GNU PRIVACY GUARD – GNUPG mini howto

Augusto Scatolini (webmaster@comunecampagnano.it)
Ver. 1.0 Aprile 2009

Philip Zimmermann (autore di PGP)

Per poter parlare di GNUPG si deve prima introdurre il suo predecessore OpenPGP

OpenPGP, ovviamente, deve essere introdotto dal capostipite PGP – Pretty Good Privacy.

Pretty Good Privacy - PGP

Da Wikipedia, l'enciclopedia libera.
http://www.pgp.com/

INTRODUZIONE STORICA

Pretty Good Privacy (PGP) traducibile in “riservatezza abbastanza buona” è probabilmente il programma di crittografia più usato al mondo.

*La parola **crittografia** deriva dall'unione di due parole greche: κρύπτος (kryptós) che significa "nascosto", e γράφειν (gráphein) che significa "scrivere". La crittografia tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile a persone non autorizzate a leggerlo. Un tale messaggio si chiama comunemente crittogramma.*

1991 - La storia della sua nascita è alquanto ***avventurosa***, il suo autore Phil Zimmermann (statunitense) era un attivista anti-nucleare e creò PGP al fine di permettere ai suoi compagni di scambiarsi messaggi “***in sicurezza***” tramite sistemi **BBS**. Date le sue caratteristiche, praticamente, era un software Opensource.

*Una **BBS** (o **Bulletin Board System**) è un computer che utilizza un software per permettere a utenti esterni di connettersi ad esso attraverso la linea telefonica, dando la possibilità di utilizzare funzioni di messaggistica e file sharing centralizzato. Il sistema è stato sviluppato negli anni '70 e ha costituito il fulcro delle prime comunicazioni telematiche amatoriali, dando vita alla telematica di base.*

L'uso di PGP passò rapidamente e automaticamente dai sistemi BBS a **Usenet** e quindi ad **Internet**

***Usenet** (contrazione inglese di "user network", in italiano"rete utente") è una rete mondiale formata da migliaia di server tra loro interconnessi ognuno dei quali raccoglie gli articoli (o news, o messaggi, o post) che le persone aventi accesso a quel certo server si inviano, in un archivio pubblico e consultabile da tutti gli abbonati, organizzato in gerarchie tematiche e newsgroup flussi di articoli sullo stesso tema (topic, o thread).*

Quando la diffusione di PGP (che adottava chiavi maggiori di **128 bit**) varcò i confini statunitensi Zimmermann fu formalmente indagato con l'accusa di "esportazione di armi senza apposita licenza", questo perché per il Regolamento per l'Esportazione dei prodotti e servizi USA del Dipartimento di Stato i sistemi di crittografia che utilizzassero una chiave maggiore di **40 bit** erano considerati come **munizioni**. Era il febbraio 1993.

Quando la giurisdizione del citato regolamento è passata al Dipartimento del Commercio la classificazione dei sistemi di crittografia è cambiata, poi con la semplificazione avvenuta nel **2000**, incluso l'innalzamento della soglia dei **40 bit**, PGP non è più definibile come "arma non esportabile" e **può essere utilizzato (ed esportato) ovunque.**
L'incriminazione a carico di Zimmerman è stata archiviata senza che siano state rubricate condotte criminali in capo allo stesso o ad altri soggetti.

1996 - Zimmermann ed il suo gruppo fondarono una compagnia per produrre nuove versioni di PGP. Si fusero con Viacrypt (alla quale Zimmermann aveva venduto i diritti commerciali di PGP e che aveva acquistato la licenza RSA direttamente dalla RSADSI), che cambiò nome in **PGP Incorporated**.

1997 - la PGP Inc. venne acquistata dalla **Network Associates, Inc**., NAI di cui Zimmermann ed il gruppo PGP divennero dipendenti.

2001 - Zimmermann lasciò la NAI.

2001 - la NAI ha annunciato che i suoi diritti sul PGP erano in vendita e che avrebbe sospeso lo sviluppo di PGP.

2002 - la NAI ha cancellato ogni progetto riguardante PGP.

2002 - alcuni ex-membri del gruppo PGP hanno acquistato i diritti di PGP dalla NAI (eccetto per la versione a linea di comando), e, nell'agosto dello stesso anno, hanno formato una nuova compagnia, la **PGP Corporation**.

2002 - la PGP Corp ha rilasciato PGP 7.2 per Mac OS 9, seguito rapidamente da PGP 8.0 e PGP 8.0 Personal per Mac e Windows, e da una versione freeware ed una open source.

2003 - la PGP Corp ha rilasciato PGP 8.0.1DE per gli utenti tedeschi, PGP Universal (basato su una nuova concezione di PGP per server, che implementa un'architettura di sicurezza che si auto-gestisce).

2004 - ha rilasciato PGP Desktop 8.1 per Mac e Windows, PGP Command Line 8.5 per Windows, Solaris e Linux (l'accordo riguardo la linea di comando tra la PGP Corp. e la NAI scadeva nel Gennaio 2004) e PGP Universal 1.2.

2005 - hanno rilasciato PGP Desktop 9.0, PGP Universal 2.0 e PGP Command Line 9.0.

Zimmermann ora lavora come consulente speciale alla PGP Corp., e continua il suo lavoro alla Hush Communications e alla Verdis, e infine gestisce una propria compagnia di consulenza.

Philip Zimmermann si sta dedicando alla promozione della nuova tecnologia standard di crittografia delle telefonate, basata sui medesimi principi di libertà di PGP e chiamata **ZRTP**. Assieme alla società ticinese KHAMSA SA ha sviluppato l'estensione crittografica ZRTP/S per la protezione delle comunicazioni mobili GSM e UMTS.

PGP è stato così influente che il suo progetto è stato trasformato dalla **IETF** in uno standard Internet chiamato **OpenPGP**. Le versioni di PGP più recenti dello standard sono, bene o male, con esso compatibili.

*La **Internet Engineering Task Force** - **IETF** - è una comunità aperta di tecnici, specialisti e ricercatori interessati all'evoluzione tecnica e tecnologica di Internet. Ciò che differenzia IETF dagli Enti di standardizzazione più tradizionali è la sua struttura aperta: il lavoro viene svolto da gruppi di lavoro (working groups) che operano soprattutto tramite Mailing list, aperte alla partecipazione di chiunque sia interessato, e che si riuniscono tre volte l'anno. I gruppi di lavoro si occupano ciascuno di uno specifico argomento e sono organizzati in aree (protocollo applicativi, sicurezza, ecc...).*

COME FUNZIONA PGP

CRITTOGRAFIA CONVENZIONALE A CHIAVE SINGOLA (simmetrica).

Supponiamo che A voglia inviare un messaggio a B e che solo B lo possa leggere. A crea una chiave crittografica per cifrare il messaggio, cifra il messaggio ovvero lo rende illeggibile (indecifrabile), e lo invia a B. B riceve il messaggio cifrato e lo decifra con la stessa chiave (creata da A) che deve aver ricevuto in precedenza da A tramite un canale sicuro. Questo sistema è alquanto scomodo e perfino illogico perché se esiste un canale sicuro per trasmettere la chiave si può usare lo stesso canale per trasmettere il messaggio in chiaro. Ovviamente non esiste un canale con tale sicurezza.

CRITTOGRAFIA A CHIAVE PUBBLICA (asimmetrica).

Questo sistema presuppone che tutti gli attori posseggano 2 specifiche chiavi crittografiche complementari: una pubblica e una privata. Ogni chiave sblocca il codice che l'altra crea. La conoscenza della chiave pubblica non aiuta a dedurre la chiave privata corrispondente e quindi può essere distribuita e diffusa attraverso qualunque canale.

INVIARE MESSAGGI - RISERVATEZZA

Quindi, se A vuole inviare un messaggio a B e vuole che solo B lo possa leggere, A cifra il messaggio con la chiave pubblica di B (è facilmente reperibile) e lo invia a B. B riceve il messaggio cifrato con la sua chiave pubblica e lo decifra con la sua chiave privata.

Solo chi è in possesso della chiave privata di B (cioè B) potrò decifrare e leggere il messaggio cifrato con la chiave pubblica di B. Nemmeno A potrà decifrare il messaggio cifrato dallo stesso A con la chiave pubblica di B.

FIRMARE DOCUMENTI/MESSAGGI – AUTENTICITA' (non ripudio)

Se A vuole inviare un messaggio a B e vuole che B abbia la certezza sull'autenticità del mittente (che sia veramente A), A cifra il messaggio con la sua chiave privata e lo invia a B. B decifra il messaggio con la chiave pubblica di A (facilmente reperibile) e se il messaggio ritorna in chiaro (leggibile) avrà la certezza circa l'identità del mittente (ovvero A)

RISERVATEZZA E AUTENTICITA'

La combinazione dei due metodi appena descritti permettono di garantire sia la riservatezza che l'autenticità:

A cifra il messaggio in chiaro con la propria chiave privata (FIRMA) poi cifra il messaggio cifrato con la chiave pubblica di B (RISERVATEZZA) ed invia il messaggio a B.

B decifra il messaggio prima con la sua chiave privata (RISEVATEZZA) e poi con la chiave pubblica di A (AUTENTICITA')

SITEMA MISTO

Dato che la velocità della crittografia a chiave pubblica è molto inferiore rispetto a quella convenzionale a chiave singola, si preferisce usare , per la cifratura, una chiave singola casuale e temporanea.

A cifra il messaggio in chiaro con la chiave singola casuale e temporanea, poi cifra la chiave temporanea con la chiave pubblica di B ed invia messaggio e chiave cifrata a B.

B decifra la chiave cifrata con la sua chiave privata, recupera la chiave singola temporanea e quindi, con quest'ultima, decifra il messaggio cifrato che produrrà il messaggio originale.

La chiave pubblica è conservata in un "**certificato di chiave pubblica**" che comprende l'ID del proprietario, il momento in cui la chiave è stata generata e la chiave stessa

Analogamente esiste il "**certificato di chiave privata**"

Per garantire la sicurezza della chiave privata, questa viene a cifrata a sua volta con una "**frase chiave**"

Il portachiavi è un file che può contenere uno o più di questi certificati

Quindi esistono portachiavi pubblici, privati e misti.

Al contrario di protocolli di sicurezza come SSL, che proteggono i soli dati "in transito" (ovvero solo mentre gli stessi vengono trasmessi su una connessione di rete), PGP può essere utilizzato anche per proteggere dati su disco, o dati di backup.

Firma Digitale Odierna

Non è difficile asserire che Zimmermann sia stato il papa' involontario dell'attuale firma digitale, quella che oggi viene rilasciata a chiunque dalla Camera di Commercio in soli 12 minuti

La **firma digitale**, o **firma elettronica qualificata, basata sulla tecnologia della crittografia a chiavi asimmetriche**, è un sistema di autenticazione di documenti digitali analogo alla firma autografa su carta. La firma digitale è un sistema di autenticazione forte in quanto si basa sull'uso di un certificato digitale memorizzato su di un dispositivo hardware. I certificati su cui si basa possono essere più di uno.

Kriptonite - Una lettura divertente e illuminante:
http://www.ol-service.com/sikurezza/crittografia/kriptonite/kriptonite.html

Il sito internet di Zimmermann: http://www.philzimmermann.com/IT/background/index.html

guida pratica : http://www.pgpi.org/docs/g_pgp952.htm

manuale d'uso di PGP scritto da Zimmerman nel 1994 – tradotto in italiano :
http://www.pgpi.org/docs/italian.html

OpenPGP

Da Wikipedia, l'enciclopedia libera.
http://www.openpgp.org/

Nel giugno 1997 la PGP Inc. ha proposto al IETF la creazione di uno standard chiamato OpenPGP. Hanno dato il permesso al IETF di usare il nome OpenPGP per descrivere questo nuovo standard e qualsiasi programma che lo supportasse ('PGP', 'Pretty Good Privacy' e 'Pretty Good' sono tutti marchi registrati della PGP Corporation, al 2002). Lo IETF ha accettato la proposta e ha creato lo OpenPGP Working Group.
OpenPGP è diventato uno standard Internet: è definito dalle RFC 2440 e 3156.

La commercializzazione di PGP ha prodotto lo standard OpenPGP che è stato utilizzato dal mondo OpenSource per produrre un vero software a codice aperto con licenza GNU GPL ovvero GNU Privacy Guard.

GNU PRIVACY GUARD - GNUPG - GPG

Da Wikipedia, l'enciclopedia libera.
http://www.gnupg.org/

GNU Privacy Guard (GnuPG o GPG), rilasciato sotto la licenza GNU GPL, è un programma progettato per sostituire la suite crittografica **PGP**. GPG è completamente compatibile con gli standard **OpenPGP** dell'IETF ed è sostenuto dal governo tedesco. Fa parte del software sviluppato dalla **Free Software Foundation**.

GPG venne sviluppato inizialmente da Werner Koch; la versione 1.0.0 fu rilasciata il 7 settembre 1999. Nel 2000 il ministro dell'Economia e della Tecnologia della Germania Federale fa partire il progetto di creazione della documentazione e di porting per Microsoft Windows.

GPG è un programma distribuito con parecchi sistemi operativi liberi come FreeBSD, OpenBSD, e NetBSD, oltre che, ovviamente, con tutte le distribuzioni GNU/Linux. È disponibile anche per le varie versioni dei sistemi operativi proprietari Microsoft Windows e Mac OS X, e grazie alla sua portabilità ed alla disponibilità del codice sorgente è possibile crearne una versione per qualsiasi OS.

Nonostante la versione di base di GPG fornisca un'interfaccia a linea di comando completa, in perfetta aderenza alla filosofia OpenSource sono state sviluppate parecchie interfacce grafiche:
Seahorse per GNOME, (GNU/Linux)
KGPG per KDE (GNU/Linux)
GpG4win (Windows)

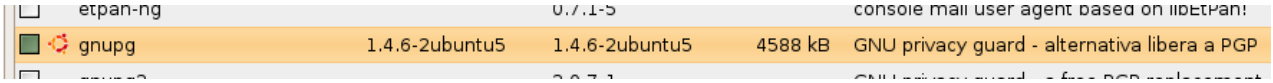
GPG cifra i messaggi utilizzando una coppia di chiavi (pubblica e privata) generate dall'utente. Le chiavi pubbliche possono essere scambiate tra gli utenti in vari modi, principalmente email e keyserver. Tuttavia bisogna prestare particolare attenzione alla corrispondenza tra chiave e (presunta) identità: il problema di tutti i sistemi di crittografia asimmetrica è la certificazione dell'autenticità della chiave, solitamente risolto con la presenza di un'autorità centrale oppure con la firma delle chiavi (un utente firma la chiave pubblica di un altro utente per certificarne l'effettiva autenticità). Su questo delicato punto si basa anche la firma digitale di file (messaggi) per garantire l'autenticità del contenuto e del mittente.

GPG non fa utilizzo di algoritmi brevettati (o con ambiti di utilizzo ristretti da particolari licenze) come IDEA, presente in PGP sin dalle prime versioni. Vengono invece usati algoritmi come Digital Signature Algorithm (DSA), RSA, ElGamal, CAST5, Triple DES (3DES), AES e Blowfish. È tuttavia ancora possibile utilizzare IDEA ma si deve scaricare un apposito plugin (e, in alcuni paesi, registrare una licenza di utilizzo).

Come prevede lo standard OpenPGP, GPG è un sistema di crittografia "ibrido", che combina algoritmi a chiave simmetrica a causa della loro velocità e algoritmi a chiave pubblica per la facilità di scambio delle chiavi: ogni volta che si deve cifrare un messaggio viene generata una chiave di sessione (utilizzata un'unica volta, per l'algoritmo simmetrico) che viene a sua volta cifrata con la chiave pubblica del destinatario. Si noti come questo passaggio renda impossibile la lettura del messaggio anche al mittente (a meno che questo non cifri la chiave di sessione anche con la propria chiave pubblica, opzione che è possibile abilitare).

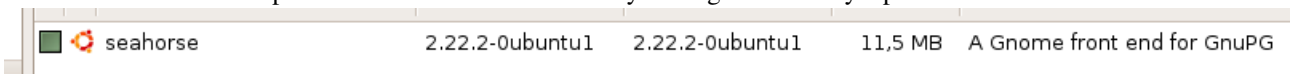
GPG per GNU/Linux

Per i sistemi Debian e Debian derivati (Ubuntu) è sufficiente scaricare GPG tramite Synatpic

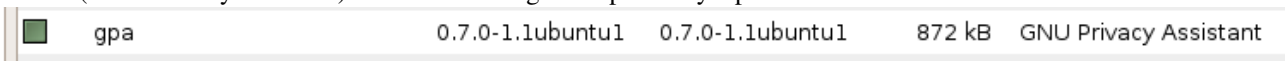


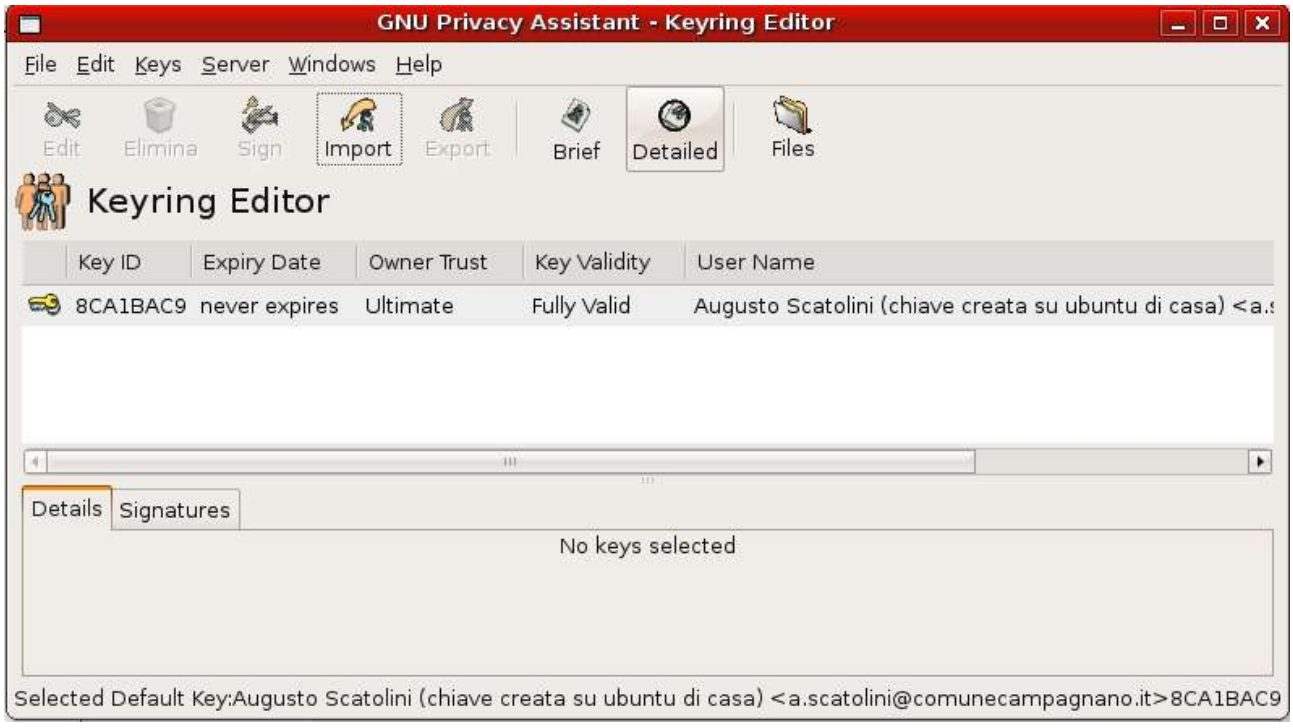
Interfaccia grafica per GNU/Linux

Per l'ambiente Gnome si può installare **Seahorse** come Key Manager tramite Synaptic



e **GPA** (GNU Privacy Assistant) come File Manager sempre da Synaptic



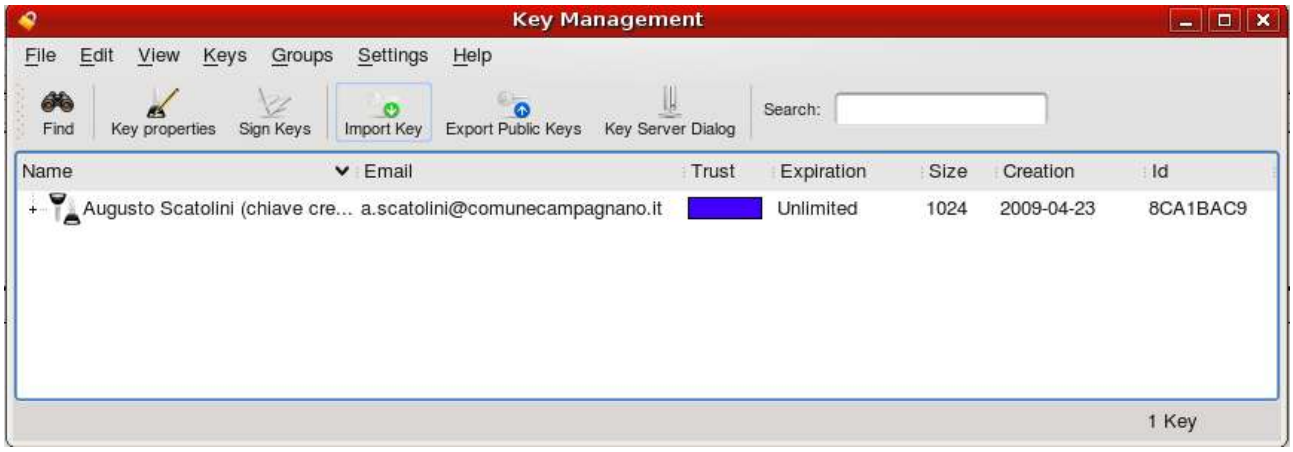


Per Ambiente KDE si può installare KPGP tramite Synaptic (anche per la versione 4 oltre alla versione 3.5)

■	kgpg	4:3.5.10-0ubuntu1~	4:3.5.10-0ubuntu1~	1438 kB	GnuPG frontend for KDE
■	kgpg-kde4	4:4.0.3-0ubuntu4	4:4.0.3-0ubuntu4	1970 kB	GnuPG frontend for KDE 4

KDE versione 3.5

KDE versione 4



GPG per Windows

Per i sistemi Windows si scarica un eseguibile via **FTP** dal sito http://www.gnupg.org/download/index.it.html

C'è anche una versione compilata per **MS-Windows**. Si noti che è una versione a linea di comando che comprende uno strumento di installazione grafico.

· GnuPG 1.4.9 compilato per Microsoft Windows. B FTP

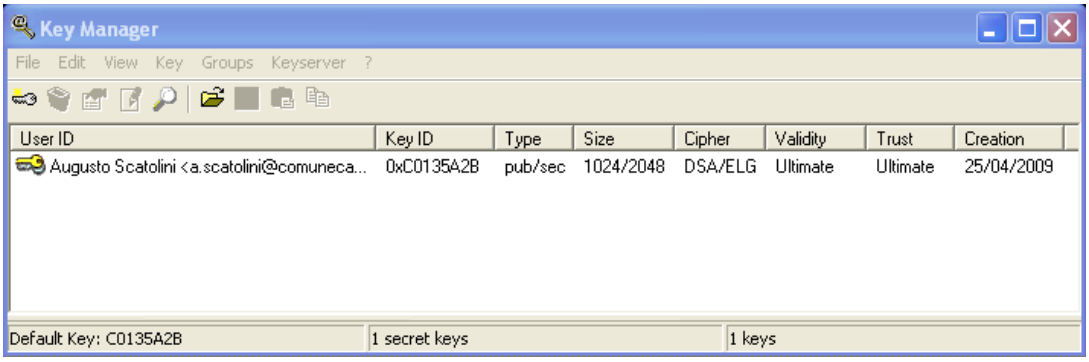
Interfaccia grafica per Windows

Per i sistemi Windows si può scaricare **Gpg4win** dal sito http://www.gpg4win.org/

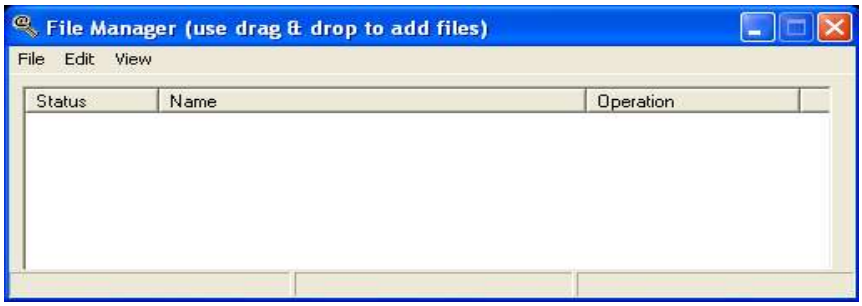
Una volta installato si può lanciare il programma **WinPT**

Dall'icona **WinPT** che si posiziona sulla barra in basso a destra, tramite il tasto destro del mouse, si può accedere

al **Key Manager**



e al **File Manager**



** in entrambi i casi, una volta generate le chiavi (pubblica e privata)
** la chiave pubblica si può distribuire con vari mezzi, e-mail, server, pen drive, ...
** la chiave privata risiede sul computer (cifrata a sua volta tramite pass phrase)
** ma è buona norma fare un backup dei portachiavi su qualche supporto
**** in mancanza di backup, in caso di crash del Computer non sarà più possibile decifrare i file cifrati.**

ALTRE SOLUZIONI PIU' SEMPLICI (ma meno sicure)

* Un'altra soluzione OpenSource cross-plattform (Gnu/Linux e Windows) è **TrueCrypt** http://www.truecrypt.org/
cifra interi dischi e partizioni

* OpenSource **NeoCrypt** per Windows http://neocrypt.sourceforge.net/

* Altra soluzione (solo per Windows) **HandyBits EasyCripto Deluxe** (versione 5.5. free of charge for personal use http://www.handybits.com/easycrypto.htm

* **Blowfish Advanced CS** (Personal Edition) Freeware per Windows http://www.lassekolb.info/bfacs.htm

* **KPKFile PRO** Freeware per Windows http://kpkfilec.ipower.com/index.html (anche STEGANOGRAFIA)

FINE