PGP 7.0.3 Freeware utilizza una cifratura a chiave simmetrica ed una cifratura a chiave asimmetrica (altrimenti detta a chiave pubblica) per garantire la riservatezza. In pratica:

1. Il mittente scrive un messaggio e decide di cifrarlo;
2. Il programma, sfruttanto il generatore di numeri casuali interno ed i dati casuali raccolti durante la creazione della chiave dell'utente, genera un numero casuale da utilizzare come chiave di sessione;
3. La chiave di sessione viene cifrata utilizzando l'algoritmo crittografico asimmetrico associato alla chiave pubblica dei singoli destinatari (RSA oppure DH (ElGamal)) ed il risultato diviene l'inizio del messaggio da inviare;
4. Il programma comprime il messaggio originale mediante l'uso di un algoritmo di compressione (algoritmo ZIP) e lo cifra utilizzando la chiave di sessione applicata all'algoritmo crittografico simmetrico scelto dall'utente fra quelli disponibili (TripleDES, IDEA, CAST, AES, Twofish). Poi prende il risultato e lo accoda a quanto ottenuto dall'elaborazione della chiave nel punto precedente, dopo di che invia il tutto al destinatario;
5. A questo punto il programma ricevente decifra la chiave di sessione utilizzando la chiave privata (RSA oppure DH) del destinatario;
6. Con la chiave di sessione, il programma decifra il messaggio ed inverte il processo di compressione.

Firma digitale

La firma digitale utilizza un algoritmo di hash o message digest ed un algoritmo di firma a chiave pubblica (RSA o DSA). La sequenza utilizzata è la seguente:

1. Il mittente crea il messaggio;
2. Il programma del mittente genera un codice di hash del messaggio utilizzando un algoritmo di hash (MD5 se la chiave utilizzata è RSA Legacy altrimenti SHA-1 per RSA V4 e DH (ElGamal));
3. Utilizzando la chiave privata del mittente, associata all'algoritmo asimmetrico utilizzato per la firma (RSA oppure DSA), viene cifrato l'hash ottenuto al punto precedente;
4. La firma digitale appena ottenuta viene allegata al messaggio ed il tutto viene inviato;
5. Il programma del destinatario estrae una copia della firma dal messaggio;
6. Genera un nuovo codice di hash per il messaggio ricevuto e lo verifica confrontandolo con quello estratto in precedenza. Se i due coincidono allora il messaggio viene considerato autentico.

Non dimentichiamoci che, i due servizi, quello di firma e quello di cifratura, potrebbero essere utilizzati contemporaneamente sullo stesso messaggio. In tal caso le operazioni appena viste, si integrerebbero tra di loro.

Le novità introdotte in questa versione sono diverse. A mio avviso quelle principali sono:

- **Nuovi algoritmi crittografici**: completo supporto per i nuovi algoritmi crittografici simmetrici a 256 bits: Advanced Encryption Standard (AES 256/192/128) e Twofish;
- **Supporto di MS Windows Millennium**: è possibile installare ed utilizzare il programma anche con MS Millennium Edition;
- **Chiavi RSA versione V4**: fornisce il completo supporto per la creazione, la gestione e l'utilizzo di chiavi RSA con grandezza e funzionalità pari a quelle DH;
- **Ricostruzione della chiave**: permette di ricostruire la chiave, sfruttandone la precedente suddivisione, dopo aver risposto ad una sequenza di cinque domande decise dall'utente;
- **Virtual Private Network (VPN)**: supporto per la gestione integrata di connessioni virtuali peer-to-peer basate sull'uso di IPsec;
- **IKE Aggressive Mode**: consente agli utenti di stabilire una connessione VPN sicura, utilizzando nome utente/password, anche con un indirizzamento dinamico;
- **IKE Extended Authentication**: permette l'utilizzo di metodi di autenticazione quali Radius e SecureID nella fase di apertura di una connessione VPN con gateway compatibili;
- **Portachiavi multipli**: il programma è in grado di gestire più portachiavi contemporaneamente;
- **Cancellazione sicura files**: la funzionalità era già presente nelle precedenti versioni ma ora è anche possibile mantenerla sempre attiva ed associarla alle operazioni di pulizia del cestino di Windows.

Installazione

I requisiti minimi, consigliati dal produttore, per installare PGP 7.0.3 Freeware in un sistema MS Windows sono:

- Processore Intel Pentium 166 MHz o superiore;
- Windows 95B (OSR2), Windows 98, Windows NT 4.0 con Service Pack 4 o successivo, Windows 2000, Windows 2000 con Service Pack 1, o Windows Millennium Edition;
- 32 MB RAM (64 MB RAM per Windows NT e 2000);
- 32 MB di spazio disco.

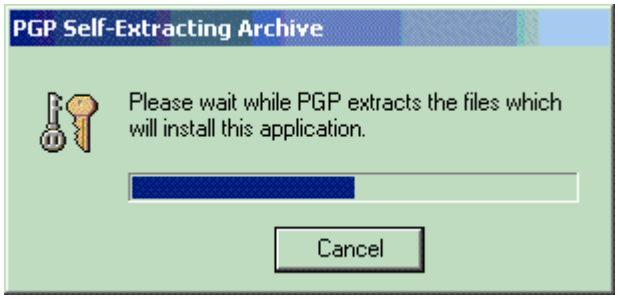
Procedura di installazione

Le procedure guidate di installazione e di aggiornamento sono sostanzialmente simili. Come esempio, proviamo a vedere insieme quella di installazione.

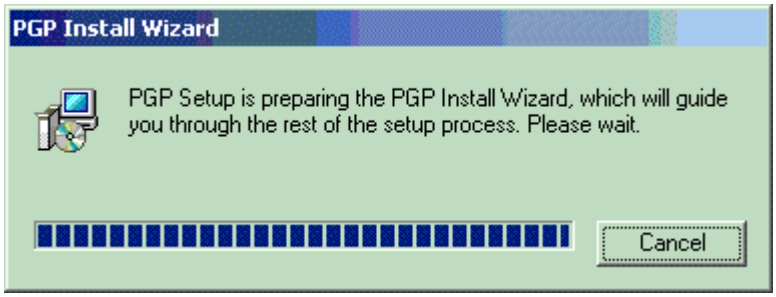
Una volta scaricato il file e dopo averlo scompattato utilizzando un qualsiasi programma compatibile con l'algoritmo di compressione zip, otterrete due files:

- **PGPfreeware 7.0.3.exe**: il programma di installazione vero e proprio;
- **PGPfreeware 7.0.3.exe.sig**: la firma associata al programma necessaria per verificarne l'integrità e la provenienza. Per effettuare l'operazione è necessario aver installato una precedente versione di PGP e che all'interno del proprio portachiavi pubblico vi sia almeno la chiave pubblica di Phil Zimmermann.

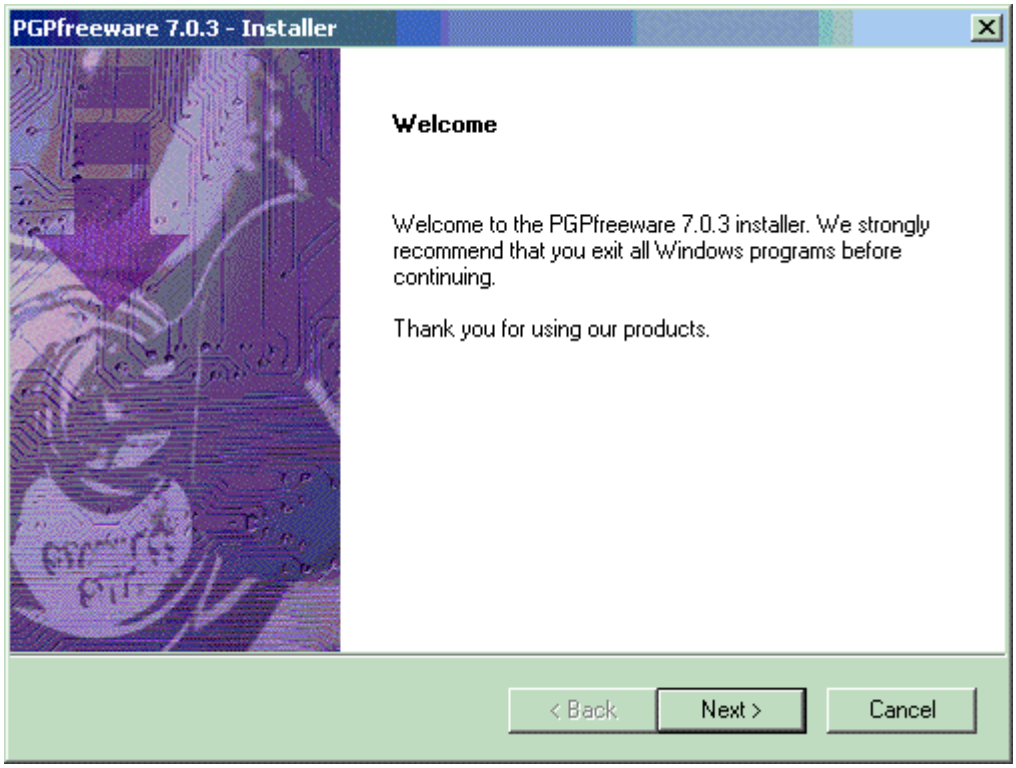
1. Avviamo la procedura di installazione eseguendo il programma PGPfreeware 7.0.3.exe. Per fare questo, basta fare doppio clic sull'icona del programma.



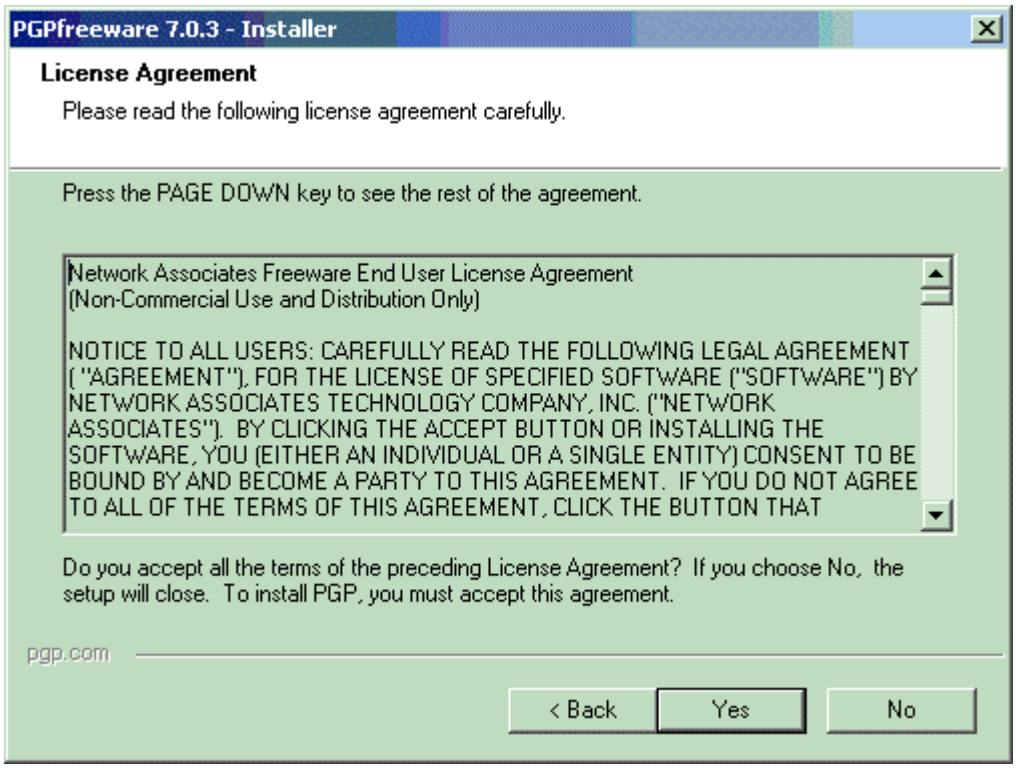
2. Dopo aver estratto i files necessari ad installare l'applicazione, il programma passerà a preparare la relativa procedura guidata.



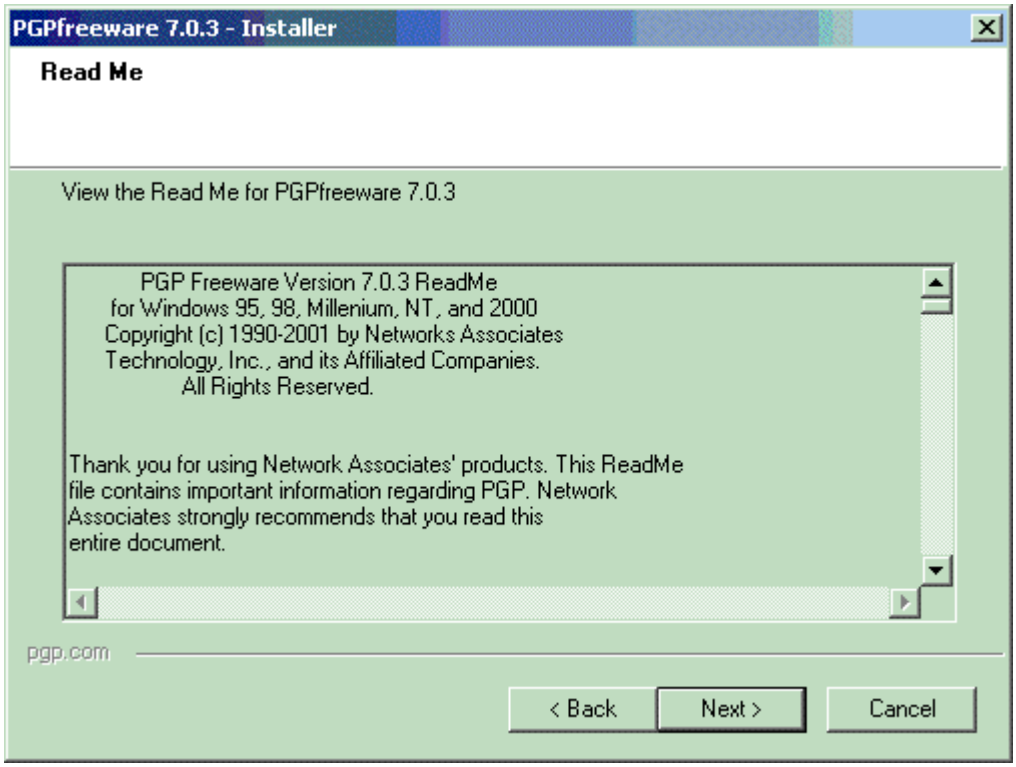
3. Dopo di che, vi verrà chiesto di chiudere tutte le applicazioni attive per consentire una corretta installazione del programma.



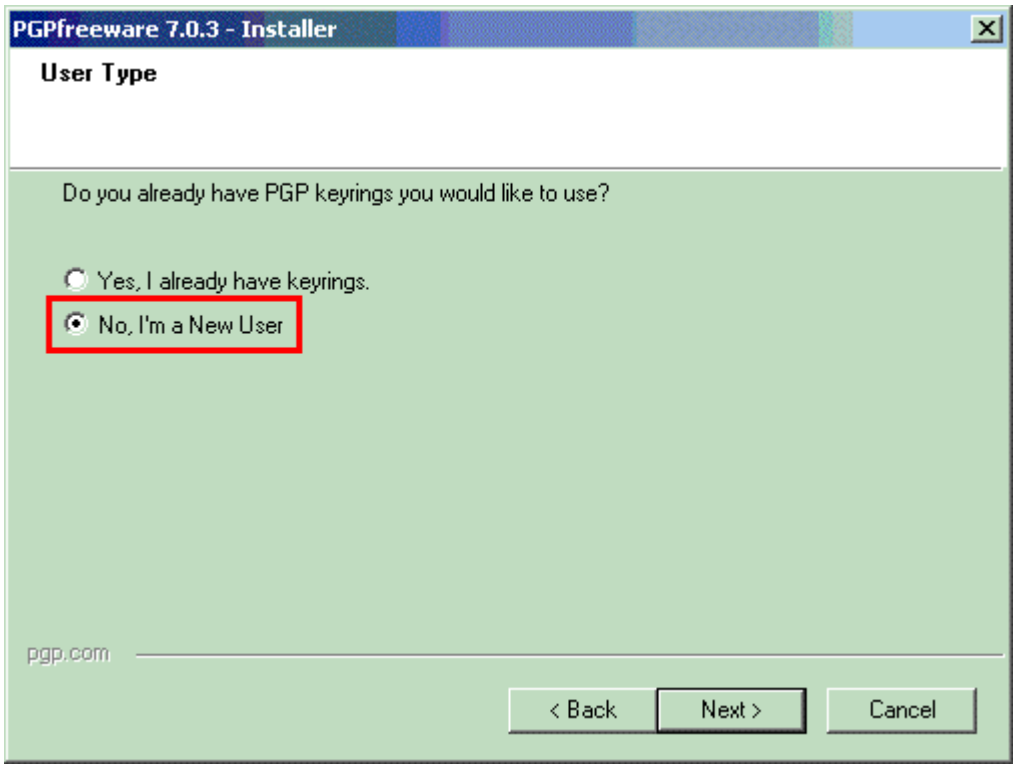
4. Quindi vi verrà proposto di leggere ed accettare la licenza associata al programma. Per farlo, e quindi continuare nell'installazione, selezionate 'Yes'.



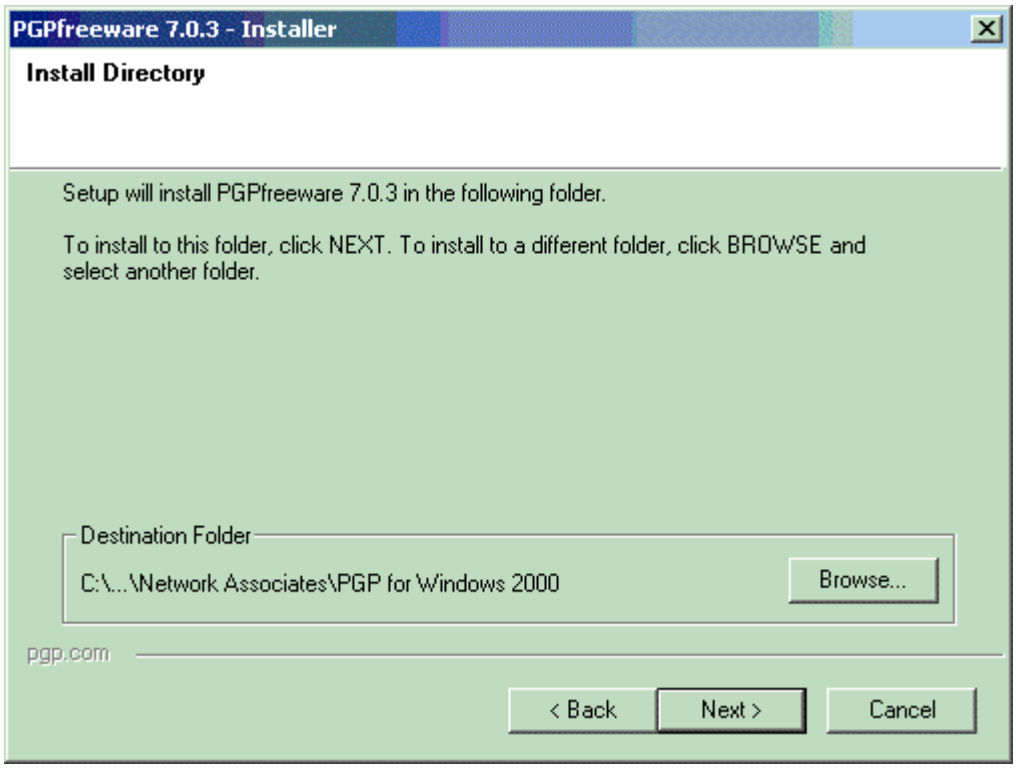
5. Dopo aver letto attentamente le informazioni associate al programma, selezionate 'Next'.



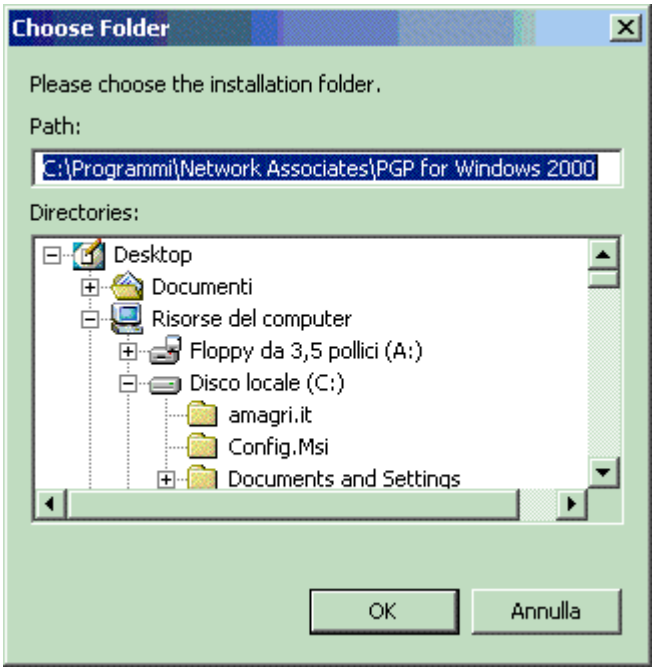
6. Se il programma non rileva una precedente installazione, vi chiede di scegliere la vostra tipologia di utente. Nel nostro esempio, trattandosi di una nuova installazione, non siamo in possesso di nessun portachiavi quindi selezioneremo 'No, I'm a New User'. Dopo di che 'Next'.



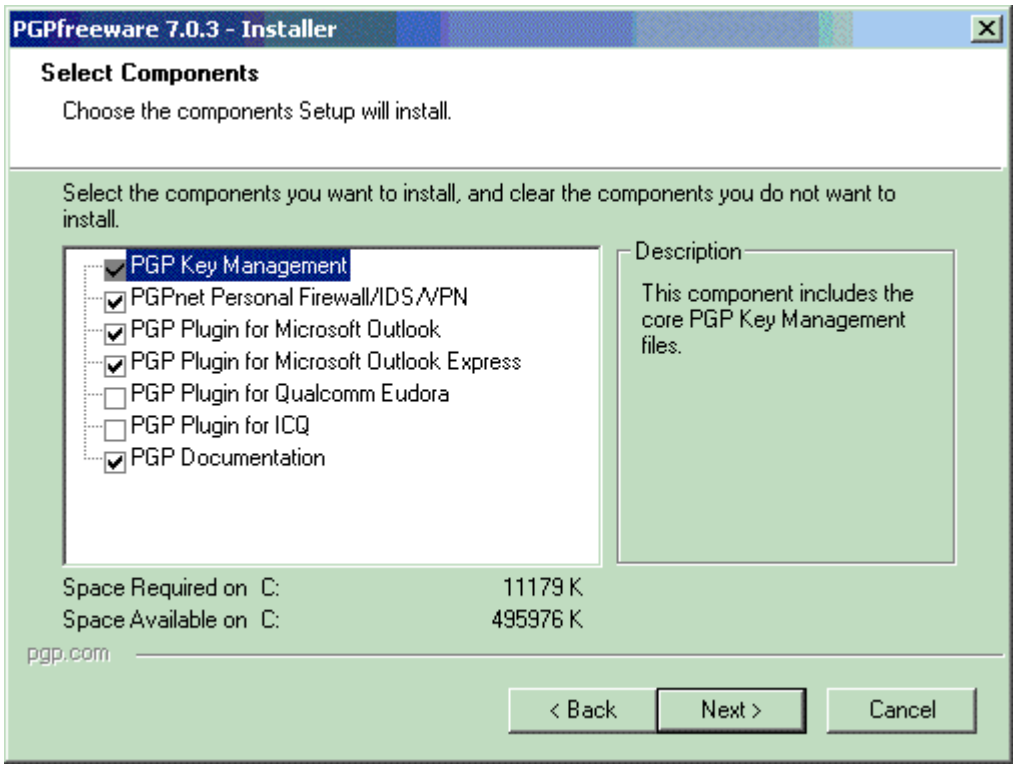
7. Bisognerà quindi scegliere la cartella all'interno della quale copiare i files del programma. Se la destinazione predefinita non vi va bene, basta selezionare il pulsante 'Browse'.



Vi verrà presentata una finestra che vi faciliterà la scelta del percorso relativo alla cartella destinazione.

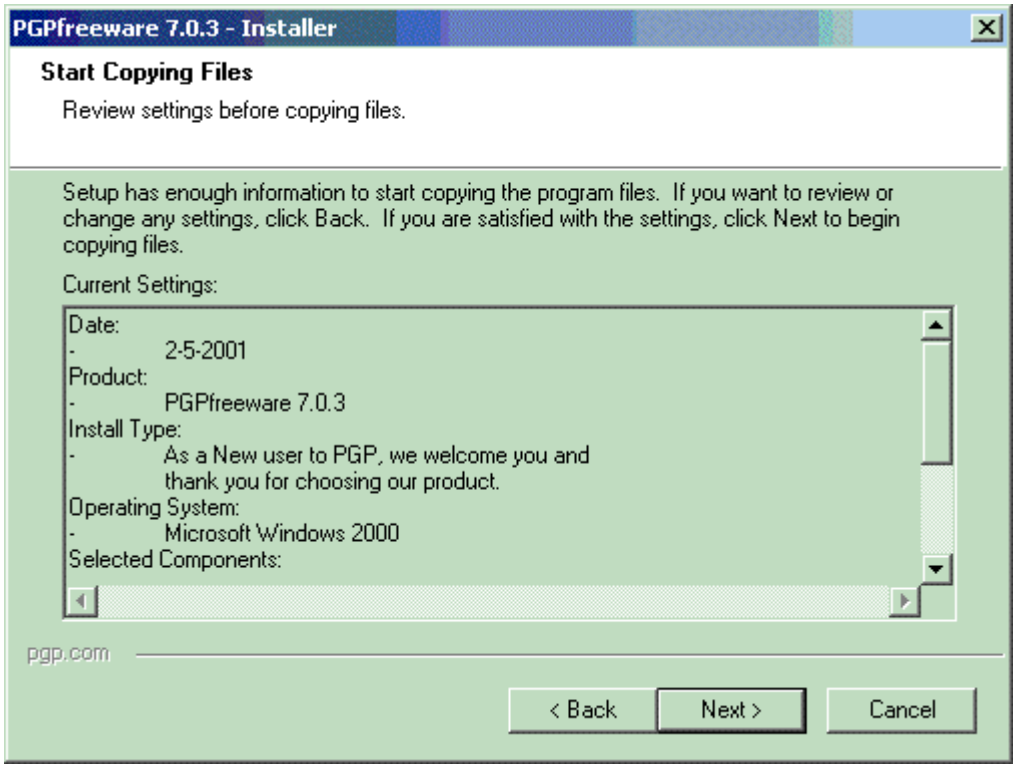


8. Si passa quindi alla scelta dei componenti da installare.

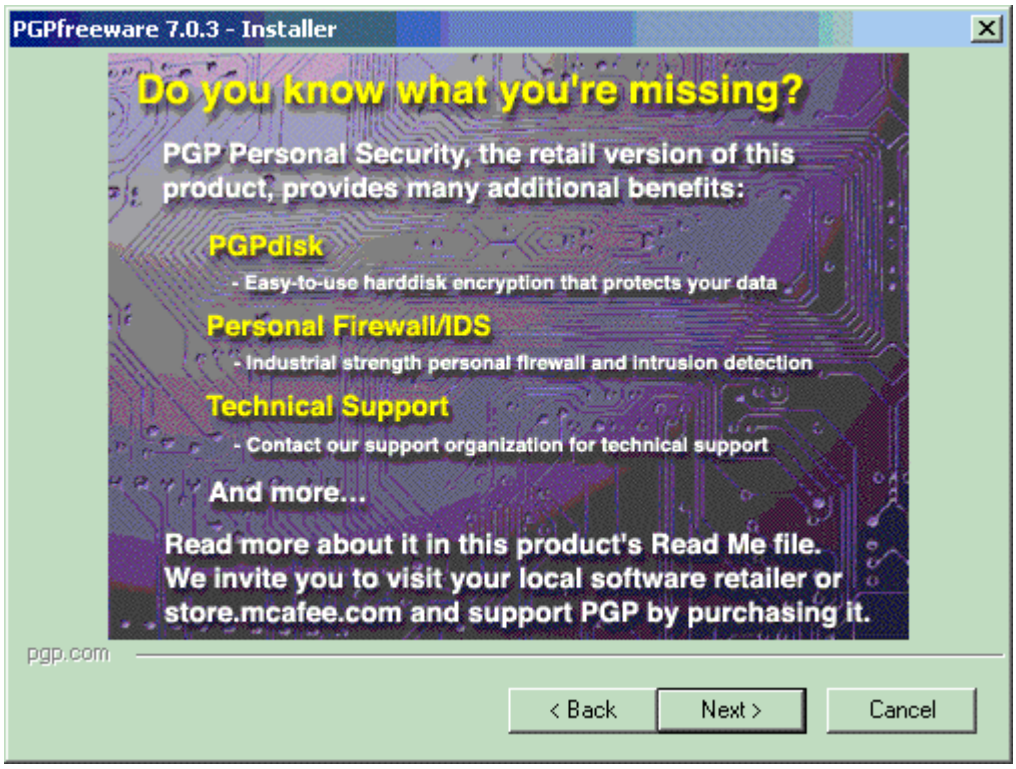


- **PGP Key Management**: contiene le funzioni principali del programma. Installazione obbligatoria;
- **PGPnet Personal Firewall/IDS/VPN**: funzionalità di Firewall, Intrusion Detection System (IDS) e Virtual Private Network (VPN). Attenzione perchè da prove fatte, l'installazione di questo componente su sistemi Microsoft Windows 2000 e Windows XP potrebbe creare dei problemi;
- **PGP Plugin for Microsoft Outlook**: componente integrata nel programma MS Outlook che permette di utilizzare tutte le funzionalità di PGP direttamente dall'interno dell'applicazione;
- **PGP Plugin for Microsoft Outlook Express**: componente integrata nel programma MS Outlook Express che permette di utilizzare tutte le funzionalità di PGP direttamente dall'interno dell'applicazione;
- **PGP Plugin for Qualcomm Eudora**: componente integrata nel programma Qualcomm Eudora che permette di utilizzare tutte le funzionalità di PGP direttamente dall'interno dell'applicazione;
- **PGP Plugin for ICQ**: componente integrata nel programma ICQ che permette di utilizzare tutte le funzionalità di PGP direttamente dall'interno dell'applicazione;
- **PGP Documentation**: documentazione a corredo di PGP.

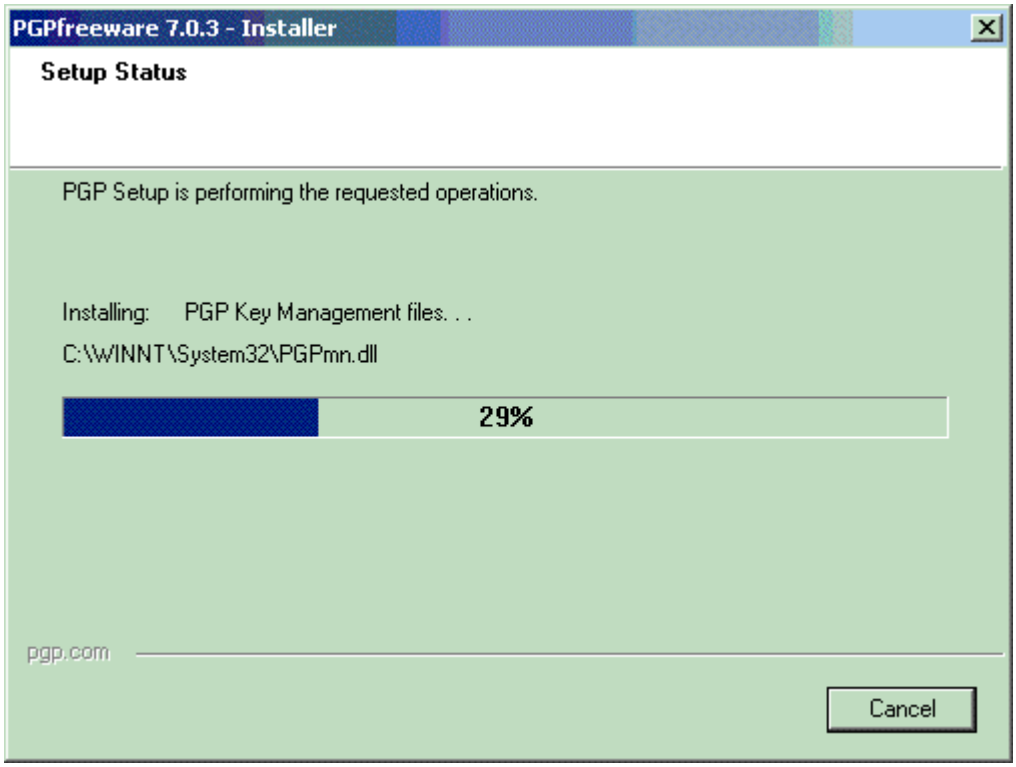
9. Il programma, prima di passare a copiare i file necessari, vi presenterà un riepilogo delle opzioni selezionate. Dopo aver verificato la corrispondenza con quanto da voi scelto, per proseguire selezionate 'Next'.



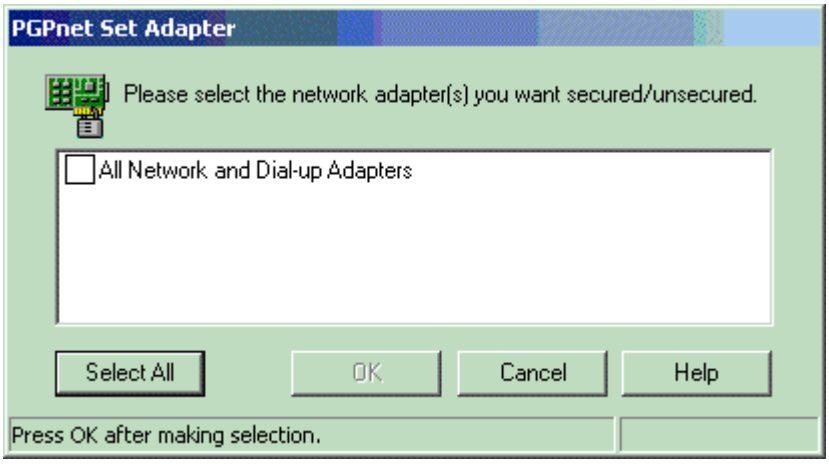
10. Quali sono le differenze fra la versione Freeware di PGP e quella Personal Security? Eccovele riassunte in questo messaggio. Selezionate 'Next' per proseguire.



11. Dopo di che vengono effettuate le operazioni richieste

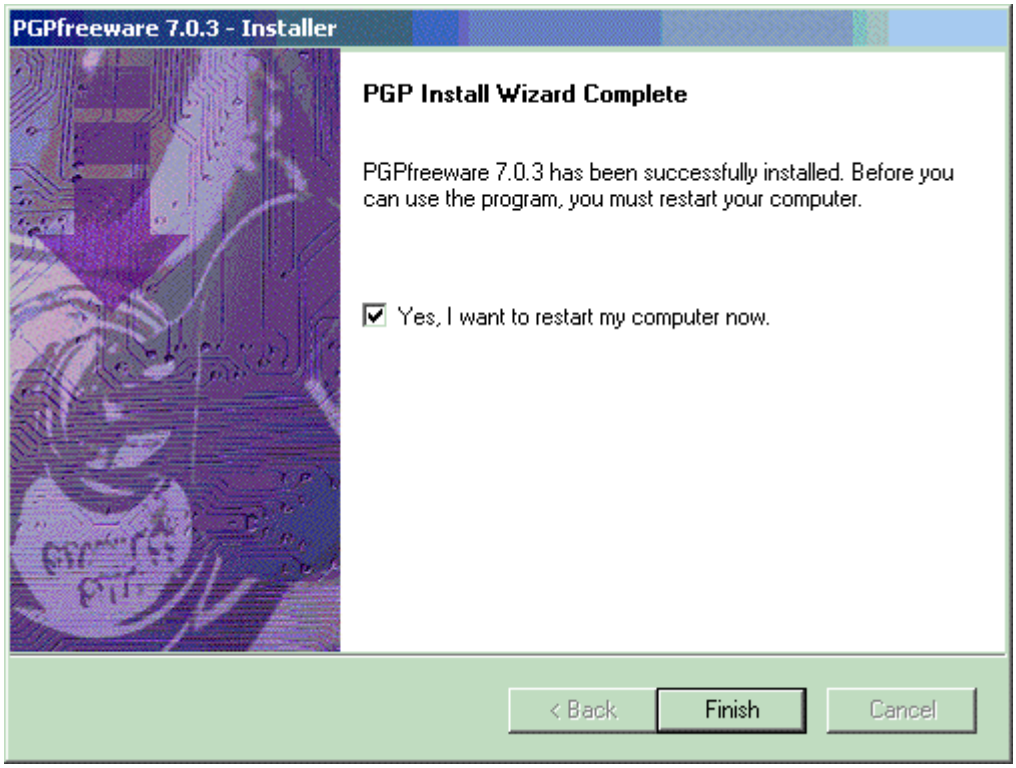


12. Vi viene presentata una finestra dalla quale scegliere l'adattatore di rete da utilizzare per le funzionalità integrate in PGPnet. Una volta fatta la scelta, selezionate 'OK'.



13. Il programma installerà, avvierà o cancellerà tutta una serie di servizi e drivers legati alle componenti selezionate.

14. Fino a presentarvi l'ultima schermata, richiedendovi di riavviare il sistema per ultimare l'installazione. Selezionate 'Finish'.



Modifiche apportate

Le principali modifiche apportate riguardano il filesystem, l'interfaccia utente ed il Registro di sistema.

Modifiche al filesystem

Queste sono le principali modifiche apportate in un sistema MS Windows 2000 Server ITA dopo aver installato il programma utilizzando come utente Administrator:

Creazione delle seguenti cartelle:

- C:\Programmi\Network Associates\PGP for Windows 2000\
- C:\Programmi\Network Associates\PGP for Windows 2000\PGP Uninstall Information\
- C:\Programmi\Network Associates\PGP for Windows 2000\Default Keys\
- C:\Programmi\Network Associates\PGP for Windows 2000\Sample Keys\
- C:\Programmi\Network Associates\PGP for Windows 2000\Documentation\
- C:\Documents and Settings\Administrator\Documenti\PGP\
- C:\Documents and Settings\All Users\Dati applicazioni\Network Associates\PGP
- C:\Documents and Settings\Administrator\Dati applicazioni\NetworkAssociates\PGP
- C:\Documents and Settings\Administrator\Impostazioni locali\Dati applicazioni\NetworkAssociates\PGP
- C:\Documents and Settings\All Users\Dati applicazioni\Network Associates\PGP

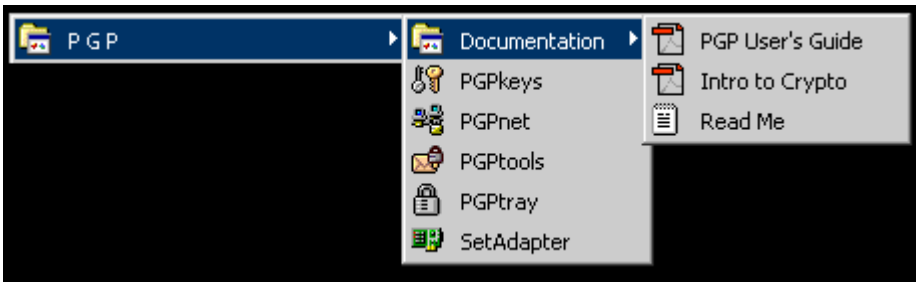
Aggiunta dei seguenti files:

- C:\Programmi\Network Associates\PGP for Windows 2000\PGP Uninstall Information\Setup.exe
- C:\Programmi\Network Associates\PGP for Windows 2000\PGPkeys.exe
- C:\Programmi\Network Associates\PGP for Windows 2000\PGPtools.exe
- C:\Programmi\Network Associates\PGP for Windows 2000\PGPtray.exe

- C:\Programmi\Network Associates\PGP for Windows 2000\PGPlog.exe
- C:\WINNT\System32\PGPsdkServ.exe
- C:\Programmi\Network Associates\PGP for Windows 2000\PGPnet.exe
- C:\Programmi\Network Associates\PGP for Windows 2000\SetAdapter.exe
- C:\Programmi\Network Associates\PGP for Windows 2000\PGPservice.exe
- C:\WINNT\System32\PGPclientLib.dll
- C:\WINNT\System32\PGPhk.dll
- C:\WINNT\System32\PGPsc.dll
- C:\WINNT\System32\PGPnotify.dll
- C:\WINNT\System32\PGPsdk.dll
- C:\WINNT\System32\PGPsdkNL.dll
- C:\WINNT\System32\PGPsdkUI.dll
- C:\WINNT\System32\PGPexch.dll
- C:\WINNT\System32\PGPoe.dll
- C:\Programmi\Network Associates\PGP for Windows 2000\Sample Keys\SampleKeys.asc
- C:\WINNT\System32\Drivers\PGPnet.sys
- C:\WINNT\System32\Drivers\PGPcfg.sys
- C:\WINNT\System32\drivers\PGPcfgwin2k.sys
- C:\WINNT\System32\drivers\PGPnetwin2k.sys
- C:\WINNT\System32\drivers\PGPsdk.sys
- C:\Programmi\Network Associates\PGP for Windows 2000\PGPalert0.wav
- C:\Programmi\Network Associates\PGP for Windows 2000\PGPnet.chm
- C:\WINNT\System32\PGP.chm
- C:\Programmi\Network Associates\PGP for Windows 2000\PGP.chm
- C:\WINNT\inf\pgpcfg2k.inf
- C:\WINNT\inf\PGPnet.inf
- C:\WINNT\inf\PGPnet_m.inf
- C:\Programmi\Network Associates\PGP for Windows 2000\Documentation\IntroToCrypto.pdf
- C:\Programmi\Network Associates\PGP for Windows 2000\Documentation\PGPWinUsersGuide.pdf
- C:\Programmi\Network Associates\PGP for Windows 2000\Documentation\ReadMe.htm
- C:\Programmi\Network Associates\PGP for Windows 2000\Sample Keys\WhatIsThis.txt
- C:\Programmi\Network Associates\PGP for Windows 2000\Documentation\ReadMe.txt
- C:\Programmi\Network Associates\PGP for Windows 2000\Documentation\RSALicense.txt
- C:\Documents and Settings\Administrator\Dati applicazioni\Network Associates\PGP\PGPprefs.txt
- C:\Documents and Settings\All Users\Dati applicazioni\Network Associates\PGP\PGPnetPrefs.txt
- C:\Programmi\Network Associates\PGP for Windows 2000\Default Keys\ PubRing.pkr
- C:\Programmi\Network Associates\PGP for Windows 2000\Default Keys\ SecRing.skr
- C:\Documents and Settings\Administrator\Documenti\PGP\pubring.pkr
- C:\Documents and Settings\Administrator\Documenti\PGP\secring.skr
- C:\Documents and Settings\All Users\Dati applicazioni\Network Associates\PGP\randseed.rnd
- C:\Documents and Settings\All Users\Dati applicazioni\Network Associates\PGP\randseed.rnd
- C:\WINNT\inf\PGPnet.PNF
- C:\WINNT\inf\pgpcfg2k.PNF
- C:\WINNT\inf\PGPnet_m.PNF
- C:\Documents and Settings\All Users\Dati applicazioni\Network Associates\PGP\PGPnetLog.dat
- C:\Programmi\Network Associates\PGP for Windows 2000\PGP Uninstall Information\layout.bin
- C:\Programmi\Network Associates\PGP for Windows 2000\PGP Uninstall Information\data1.hdr
- C:\Programmi\Network Associates\PGP for Windows 2000\PGP Uninstall Information\data1.cab
- C:\Programmi\Network Associates\PGP for Windows 2000\PGP Uninstall Information\Setup.ini
- C:\Programmi\Network Associates\PGP for Windows 2000\PGP Uninstall Information\setup.inx

Modifiche all'interfaccia utente

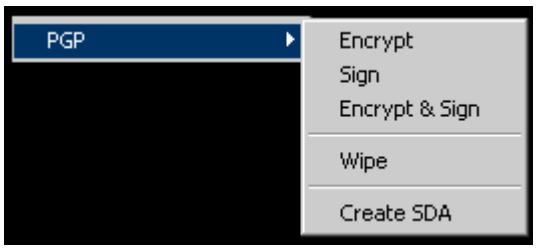
L'installazione, in un sistema MS Windows 2000 Server ITA, aggiunge un gruppo di programmi PGP alla barra Start sotto la voce 'Programi'.



L'installazione aggiunge anche un nuovo strumento all'interno del system tray. Si tratta del PGPtray e viene visualizzato in due modi, come un lucchetto chiuso isolato oppure come un lucchetto chiuso collegato ad un cavo di rete.

Premendo uno qualsiasi dei due pulsanti del mouse sull'icona del lucchetto nel system tray verrà visualizzato questo menu a tendina:

Un altra modifica riguanda Esplora risorse dove vengono aggiunte nuove estensioni. In pratica, dopo aver selezionato un file, basterà premere il tasto destro del mouse per avere fra le opzioni quelle relative al PGP:



Infine, visto che è stato scelto in fase di installazione, verrà anche installato il plug-in per la gestione delle funzionalità crittografiche di PGP all'interno del programma MS Outlook Express.

PGP 7.0.3 Freeware: Modifiche al registro di sistema.

Queste sono le principali chiavi create in fase di installazione di PGP 7.0.3 Freeware in un sistema MS Windows 2000 Server ITA. Quelle contrassegnate con (*) vengono automaticamente cancellate dal programma di installazione:

CHIAVE	VALORE
HKLM\Software\Network Associates\PGP	
HKLM\Software\Network Associates\PGP\7.01	
HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\PGPTray.Exe	
HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\PGPTray.Exe\Path	"C:\Programmi\Network Associates\PGP for Windows 2000"
HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\PGPTray.Exe\(Default)	"C:\Programmi\Network Associates\PGP for Windows 2000\PGPTray.Exe"
HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\ {EA61CE20-860C-11D3-A05D-00104B6909D0}\UninstallString	"RunDll32 C:\PROGRA~1\FILECO~1\INSTAL~1\engine\6\INTEL3~1\ctor.dll,LaunchSetup "C:\Programmi\Network Associates\PGP for Windows 2000\PGP Uninstall Information\setup.exe" "
HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\ {EA61CE20-860C-11D3-A05D-00104B6909D0}\LogFile HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\ {EA61CE20-860C-11D3-A05D-00104B6909D0}\DisplayName	"C:\Programmi\Network Associates\PGP for Windows 2000\PGP Uninstall Information\setup.ilg"
HKCR\.asc\(Default)	"PGP"
HKCR\.skr\(Default)	"PGP Armored File"
HKCR\.shf\(Default)	"PGP Private Keyring"
HKCR\.rnd\(Default)	"PGP Share"
HKCR\.pgr\(Default)	"PGP Random Seed"
HKCR\CLSID\{969223c0-26aa-11d0-90ee-444553540000}\(Default)	"PGP Groups"
HKCR\CLSID\{969223c0-26aa-11d0-90ee-444553540000}\InProcServer32\(Default)	"PGP Shell Extension"
HKCR\PGP Encrypted File	"pgpmn.dll"
HKCR\PGP Encrypted File\(Default)	
HKCU\PGP Encrypted File\DefaultIcon	"PGP Encrypted File"

CHIAVE	VALORE
HKCU\PGP Encrypted File\shell	
HKCU\PGP Encrypted File\shell\open	
HKCU\PGP Encrypted File\shell\open\command	
HKCR\PGP Encrypted File\shell\open\command\(Default)	
HKCU\PGP Armored File	"C:\Programmi\Network Associates\PGP for Windows 2000\pgptools.exe %1"
HKCR\PGP Armored File\(Default)	"PGP Armored File"
HKCU\PGP Armored File\DefaultIcon	
HKCR\PGP Armored File\DefaultIcon\(Default)	"pgpsc.dll,-143"
HKCU\PGP Armored File\shell	
HKCU\PGP Armored File\shell\open	
HKCU\PGP Armored File\shell\open\command	
HKCR\PGP Armored File\shell\open\command\(Default)	"C:\Programmi\Network Associates\PGP for Windows 2000\pgptools.exe %1"
HKCR\.aexpk\(Default)	"PGP Armored Extracted Public Key"
HKCU\PGP Armored Extracted Public Key	
HKCR\PGP Armored Extracted Public Key\(Default)	"PGP Armored Extracted Public Key"
HKCR\PGP Armored Extracted Public Key\DefaultIcon	
HKCR\PGP Armored Extracted PublicKey\DefaultIcon\(Default)	"pgpsc.dll,-147"
HKCR\PGP Armored Extracted Public Key\shell	
HKCR\PGP Armored Extracted Public Key\shell\open	
HKCR\PGP Armored Extracted Public Key\shell\open\command	
HKCR\PGP Armored Extracted Public Key\shell\open\command\(Default)	"C:\Programmi\Network Associates\PGP for Windows 2000\pgpkeys.exe %1"
HKCR\PGP Binary Extracted Public Key	
HKCR\PGP Binary Extracted Public Key\(Default)	"PGP Binary Extracted Public Key"
HKCU\PGP Binary Extracted Public Key\DefaultIcon	
HKCR\PGP Binary Extracted Public Key\DefaultIcon\(Default)	"pgpsc.dll,-147"
HKCR\PGP Binary Extracted Public Key\shell	
HKCR\PGP Binary Extracted Public Key\shell\open	
HKCR\PGP Binary Extracted Public Key\shell\open\command	
HKCR\PGP Binary Extracted Public Key\shell\open\command\(Default)	"C:\Programmi\Network Associates\PGP for

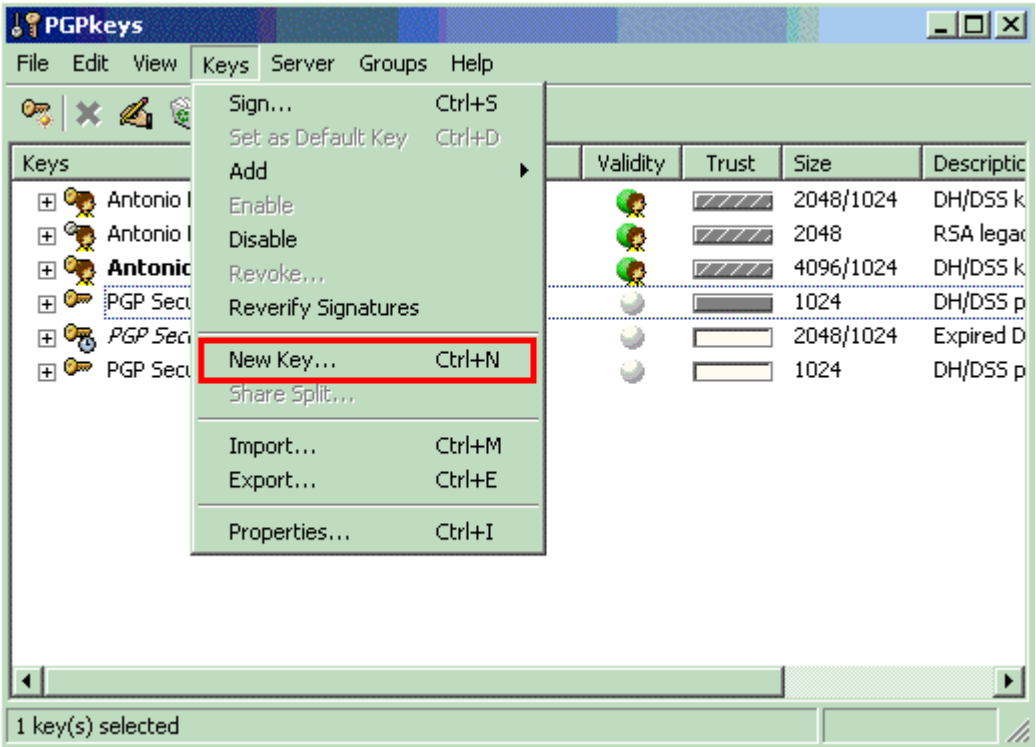
CHIAVE	VALORE
	Windows 2000\pgpkeys.exe %1"
HKCR\PGP Detached Signature File	
HKCR\PGP Detached Signature File\(Default)	"PGP Detached Signature File"
HKCU\PGP Detached Signature File\DefaultIcon	
HKCR\PGP Detached Signature File\DefaultIcon\(Default)	"pgpsc.dll,-142"

Generare le chiavi

Per avviare la procedura di generazione di una nuova coppia di chiavi potete:

- utilizzare l'apposita icona presente nella barra degli strumenti:

- selezionare la voce di menu Keys > New Key...



In entrambi i casi, partirà l'autocomposizione guidata:

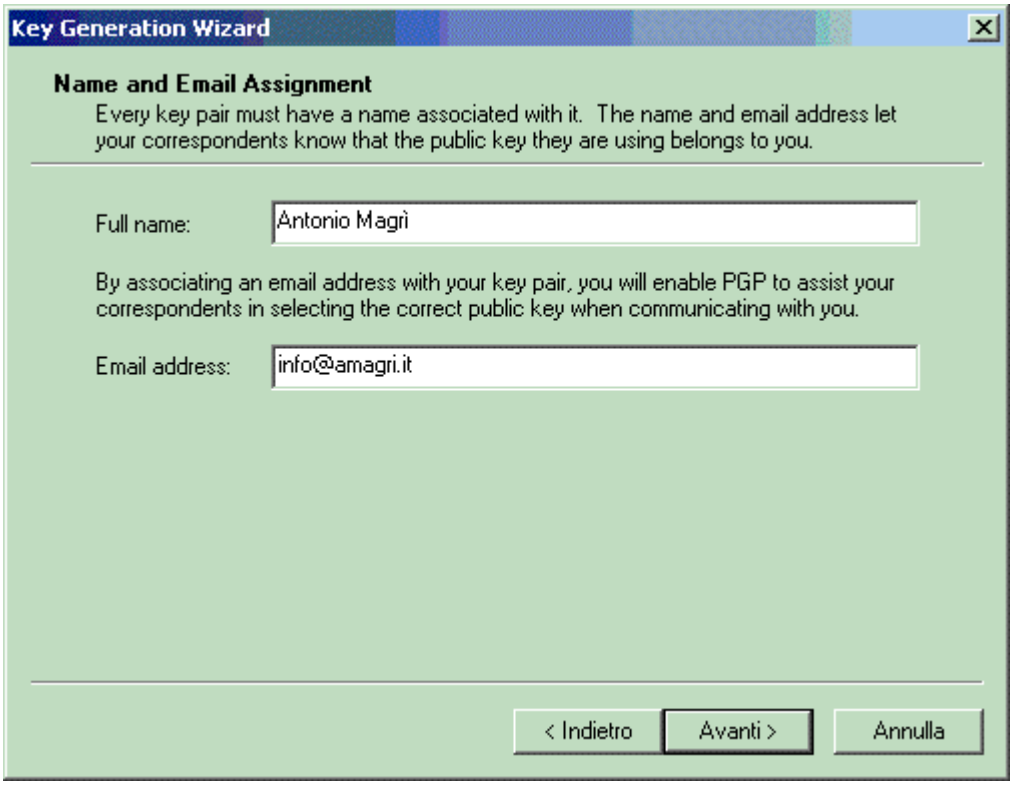
A questo punto, dopo aver letto le informazioni visualizzate, le possibilità a nostra disposizione sono due:

- proseguire, selezionando il pulsante 'Avanti >', ed utilizzare la Procedura semplificata;
- oppure cliccare sul pulsante 'Expert' e passare alla Procedura per esperti.

Procedura semplificata

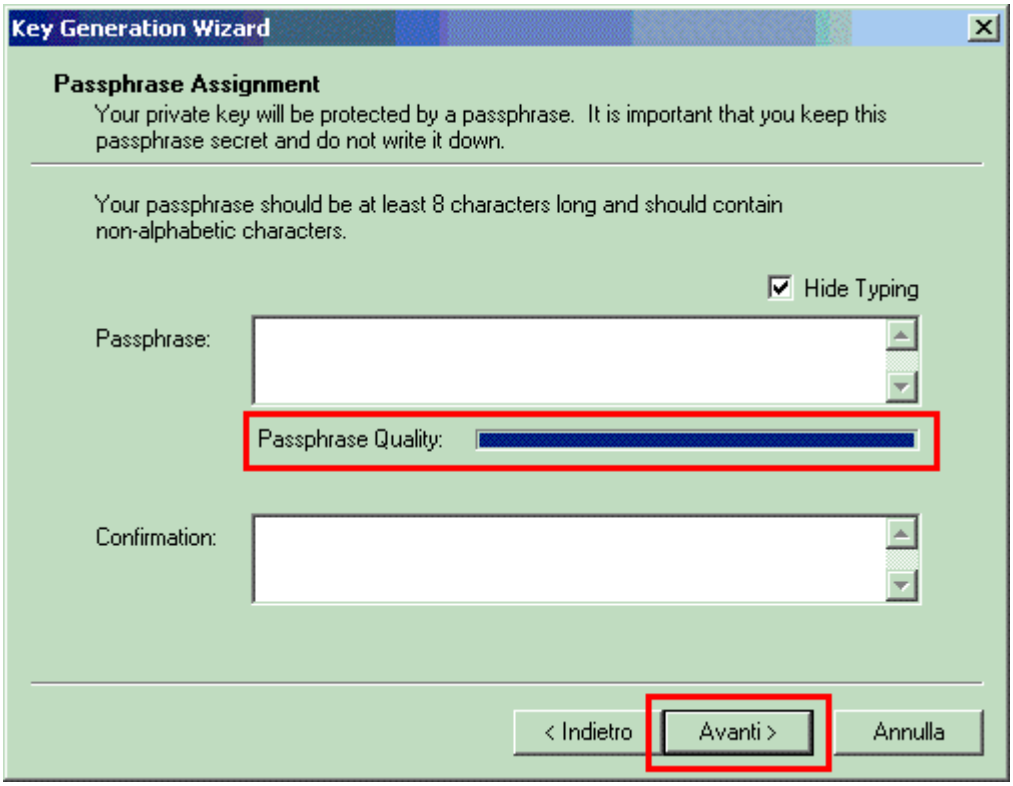
1. Abbiamo selezionato 'Avanti', quindi vogliamo utilizzare la procedura semplificata.

2. Vi verrà richiesto di inserire il vostro nome e cognome nel campo 'Full name' ed il vostro indirizzo di posta elettronica nel campo 'Email address'. Come consigliato dal programma, sarebbe preferibile utilizzare dei dati reali o che almeno vi rendano facilmente identificabili dai vostri corrispondenti.



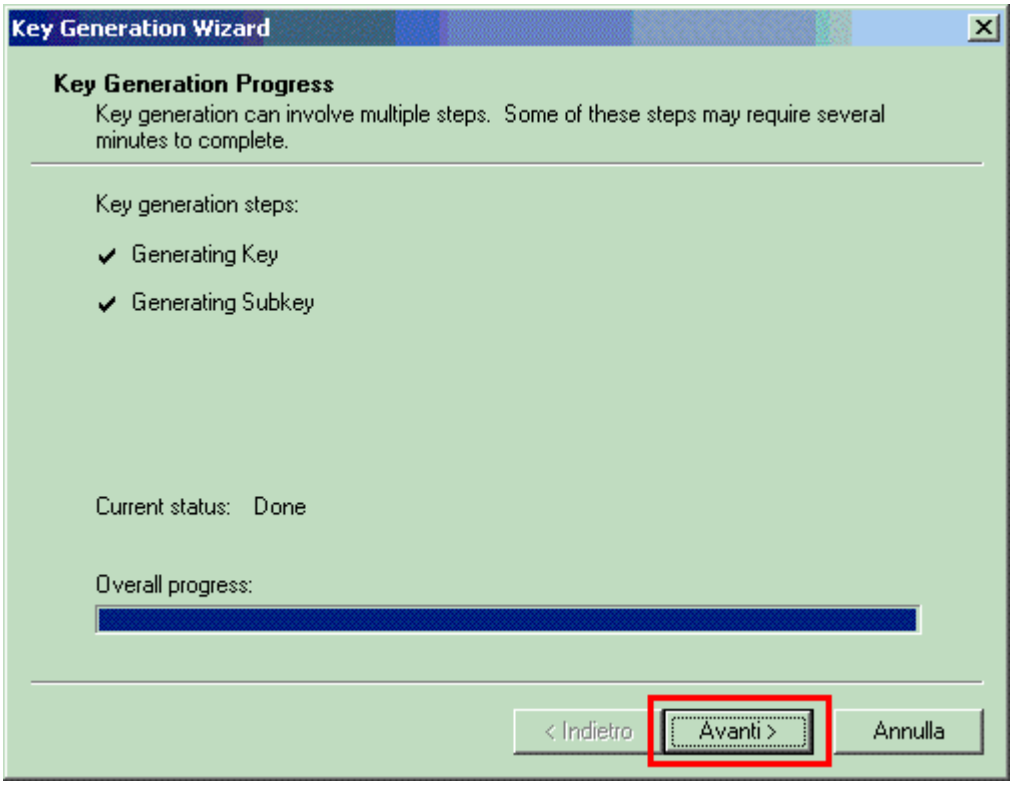
Terminato l'inserimento dei dati, selezionate 'Avanti >'.

3. La nuova finestra permette di definire uno degli elementi più importanti di tutta la procedura guidata: la frase password. E' importante che questa sia più lunga di 8 caratteri e che contenga anche dei caratteri non alfabetici. La 'bontà' della vostra frase password vi verrà segnalata da un apposito indicatore grafico.



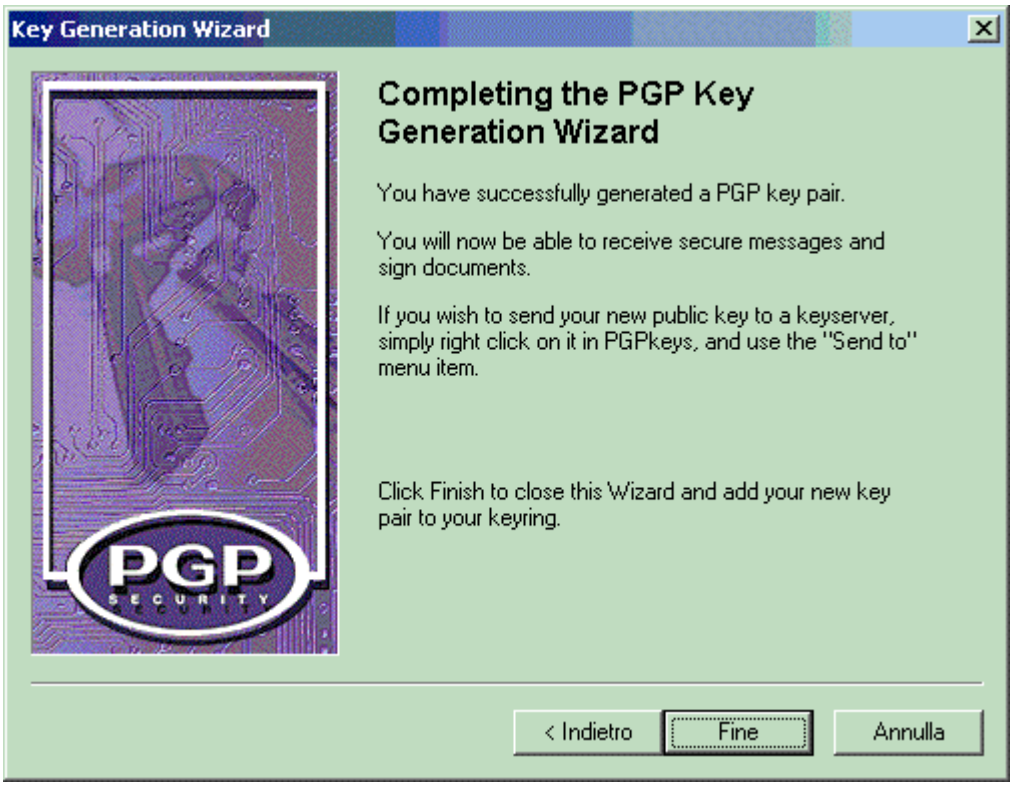
Ricordatevi di confermare la frase password inserita, dopo di che selezionate 'Avanti'.

4. Si passa alla generazione delle chiavi vere e proprie:

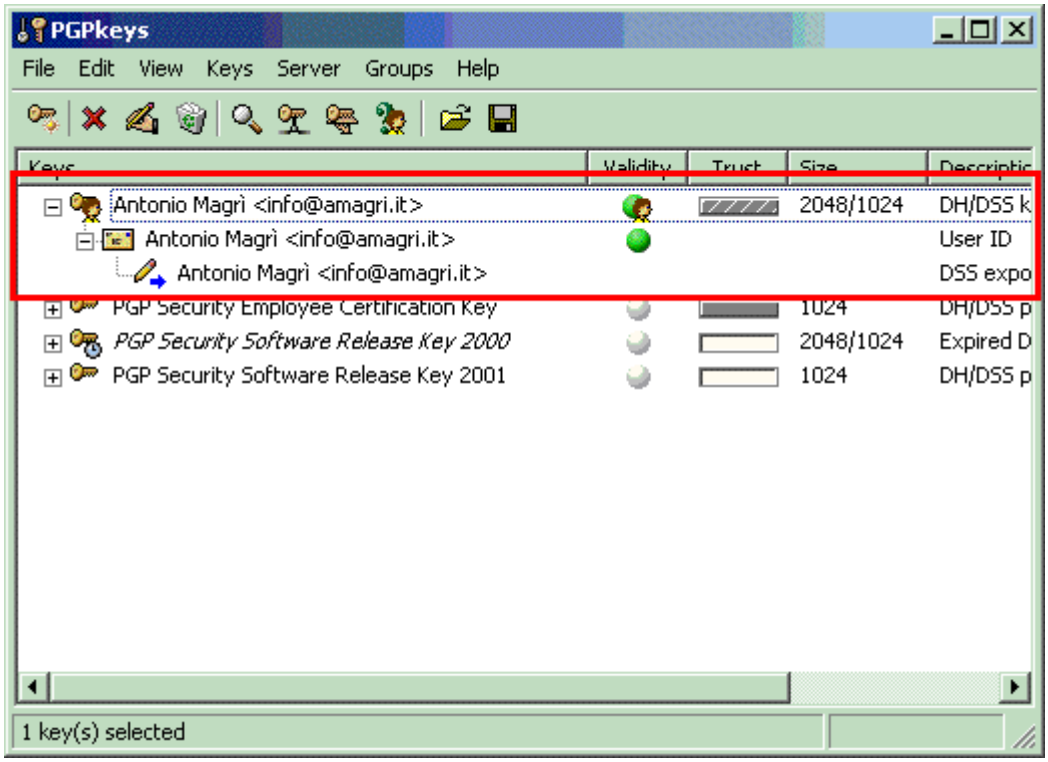


Il termine dell'operazione sarà segnalato dalla dicitura: 'Current status: Done'. Selezionate 'Avanti >' per continuare.

5. La procedura è terminata. Per aggiungere la chiave appena generata al vostro portachiavi, selezionate 'Fine'.



6. Come potete vedere, dando un'occhiata al vostro portachiavi nel PGPkeys, la chiave è stata generata utilizzando gli algoritmi DH e DSS con una grandezza di 2048 e 1024 bits.

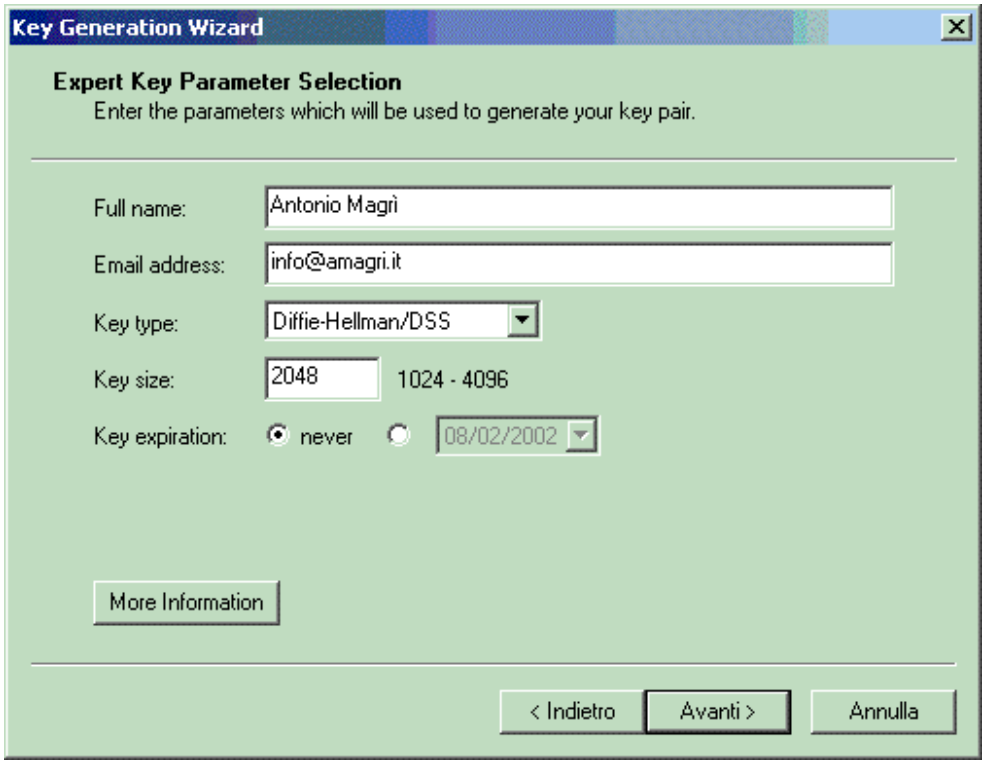


Procedura per esperti

1. Abbiamo selezionato 'Expert', quindi vogliamo utilizzare la procedura per esperti.

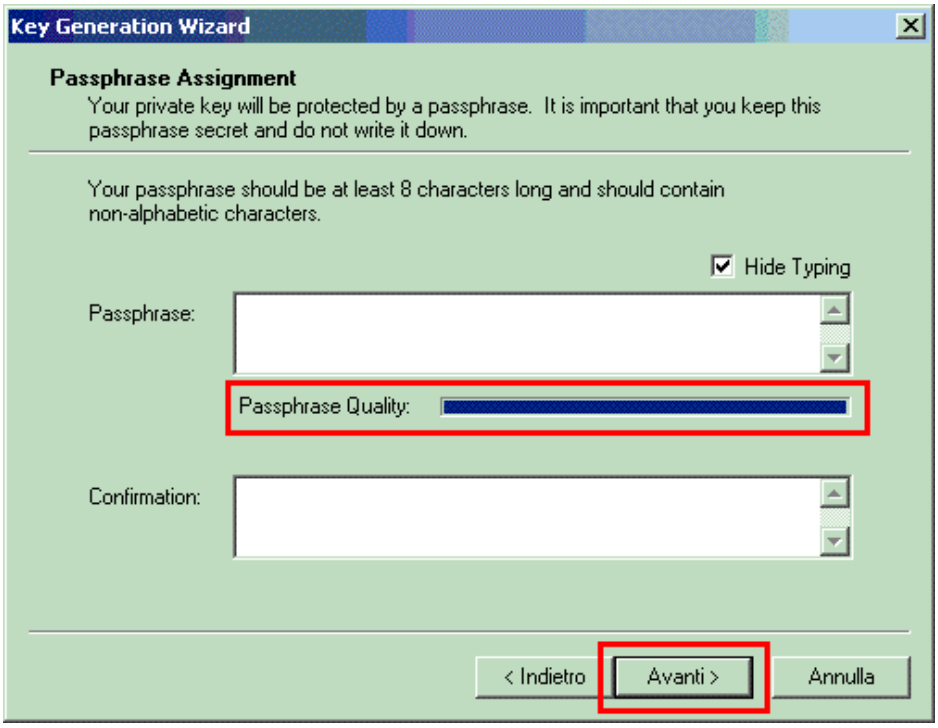
2. Inseriamo il nostro nome e cognome nel campo 'Full name' ed il nostro indirizzo di posta elettronica nel campo Email address dopo di che passiamo a scegliere l'algoritmo crittografico da utilizzare. Abbiamo diverse scelte:

- **Diffie-Hellman/DSS**: l'accoppiata di algoritmi crittografici Diffie-Hellman/DSS con grandezza massima 4096/1024. La coppia di chiavi generata sarà compatibile con le versioni di PGP dalla 5.x in poi.
- **RSA**: la nuova versione delle chiavi RSA V4 con grandezza massima di 4096 bits e caratteristiche simili alle chiavi DH. Se selezioniamo questa opzione, il programma ci avvertirà che la coppia di chiavi generata (in realtà due coppie) sarà compatibile con le versioni di PGP dalla 7.x in poi.
- **RSA Legacy**: come segnalato dal programma, è compatibile con tutte le versioni di PGP. Grandezza massima della chiave 2048 bits.



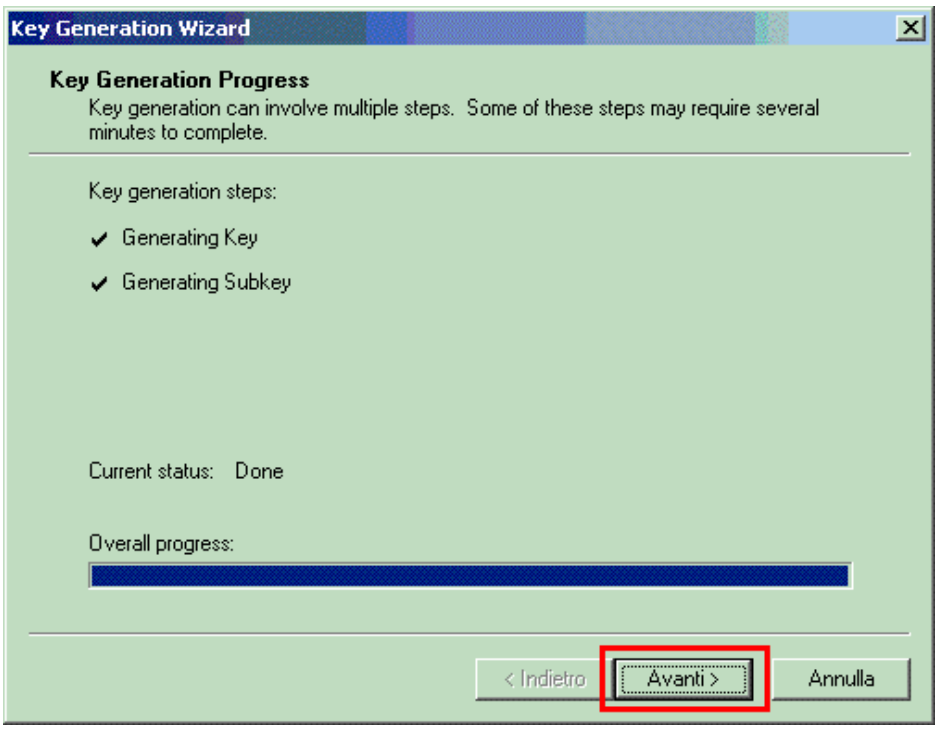
Dopo aver scelto il tipo di chiave ed aver risposto 'OK' agli eventuali messaggi che ci avvertono dei problemi di compatibilità esistenti, scegliamone la grandezza e l'eventuale scadenza dopo di che per continuare selezioniamo 'Avanti >'.

3. La nuova finestra permette di definire uno degli elementi più importanti di tutta la procedura guidata: la frase password. E' importante che questa sia più lunga di 8 caratteri e che contenga anche dei caratteri non alfabetici. La 'bontà' della vostra frase password vi verrà segnalata da un apposito indicatore grafico.



Ricordatevi di confermare la frase password inserita, dopo di che selezionate 'Avanti'.

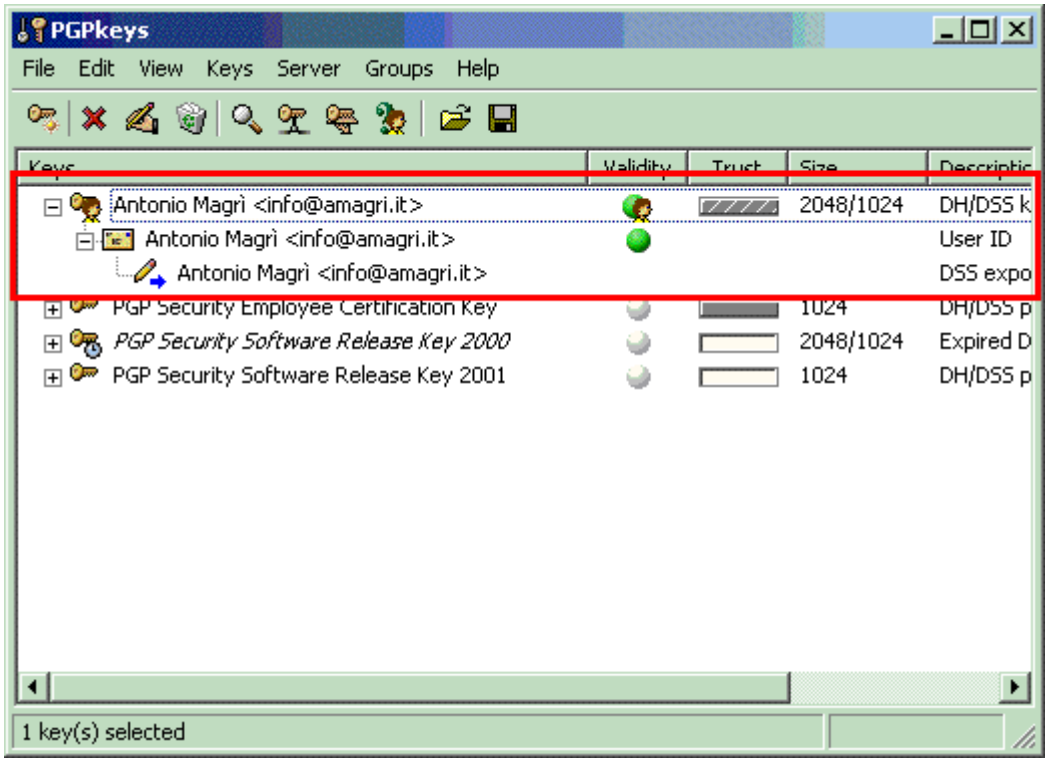
4. Si passa alla generazione delle chiavi vere e proprie:



Il termine dell'operazione sarà segnalato dalla dicitura: 'Current status: Done'. Selezionate 'Avanti >' per continuare.

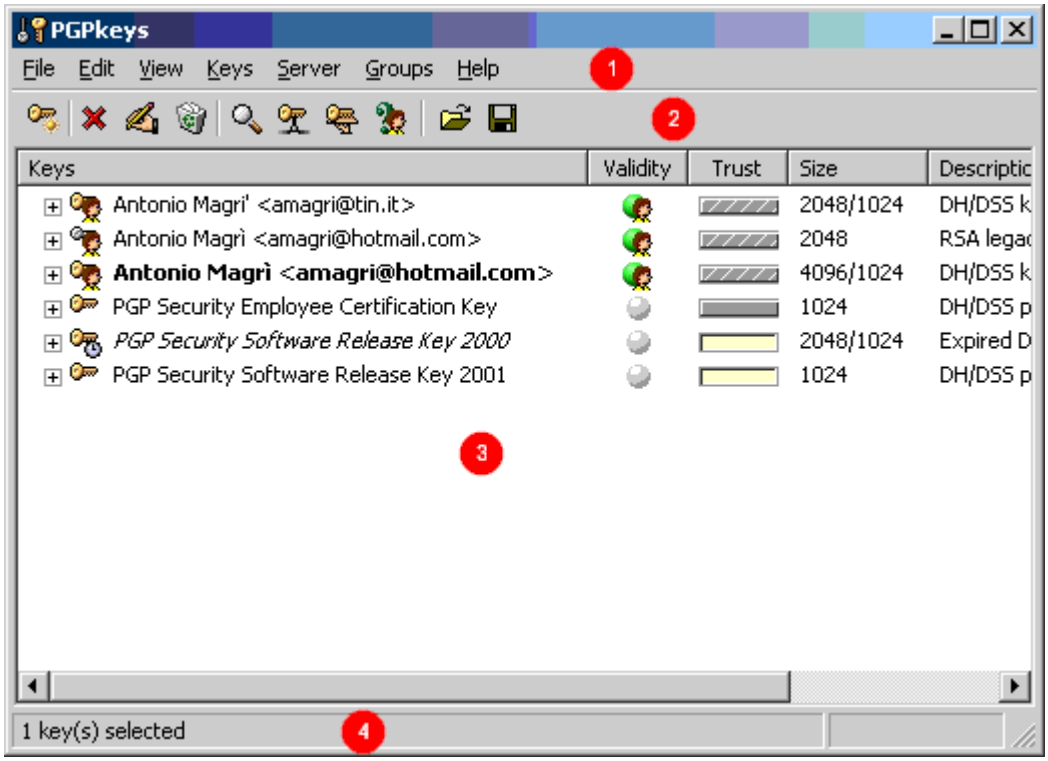
5. La procedura è terminata. Per aggiungere la chiave appena generata al vostro portachiavi, selezionate 'Fine'.

7. Ritorneremo al PGPkeys con la chiave appena generata selezionata e visualizzata completamente espansa.



PGPkeys

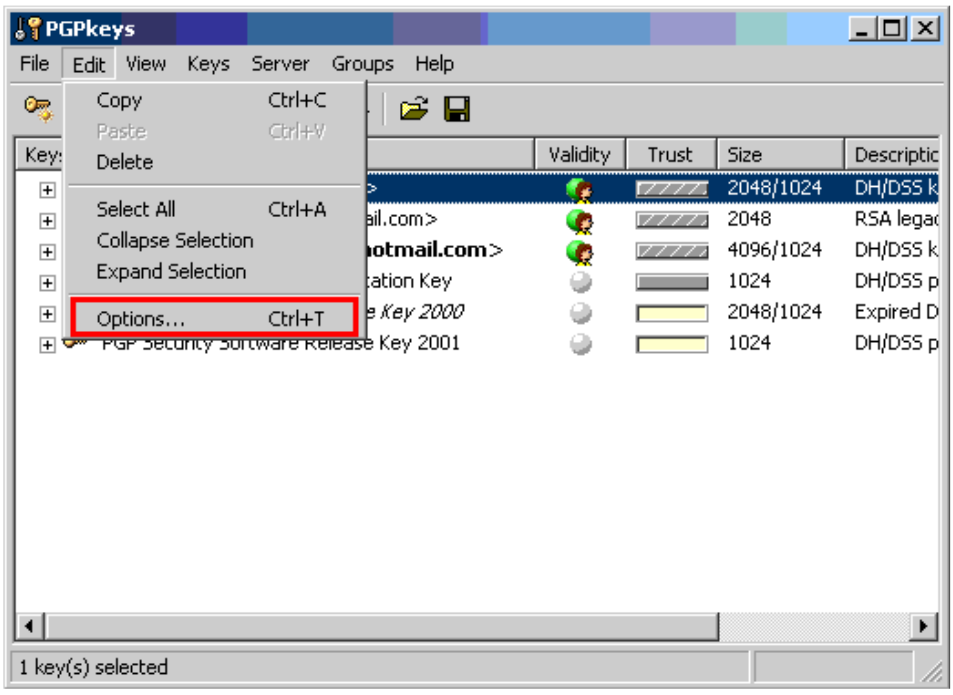
La finestra dell'applicazione del programma PGPkeys può essere facilmente suddivisa in quattro aree principali:



1. **Barra dei menu**;
2. **Barra degli strumenti**: contenente i pulsanti per l'accesso rapido alle funzioni di utilizzo comune;
3. **Riquadro principale**: visualizza le informazioni fondamentali relative alle chiavi contenute all'interno del portachiavi selezionato;
4. **Barra di stato**: fornisce maggiori informazioni sull'operazione in corso.

Opzioni

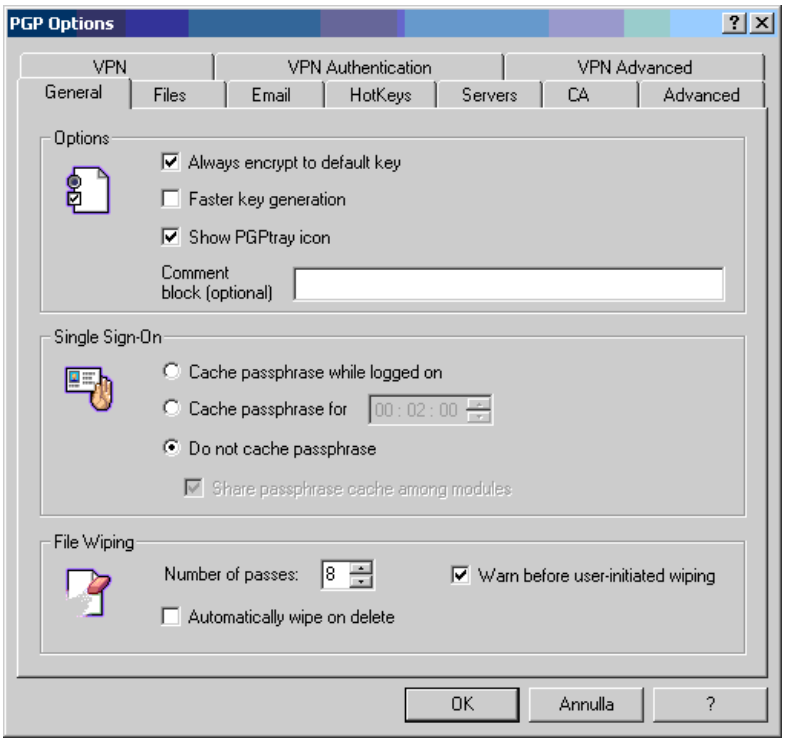
Per accedere alle opzioni basta selezionare l'apposita voce di menu Edit > Options:



Verrà aperta una nuova finestra contenente tutti i fogli di proprietà disponibili. Vediamoli insieme partendo da quello 'General'.

Foglio di proprietà 'General'

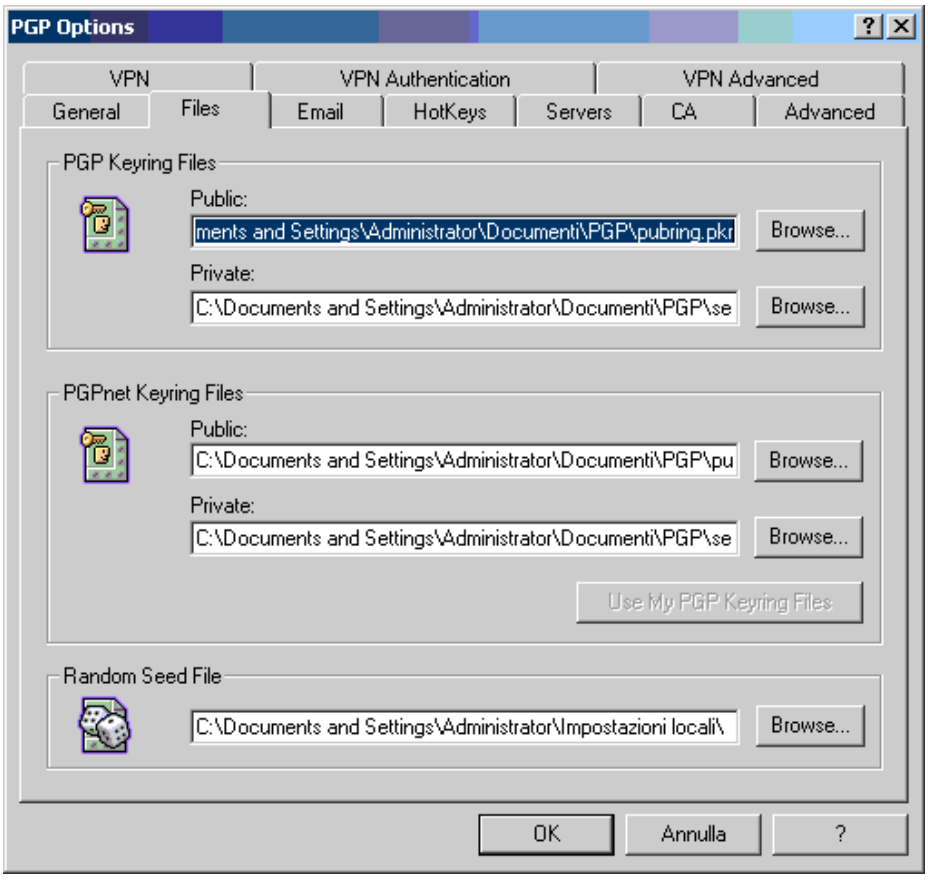
Contiene le opzioni di uso generale.



- **Always encrypt to default key**: quando selezionato, tutti i messaggi o allegati cifrati con la chiave pubblica di un eventuale destinatario sono anche cifrati con la vostra chiave pubblica di default, così da permettervi di rileggerne il contenuto.
- **Faster key generation**: quando selezionato, permette di risparmiare del tempo nel processo di generazione di una coppia di chiavi Diffie-Hellman di lunghezza compresa tra quelle disponibili tra 1024 e 4096 bits. In pratica sceglie i numeri primi necessari alla generazione da un set già pronto invece di calcolarli al momento. Per aumentare la sicurezza è conveniente disabilitare questa opzione.
- **Show PGPtray icon**: se selezionato, integra uno strumento, che consente l'accesso alle principali funzionalità del programma, all'interno del System tray.
- **Comment block**: commento visualizzato in tutti i messaggi cifrati tra il testo di intestazione -- BEGIN PGP MESSAGE BLOCK -- ed il numero della versione di PGP.
- **Cache passphrase while logged on**: quando selezionato, per ogni tipologia di azione, memorizza in memoria la frase password fino al log off dell'utente.
- **Cache passphrase for**: memorizza la frase password in memoria per il tempo indicato e per la singola tipologia di azione.
- **Do not cache passphrase**: non memoriazza in memoria la frase password.
- **Share passphrase cache among modules**: permette di passare da un modulo all'altro senza digitare nuovamente la frase password.
- **Number of passes**: numero di passaggi effettuati sul disco dalla funzione di cancellazione sicura.
- **Warn before user-initiated wiping**: vi avvisa prima di procedere nell'operazione di cancellazione sicura.
- **Automatically wipe on delete**: quando selezionato, cancella in modo sicuro i files presenti all'interno del cestino, all'atto dello svuotamento dello stesso.

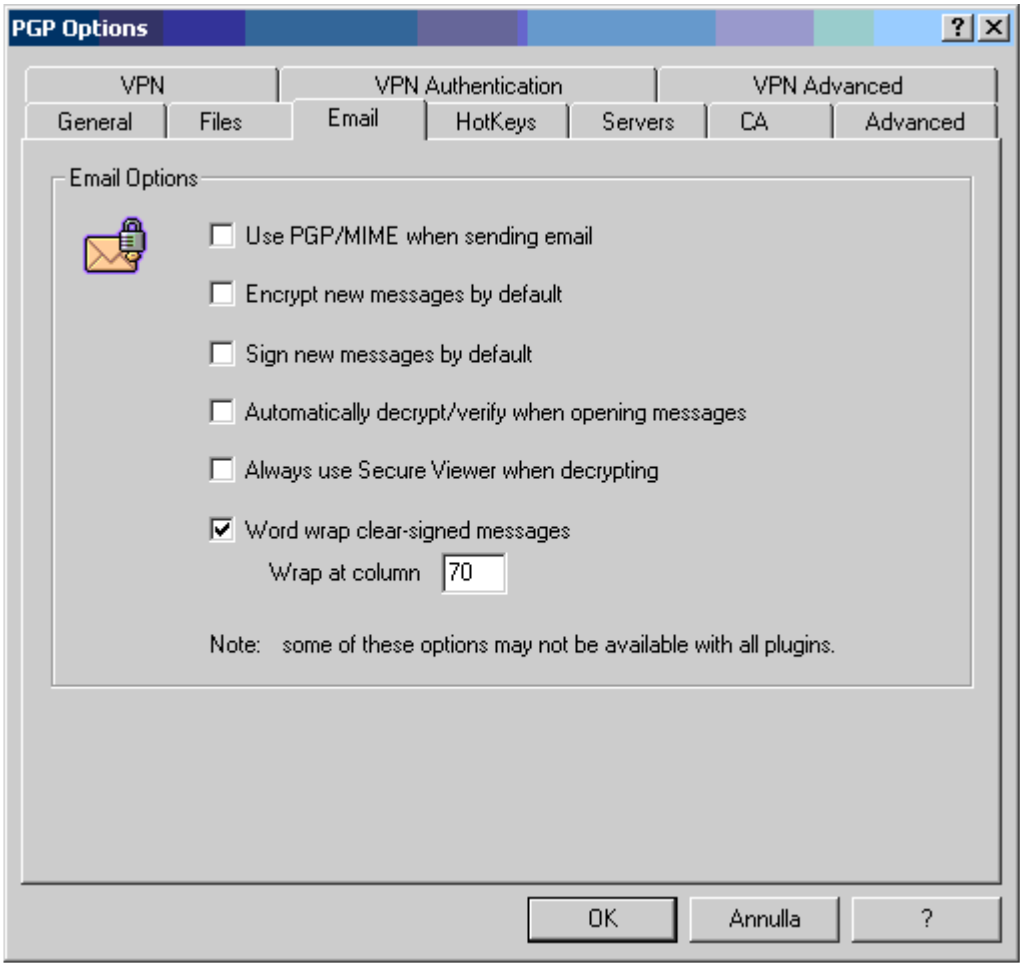
Foglio di proprietà 'Files'

Specifica la posizione ed il nome dei files utilizzati come portachiavi, sia dal programma che dal PGPnet, e la posizione del file utilizzato come raccolta di dati casuali necessari durante la generazione di una nuova coppia di chiavi.



- **PGP keyring files - Public**: percorso e nome del file portachiavi contenente le chiavi pubbliche utilizzate dal programma PGP. Utilizzando il pulsante 'Browse', comune a tutte le opzioni presenti nel foglio di proprietà, viene facilitata la localizzazione e la scelta del file all'interno del filesystem.
- **PGP keyring files - Private**: percorso e nome del file portachiavi contenente le chiavi private utilizzate dal programma PGP.
- **PGPnet keyring files - Public**: percorso e nome del file portachiavi contenente le chiavi pubbliche utilizzate dal programma PGPnet.
- **PGPnet keyring files - Private**: percorso e nome del file portachiavi contenente le chiavi private utilizzate dal programma PGPnet.
- **Random Seed File**: percorso e nome del file contenente l'insieme dei dati casuali necessari durante la generazione di una nuova coppia di chiavi.

Foglio di proprietà 'Email' Configura le opzioni relative alle applicazioni di posta elettronica supportate dai plug-in di PGP.

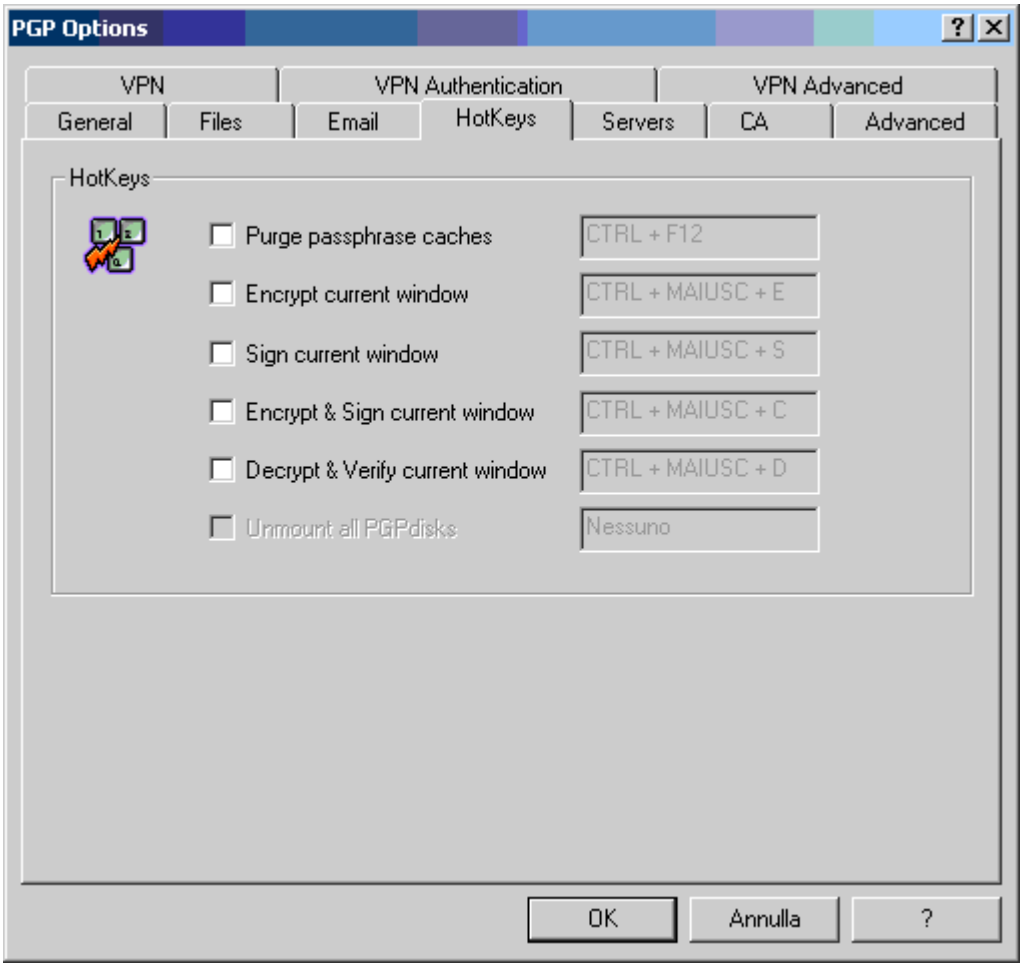


- **Use PGP/MIME when sending email**: se il programma di posta elettronica supporta il formato PGP/MIME basta abilitare questa opzione per far si che il messaggio venga automaticamente cifrato e firmato prima di essere inviato al destinatario. Quest'ultimo deve a sua volta avere un programma di posta elettronica compatibile con il formato PGP/MIME (per esempio Eudora) per poter leggere il tutto.
- **Encrypt new messages by default**: cifra automaticamente tutta la posta in uscita.
- **Sign new messages by default**: firma automaticamente tutta la posta in uscita.
- **Automatically decrypt/verify when opening messages**: cerca di decifrare/verificare automaticamente un messaggio quando questo viene aperto. Se richiesto richiede la frase password.

- **Always use Secure Viewer when decrypting**: se selezionato, per evitare un attacco TEMPEST visualizza i files decifrati utilizzando dei caratteri speciali all'interno della finestra Secure Viewer. I messaggi che vengono cifrati con questa opzione attiva non possono essere salvati in chiaro visto che sono visibili esclusivamente nella finestra Secure Viewer.
- **Word wrap clear-signed messages**: se selezionato indica il numero di colonne dopo le quali applicare obbligatoriamente un ritorno a capo all'interno del testo che costituisce la firma digitale. E' stato introdotto perchè alcuni programmi di posta elettronica potrebbero inserire dei ritorni a capo in modo errato all'interno della firma e comprometterne quindi la leggibilità.
- **Wrap at column**: indica da quale colonna applicare obbligatoriamente il ritorno a capo.

Foglio di proprietà 'HotKeys'

Configura i tasti o le combinazioni di tasti da utilizzare per effettuare in modo rapido buona parte delle operazioni di elaborazione crittografica del programma.

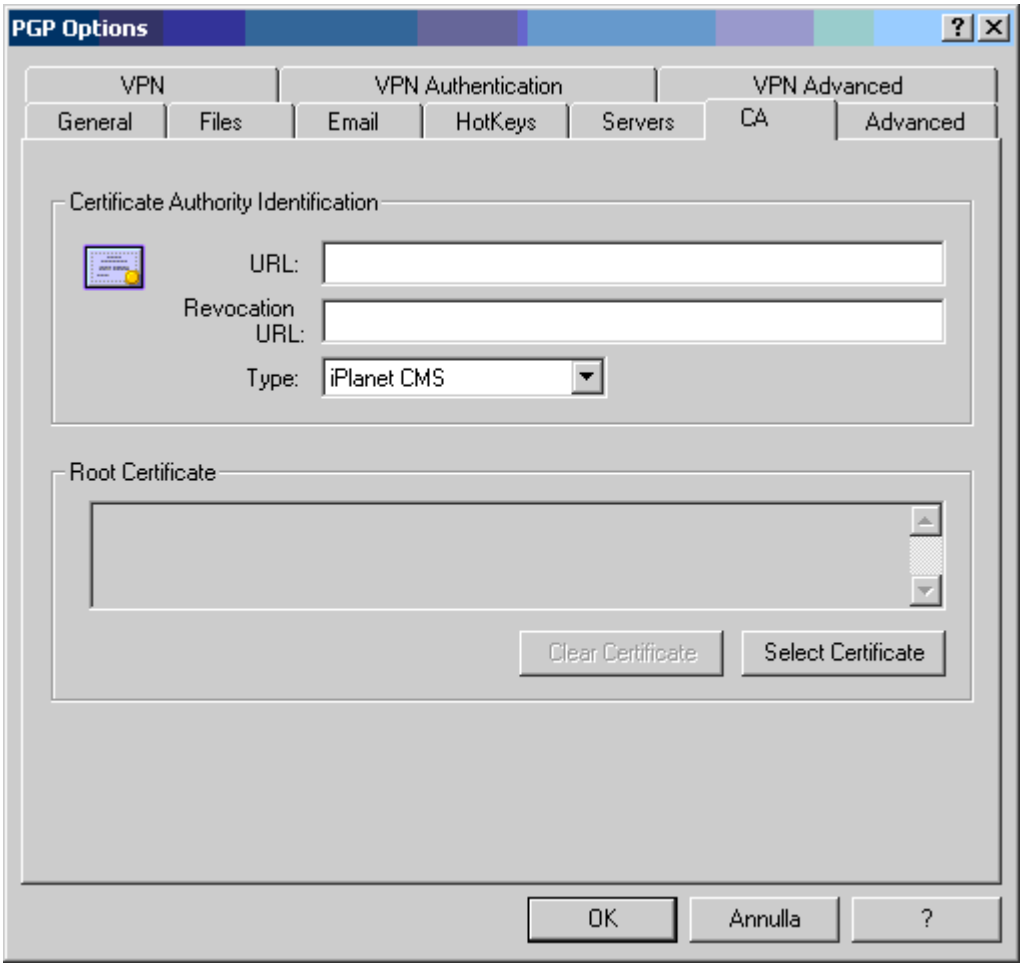


- **Lista Server**: visualizza i key server da visualizzare o meno nella finestra di ricerca di PGPkeys. Un circoletto verde nella colonna 'Listed' indica quelli da visualizzare mentre un circoletto grigio quelli da non visualizzare. Per modificare le informazioni relative al singolo server, basta selezionarlo e poi cliccare su:
  - **New**: permette di inserire un nuovo key server. Non occorre aver selezionato alcuna voce.
  - **Remove**: rimuove il key server selezionato.
  - **Edit**: modifica le specifiche relative al key server selezionato.
  - **Set as Root**: imposta il key server selezionato come predefinito per la ricerca.
  - **Move Up**: sposta il server selezionato di una posizione in alto nella lista di ricerca.
  - **Move Down**: sposta il server selezionato di una posizione in basso nella lista di ricerca.
- **Synchronize With Server Upon**: specifica quando bisogna effettuare una sincronizzazione fra le chiavi presenti all'interno del portachiavi locale ed il certificate server:

- **Encrypting to Unknown Keys**: se la chiave del destinatario del messaggio cifrato non è all'interno del portachiavi pubblico locale.
- **Signing Keys**: aggiorna la chiave che verrà utilizzata per la firma prima che questa avvenga e la restituisce al server al termine dell'operazione.
- **Adding Names/Photos/Revokers**: prima di effettuare una qualsiasi operazione di aggiunta nome, aggiunta foto o aggiunta addetti alla revoca, aggiorna la chiave con quella presente sul server e la invia nuovamente a quest'ultimo al termine dell'operazione.
- **Revocation**: aggiorna la chiave che verrà revocata prima che questo avvenga e la restituisce al server al termine dell'operazione.
- **Verification**: all'atto della verifica di un messaggio o file firmato del quale non si ha la chiave pubblica del mittente, il programma ricercherà automaticamente ed importerà la chiave dal key server.

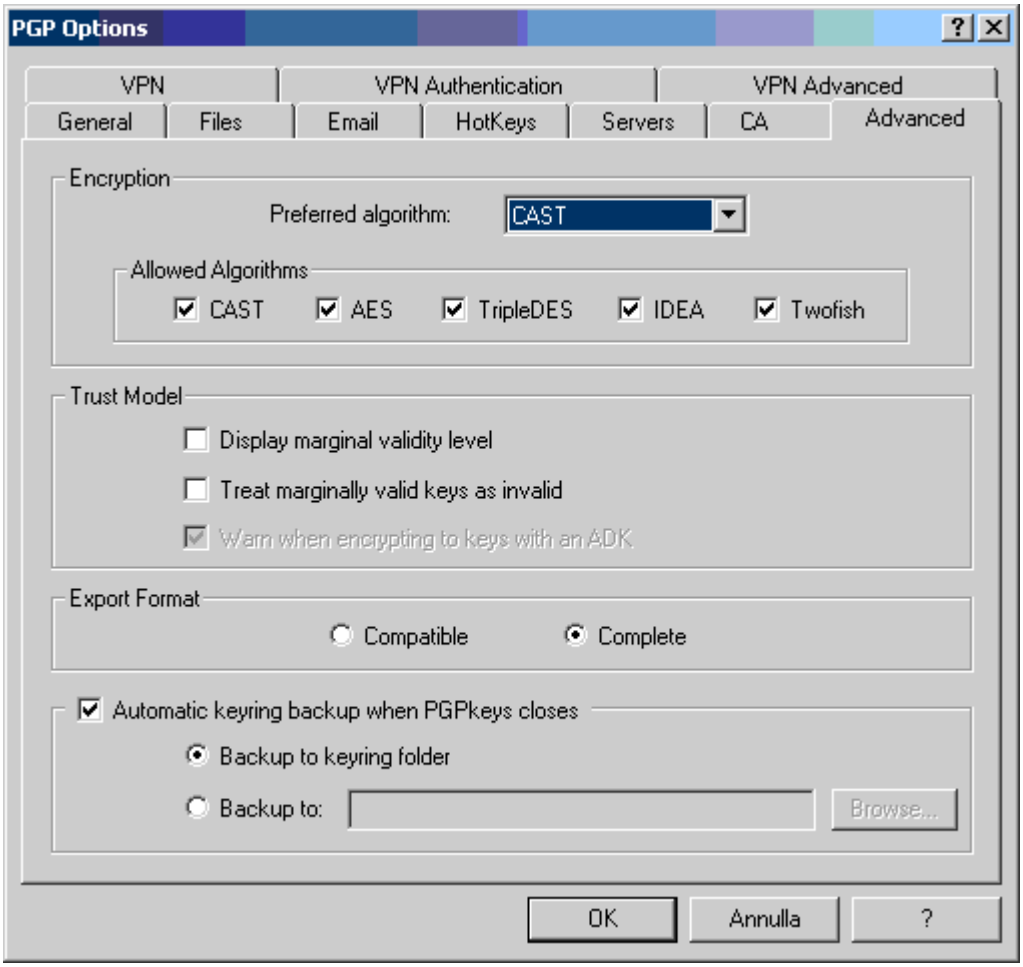
Foglio di proprietà 'CA'

Opzioni relative alla Certification Autority (CA).



- **URL**: l'URL della Root Certificate Authority.
- **Revocation URL**: l'URL alla quale è disponibile la Certificate Revocation List della CA.
- **Type**: tipo di CA utilizzata.
- **Root Certificate**: informazioni sul certificato della root CA.
- **Clear Certificate**: cancella le informazioni visualizzate all'interno della finestra Root Certificate.
- **Select Certificate**: specifica un certificato di root CA.

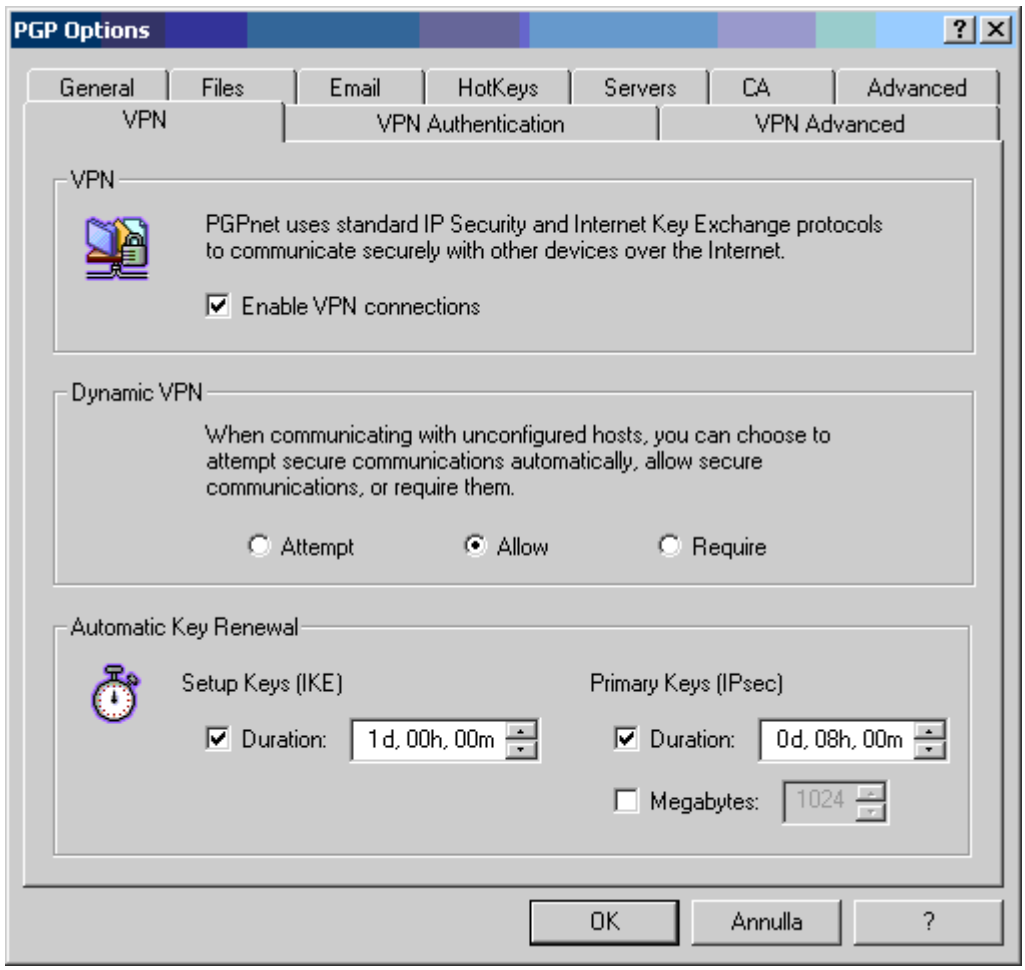
Foglio di proprietà 'Advanced'



- **Preferred algorithm**: permette di selezionare l'algoritmo crittografico utilizzato da PGP per cifrare. Di default viene utilizzato il CAST. Se si vuole utilizzare un altro algoritmo bisogna selezionare l'apposita voce prima di generare la propria coppia di chiavi.
- **Allowed Algorithms**: solo gli algoritmi selezionati vengono utilizzati per cifrare.
- **Display Marginal Validity Level**: visualizza le chiavi in parte non valide oppure permette di visualizzarne la validità mediante circoletti. Verde per una chiave valida, grigio per una chiave non valida.
- **Treat Marginally Valid Keys as Untrusted**: se selezionato, tratta tutte le chiavi parzialmente valide come non degne di fiducia e vi avvisa di questo.
- **Warn When Encrypting Keys to keys with an ADK**: vi avvisa prima di procedere nell'utilizzo di una chiave pubblica processata utilizzando l'Additional Decrytpion Key (ADK).
- **Export format - Compatible**: esporta le chiavi in un formato compatibile con le versioni precedenti di PGP.
- **Export format - Complete**: esporta le chiavi nel nuovo formato che include fra l'altro ID fotografico ed i certificati X.509.
- **Automatic keyring backup when PGPkeys closes**: effettua un copia di riserva dei portachiavi alla chiusura del programma PGPkeys.
- **Backup to keyring folder**: crea una copia di riserva dei portachiavi all'interno della cartella utilizzata normalmente da questi ultimi.
- **Backup to**: vi permettere di scegliere, anche utilizzando il pulsante 'Browse', il percorso in cui salvare la copia di riserva dei portachiavi.

Foglio di proprietà 'VPN'

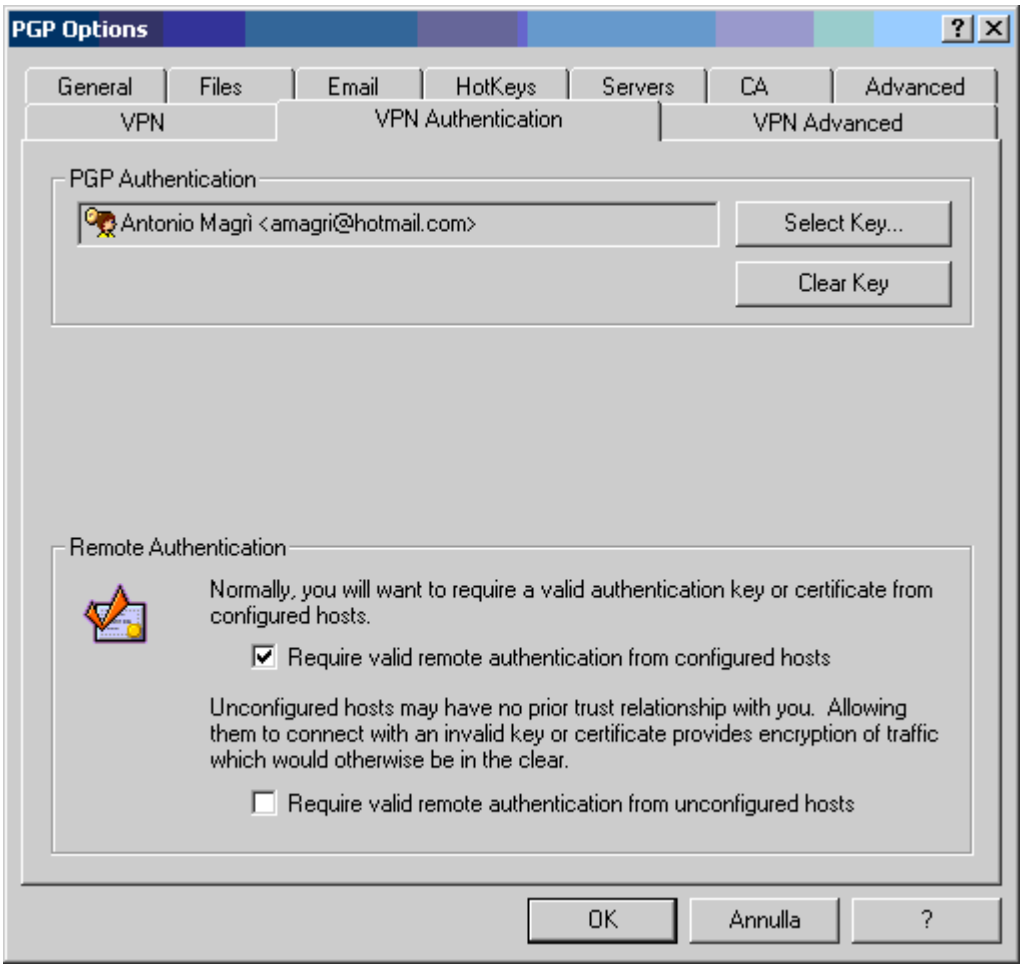
Permette di configurare le proprietà di base del servizio VPN.



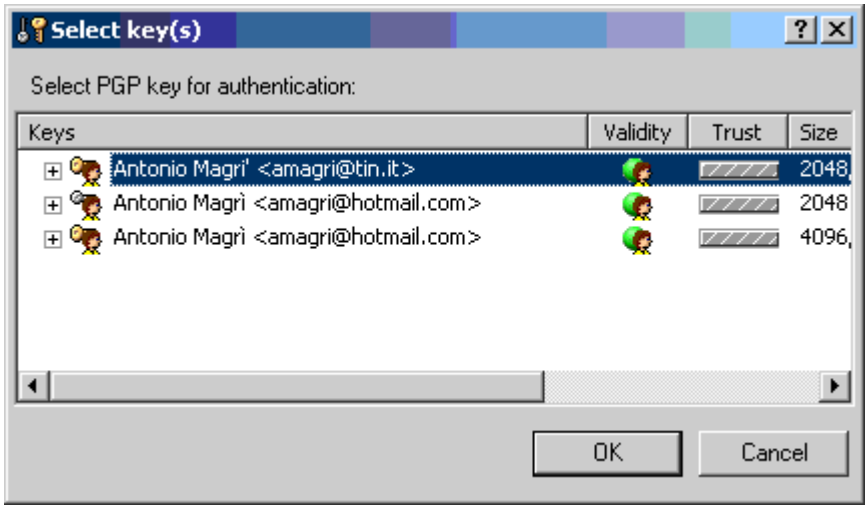
- **Enable VPN connection**: se selezionato, utilizzando IPSec ed IKE, permette l'utilizzo di connessioni VPN.
- **Dynamic VPN**: imposta la modalità di connessione utilizzata per instaurare una VPN dinamica con i sistemi non configurati:
  - **Attempt**: cerca di instaurare in ogni modo una connessione anche con un sistema per il quale non è stata prevista una Security Association (SA) cioè un insieme di regole utilizzate per la connessione stessa (algoritmo crittografico, la durata delle regole ed il metodo di autenticazione). In pratica, inizialmente cerca di connettersi utilizzando una connessione insicura, in chiaro, se viene rilevata una SA, passa ad utilizzare le regole definite in quest'ultima e quindi, in modo cifrato.
  - **Allow**: a differenza della precedente opzione, non cerca di instaurare una connessione con sistemi per cui non sia stata configurata una SA.
  - **Require**: tutto il traffico non sicuro viene automaticamente scartato.
- **Setup Keys - Duration**: quando selezionato, permette di impostare la durata temporale delle chiavi IKE. Se non selezionato, viene utilizzata la durata predefinita di otto ore. Da notare anche che, in una connessione viene sempre utilizzata la durata inferiore fra quelle impostate sui due sistemi.
- **Primary Keys - Duration**: quando selezionato, permette di impostare la durata temporale delle chiavi IPSec. Come per le chiavi IKE, se l'opzione non viene selezionata, viene utilizzata la durata predefinita di otto ore e in una connessione la durata inferiore fra quelle impostate sui due sistemi.
- **Primary Keys - Megabytes**: quando selezionato, permette di impostare il rinnovo della chiave basandosi sulla quantità di traffico effettuato. Come per le opzioni viste in precedenza, in una connessione viene sempre utilizzata la durata inferiore fra quelle impostate sui due sistemi.

Foglio di proprietà 'VPN Authentication'

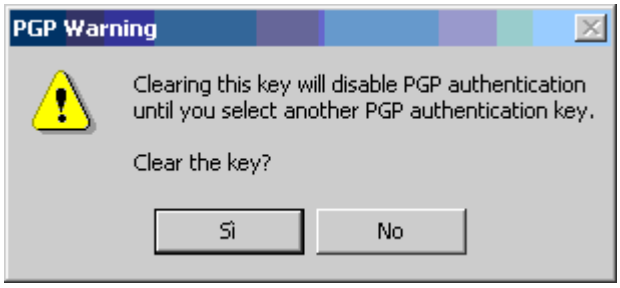
In questo foglio di proprietà l'utente ha la possibilità di scegliere i metodi di autenticazione utilizzati dal servizio VPN.



- **PGP Authentication**: configura la chiave da utilizzare durante una connessione con PGPnet.
- **Select Key...**: selezionando questo pulsante vi viene presentata una finestra per consentirvi di scegliere la chiave da utilizzare con PGPnet.



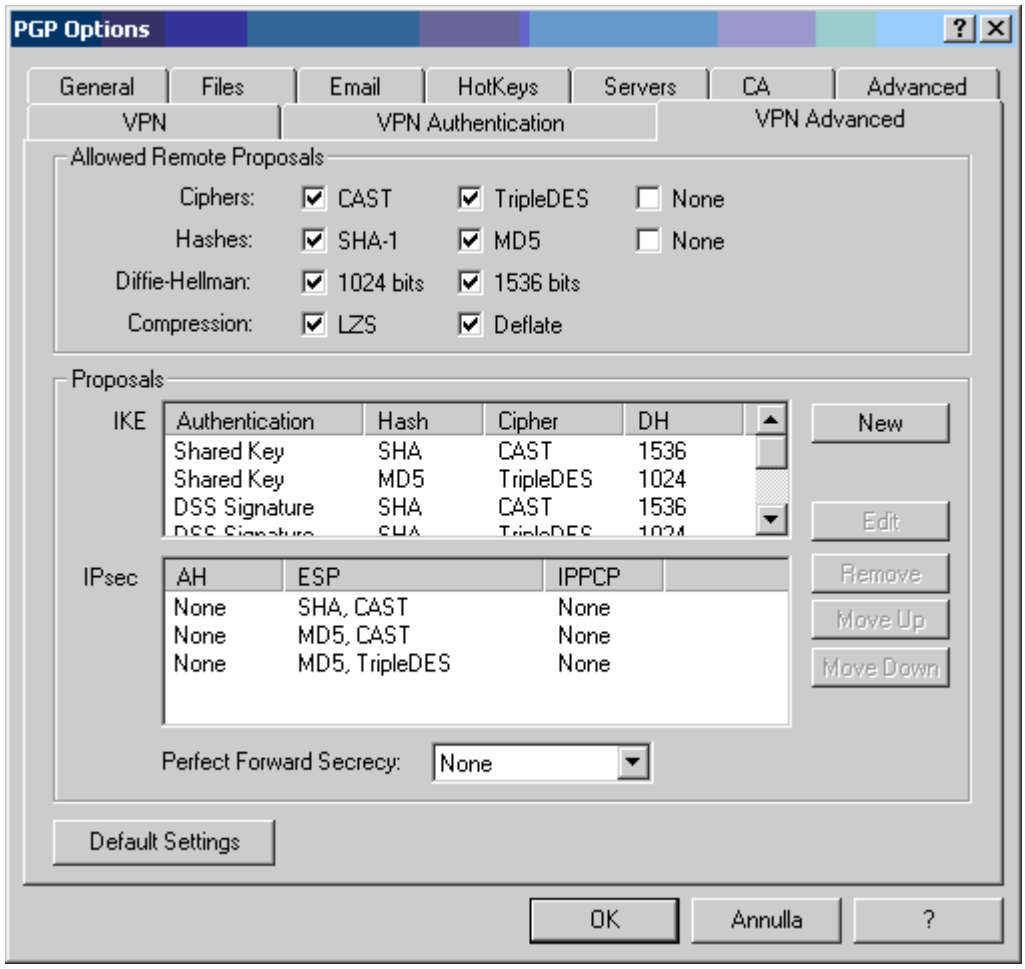
- **Clear Key**: elimina la chiave precedentemente selezionata. Prima di continuare vi viene richiesto di confermare l'operazione.



- **Require valid remote authentication from configured hosts**: se selezionato, richiede l'uso di un'autenticazione remota valida da parte di un sistema già configurato.
- **Require valid remote authentication from unconfigured hosts**: come l'opzione precedente ma riferito ad un sistema non configurato.

Foglio di proprietà 'VPN Advanced'

Questo foglio di proprietà permette di configurare in modo particolareggiato tutte le opzioni disponibili per il servizio PGPnet.



Le opzioni a nostra disposizione riguardano in particolare:

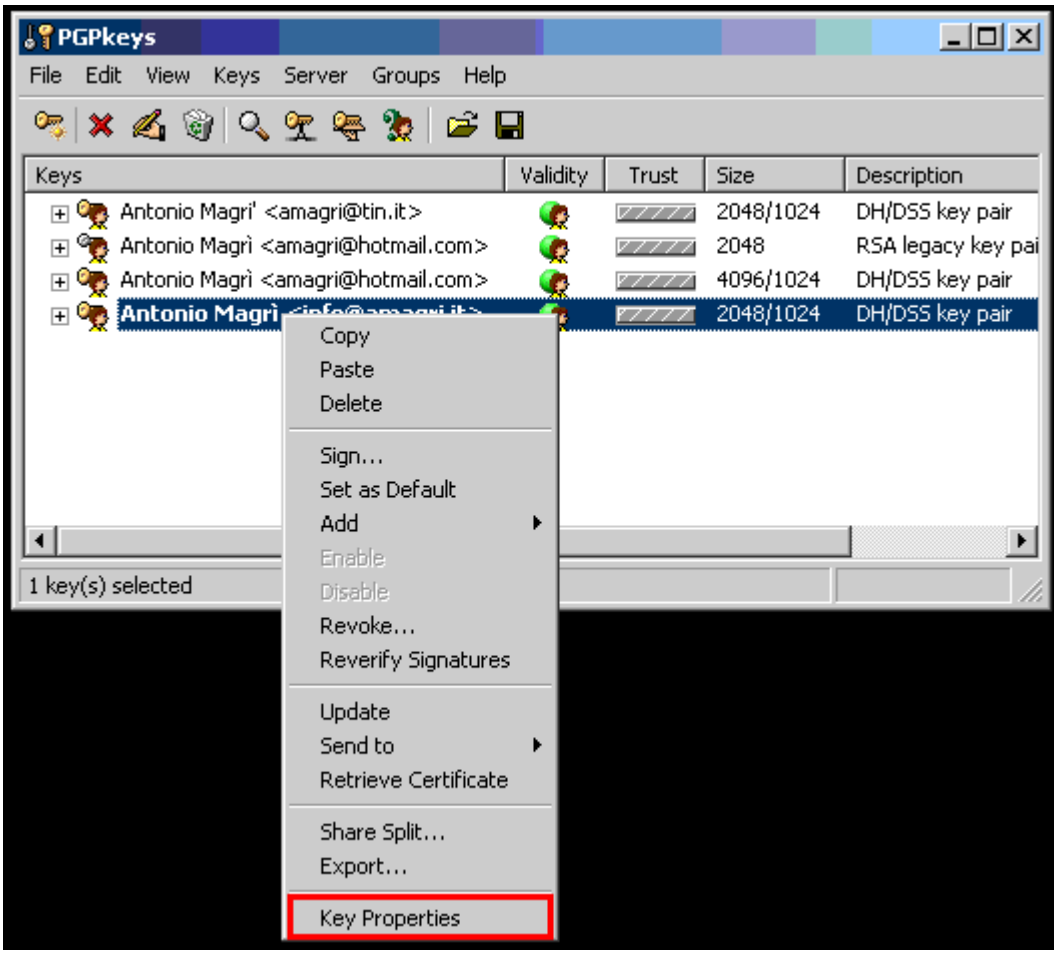
- Algoritmo crittografico utilizzato;
- Algoritmo di hash;
- Lunghezza della chiave Diffie-Hellman;
- Compressione utilizzata;
- IKE;
- IPSec;
- Perfect Forward Secrecy.

Il pulsante 'Default Settings' permette di ripristinare i valori predefiniti.

Proprietà delle chiavi

Quali sono le proprietà che caratterizzano una chiave?

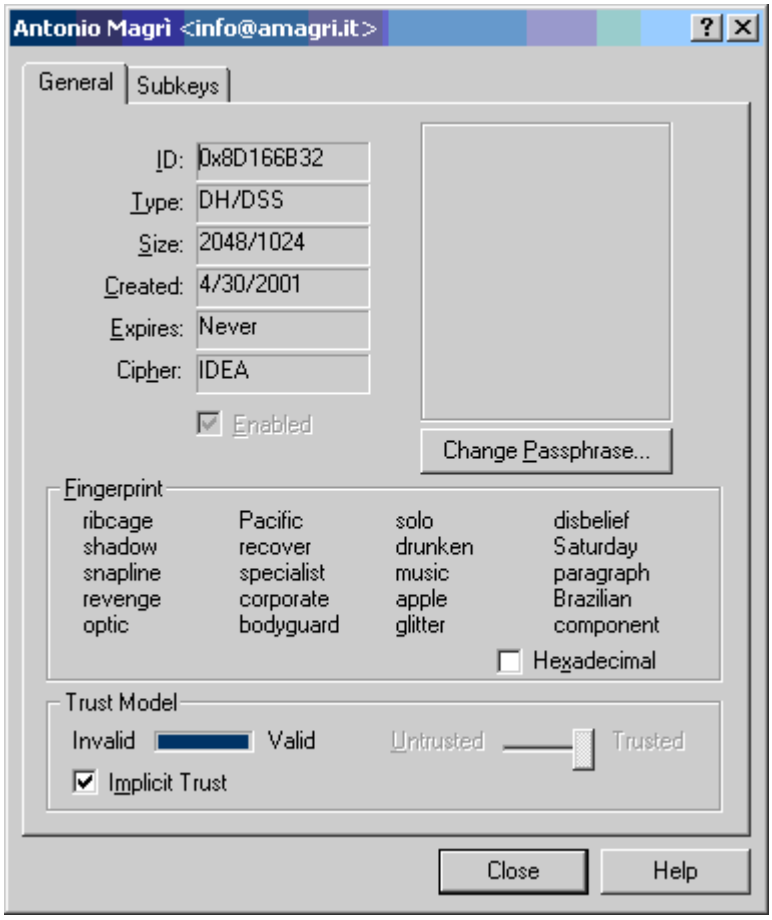
Per visualizzarle, dopo aver selezionato la chiave interessata all'interno del PGPKeys, bastarà fare un clic sul tasto destro del mouse e vi verrà proposto un menu contestuale. Scorrete le voci che vi si presentano e sezionate 'Key Properties':



Vi apparirà una nuova finestra contenente due etichette, 'General' e 'Subkeys'.

General

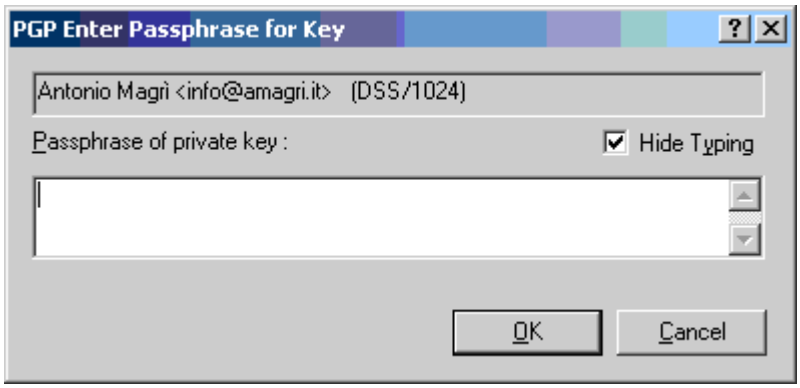
All'interno di General, sono contenute buona parte delle proprietà della chiave selezionata:



Analizziamo le singole voci:

- **ID**: identificativo univoco associato alla chiave. Per una chiave del tipo V3 (Versione 3, utilizzata da PGP 5.x) è costituito dai 64 bits meno significativi del modulo pubblico **n** della chiave RSA. Se invece si prende in esame una chiave del tipo V4 (Versione 4, introdotta da PGP 6.x.x) risulterà corrispondente ai 64 bits meno significativi del fingerprint (vedi voce relativa).
- **Type**: indica l'algoritmo a chiave pubblica utilizzato:
  - **RSA**: per le operazione di cifratura della chiave di sessione e di firma verrà utilizzato l'algoritmo RSA. Da notare che con le nuove chiavi RSA (V4) si utilizzano in realtà due coppie di chiavi. Una per le operazioni di cifratura/decifratura ed un'altra per quelle di firma/verifica;
  - **DH/DSS**: per cifrare la chiave di sessione verrà utilizzato l'algoritmo DH, ovvero una sua variante nota come ElGamal, mentre per firmare si ricorrerà a quanto previsto dal DSS, Digital Signature Standard e cioè all'algoritmo DSA, Digital Signature Algorithm.
- **Size**: grandezza della chiave. Anche qui bisognerà fare dei distinguo, in base al tipo di algoritmo utilizzato per la chiave:

  - **RSA**: la grandezza riportata sarà quella utilizzata sia per cifrare che per firmare;
  - **DH/DSS**: la grandezza sarà suddivisa in due parti distinte, xxxx/1024. La prima corrisponde alla grandezza della chiave DH (ElGamal) utilizzata per le operazioni di cifratura/decifratura mentre la seconda, sempre uguale a 1024, corrisponderà ai bits della chiave utilizzata dall'algoritmo DSA per firmare/verificare.
- **Created**: data di creazione della chiave.
- **Expires**: data di scadenza della chiave.
- **Cipher**: algoritmo simmetrico utilizzato per le operazioni di cifratura.
- **Enabled**: selezionando/deselezionado l'opzione, la chiave non verrà cancellata dal portachiavi ma se ne impedirà o meno l'utilizzo.
- **Change Passphrase**: vi permette di modificare la frase password. Se selezionate il pulsante vi verrà presentata una nuova finestra all'interno della quale digitare la vostra nuova frase password. Fatto ciò premete 'OK' per tornare alla finestra delle proprietà.



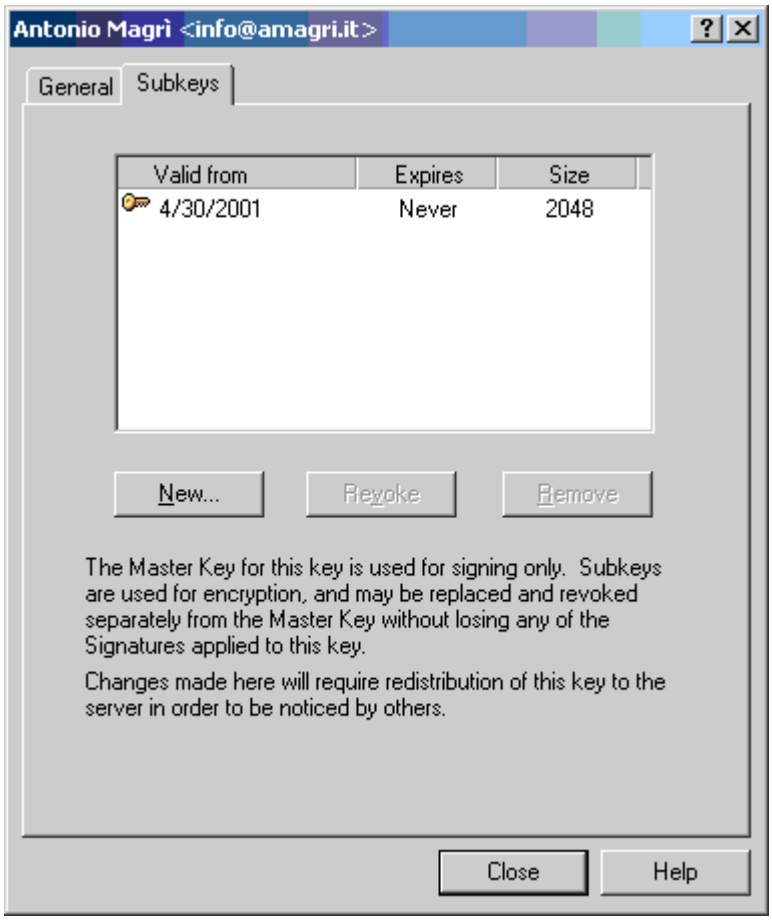
- **Fingerprint**: per una chiave V3 è il risultato dato dall'applicazione dell'algoritmo MD5 alla componente pubblica (modulo pubblico **n** ed esponente **e**) senza prendere in considerazione la lunghezza della chiave stessa. Per una chiave V4 invece, equivale ai 160 bits risultanti dall'utilizzo dell'algoritmo SHA-1 con in ingresso:
  - packet tag, che occupa un ottetto ed indica la tipologia del pacchetto (pacchetto chiave pubblica, pacchetto chiave privata, ecc.);
  - lunghezza del pacchetto, due ottetti;
  - tutto il pacchetto chiave pubblica a partire dal campo versione;
- **Hexadecimal**: permette di visualizzare il fingerprint in formato esadecimale. Se l'opzione viene disabilitata, il fingerprint verrà visualizzato utilizzando delle parole della lingua inglese dal suono caratteristico e quindi inconfondibili se dettate al telefono. Esempio:

Le ultime tre opzioni sono direttamente legate al concetto di Web of Trust.

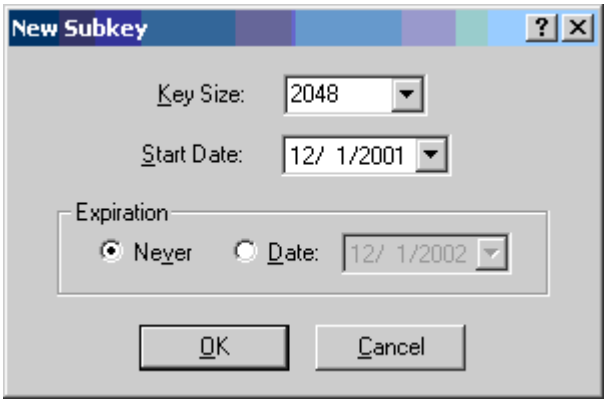
- **Trust model**: indica se la chiave è valida o meno e quindi il livello di fiducia associato al relativo proprietario.
- **Implicit Trust**: permette di considerare la chiave implicitamente valida, una caratteristica di cui godono tutte le chiavi da noi generate all'interno del programma.
- **Untrusted-Trusted**: riporta il livello di validità della chiave:
  - Non valida;
  - Marginalmente valida;
  - Valida.

Subkeys

Passiamo adesso a vedere la seconda pagina di proprietà, disponibile solo per le nuove chiavi RSA (V4) e quelle DH/DSS:



La pagina non presenta molte opzioni ma permette di impostare una caratteristica interessante, quella di avere una chiave di firma fissa, ed un insieme di chiavi di cifratura aventi una scadenza temporale differente. Basterà selezionare la voce 'Add' e vi verrà presentata una finestra dalla quale scegliere le caratteristiche desiderate per la nuova sottochiave:



- **Key Size**: grandezza della chiave;
- **Start Date**: giorno di inizio di validità della chiave;
- **Expiration**: si può scegliere o meno una data di scadenza per la chiave;

dopo di che basterà selezionare 'OK' per proseguire nella generazione.

Come riportato nella finestra principale, non dimentichiamoci di distribuire nuovamente la chiave, inviandola, se necessario, ad un keyserver, così che le modifiche effettuate siano rese pubbliche ed i nostri eventuali corrispondenti possano utilizzarla.

Cifrare

Utilizzando PGP potrete cifrare in modo semplice ed immediato:

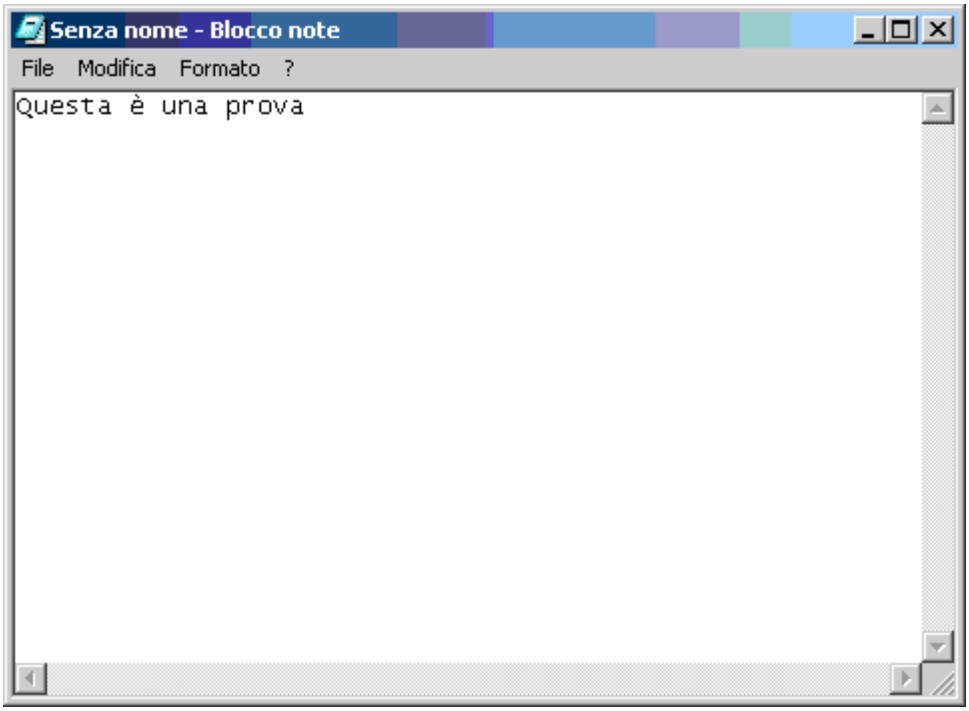
- un brano all'interno di un qualsiasi programma di elaborazione testi;
- un messaggio di posta elettronica;
- un file.

Cifrare un brano

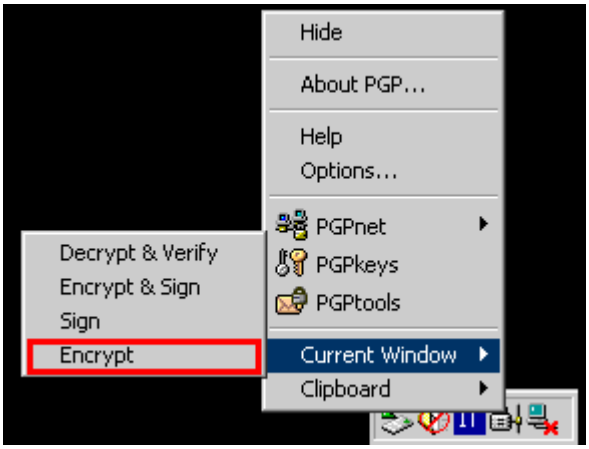
In questo primo esempio, cifreremo un breve brano all'interno di Blocco note, forse uno dei più semplici programmi per l'elaborazione del testo disponibili per la piattaforma MS Windows.

1. Lanciamo il programma Blocco note. Per fare questo selezionate Start > Programmi > Accessori > Blocco note;

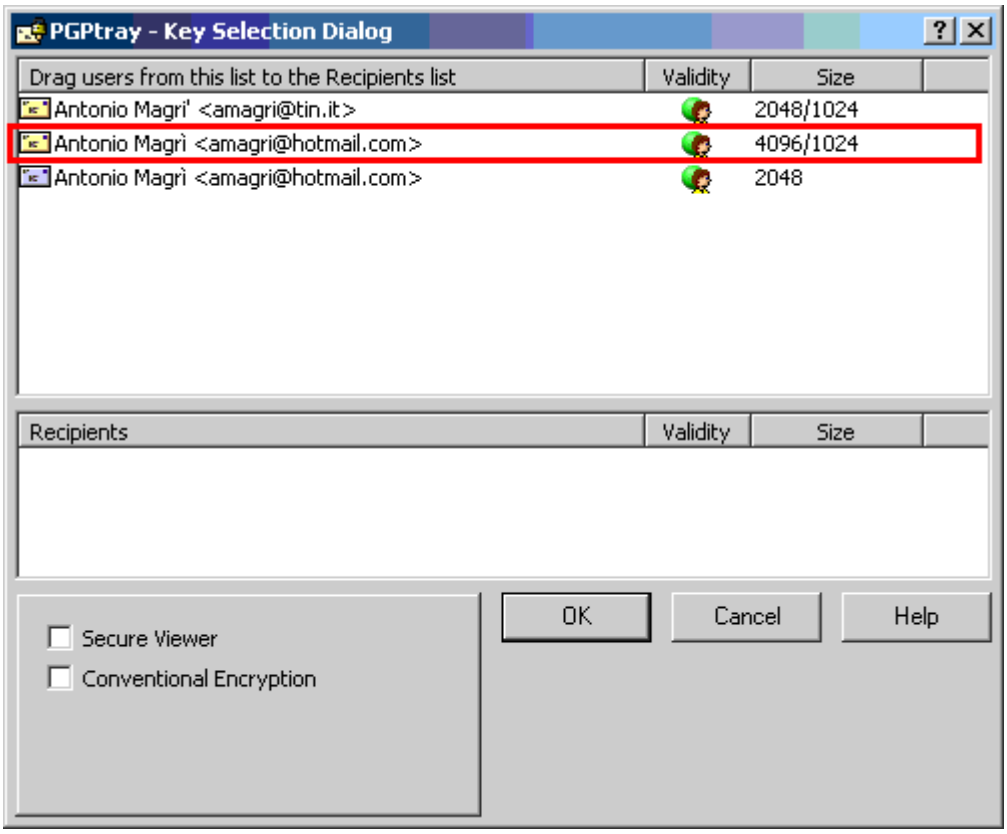
2. All'avvio, il programma Blocco note aprirà un documento 'Senza nome' e vi presenterà un'area vuota con il cursore lampeggiante. Come testo digitiamo: Questa è una prova.



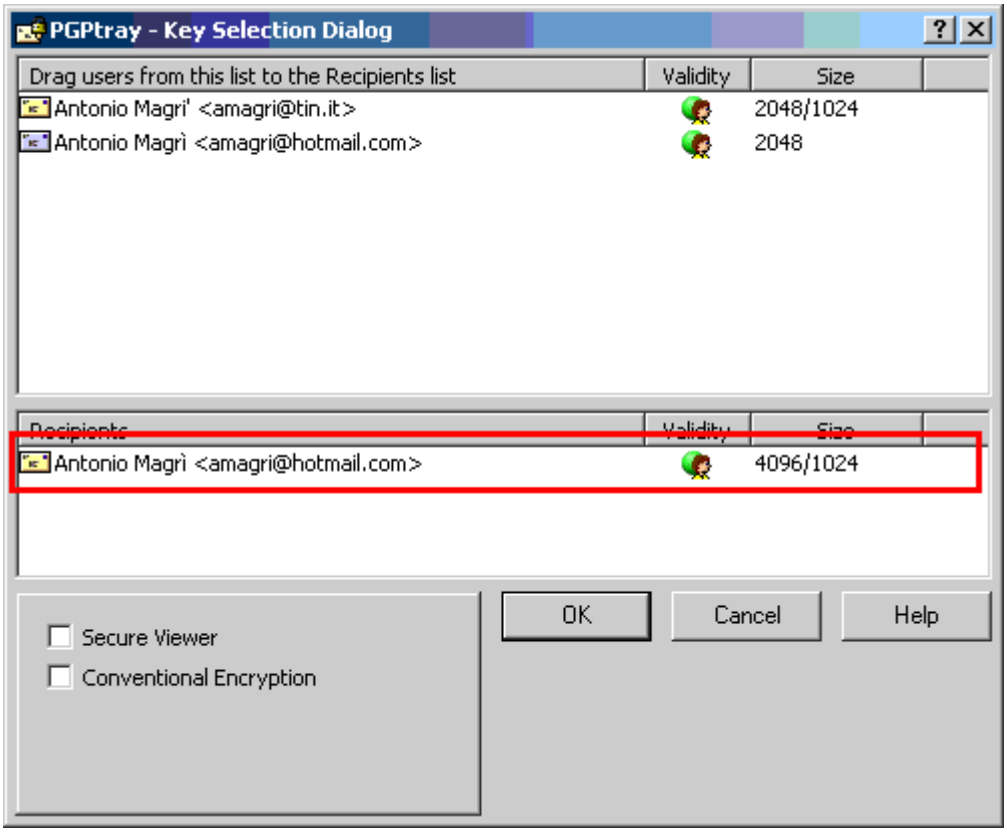
3. Terminato l'inserimento del testo, spostatevi sul System Tray, quindi, clic del mouse sull'icona del lucchetto (PGPtray) e nel menu che vi verrà proposto selezionate Current Window > Encrypt.



4. Vi dovrebbe apparire una finestra contenente la lista di tutte le chiavi pubbliche contenute nel vostro portachiavi.



5. Selezionate la chiave associata all'utente per cui state cifrando il documento e trascinatela verso il basso, nella Recipients List.

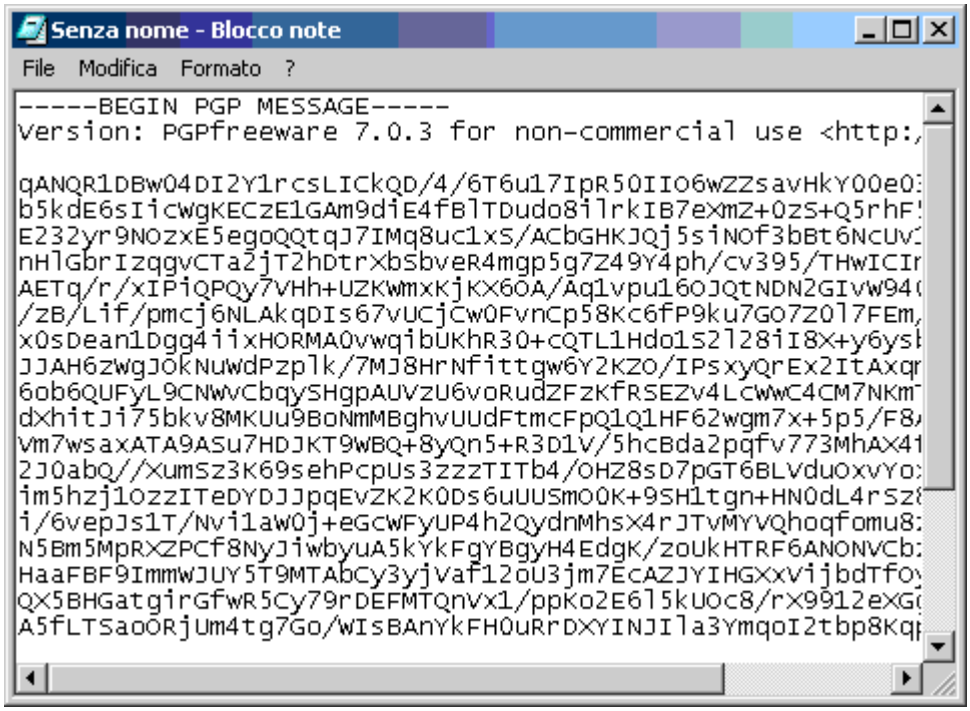


6. Le opzioni disponibili sono:

- **Secure Viewer**: protegge i dati da un attacco TEMPEST, visualizzandoli, al momento della decifratura, utilizzando uno speciale set di caratteri. L'opzione non è compatibile con le versioni precedenti di PGP.
- **Conventional Encryption**: cifra i dati utilizzando un algoritmo crittografico simmetrico e quindi utilizzando una chiave condivisa con il destinatario.

per questo esempio non è necessario selezionare nessuna opzione ma basta proseguire con OK.

7. Il programma cifra quindi il contenuto del nostro documento 'Senza nome' utilizzando la chiave pubblica del destinatario selezionato in precedenza.



Cifrare un messaggio di posta elettronica

Proviamo a mandare un messaggio cifrato di posta elettronica utilizzando MS Outlook Express 5.

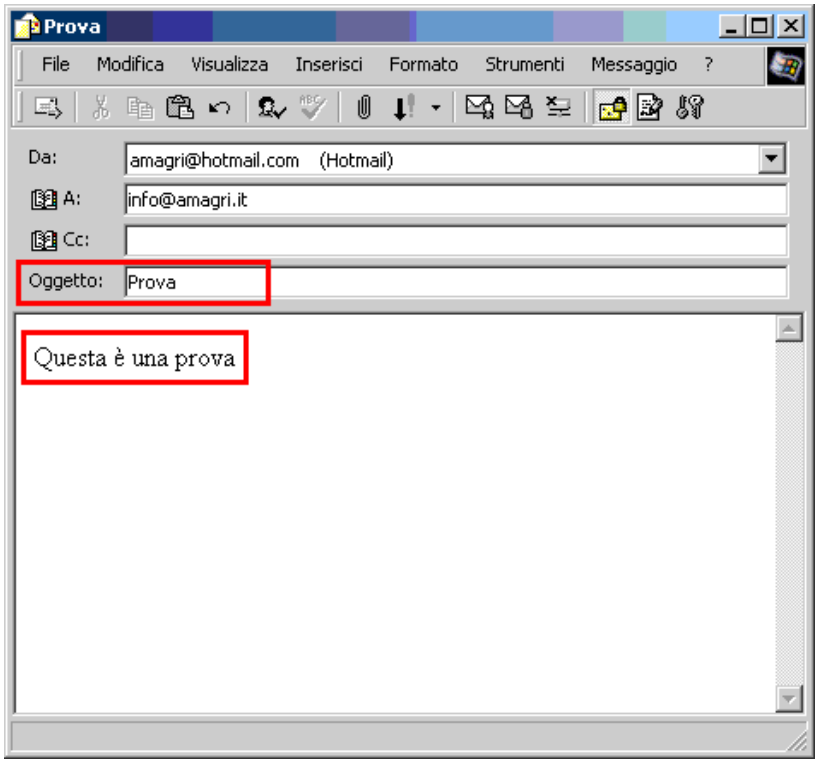
1. Prima di tutto bisogna avviare MS Outlook Express. Per fare questo è possibile utilizzare diverse strade, o attraverso Start > Programmi > Outlook Express, oppure cliccando sull'icona di Outlook Express presente di solito all'interno dell'Avvio veloce.

2. Scriviamo un nuovo messaggio utilizzando l'apposita opzione del menu File (File > Nuovo > Messaggio di posta) oppure l'icona corrispondente nella barra degli strumenti.

3. Selezionate l'icona nella barra degli strumenti contenente una busta ed un lucchetto di colore oro. Fate attenzione, perchè nella barra degli strumenti è presente anche un'altra icona dall'aspetto simile, ma con colori diversi (la busta è bianca ed il lucchetto è blu). Se per errore selezionate questa icona, Outlook non utilizzerà PGP per l'invio della posta ma S/MIME.

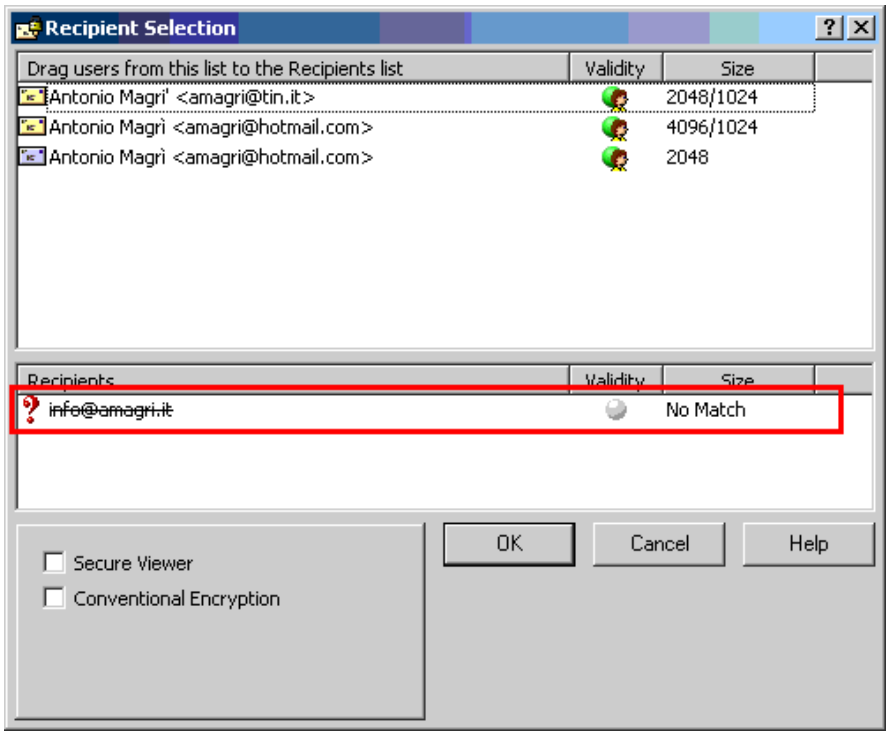
4. Nel campo 'A:' digitate l'indirizzo di posta elettronica del destinatario del messaggio cifrato.

5. Compiliamo il resto del messaggio inserendo Oggetto e Corpo.

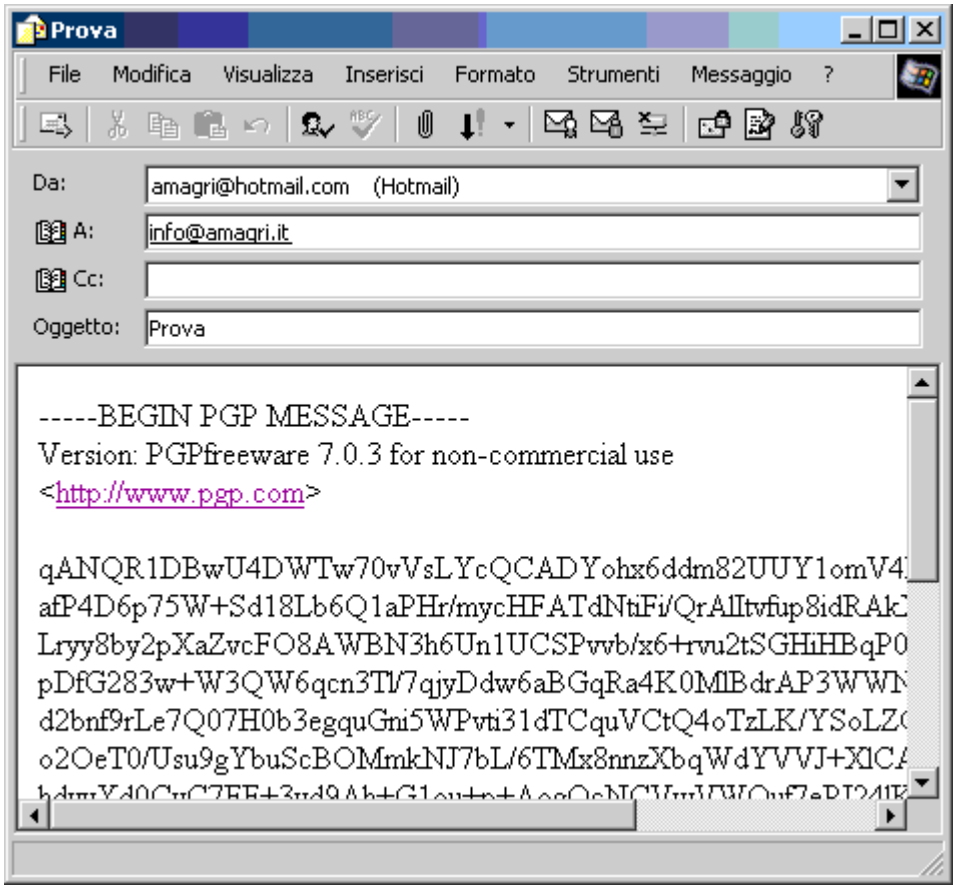


6. Dopo di che inviamo il messaggio utilizzando l'apposita voce del menu File (File > Invia messaggio) oppure la corrispondente icona della barra degli strumenti.

7. Il programma PGP ricercherà automaticamente la chiave del destinatario all'interno del portachiavi pubblico utilizzando l'indirizzo di posta elettronica inserito. Se questo non viene trovato, viene visualizzata una finestra per permettere la scelta della chiave associata al destinatario.



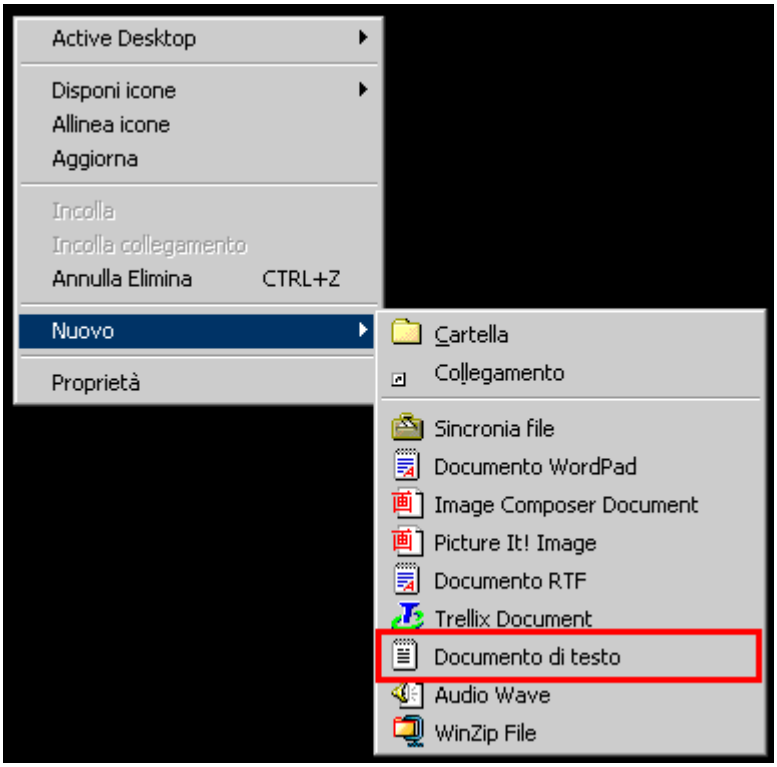
7. Una volta selezionata la chiave desiderata, sarà necessario spostarla all'interno dell'area 'Recipiets'. Dopo di che, selezionando 'OK', il messaggio verrà cifrato ed inviato.



Cifrare un file

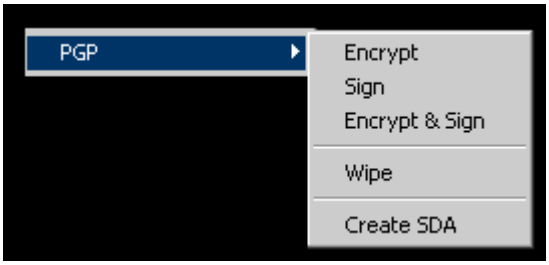
Cifrare un file è un'operazione molto semplice che può essere svolta in qualsiasi punto del sistema, grazie alle estensioni che sono state introdotte in fase di installazione dal programma PGP all'interno della Shell di MS Windows.

1. Creiamo un file di testo all'interno del Desktop da utilizzare come esempio. Per fare questo, clic del tasto destro del mouse sul Desktop e dalla voce di menu 'Nuovo' scegliamo 'Documento di testo'.



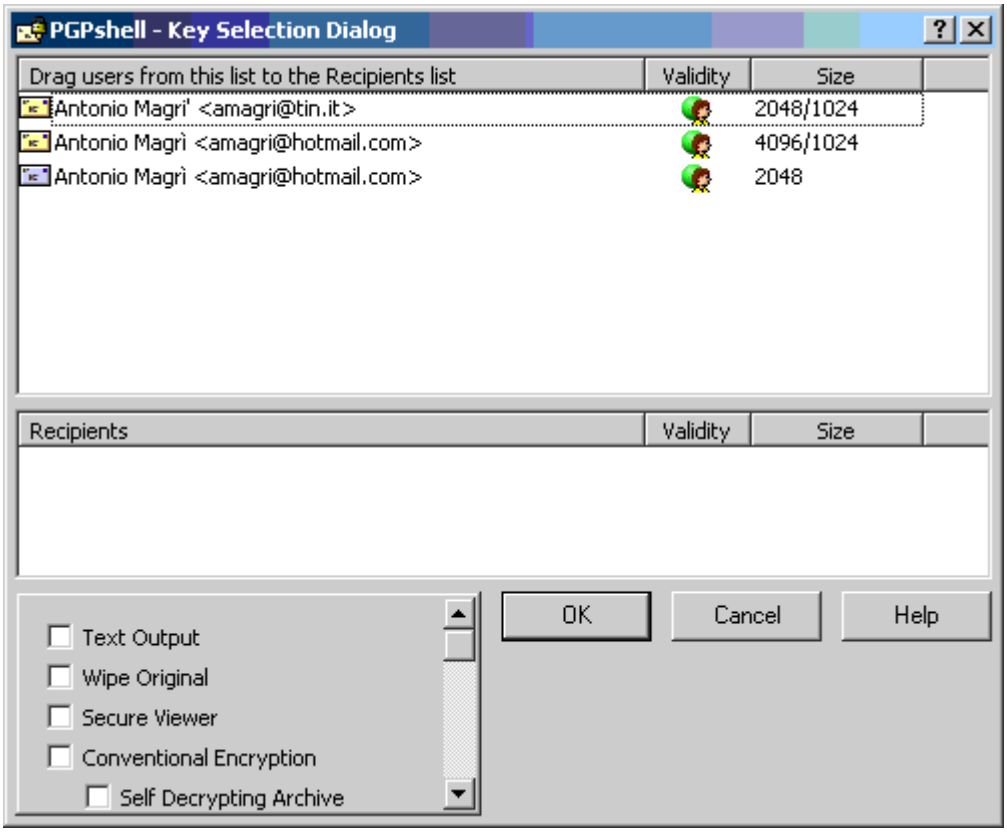
Verrà creato un documento avente nome 'Nuovo Documento di testo.txt'

3. Facendo clic con il tasto destro del mouse sul documento vi apparirà un menu contestuale contenente fra le varie voci anche queste:



vi basterà scegliere la voce 'PGP' e quindi 'Encrypt'.

4. Vi verrà presentata una finestra con la lista delle chiave pubbliche contenute all'interno del portachiavi pubblico.



Oltre a questo, la finestra ha diverse opzioni:

- **Text Output**: salve il file cifrato in formato testuale.
- **Wipe Original**: rimuove e sovrascrive il file originale.
- **Secure Viewer**: protegge i dati da un attacco TEMPEST, visualizzandoli, al momento della decifratura, utilizzando uno speciale set di caratteri. L'opzione non è compatibile con le versioni precedenti di PGP.
- **Conventional Encryption**: cifra i dati utilizzando un algoritmo crittografico simmetrico e quindi utilizzando una chiave condivisa con il destinatario.
    - **Self Decrypting Archive**: crea un eseguibile contenente il file cifrato con una chiave di sessione che cifra (o decifra) utilizzando una frase password concordata. Questa opzione è particolarmente utile per l'invio di materiale crittografato ad utenti aventi la stessa piattaforma ma che non hanno installato PGP. In pratica l'utente che riceve il file dovrà solo eseguirlo ed inserire la frase password concordata per avere il file decifrato.

Per il momento non attivate nessuna di queste opzioni ma, dopo aver trascinato la chiave pubblica che intendete utilizzare, selezionate OK per andare avanti.

5. Dovreste ottenere sul vostro Desktop un nuovo file avente lo stesso nome dell'originale ma con estensione .pgp

Decifrare

Utilizzando PGP potrete decifrare in modo semplice ed immediato:

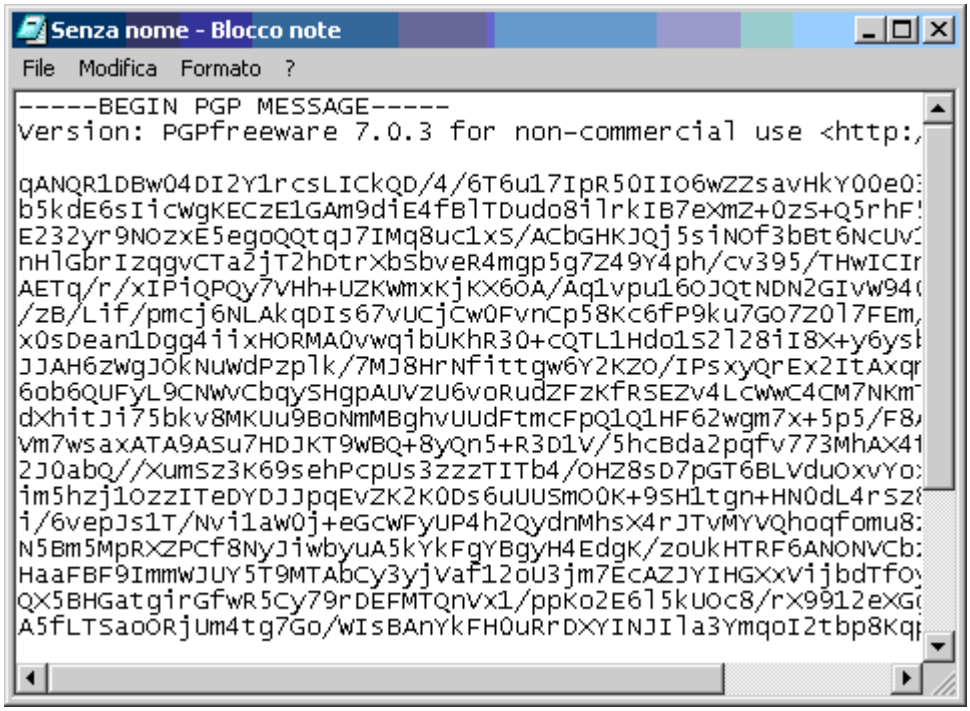
- un brano all'interno di un qualsiasi programma di elaborazione testi;
- un messaggio di posta elettronica
- un file

naturalmente cifrati utilizzando PGP.

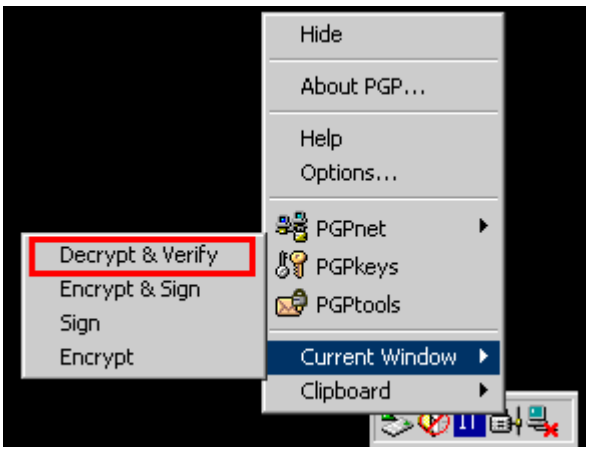
Decifrare un brano

Abbiamo ricevuto un brano di testo cifrato e lo dobbiamo decifrare.

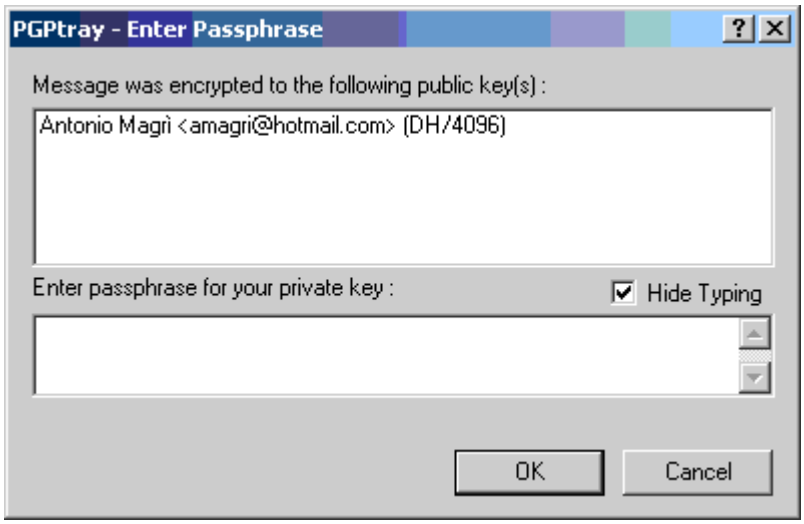
1. Apriamo il file contenente il brano.



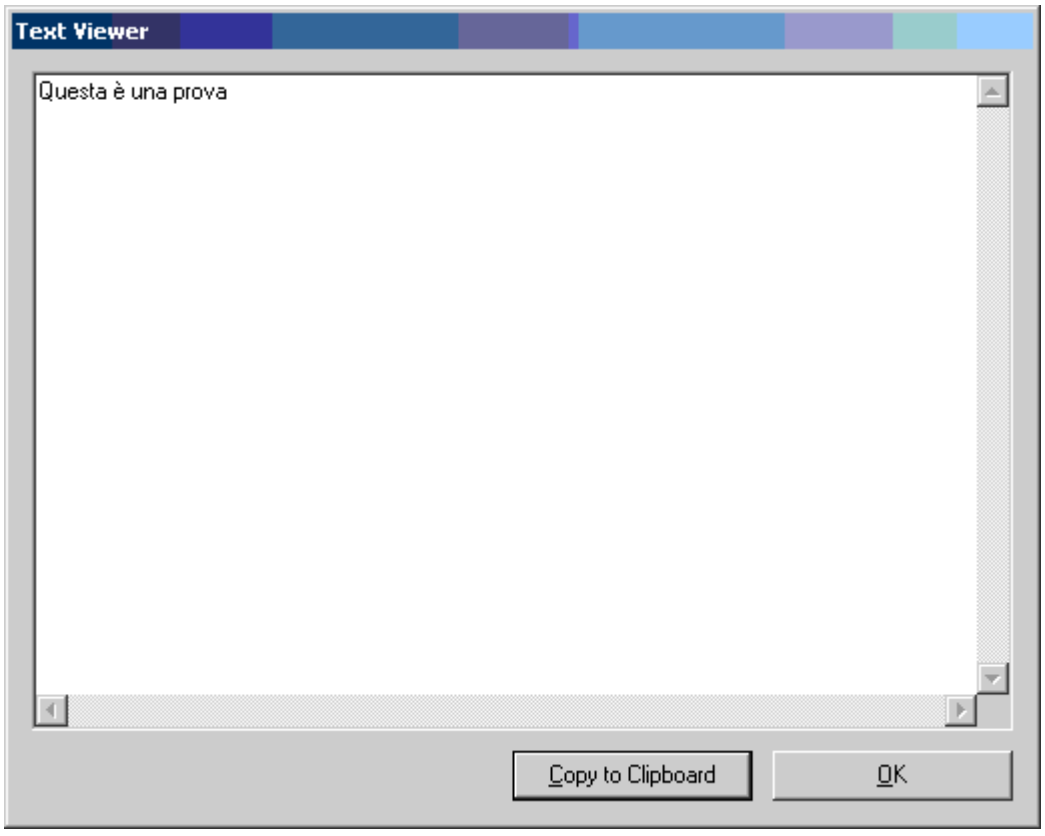
2. Per decifrare il contenuto della finestra corrente, utilizziamo l'apposita opzione del PGPtray.



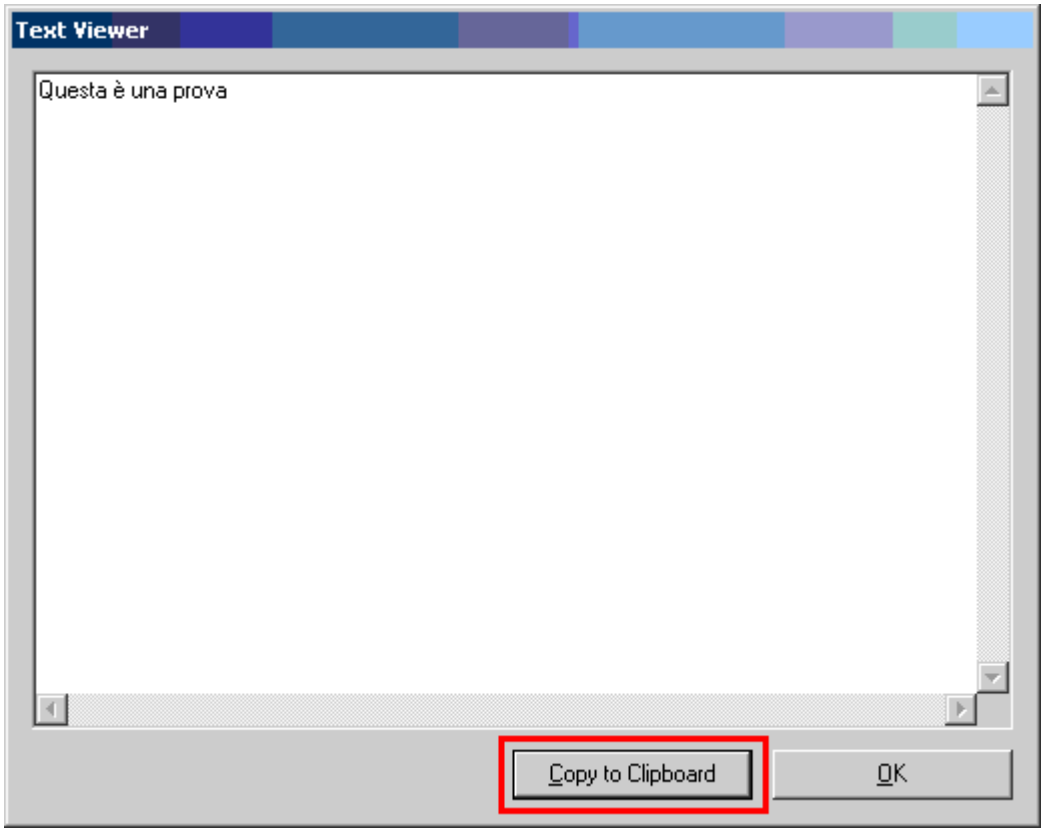
3. Vi verrà chiesto di inserire la frase password associata alla chiave privata necessaria per completare l'operazione.



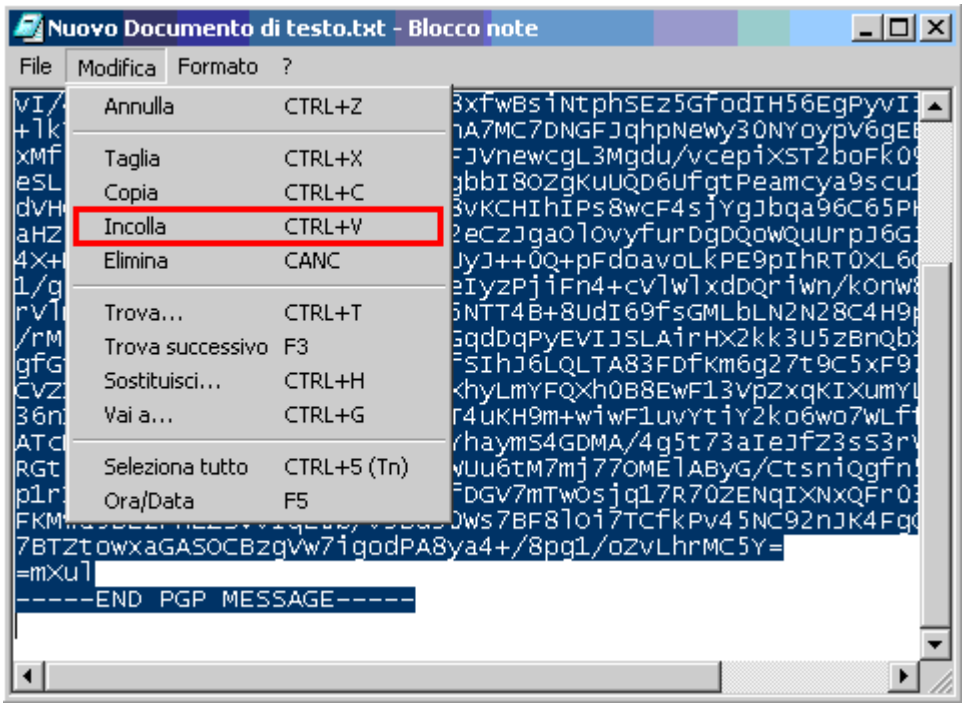
4. PGP visualizzerà all'interno del Text Viewer il contenuto del brano in chiaro.



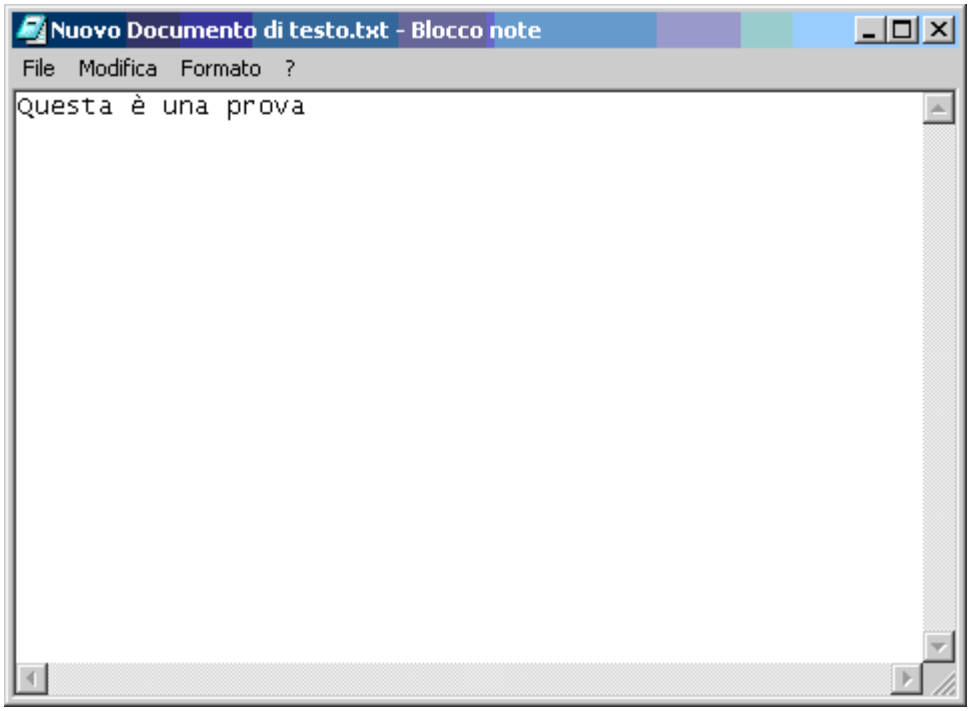
5. Per copiare il tutto all'interno degli Appunti, selezionate il pulsante 'Copy to Clipboard'.



6. Una volta copiato il brano in chiaro all'interno degli Appunti bisognerà trasferirne il contenuto all'interno della finestra contenente il brano cifrato. Per fare questo selezioniamo la voce di menu Modifica, quindi Incolla.



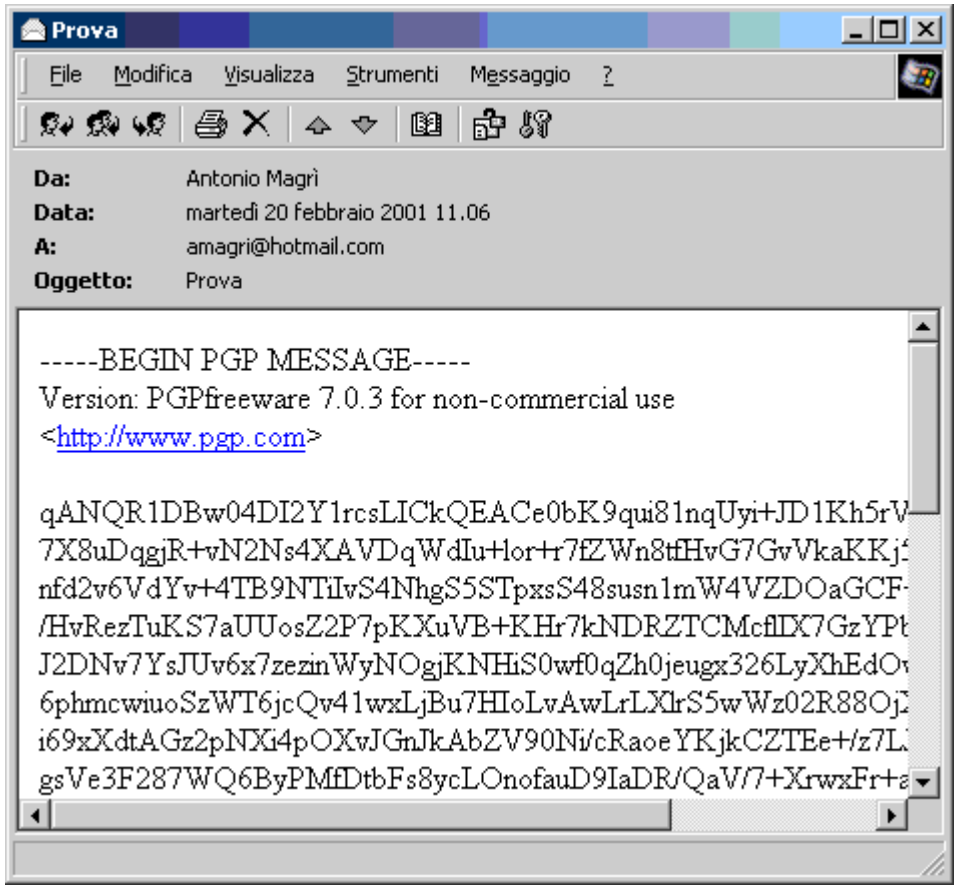
7. La finestra conterrà ora il brano in chiaro.



Decifrare un messaggio di posta elettronica

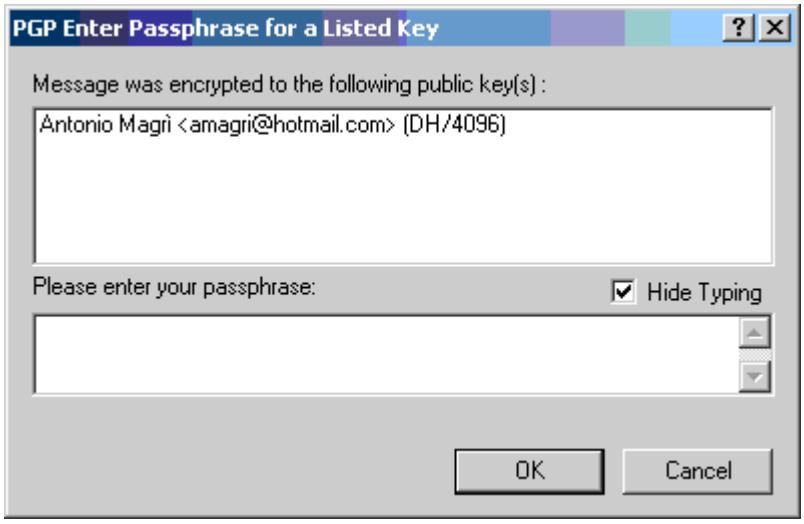
Cosa bisogna fare se si riceve un messaggio di posta elettronica cifrato?

1. Apriamo il messaggio facendovi sopra doppio clic con il tasto sinistro del mouse.

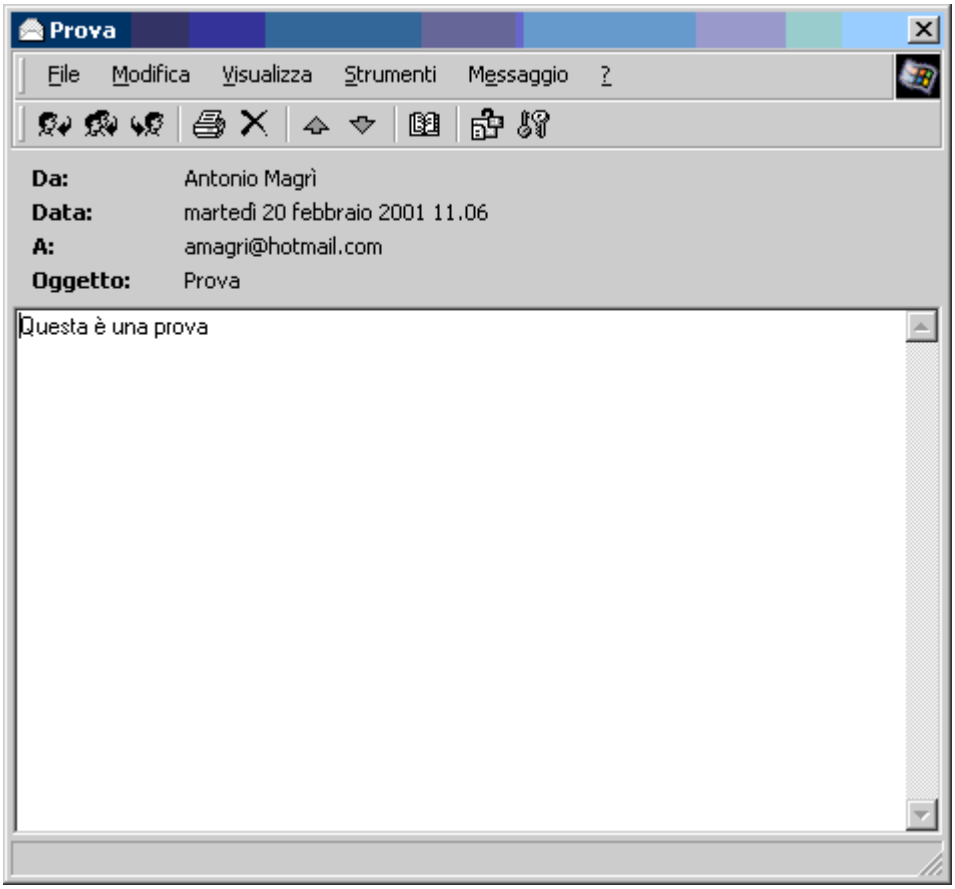


2. Selezioniamo l'apposita icona per decifrarne il contenuto.

3. Vi verrà chiesto di inserire la frase password associata alla chiave privata necessaria per completare l'operazione.



4. Se la frase password è stata inserita correttamente, otterrete automaticamente il messaggio di posta elettronica in chiaro.

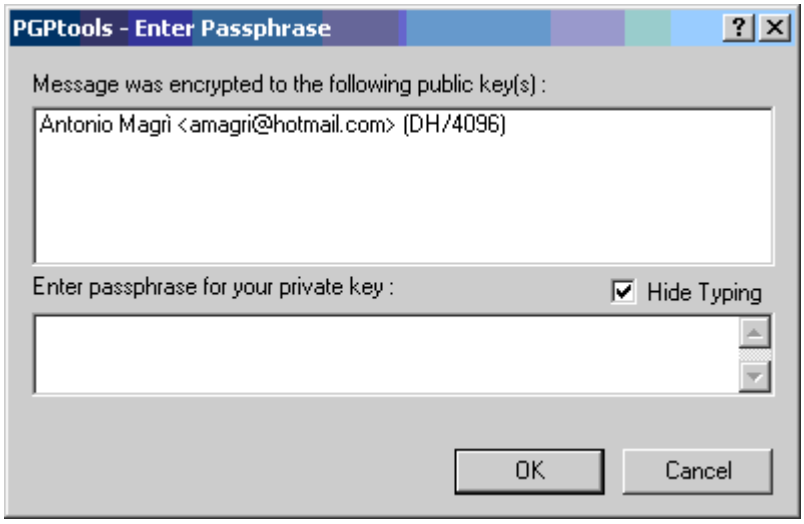


Decifrare un file

Così come abbiamo visto per la cifratura, anche decifrare un file è un'operazione molto semplice sfruttando le estensioni che sono state introdotte in fase di installazione dal programma PGP all'interno della Shell di MS Windows.

1. Doppio clic del mouse sull'icona rappresentate il file cifrato.

2. Vi verrà chiesto di inserire la frase password associata alla chiave privata necessaria per completare l'operazione.



3. Se la frase password è stata inserita correttamente, otterrete automaticamente il file in chiaro.

Firmare

Utilizzando PGP potrete firmare in modo semplice ed immediato:

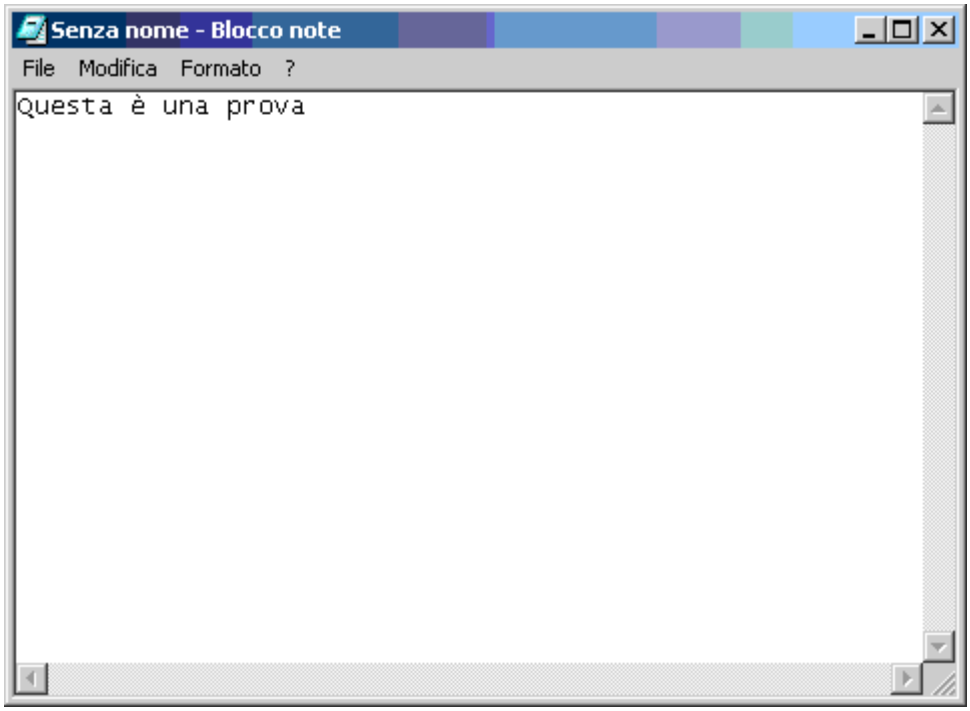
- un brano all'interno di un qualsiasi programma di elaborazione testi;
- un messaggio di posta elettronica;
- un file.

Firmare un brano

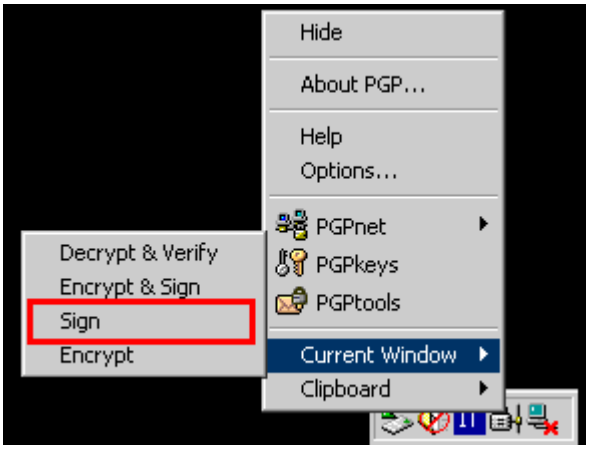
Così come abbiamo fatto per la cifratura, anche in questo caso utilizzeremo il programma Blocco note per creare il brano di prova.

1. Lanciamo il programma Blocco note. Per fare questo selezionate Start > Programmi > Accessori > Blocco note;

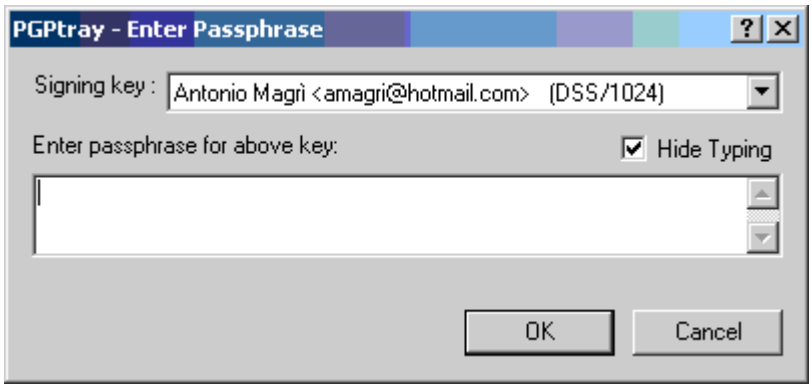
2. All'avvio, il programma Blocco note aprirà un documento 'Senza nome' e vi presenterà un'area vuota con il cursore lampeggiante. Come testo digitiamo: Questa è una prova.



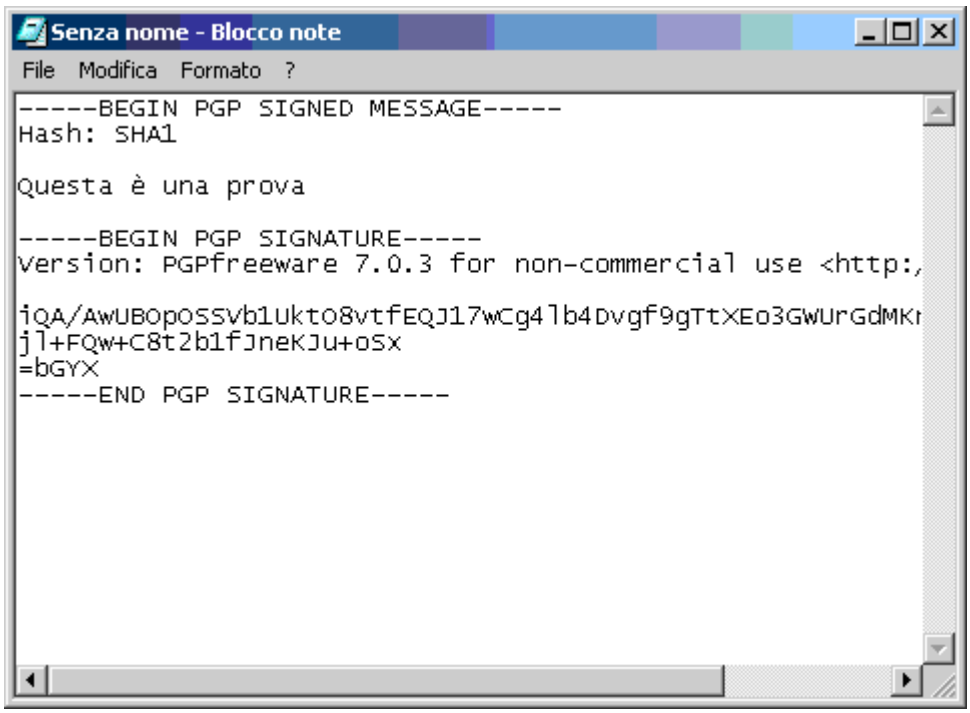
3. Terminato l'inserimento del testo, spostatevi sul System Tray, quindi, Clic del mouse sull'icona del lucchetto (PGPtray) e nel menu che vi verrà proposto selezionate Current Window > Sign.



4. Per poter utilizzare la chiave dedicata alla firma, il programma vi chiederà di inserire la vostra frase password.



5. Ritornando all'interno di Blocco note potrete notare che il vostro brano è stato modificato in modo sostanziale da PGP.



Oltre al brano originale, sono stati introdotti dal programma diversi elementi:

- Un'intestazione, che indica il tipo di messaggio trattato (PGP SIGNED MESSAGE);
- Il tipo di algoritmo di hash utilizzato (Hash: SHA 1);
- La firma vera e propria racchiusa fra appositi delimitatori (BEGIN PGP SIGNATURE/END PGP SIGNATURE)

Firmare un messaggio di posta elettronica

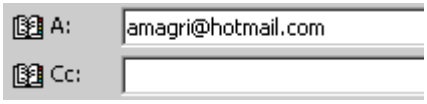
Proviamo a mandare un messaggio firmato di posta elettronica utilizzando MS Outlook Express 5.

1. Prima di tutto bisogna avviare MS Outlook Express. Per fare questo è possibile utilizzare diverse strade, o attraverso Start > Programmi > Outlook Express, oppure cliccando sull'icona di Outlook Express presente di solito all'interno dell'Avvio veloce.

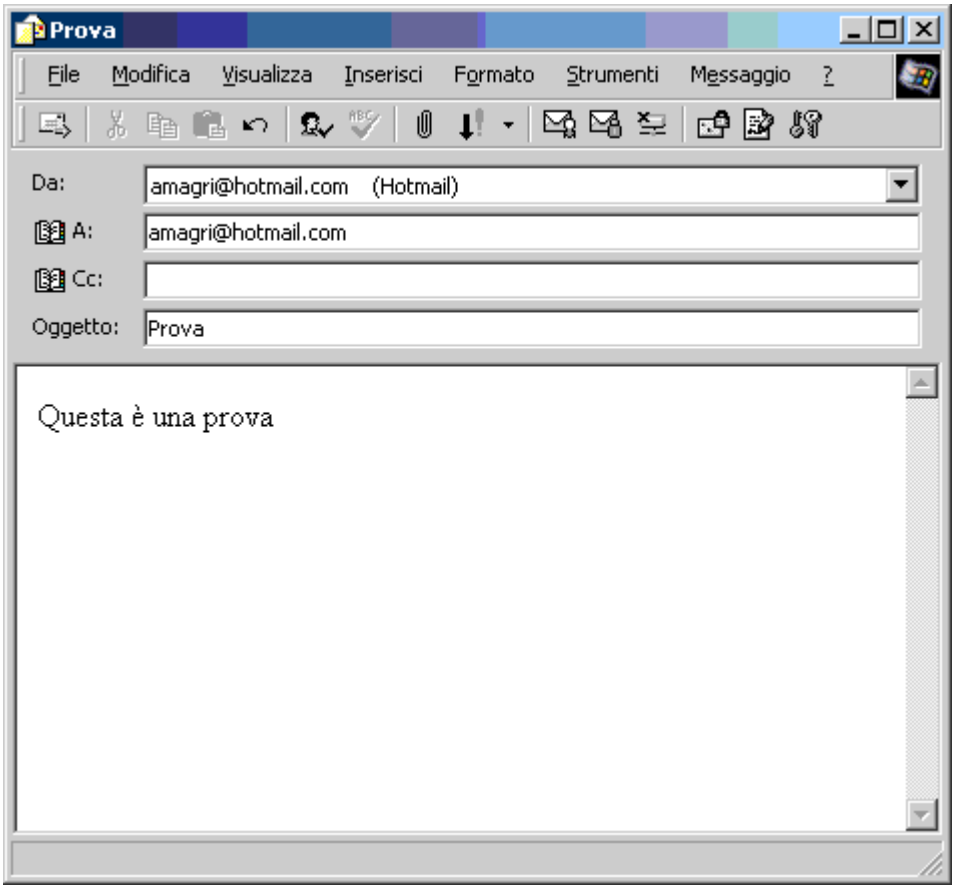
2. Scriviamo un nuovo messaggio utilizzando l'apposita opzione del menu File (File > Nuovo > Messaggio di posta) oppure l'icona corrispondente nella barra degli strumenti.

3. Selezionate l'icona nella barra degli strumenti contenente una matita che firma un foglio.

4. Nel campo 'A:' digitate l'indirizzo di posta elettronica del destinatario del messaggio cifrato.

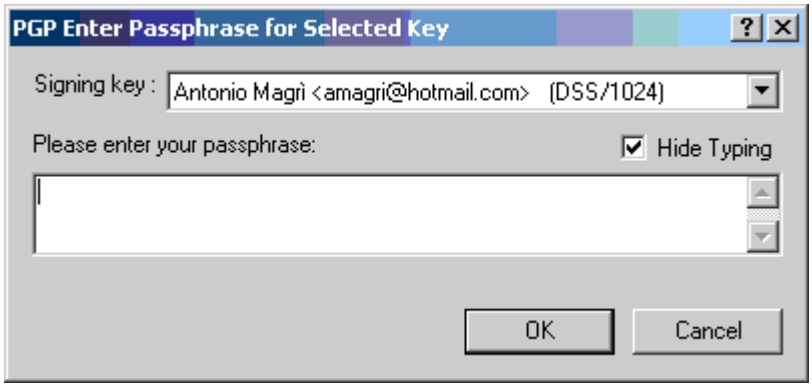


5. Compiliamo il resto del messaggio inserendo Oggetto e Corpo.



6. Dopo di che inviamo il messaggio utilizzando l'apposita voce del menu File (File > Invia messaggio) oppure la corrispondente icona della barra degli strumenti.

7. Per poter utilizzare la chiave dedicata alla firma, il programma vi chiederà di inserire la vostra frase password.

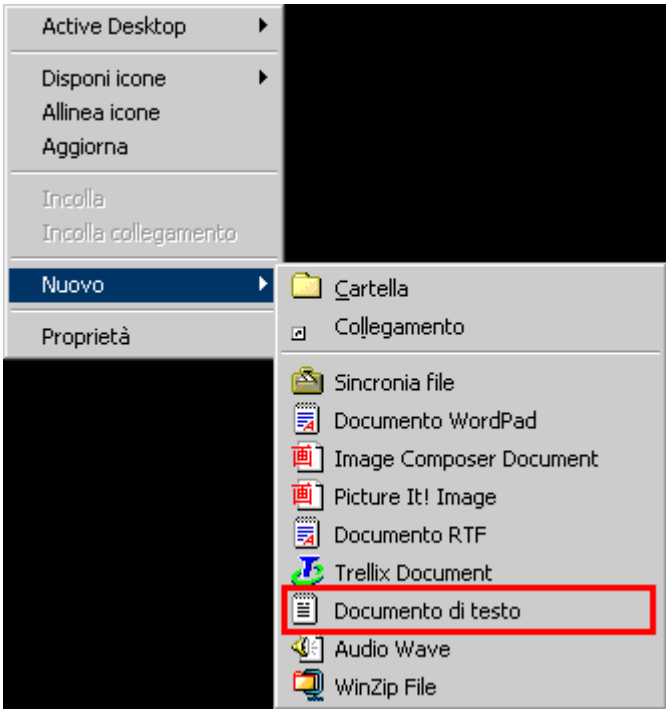


8. Il messaggio verrà quindi firmato ed inviato.

Firmare un file

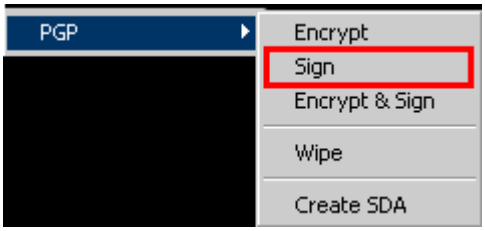
Firmare un file è un'operazione molto semplice che può essere svolta in qualsiasi punto del sistema, grazie alle estensioni che sono state introdotte in fase di installazione dal programma PGP all'interno della Shell di MS Windows.

1. Creiamo un file di testo all'interno del Desktop da utilizzare come esempio. Per fare questo, clic del tasto destro del mouse sul Desktop e dalla voce di menu 'Nuovo' scegliamo 'Documento di testo'.



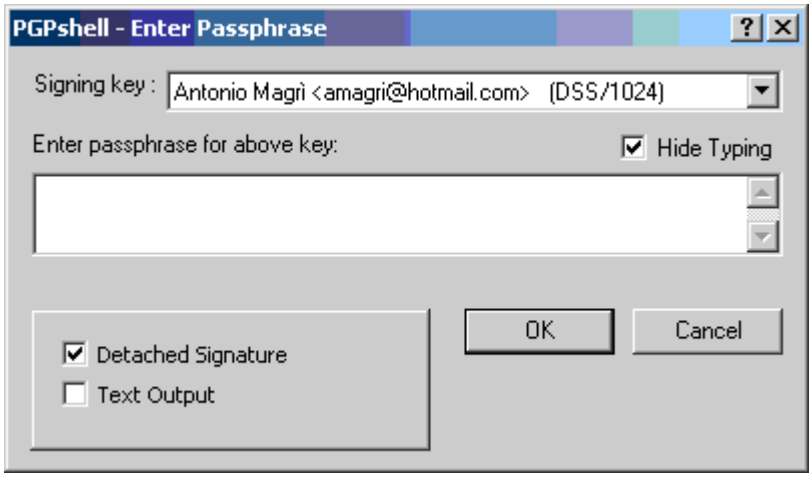
Verrà creato un documento avente nome 'Nuovo Documento di testo.txt'.

3. Facendo clic con il tasto destro del mouse sul documento ci apparirà questo menu:



da cui basterà scegliere la voce 'PGP' e quindi 'Sign'.

4. Il programma vi chiederà di inserire la frase password per completare la procedura.



Oltre a questo la finestra ha diverse opzioni:

- **Detached Signature**: salva la firma in un file separato con estensione .sig creato nella stessa posizione del file firmato.
- **Text Output**: salve il file cifrato in formato testuale.

Per il momento lasciate attiva la prima opzione e selezionate OK per andare avanti.

5. Dovreste ottenere sul vostro Desktop un nuovo file avente lo stesso nome dell'originale ma con estensione .sig

Verificare

Utilizzando PGP potrete verificare in modo semplice ed immediato:

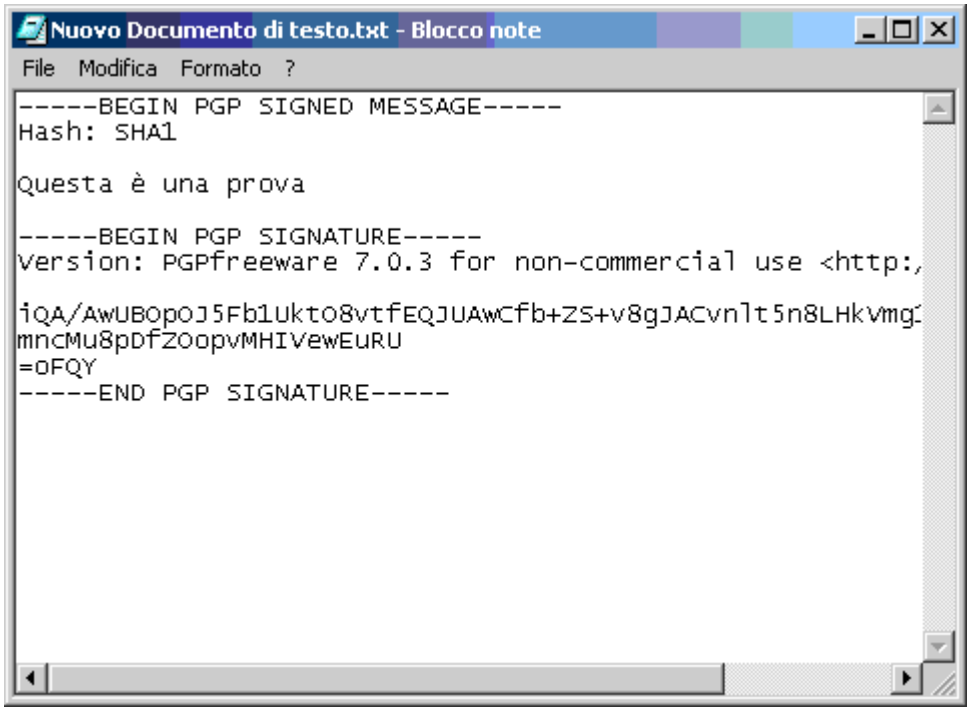
- un brano all'interno di un qualsiasi programma di elaborazione testi;
- un messaggio di posta elettronica;
- un file.

naturalmente firmati utilizzando PGP.

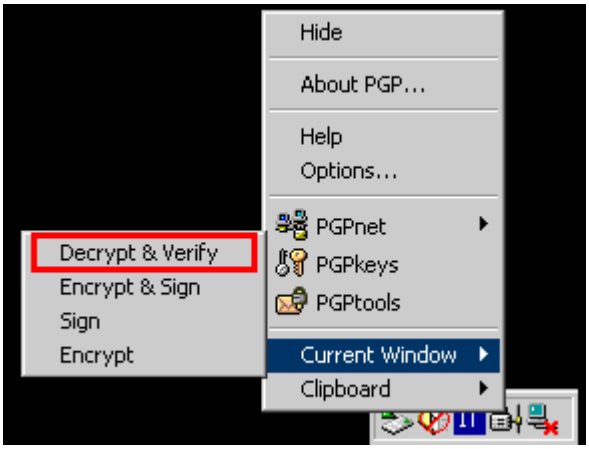
Verificare un brano

Proviamo a vedere come fare per verificare l'integrità e la firma di un brano di testo ricevuto.

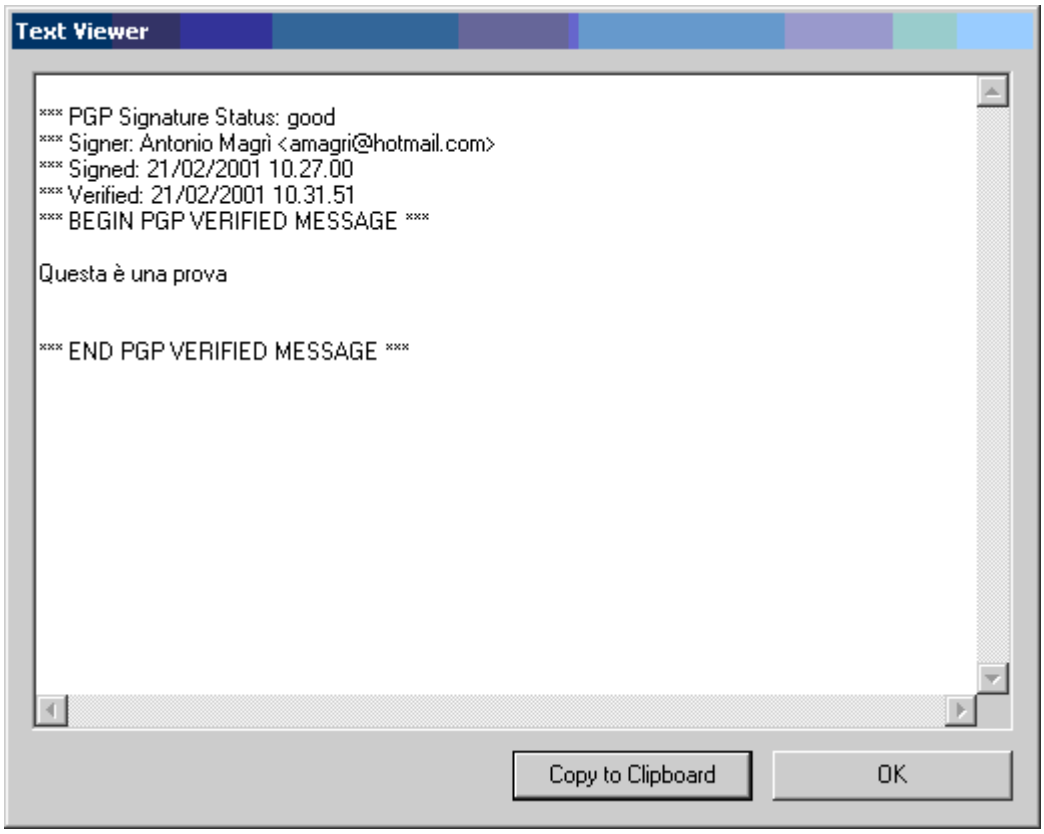
1. Abbiamo ricevuto un brano di testo firmato e lo vogliamo verificare.



2. Basterà spostarsi sul System Tray, quindi, Clic del mouse sull'icona del lucchetto (PGPtray) e nel menu che vi verrà proposto selezionate Current Window > Decrypt & Verify.



3. Il programma utilizzerà per la verifica la corrispondente chiave pubblica associata alla chiave utilizzata per firmare il brano e vi presenterà in un'apposita finestra i risultati dell'operazione.

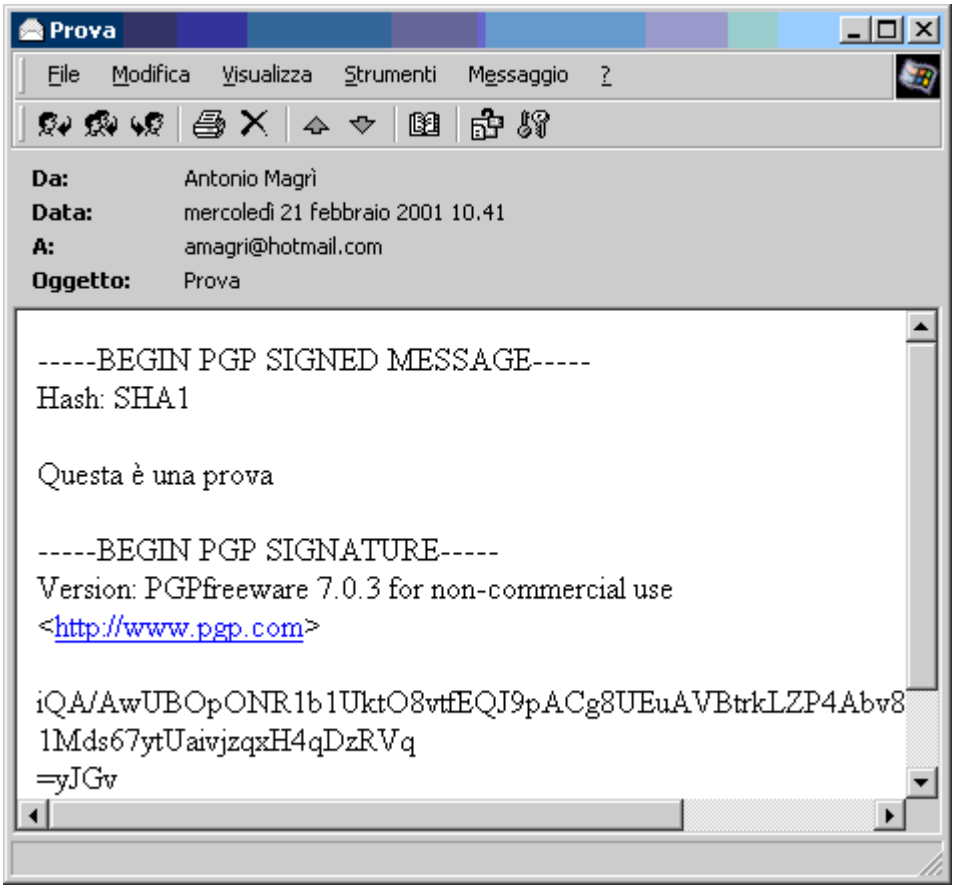


Se la verifica viene effettuata correttamente otterrete la dicitura 'PGP Signature Status: Good' altrimenti se il messaggio è stato modificato in qualche modo 'PGP Signature Status: Bad'. Per uscire dalla finestra e tornare al brano, selezionate OK.

Verificare un messaggio di posta elettronica

Cosa bisogna fare per vericare un messaggio di posta elettronica firmato?

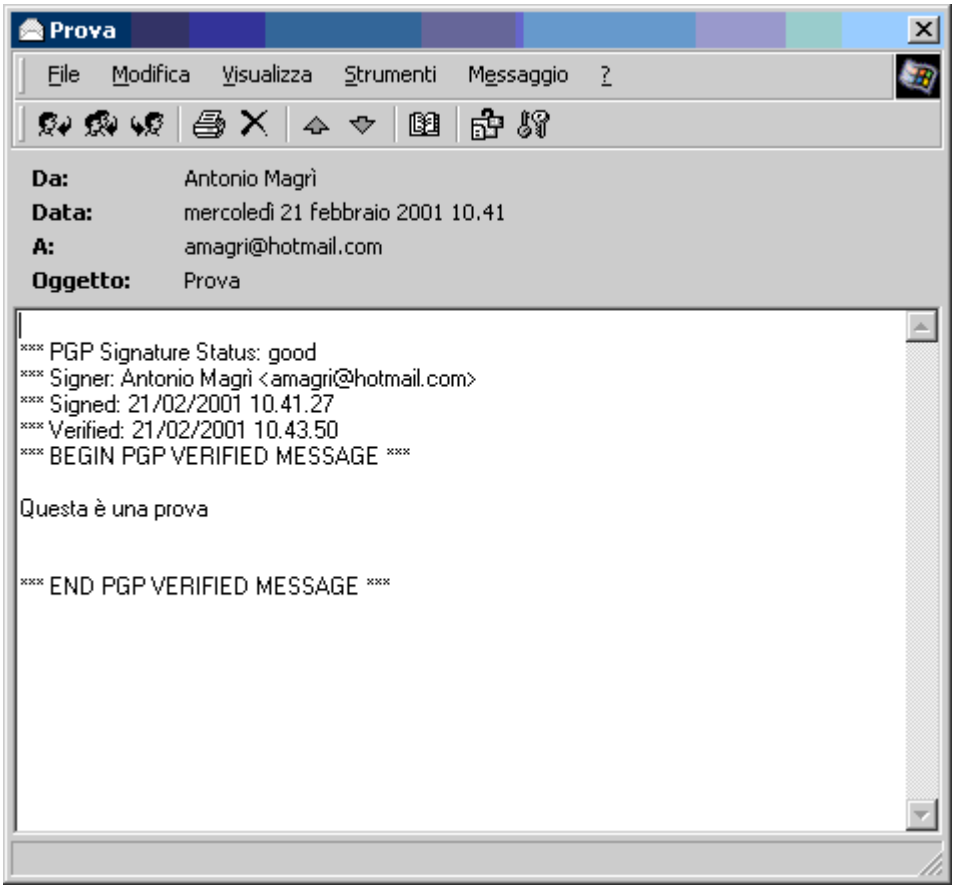
1. Avete ricevuto un messaggio di posta elettronica firmato e lo volete verificare. Prima di tutto, apriamo il messaggio facendovi sopra doppio clic con il tasto sinistro del mouse.



2. Per verificare la firma e l'integrità del messaggio basterà selezionare l'apposita icona presente all'interno della barra degli strumenti.

Da notare che l'icona è presente solo se in fase di installazione è stato selezionato l'apposito plug-in.

3. Dopo qualche secondo otterrete una nuova finestra del messaggio contenente l'esito dell'operazione. Se la firma è stata verificata con successo vi sarà la dicitura 'PGP Signature Status: Good' altrimenti se il messaggio è stato modificato in qualche modo 'PGP Signature Status: Bad'.



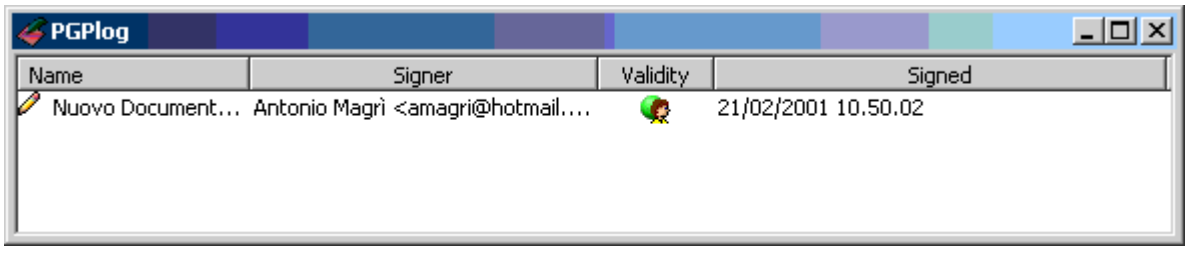
Ricordatevi che, il procedimento appena visto può essere utilizzato anche per gli articoli pubblicati nei gruppi di discussione.

Verificare un file

Così come abbiamo visto in precedenza, anche verificare un file è un'operazione molto semplice sfruttando le estensioni che sono state introdotte in fase di installazione dal programma PGP all'interno della Shell di MS Windows.

1. Doppio clic del mouse sull'icona rappresentante la firma associata al file.

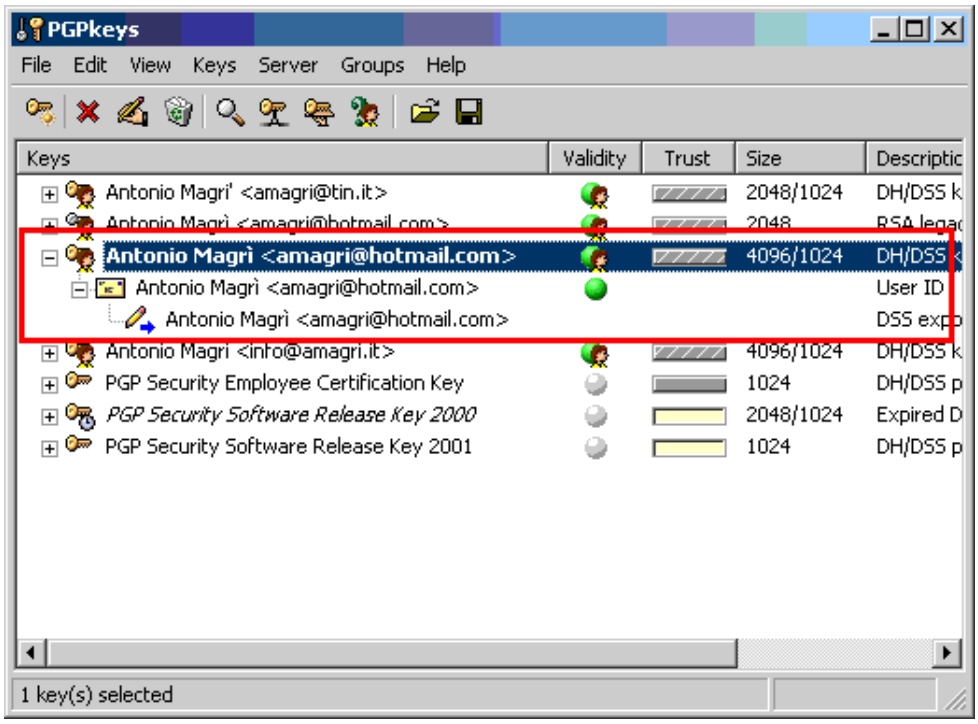
2. Verrà visualizzata la finestra PGPlog contenente informazioni sulla validità o meno della firma.



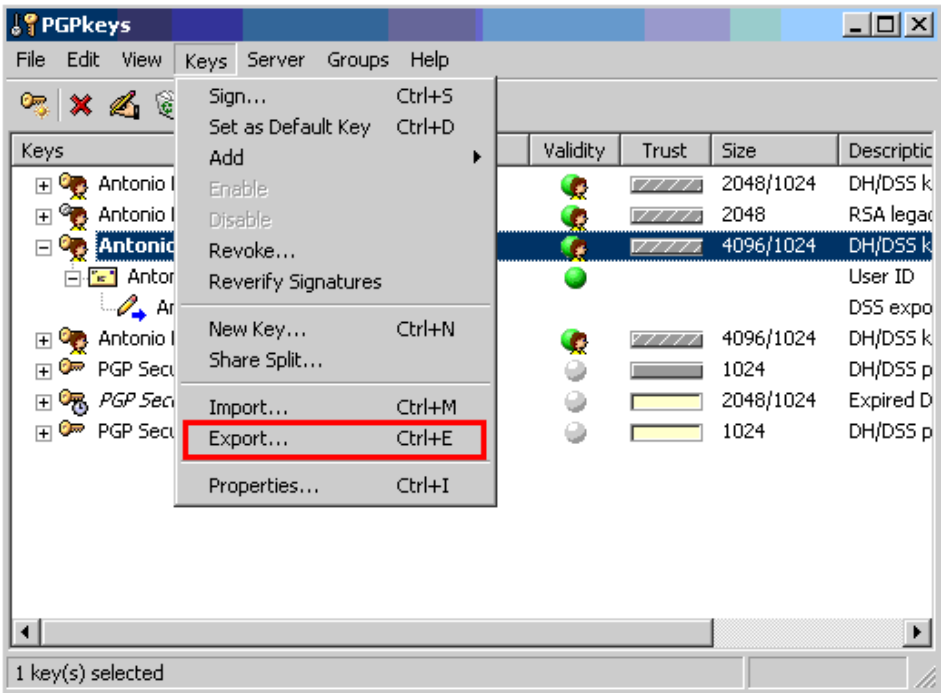
Esportare una chiave

A volte, trovandosi nella necessità di dover inviare la propria chiave pubblica ad un corrispondente oppure volendo fare una copia della propria coppia di chiavi, potrebbe essere necessario servirsi della seguente procedura di esportazione.

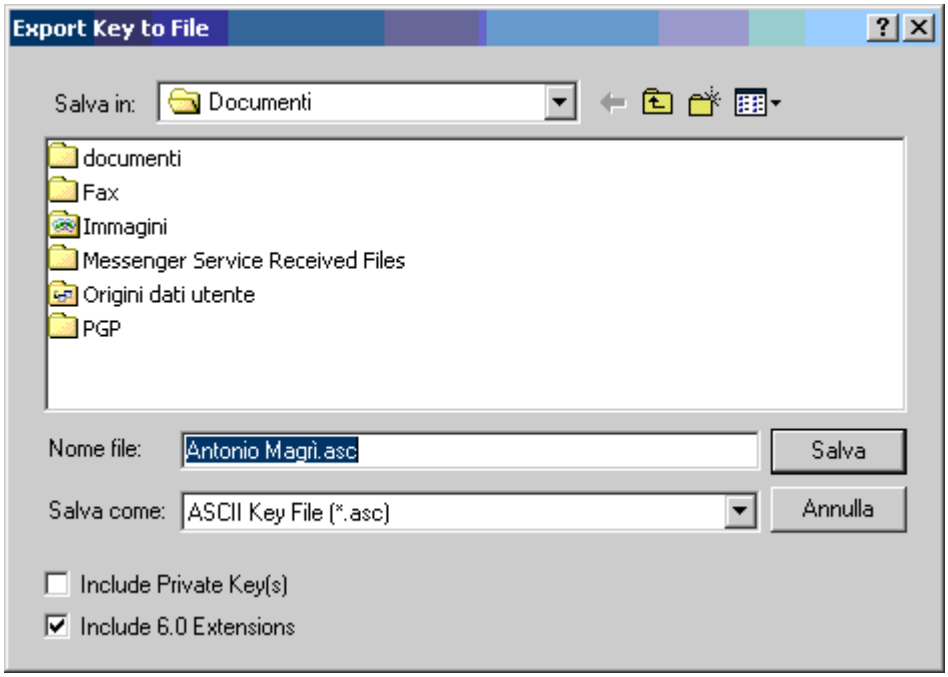
1. Selezionare la chiave che si intende esportare.



2. Scegliere dal menu la voce 'Keys' quindi 'Export'.



3. Il programma vi chiederà di specificare il percorso in cui salvare il file nonchè il nome ed il tipo di file da salvare.



La finestra di salvataggio permette di scegliere anche queste opzioni:

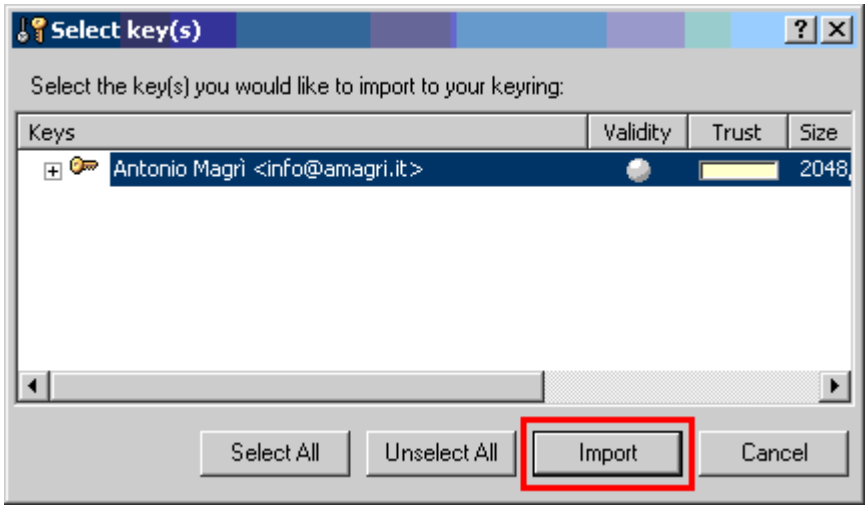
- **Include Private Key(s)**: esporta anche la componente privata della coppia di chiavi. Da usare con cautela.
- **Include 6.0 Extensions**: esporta la chiave nel nuovo formato 6.0 comprendente l'ID fotografico ed i certificati X.509.

Importare una chiave

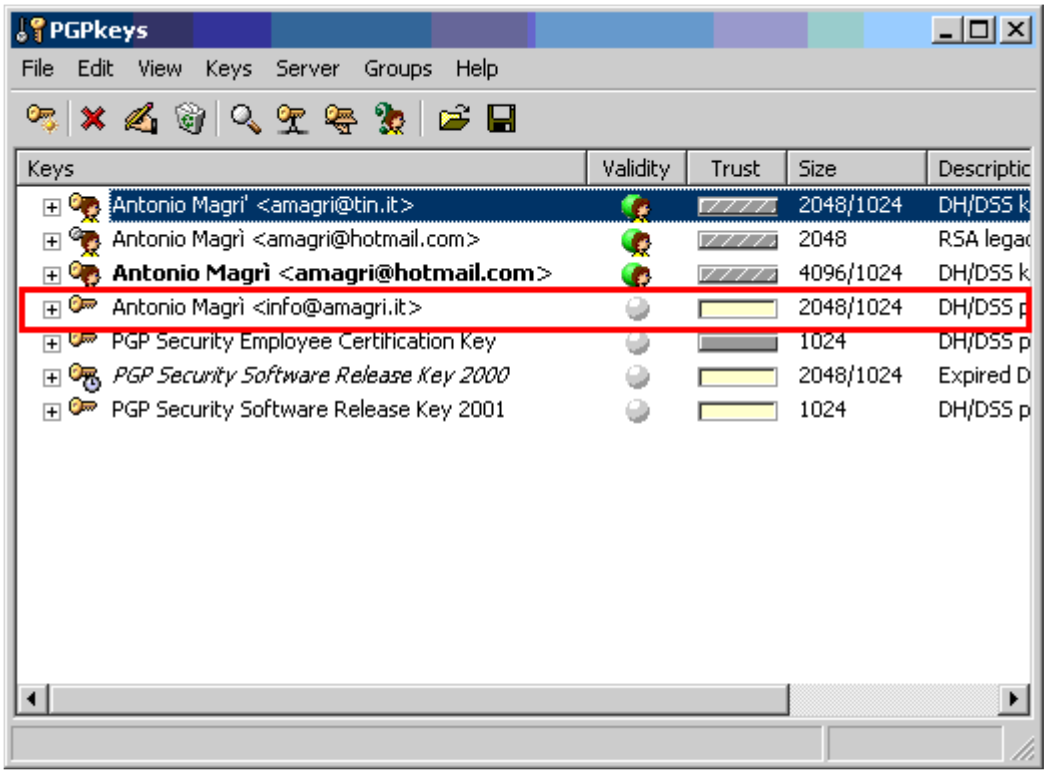
Avete appena ricevuto una chiave pubblica da un vostro nuovo corrispondente e desiderate importarla all'interno del vostro portachiavi pubblico.

1. Fate clic con il tasto destro del mouse sull'icona del file e dal menu selezionate PGP > Decrypt & Verify.

2. Il programma PGP vi presenterà una apposita finestra per consentirvi di importare la chiave. Per continuare selezionate il pulsante 'Import'.



3. La chiave verrà quindi importata all'interno del portachiavi pubblico.

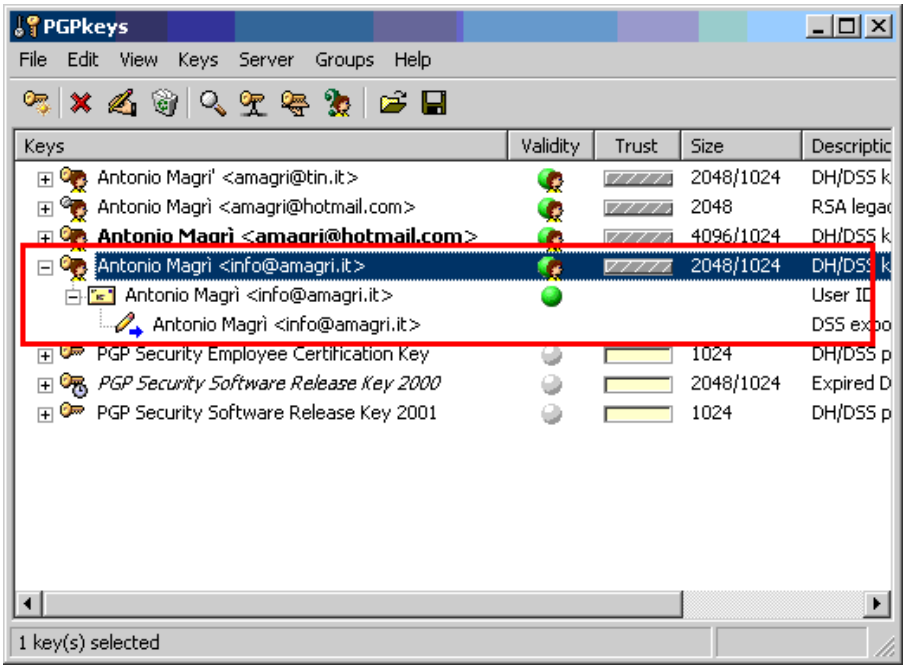


Vi ricordo che la chiave appena importata non dovrebbe essere utilizzata per le normali operazioni di cifratura se non dopo una verifica della validità. E' per questo motivo che in corrispondenza della colonna Validity associata alla chiave è presente un circoletto grigio e non uno verde.

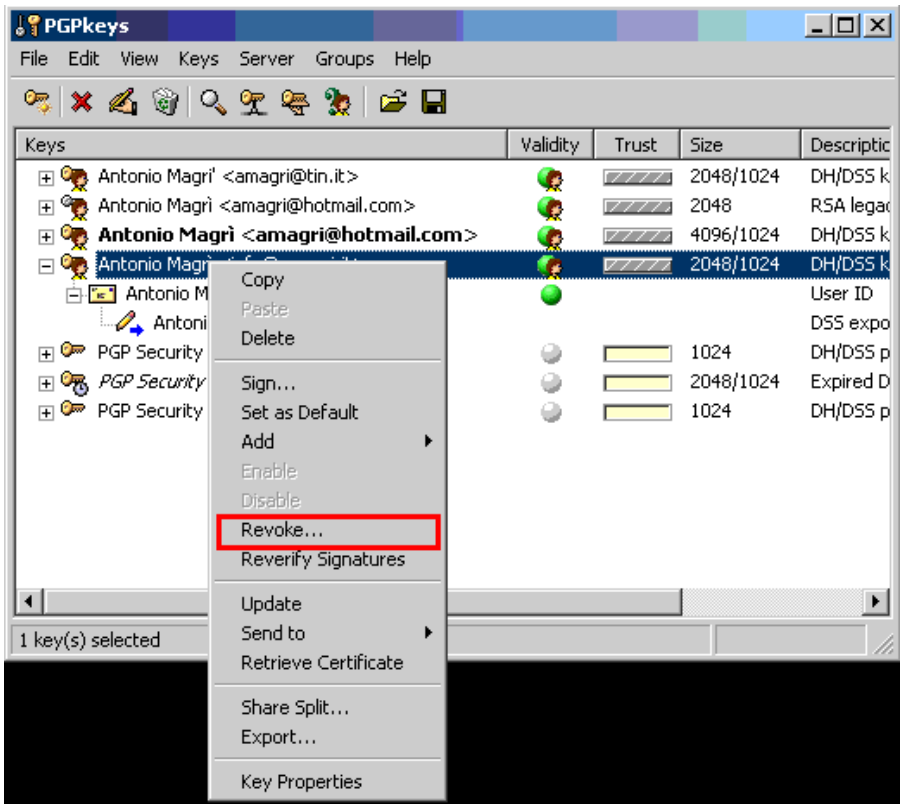
Revocare una chiave

Se, per un qualsiasi motivo, vi è la necessità di revocare una chiave, PGP vi offre una procedura semplice e veloce.

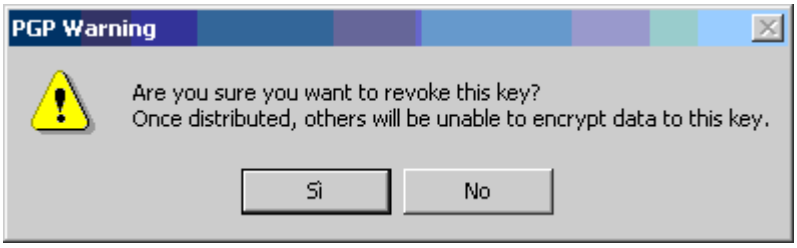
1. Selezionate la chiave che intendete revocare.



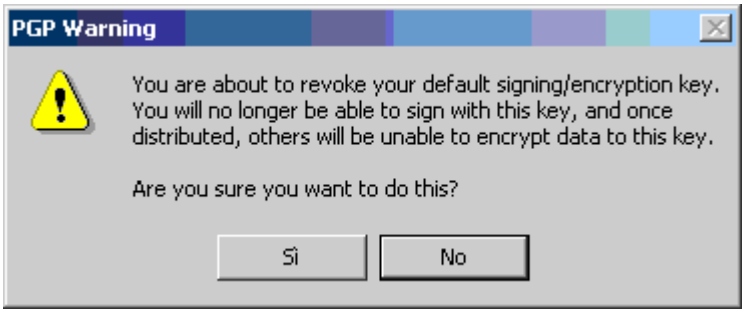
2. Premete il tasto destro del mouse sulla chiave e dal menu contestuale scegliete la voce 'Revoke...'



3. Il programma ci avverte che revocando la chiave i corrispondenti non potranno più utilizzarla per cifrare.

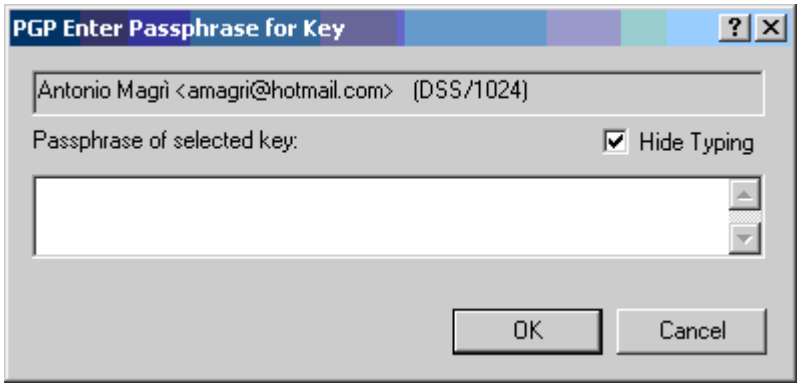


Se invece intendete revocare la chiave predefinita, il programma vi invierà un messaggio diverso, mettendovi in guardia sul fatto che, proseguendo, non sarete più in grado di firmare utilizzando la chiave e, una volta inviata la revoca ai keyservers, i vostri corrispondenti non potranno più utilizzarla per cifrare.

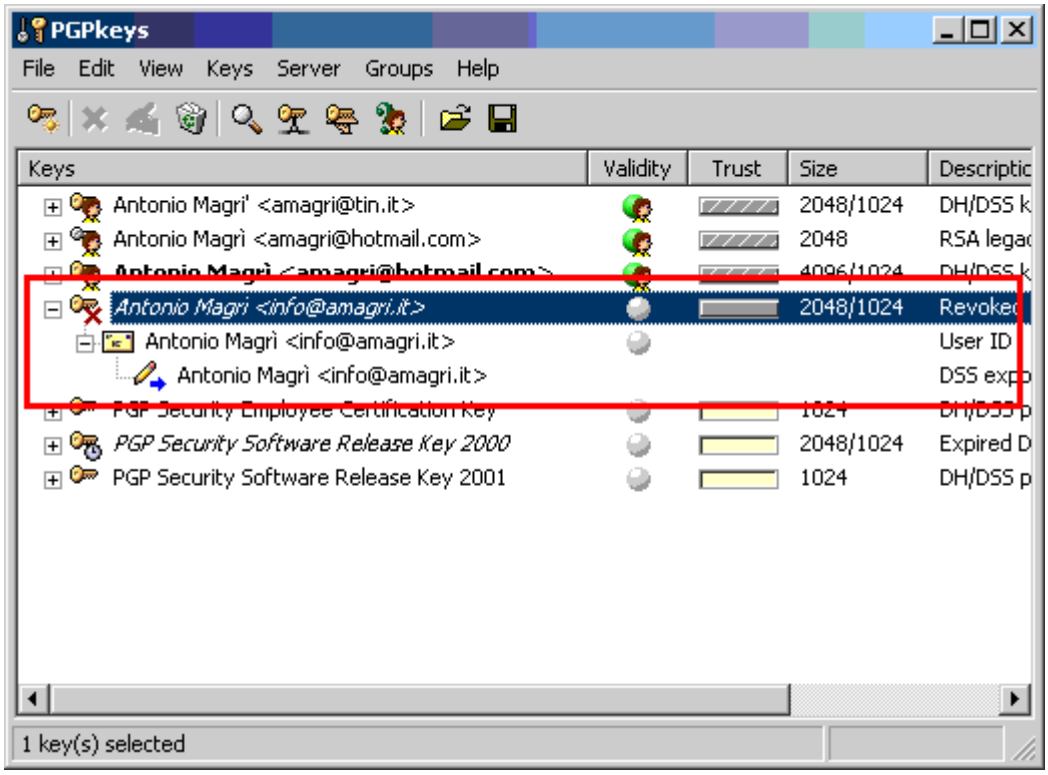


Ancora una volta, se siete veramente sicuri, continuate selezionando 'Si'.

4. Il programma vi chiederà di inserire la vostra frase password. Dopo averla inserita, selezionate 'OK'.



5. La chiave revocata dovrebbe essere ora evidenziata all'interno del programma PGPkeys da un segno di croce e dall'uso dei caratteri italici.

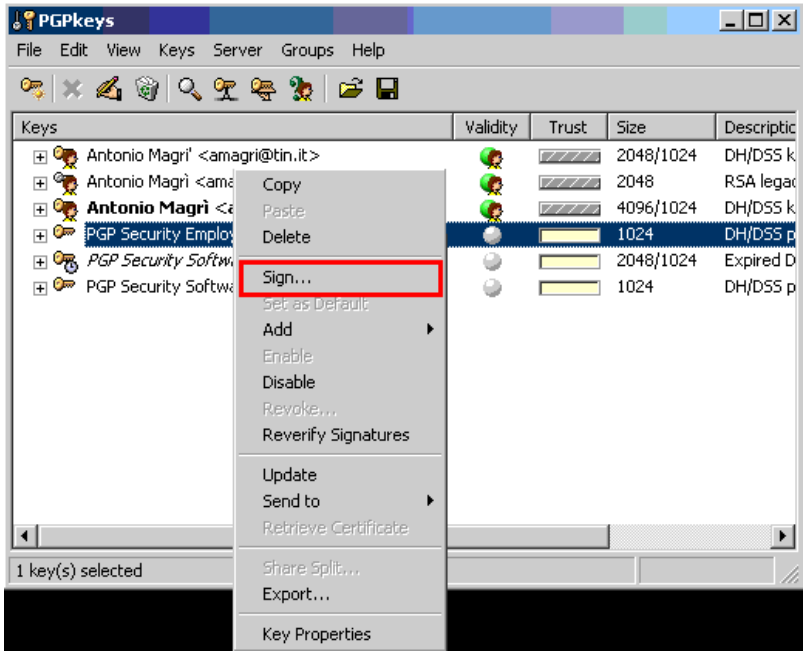


Da notare che, se è stata scelta anche l'opzione di sincronizzazione automatica con i keyservers, la chiave verrà automaticamente inviata come revocata, altrimenti, bisognerà effettuare la procedura manualmente.

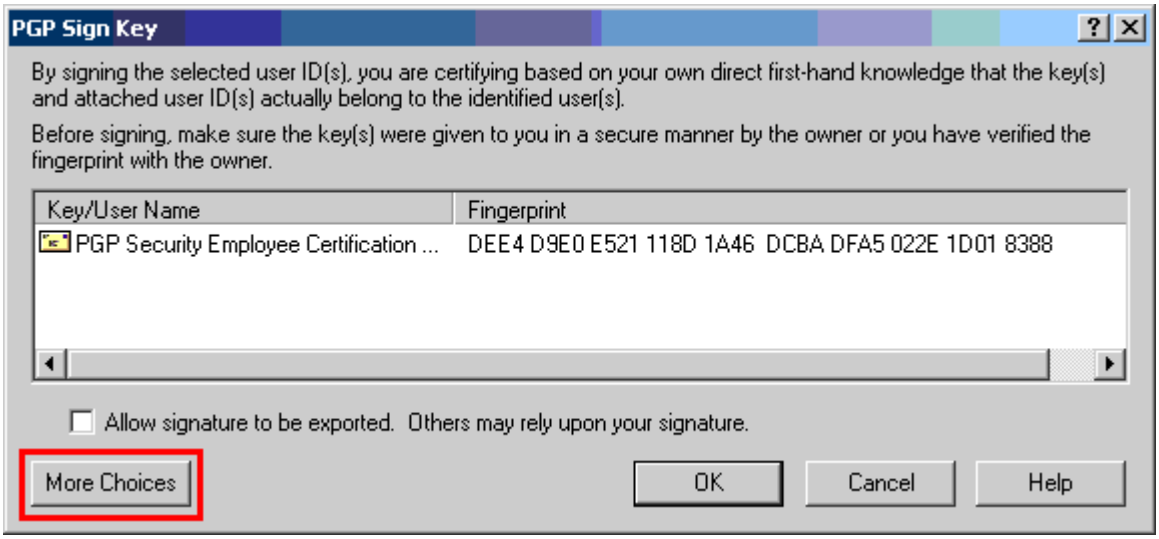
Dichiarare una chiave valida

Per dichiarare valida una chiave:

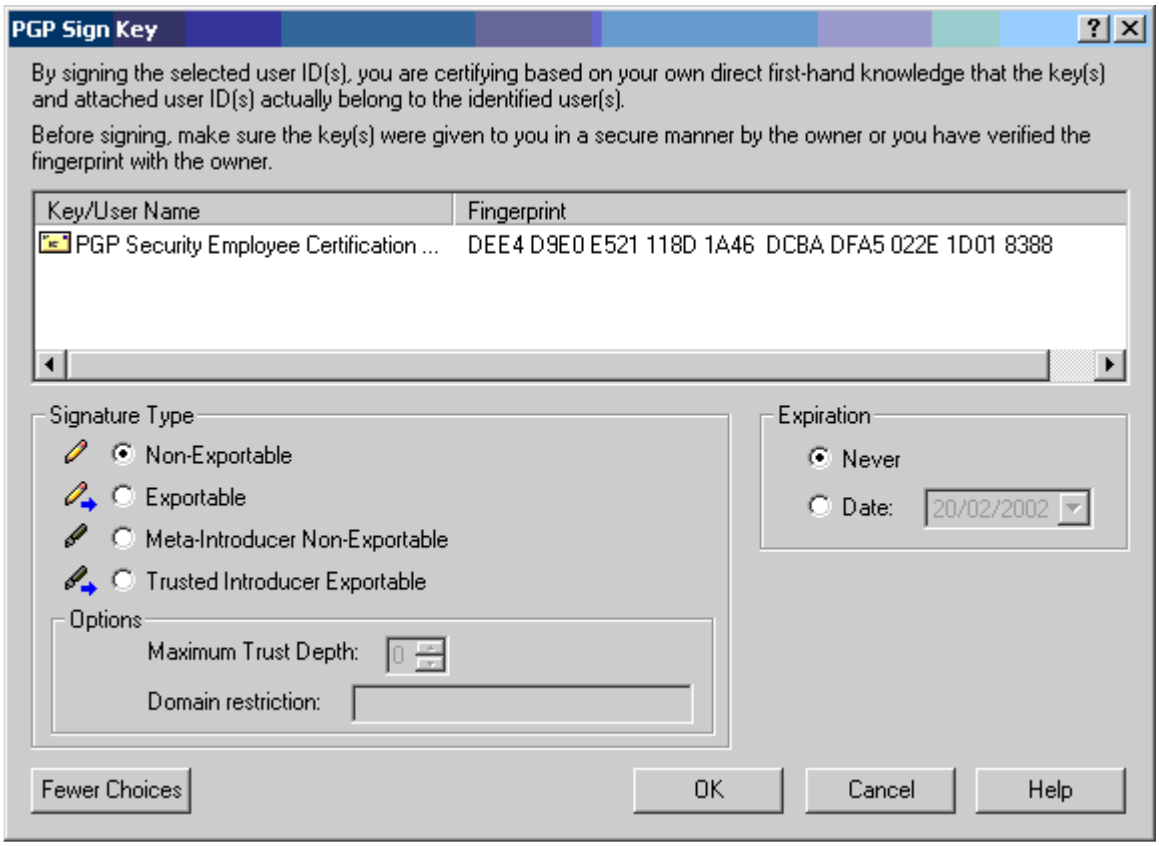
1. Cliccate con il tasto destro del mouse sulla chiave e dal menu contestuale selezionate 'Sign...'



2. Apparirà la finestra di firma contenente la chiave da firmare ed il suo fingerprint. Selezionate il pulsante 'More Choises' per vedere tutte le opzioni a vostra disposizione.



3. Vi apparirà la finestra completa.



Le opzioni offerte riguardano il tipo di firma:

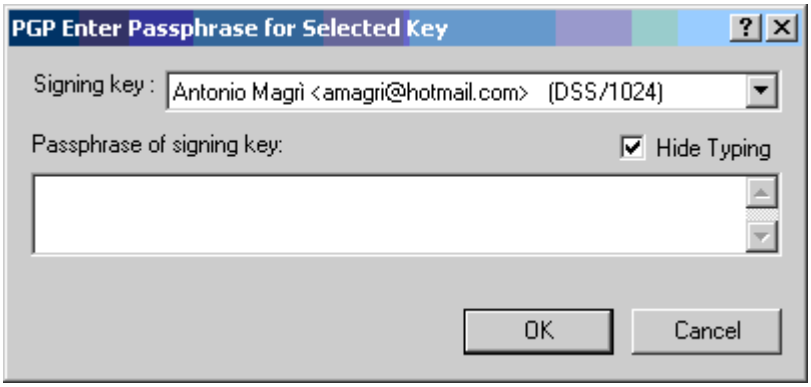
- **Non-Exportable**: la chiave è valida ma rimarrà all'interno del portachiavi pubblico e non sarà inviata al server dei certificati.
- **Exportable**: la chiave verrà inviata completa di firma al server dei certificati. Esportando la firma, dichiarate pubblicamente che la chiave è valida. Tutti coloro che hanno una fiducia completa nella vostra firma si fideranno anche di questa chiave.
- **Meta-Introducer Non-Exportable**: firmando la chiave, non solo date fiducia al proprietario della stessa ed a quelle dichiarate valide da quest'ultimo, ma anche ai trusted introducer creati dalla chiave. In pratica, le chiavi dichiarate valide da un meta-introducer o uno qualsiasi dei suoi trusted introducer saranno automaticamente valide anche per voi.
- **Trusted Introducer Exportable**: firmando la chiave, oltre a dare fiducia al proprietario della stessa, lo considerate anche garante per le chiavi da lui firmate. Ne consegue che, queste ultime, saranno automaticamente valide anche per voi.
    - **Maximum trust depth**: indica la profondità scelta come nidificazione della fiducia. Per esempio, scegliendo 1 oltre a dare fiducia al meta introducer darete fiducia esclusivamente al primo livello di trusted introducer.
    - **Domain restriction**: limita la capacità di dichiarare le chiavi valide, data al Trusted Introducer, ai certificati appartenenti al dominio di posta elettronica specificato.

E la scadenza:

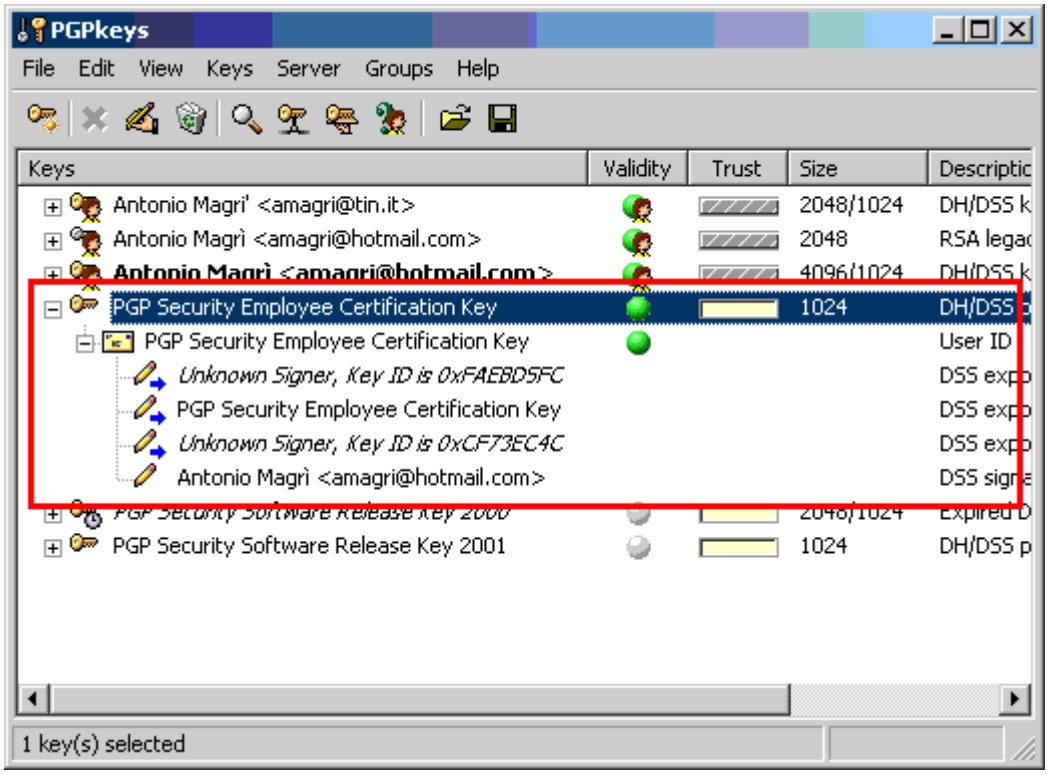
- **Never**: non scadrà mai;
- **Date**: scadrà il giorno indicato.

Prima di procedere nel firmare la chiave, è bene ricordarsi che, bisogna verificare che questa appartenga veramente al soggetto interessato mediante la verifica del fingerprint. Fatto questo, scegliete 'OK' per proseguire.

4. Il programma, ovviamente, vi chiederà di inserire la vostra frase password. Una volta fatto, selezionate 'OK'.



5. Tornando al PGPkeys, il programma ci farà notare che la chiave è stata dichiarata valida mediante un circoletto di colore verde nella colonna 'Validity'. Espandendo la chiave (fancedovi sopra doppio clic con il tasto sinistro del mouse) sarà possibile notare, fra le altre firme, anche la nostra.



Web of trust

Per descrivere il concetto di ragnatela di fiducia (web of trust) alla base di PGP, utilizzeremo le chiavi normalmente fornite a corredo del programma. Se le avete già cancellate, le importeremo dall'apposito file SampleKeys.asc presente nella cartella C:\Programmi\Network Associates\PGP for Windows 2000\Sample Keys.

Vi ricordo che il percorso è sempre relativo all'installazione del programma in un sistema MS Windows 2000 ITA Server configurato in modo standard.

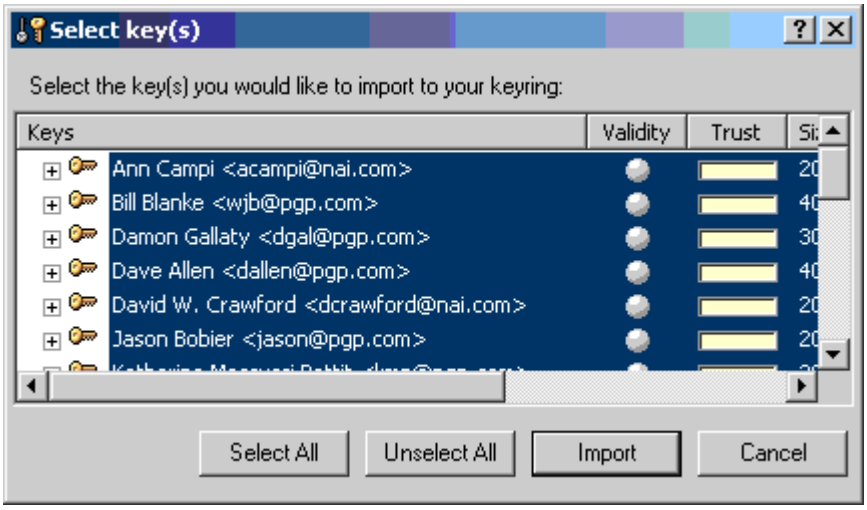
L'importazione delle chiavi contenute nel file è molto semplice, basta:

1. Aprire Esplora risorse;

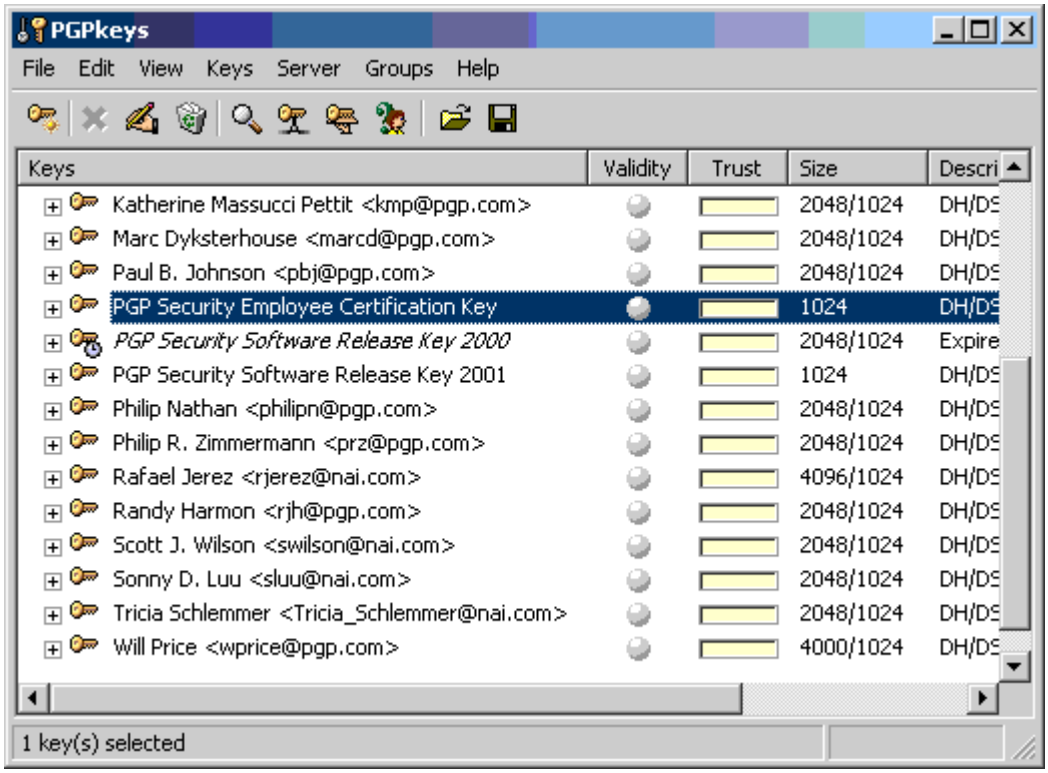
2. Spostarsi nella cartella C:\Programmi\Network Associates\PGP for Windows 2000\Sample Keys;

3. Cliccare con il tasto sinistro del mouse sul file e, mantenendo tenuto il tasto, trascinare il file all'interno del PGPkeys;

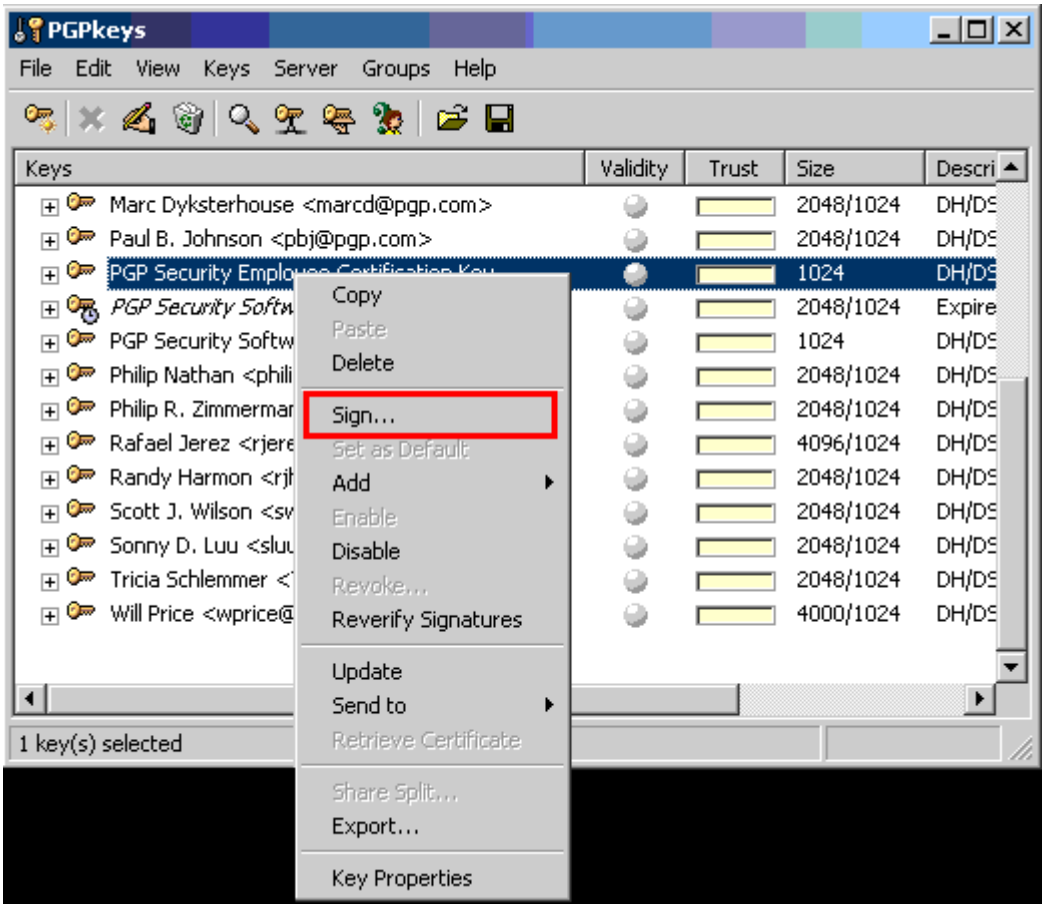
4. Il programma vi chiederà se volete importare le chiavi, cliccate sul pulsante 'Select All' quindi su 'Import'.



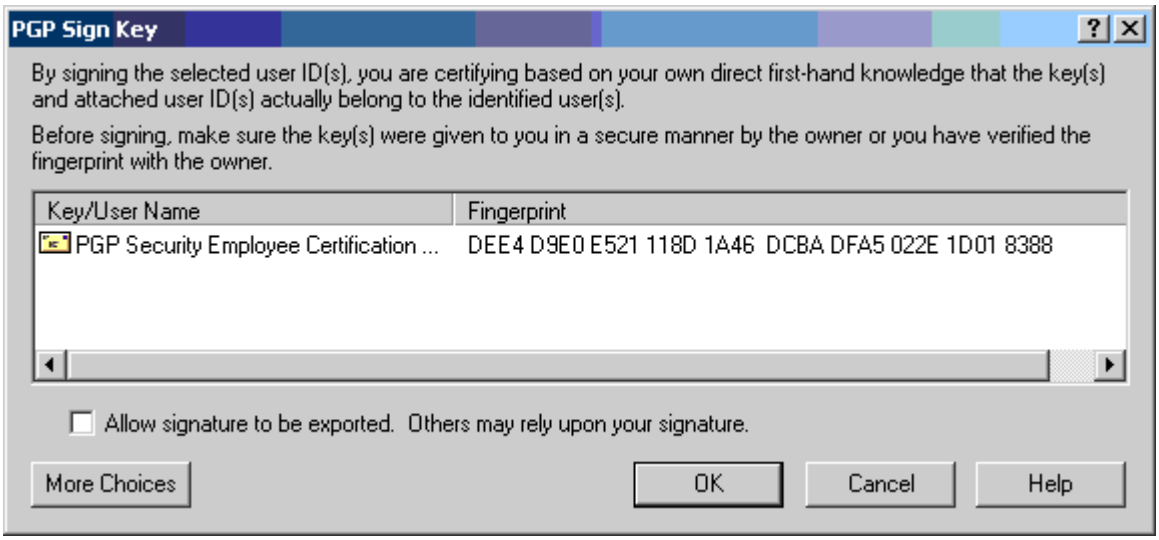
5. Dovreste ottenere una finestra simile a questa:



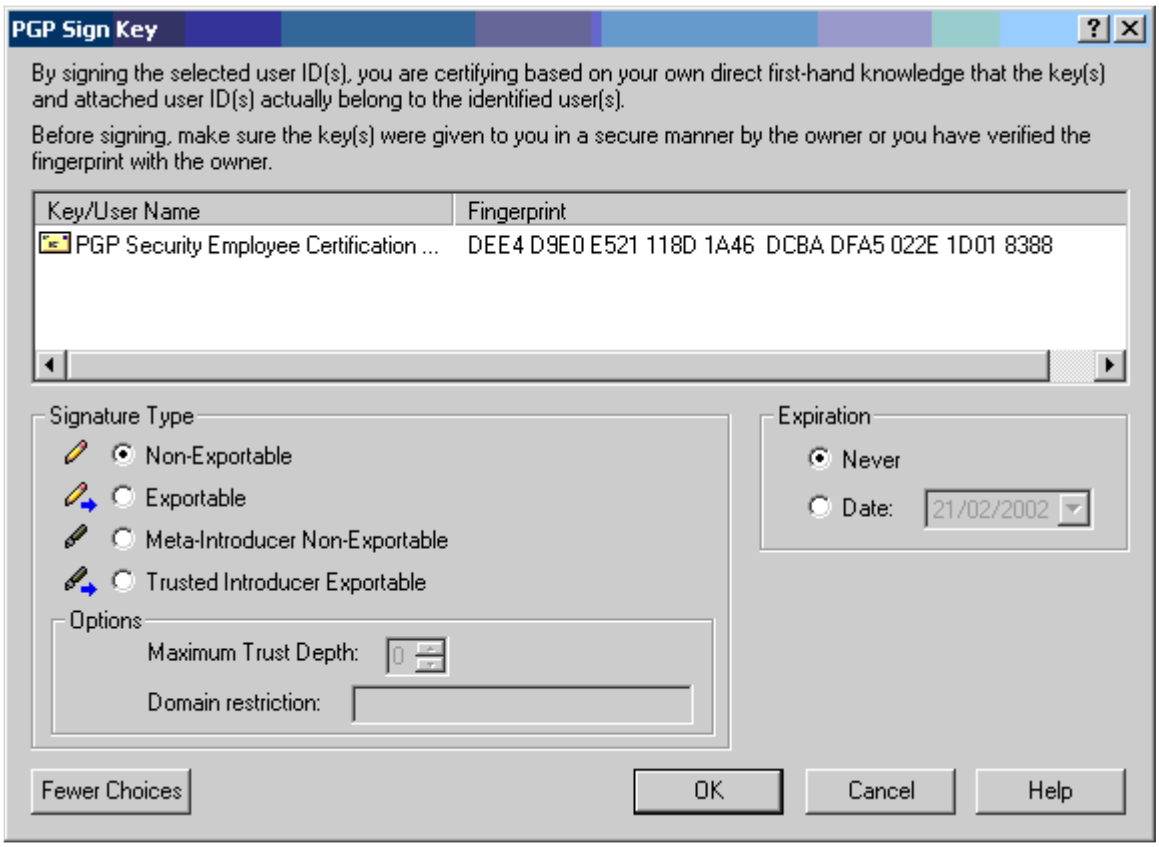
6. Selezionate la chiave evidenziata 'PGP Security Employee Certification Key'. 7. Firmate la chiave. Per fare questo, cliccate con il tasto destro del mouse sulla chiave e dal menu contestuale selezionate 'Sign...'



8. Apparirà la finestra di firma contenente la chiave da firmare ed il suo fingerprint. Selezionate il pulsante 'More Choises' per vedere tutte le opzioni a vostra disposizione.



9. Vi apparirà la finestra completa.



Le opzioni offerte riguardano il tipo di firma:

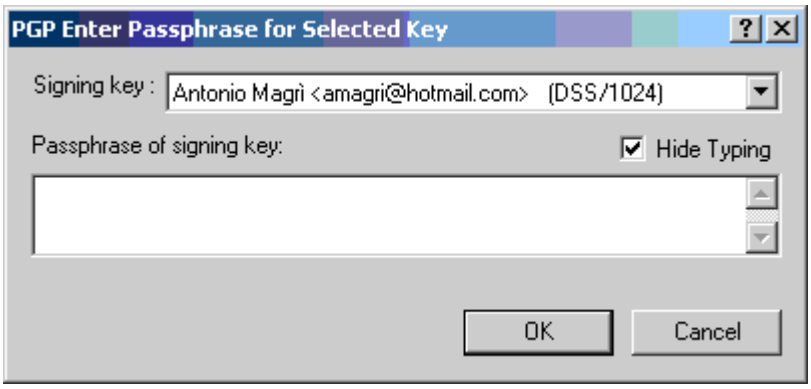
- **Non-Exportable**: la chiave è valida ma rimarrà all'interno del portachiavi pubblico e non sarà inviata al server dei certificati.
- **Exportable**: la chiave verrà inviata completa di firma al server dei certificati. Esportando la firma, dichiarate pubblicamente che la chiave è valida. Tutti coloro che hanno una fiducia completa nella vostra firma si fideranno anche di questa chiave.
- **Meta-Introducer Non-Exportable**: firmando la chiave, non solo date fiducia al proprietario della stessa ed a quelle dichiarate valide da quest'ultimo, ma anche ai trusted introducer creati dalla chiave. In pratica, le chiavi dichiarate valide da un meta-introducer o uno qualsiasi dei suoi trusted introducer saranno automaticamente valide anche per voi.
- **Trusted Introducer Exportable**: firmando la chiave, oltre a dare fiducia al proprietario della stessa, lo considerate anche garante per le chiavi da lui firmate. Ne consegue che, queste ultime, saranno automaticamente valide anche per voi.
    - **Maximum trust depth**: indica la profondità scelta come nidificazione della fiducia. Per esempio, scegliendo 1 oltre a dare fiducia al meta introducer darete fiducia esclusivamente al primo livello di trusted introducer.
    - **Domain restriction**: limita la capacità di dichiarare le chiavi valide, data al Trusted Introducer, ai certificati appartenenti al dominio di posta elettronica specificato.

E la scadenza:

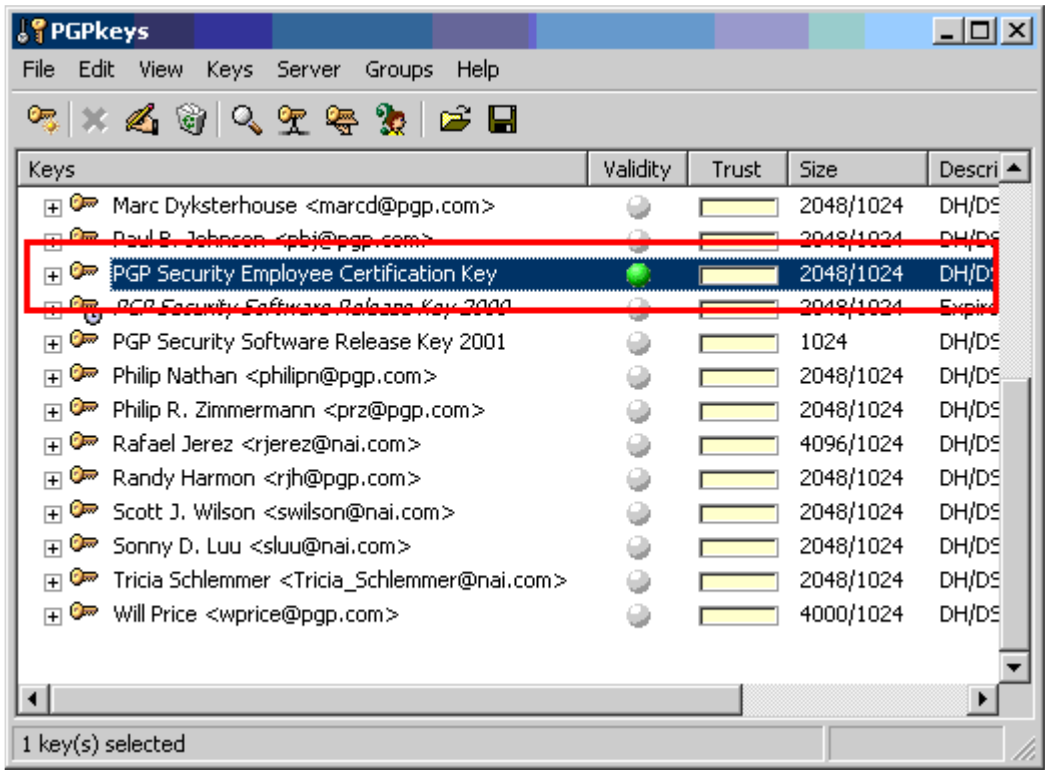
- **Never**: non scadrà mai;
- **Date**: scadrà il giorno indicato.

Prima di procedere nel firmare la chiave, è bene ricordarsi che, bisogna verificare che questa appartenga veramente al soggetto interessato mediante la verifica del fingerprint. Fatto questo, scegliete 'OK' per proseguire.

10. Il programma, ovviamente, vi chiederà di inserire la vostra frase password. Una volta fatto, selezionate 'OK'.

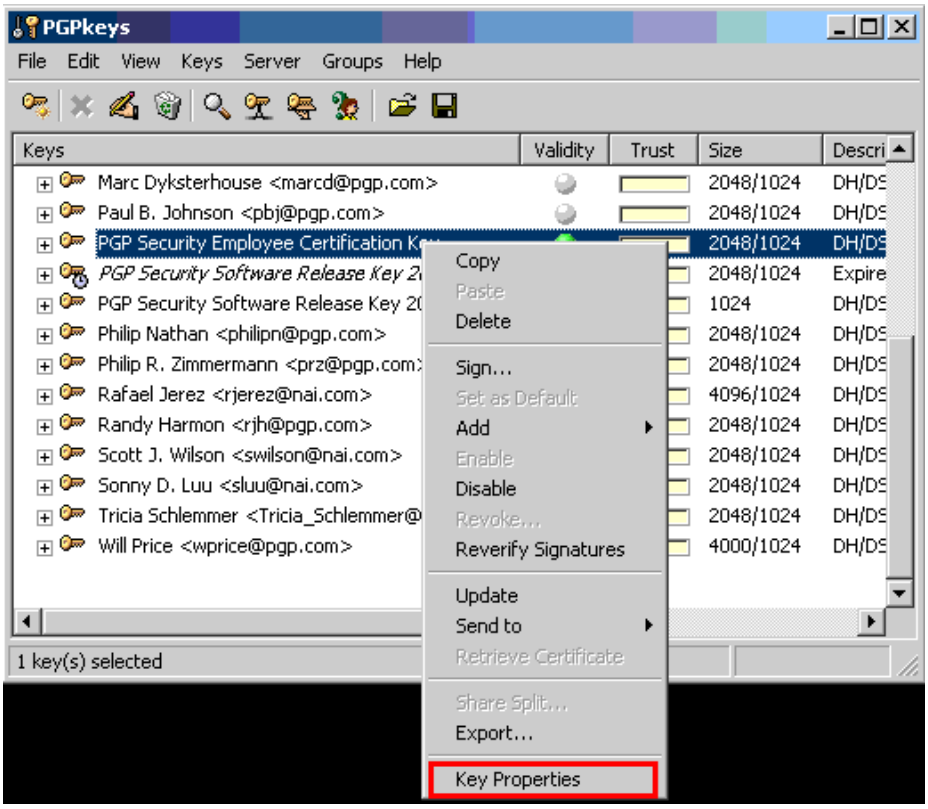


11. Tornando al PGPkeys, il programma ci farà notare che la chiave è stata stata dichiarata valida mediante un circoletto di colore verde nella colonna 'Validity'. Espandendo la chiave (fancedovi sopra doppio clic con il tasto sinistro del mouse) sarà possibile notare, fra le altre firme, anche la nostra.

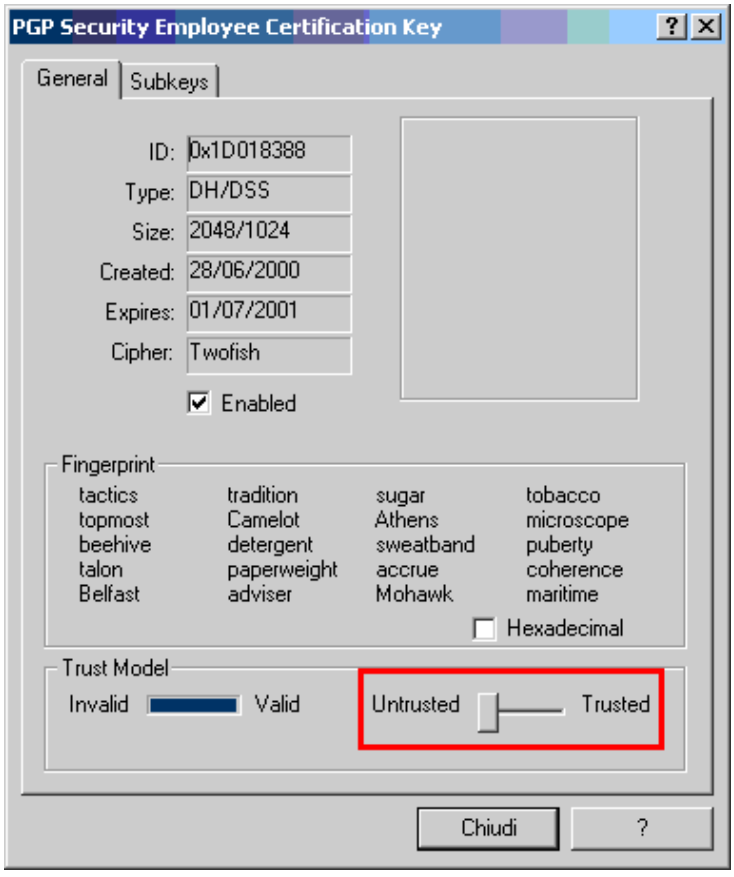


Fermandoci a questo punto la chiave potrebbe essere già utilizzata, senza sfruttare però, tutte quelle che sono le funzionalità offerte dalla ragnatela di fiducia che è alla base di PGP. In pratica, bisogna continuare.

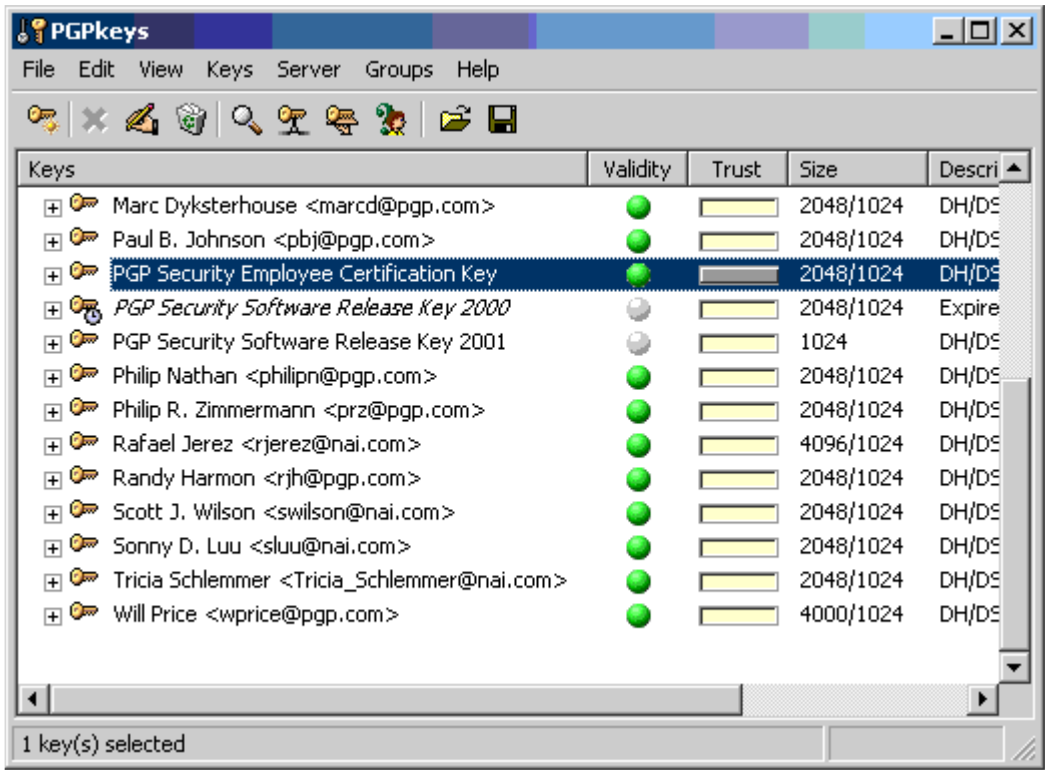
12. Clic con il tasto destro del mouse sulla chiave e dal menu contestuale selezionate 'Key Properties...'



13. Nella finestra delle proprietà relative alla chiave selezionata, bisognerà spostare il controllo a cursore relativo al trust model completamente verso la scritta 'Trusted' dopo di che selezionare 'OK'.



14. Visto che abbiamo scelto di fidarci totalmente della chiave con cui sono state firmate tutte le altre chiavi di esempio, automaticamente il PGPkey visualizzerà queste ultime come valide.



Archivio autodecifrante (SDA)

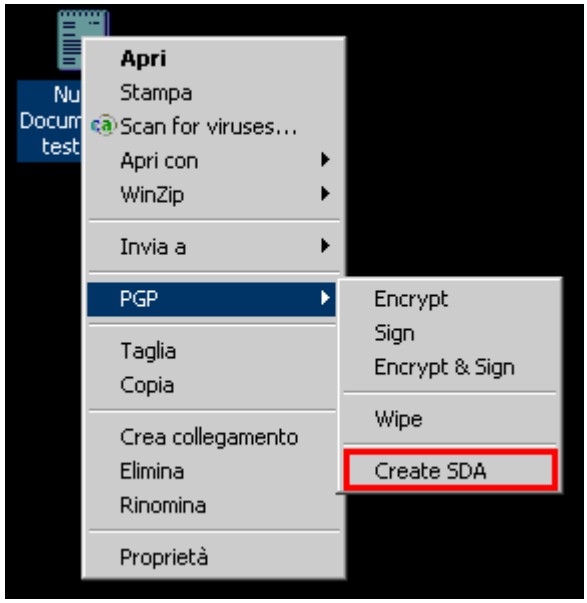
Volete inviare un file cifrato ad un vostro corrispondente ma questi non ha installato PGP. Per risolvere il problema basterà utilizzare la funzione di archivio autodecifrante (Self Decrypting Archive) integrata nel programma.

In pratica non si fa altro che utilizzare una chiave di sessione generata al momento ed una frase password per cifrare, mediante un algoritmo simmetrico, il file.

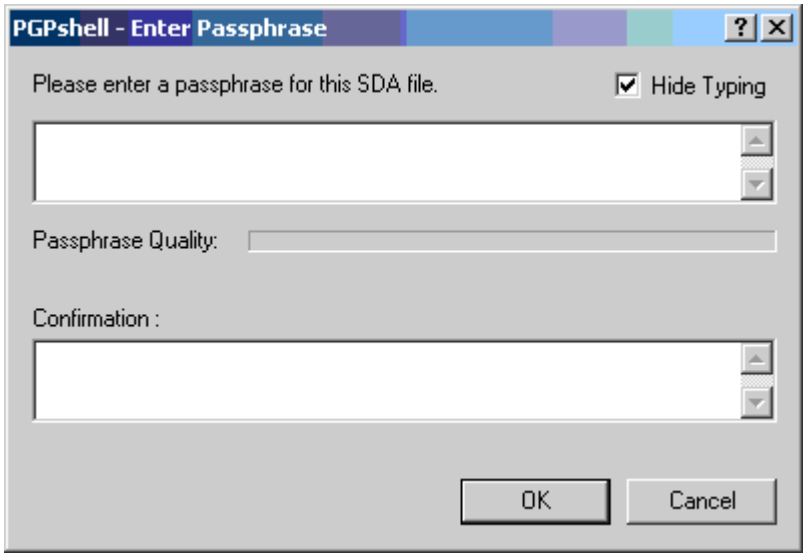
La procedura da seguire è molto semplice:

1. Selezionate il file;

2. Tasto destro sul file e dal menu contestuale scegliete PGP > Create SDA;



3. Vi comparirà una finestra di richiesta di inserimento della frase password. L'indicatore 'Passphrase quality' vi indicherà la bontà della frase che andrete man mano inserendo. Ricordatevi che una buona frase password dovrebbe essere composta da un certo numero di caratteri alfanumerici, caratteri speciali compresi.



Terminato l'inserimento, selezionate 'OK' per proseguire.

4. Il programma vi chiederà di inserire il nome del file. Notate che, come nome, vi viene proposto il nome originale del file con l'aggiunta dell'estensione .exe. Per proseguire, selezionate 'Salva'.

5. Vi ritroverete con un nuovo file eseguibile:

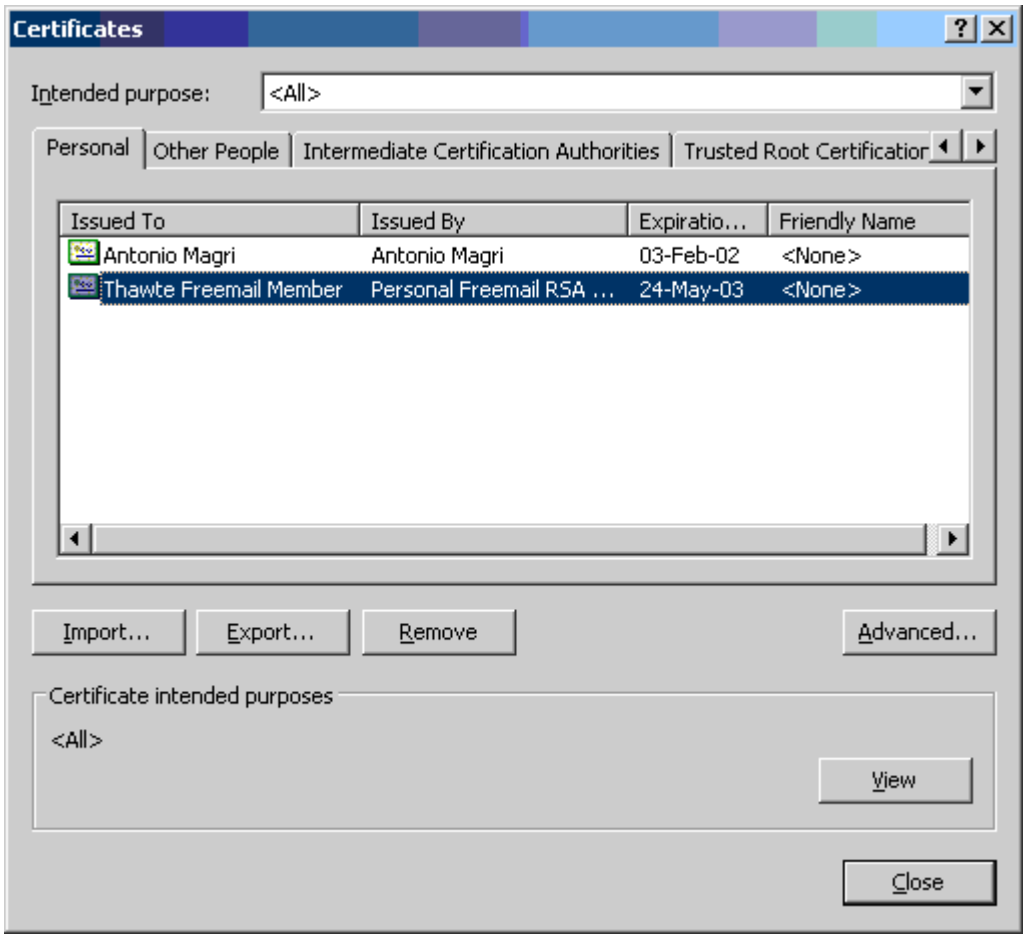
Certificati X.509

Possiamo importare un certificato X.509 ed il materiale chiave in esso contenuto all'interno di PGP? Vediamolo insieme tenendo presente che tutte le procedure sono state effettuate su un sistema MS Windows XP Professional ENG con Internet Explorer 6.0 ENG.

Esportare il certificato

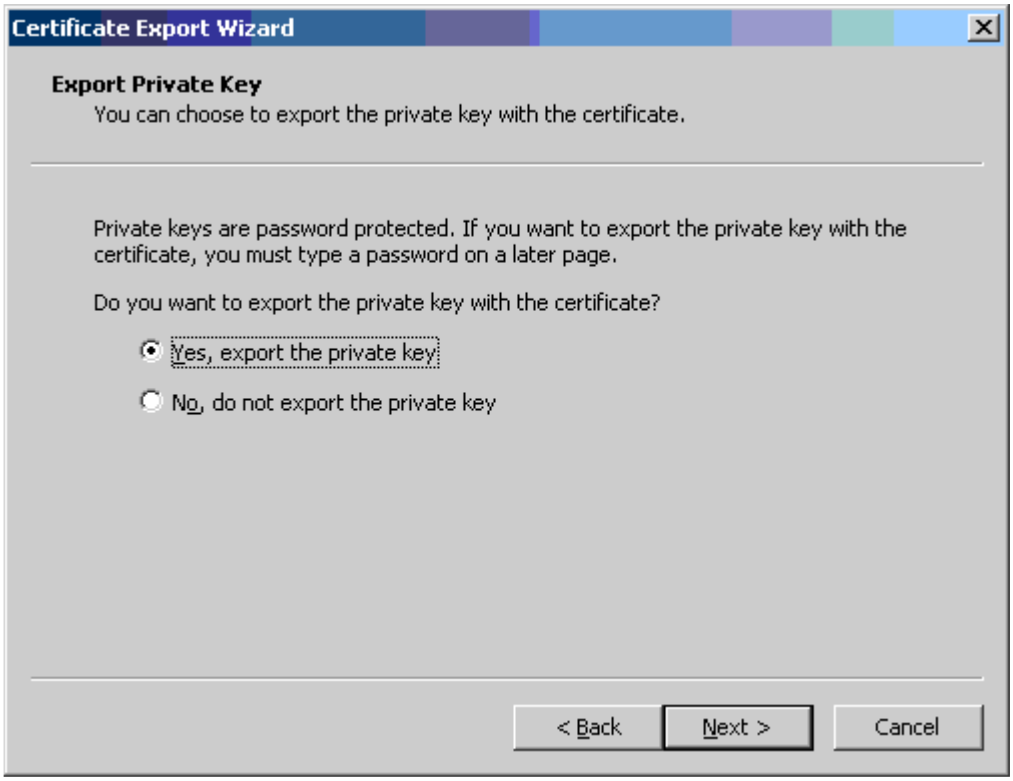
Il certificato di prova è stato richiesto utilizzando il servizio gratuito offerto da Thawte. Al termine della procedura di registrazione/emissione, il sistema rilascerà un certificato che sarà memorizzato all'interno dello store dell'utente utilizzato.

Per verificare la cosa, in Internet Explorer aprite Tools > Internet Options > Content > Certificates. Dovreste avere qualcosa di simile a questo:

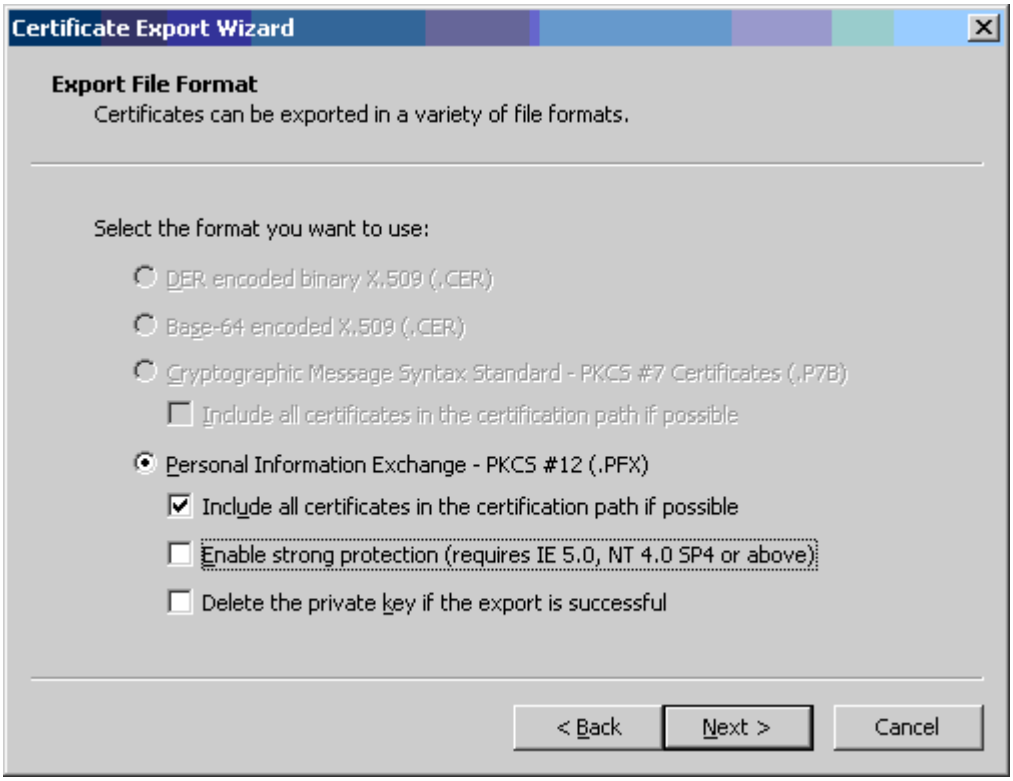


Per esportare il certificato, selezionate il pulsante 'Export'. Verrà avviata una procedura che vi guiderà nell'operazione di esportazione.

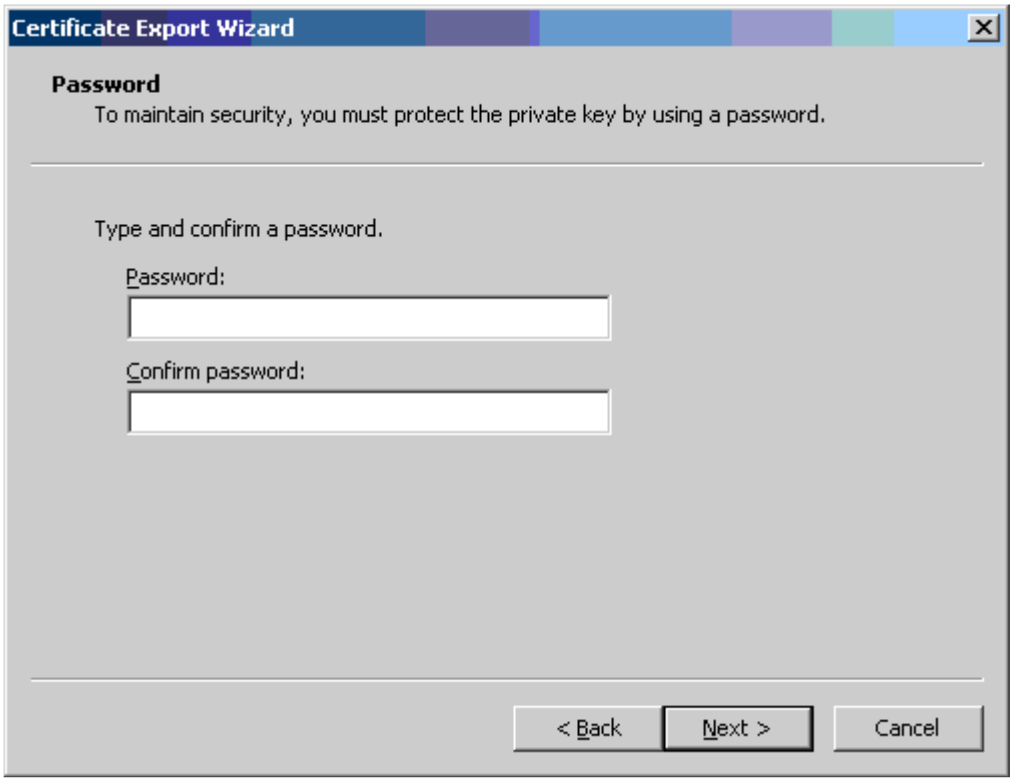
Selezionate 'Next'. Quindi nella finestra successiva assicuratevi di aver selezionato l'opzione relativa all'esportazione della chiave privata:



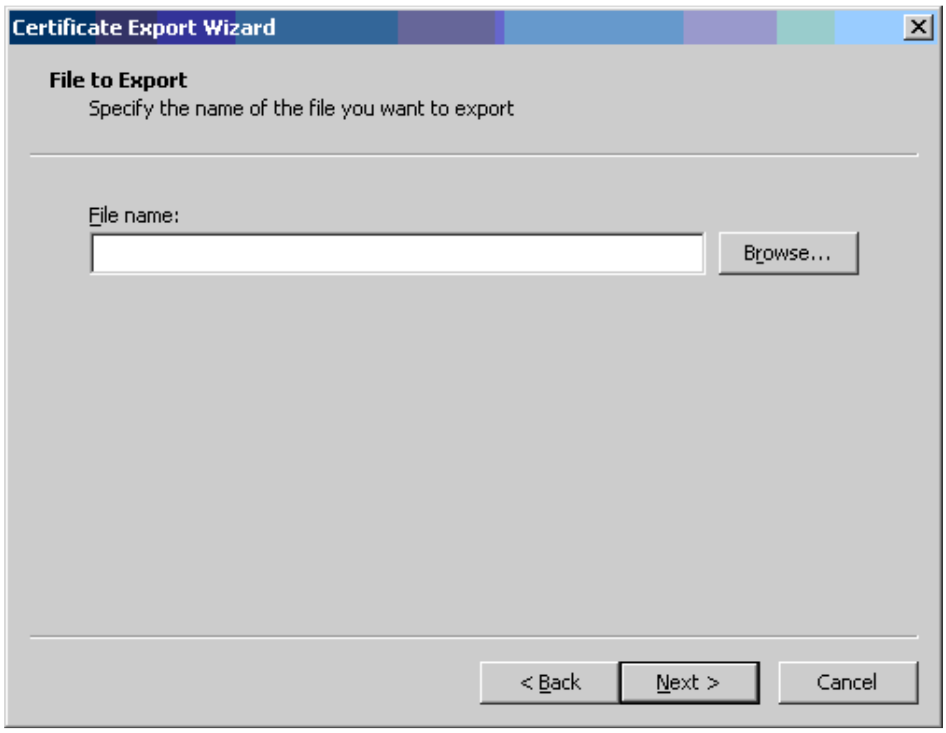
Quindi selezionate 'Next'. Dopo di che abilitate la spunta alla voce "Include all certificates ..." e disabilitate "Enable strong protection ... ", quindi cliccate 'Next'.



Vi verrà chiesto di inserire una password. Fate attenzione a quello che inserite perchè questa sarà poi la frase password da utilizzare in seguito con PGP.



Fatto questo, cliccate su 'Next' e digitate il nome del file che dovrà contenere il certificato.



Fate clic su 'Next'. Vi verrà presentato un elenco riassuntivo delle opzioni e dei parametri impostati:

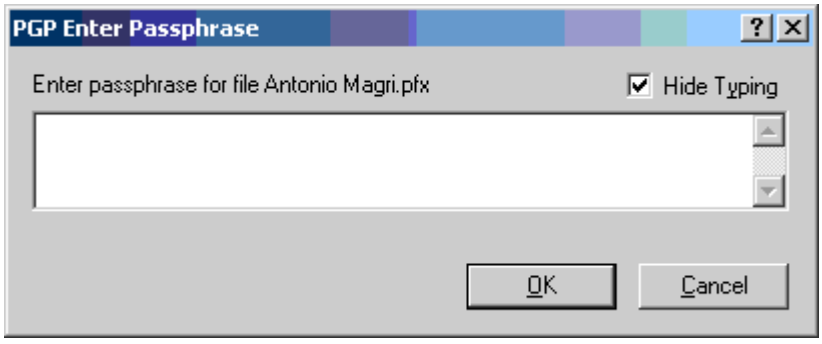
Selezionate 'Finish' per terminare la procedura.

Importare il materiale chiave

Aprite adesso PGPkeys e dalla voce di menu 'Keys' selezionate 'Import". Vi si presenterà una finestra da cui scegliere il file da importare.

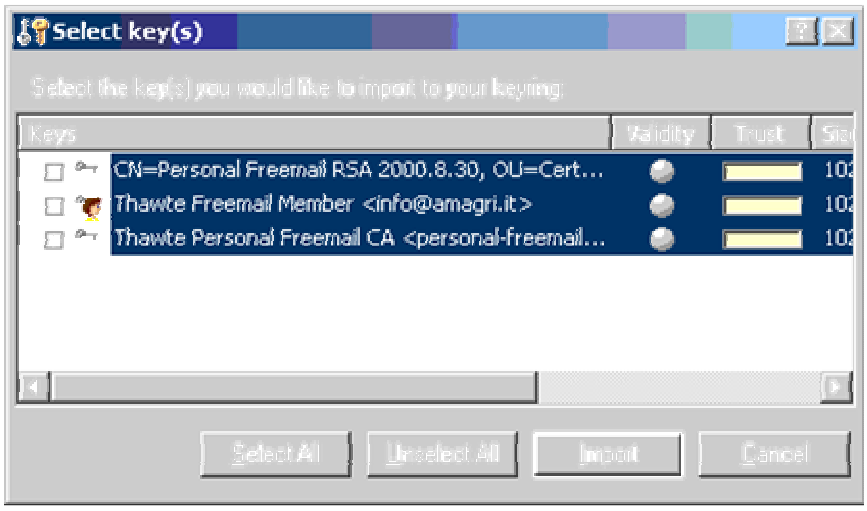
Assicuratevi che 'Files of type' sia posizionato su 'PKCS-12 Files (*.p12; *.pfx) e selezionate il file contenente il certificato salvato nella sezione precedente. Quindi fate clic su 'Open'.

Il programma vi chiederà di inserire la frase password, scelta in precedenza, associata alla chiave privata da importare.

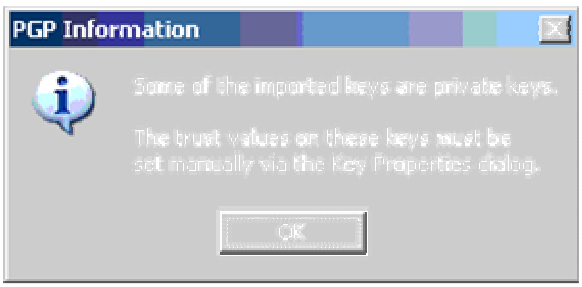


Fatto questo, selezionare 'OK' per proseguire.

La finestra successiva vi elencherà, evidenziandolo, tutto il materiale chiave presente all'interno del certificato. Cliccate su 'Import'.

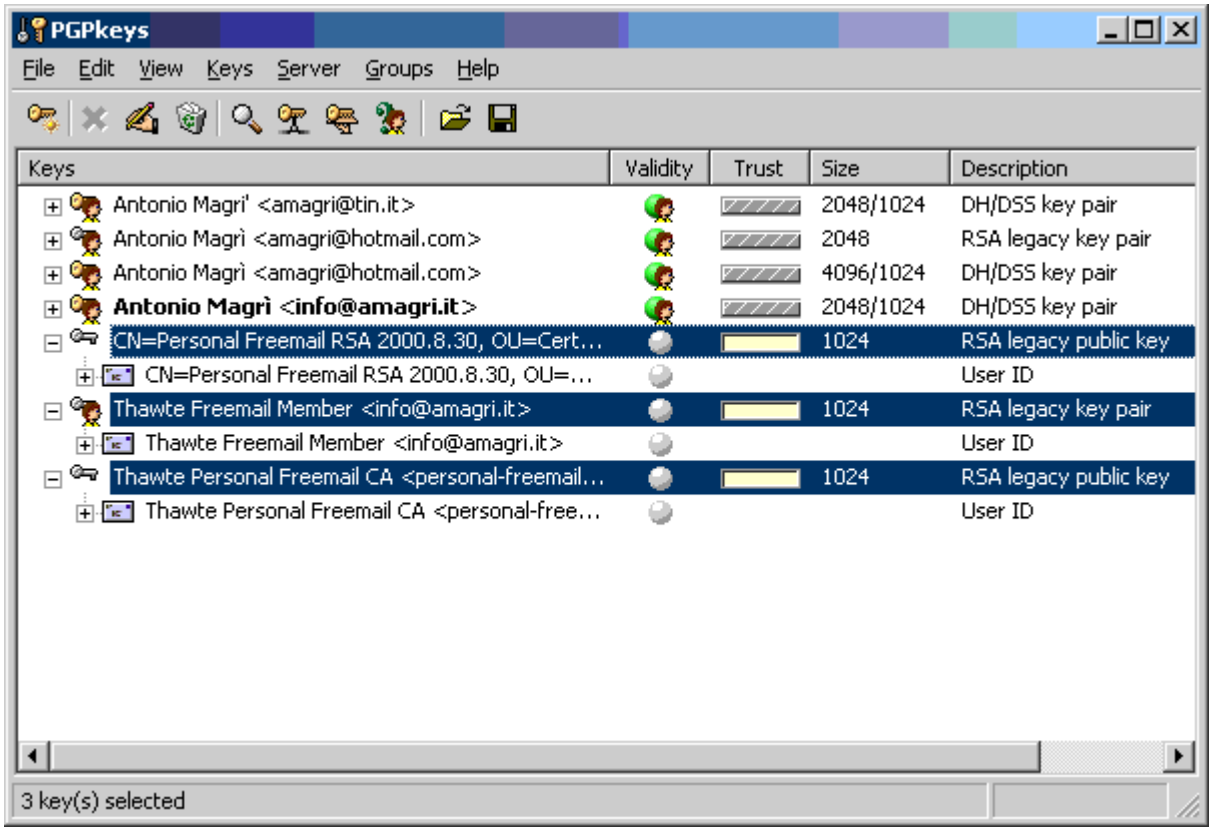


Un messaggio vi ricorderà che il materiale importato contiene anche delle chiavi private e che la validità di queste ultime dovrà essere imposta manualmente utilizzando la finestra delle proprietà della chiave.



Selezionate 'OK'.

PGPkeys visualizzerà, evidenziandolo, il materiale appena importato:



Selezionate la chiave associata al soggetto titolare del certificato dopo di che, premendo il tasto destro, passate a modificarne le proprietà, in particolare quella relativa alla validità, spuntando 'Implicit trust', nonchè la frase password, che occorrerà inserire nuovamente.