la contrasenya del volum a desencriptar (obvi no?), si volem desencriptar el volum ocult, haurem d'escriure la contrasenya del volum ocult (com ja hem dit abans).

Si els hem encriptat a partir d'un o més arxius (*keyfile*) haurem de seleccionar-los a partir del botó *“keyfile”* , lo qual te la seva lògica...

Per altra banda, si obrim les opcions:



La opció anomenada *“protect hidden volume when mounting outer volume”* serveix per activar una protecció per a la partició oculta per evitar que es sobreescrigui (recordem que abans s'ha explicat) en el cas de que es sobrepassi el espai de memòria reservada per al volum contenidor.

Una vegada ficada la contrasenya acceptem i automàticament es munta el volum.

Recordem que quan el vulguem deixar d'utilitzar l'hem de desmuntar, del contrari quedaria muntat encara que tanquéssim el Truecrypt.