Corso: Sistemi Informativi
Redatto da: Elena Tagliarini
Matricola: 328882/50

PGP [PRETTY GOOD PRIVACY]

Definizione

PGP, dall'inglese Pretty Good Privacy, è un programma che realizza la crittografia a chiave pubblica (o asimmetrica); il successo di questa tecnica di crittografia, ha portato alla popolarità PGP che si è imposto negli anni come lo standard di fatto per l'utilizzo della crittografia nella posta elettronica.
Con PGP e' infatti possibile codificare un messaggio in modo che solo il destinatario possa leggerlo, e non una persona esterna. Inoltre, offre la possibilità di autenticare il mittente ed il messaggio.
PGP risponde così all' esigenza fondamentale di riservatezza e sicurezza della corrispondenza privata.

Perché criptare un messaggio telematico

La corrispondenza per posta elettronica ha da un lato innumerevoli vantaggi, ma purtroppo presenta intrinsecamente un basso grado di sicurezza. E' infatti molto semplice per una terza persona andare a leggere messaggi privati destinati ad altri, oppure alterare un messaggio inviato da un altro, oppure ancora inviarne uno con il nome di un altro violando così la privacy di una persona. Un'ottima soluzione quindi per la protezione di dati sensibili trasferibili tramite messaggistica, la offre la crittografia a chiave pubblica, assai molto più efficace di altri sistemi.

Crittografia a chiave pubblica (asimmetrica)

La crittografia classica (che utilizza una sola chiave segreta per poter decifrare il messaggio) presenta un problema: la sicurezza del canale trasmissivo. Infatti, il mittente che vuole inviare un messaggio criptato, deve far avere al destinatario la chiave segreta e, se il canale non è sicuro, la chiave potrebbe essere intercettata facilmente. Questo notevole problema, è stato risolto con l'idea della crittografia a chiave pubblica.
Nella crittografia a chiave pubblica ad ogni utente coinvolto, vengono associate una coppia di chiavi utili per la decriptazione del messaggio personale: una chiave privata ed una pubblica. La chiave privata, personale e segreta, viene utilizzata per decodificare un documento criptato; la chiave pubblica, che deve essere distribuita, serve a criptare un documento destinato alla persona che possiede la relativa chiave privata.

Ogni utente genera così, mediante una funzione di PGP, una coppia di chiavi.
L'algoritmo matematico che effettua questa operazione e' tale che:
- un messaggio codificato con una chiave della coppia puo' essere decodificato solo con l'altra chiave della stessa coppia;
- non e' materialmente possibile, data una chiave della coppia, ricavare l'altra.
Ogni utente custodisce una chiave della propria coppia, denominata chiave segreta, e diffonde il piu' possibile l'altra, denominata chiave pubblica.
In questo modo, il problema della crittografia simmetrica viene risolto.

In particolare, la crittografia a chiave pubblica con PGP garantisce, attraverso semplici comandi:

1- Privacy:
Assumiamo che il mittente voglia inviare un messaggio al proprio destinatario di posta, e codifica quel messaggio usando la chiave pubblica di quest'ultimo. Solo il destinatario, che ha la corrispondente chiave segreta, e' in grado di decodificare e leggere il messaggio.

2- Autenticazione del mittente:
Il mittente codifica il suo messaggio con la propria chiave privata. Chiunque, avendo accesso alla chiave pubblica, puo' decodificare quel messaggio. Se la decodifica riesce, si e' allora sicuri che esso e' stato scritto proprio dal mittente, l'unica persona a possedere la corrispondente chiave segreta. Quindi si ha così certezza che il messaggio è stato scritto dal mittente in questione e si tratta di una sorta di firma.

3- Autenticazione del mittente e del messaggio:
E' possibile autenticare, oltre al mittente, anche il contenuto del messaggio.
Il mittente effettua un "hashing" del suo messaggio. Si tratta di una funzione unidirezionale, che a partire da un certo messaggio ricava un valore di lunghezza fissa, detto hash, che caratterizza il messaggio: una sorta di "checksum". Se il messaggio viene alterato, l'hash non corrisponde piu'. Il mittente aggrega allora in fondo al suo messaggio il corrispondente hash. Il mittente puo' così codificare con la propria chiave privata tutto l'insieme (per così dire firmando), oppure lasciare il messaggio vero e proprio in chiaro e firmare solo l'hash. Chiunque puo' decodificare l'insieme ricevuto o il solo hash con la chiave pubblica del mittente, ed e' così sicuro del fatto che il messaggio proviene da quel mittente. Se inoltre, una volta effettuata la decodifica, messaggio ed hash si corrispondono, si e' sicuri che nessuno dei due e' stato alterato in qualche maniera. In pratica, la firma elettronica realizzata dal PGP effettua sempre l'autenticazione sia del mittente sia del messaggio. Essa ha dunque le stesse funzioni della firma ordinaria su un documento cartaceo.

4- Trasmissione della chiave:
Col sistema di crittografia a chiave pubblica non c'e' una sola chiave segreta usata per entrambe le funzioni di codifica e decodifica, per cui non si pone il problema di dover trasmettere quella chiave. Ogni utente deve semplicemente tenere al sicuro la propria chiave segreta, e puo' diffondere senza alcun problema la propria chiave pubblica. Anzi, piu' questa viene diffusa e meglio e'.

La nascita di PGP e le sue versioni

Il PGP e' stato realizzato da Philip Zimmermann negli Stati Uniti. In seguito anche altri hanno lavorato alle versioni successive. Il programma e' freeware e opensource risulta così essere un programma libero e utilizzabile per tutti oltre che modificabile sulla base di ogni precisa esigenza.
Inoltre, le versioni per piattaforme diverse sono tutte compatibili tra di loro.
Le versioni piu' recenti del programma sono:

- *Versione MIT: PGP 2.6.2*
  Per ragioni di copyright non puo' essere esportata legalmente dagli USA. Genera messaggi non leggibili dalla versione 2.3a. Corregge alcuni bugs presenti nelle versioni 2.6 e 2.6.1.

- *Versione Internazionale: PGP 2.6.i*
  Adattamento della 2.6.1 fatto dal norvegese Stale Schumacher in modo da non sottostare al brevetto americano. Puo' trattare chiavi fino a 2048 bit (nelle altre versioni il limite e' 1024). E' compatibile con tutte le precedenti versioni 2.x. Non e' legale negli USA.

Descrizione del funzionamento di PGP nel dettaglio

La prima cosa da fare dopo l'installazione del programma, è generare le chiavi.
Sarà necessario quindi scegliere la lunghezza delle chiavi (conviene generare chiavi di 1024 bit) , scegliere lo Username (è possibile assegnare alle chiavi anche più identificativi in caso si abbiano più indirizzi e-mail) e la Pass Phrase (frase di accesso che permette di utilizzare la chiave segreta. Senza la pass phrase la chiave segreta e' inutilizzabile. Si tratta di una password estesa: puo' essere un testo di lunghezza arbitraria contenente qualunque carattere).
Una volta così generate le chiavi, esse saranno presenti al path:
- c:\pgp\secring.pgp → chiave segreta (secret ring);
- c:\pgp\pubring.pgp → chiave pubblica (public ring).
Un ulteriore passaggio da effettuare subito è quello di firmare la chiave pubblica allo scopo di rendere impossibili determinate manipolazioni della chiave pubblica da parte di terzi.
Per poter effettuare questa operazione, PGP chiederà di digitare la pass phrase, come sempre avviene quando occorre impiegare la chiave segreta.
Gestione delle chiavi:
Il secret ring (file secring.pgp) contiene la chiave segreta e va tenuto riservato come già annunciato. PGP va a cercare la chiave segreta in questo file tutte le volte che si voglia decodificare un messaggio o in caso si voglia firmare un messaggio.
Il public ring (file pubring.pgp) e' destinato a contenere, tutte le chiavi pubbliche che verranno utilizzate: è una sorta di database personale di chiavi pubbliche.
E' possibile estrarre una copia di una o piu' chiavi pubbliche dal public ring. Questa operazione consiste nel copiare la chiave in un file ASCII armored in modo da poterla passare ad altri utenti che la inseriranno a loro volta nel public ring personale.

Utilizzo degli algoritmi:
Il PGP utilizza un' intera collezione di algoritmi, tra i piu' sicuri e conosciuti nel campo della

crittografia. Supponendo di partire da un messaggio che deve essere firmato e codificato, i passaggi che PGP applica per il suo funzionamento sono:

1- *PGP applica l'algoritmo di hashing MD5 per generare l'hash del messaggio, avente lunghezza fissa pari a 128 bit. L'hash viene attaccato al messaggio;*
2- *PGP applica l'algoritmo di compressione dati ZIP per comprimere l'insieme del messaggio piu' l'hash ottenuto dal punto 1;*
3- *PGP applica un algoritmo di generazione di numeri casuali per generare una sequenza di 128 bit casuali;*
4- *PGP applica l'algoritmo di crittografia convenzionale IDEA per codificare il messaggio compresso ottenuto dal punto 2, usando come chiave ("session key") il numero casuale generato al punto 3;*
5- *PGP applica l'algoritmo di crittografia a chiave pubblica RSA per codificare la session key. Il risultato viene attaccato al messaggio codificato ottenuto al punto 4. La crittografia convenzionale e' molto piu' veloce di quella a chiave pubblica. PGP unisce i vantaggi della crittografia a chiave pubblica e la velocita' di quella convenzionale, Il messaggio viene in realta' codificato convenzionalmente, ed e' la session key usata che viene codificata con l'algoritmo a chiave pubblica.*
6- *PGP applica l'algoritmo di ASCII Armor Radix-64 per trasformare il messaggio ottenuto al punto precedente in modo che esso contenga solo caratteri ASCII bassi. Questo algoritmo trasforma ogni gruppo di tre bytes in un gruppo di quattro bytes.*

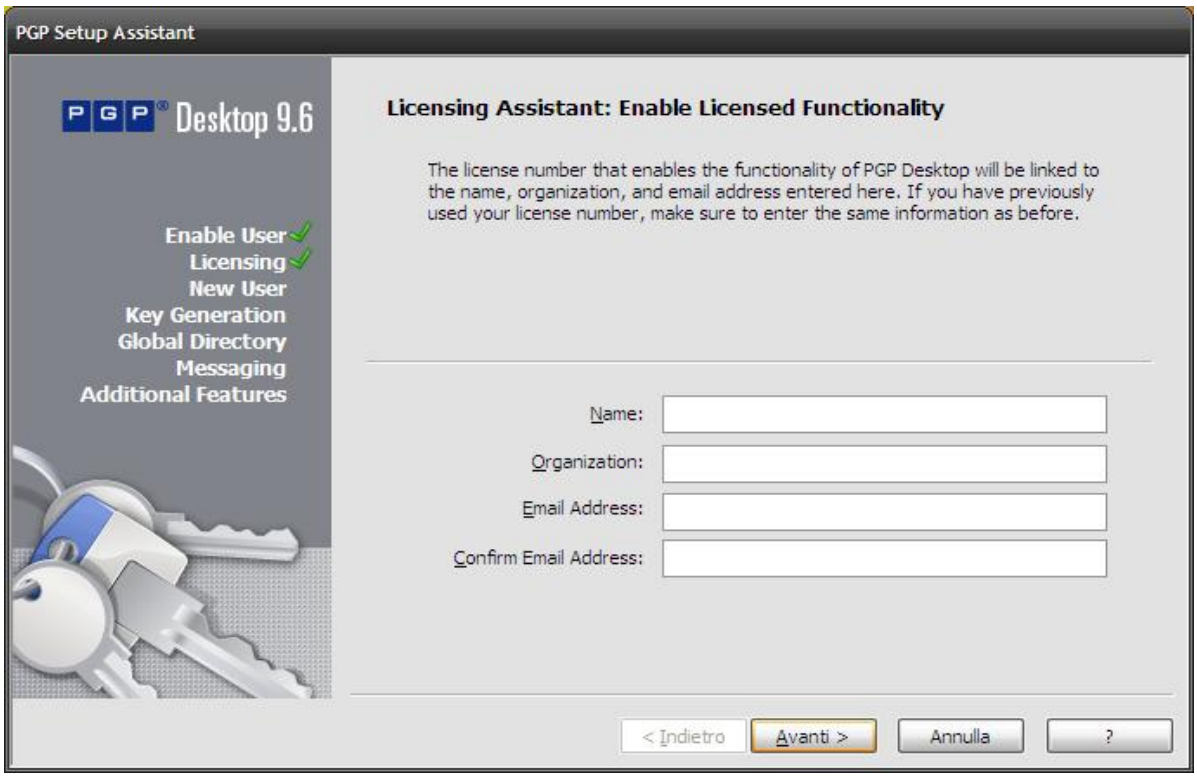
Il messaggio ottenuto al sesto passo e' quello finale, che puo' essere inviato per e-mail. Il destinatario esegue la sequenza inversa di operazioni.

Nel dettaglio, possiamo seguire i passaggi da effettuare grazie alle immagini riportate di seguito.

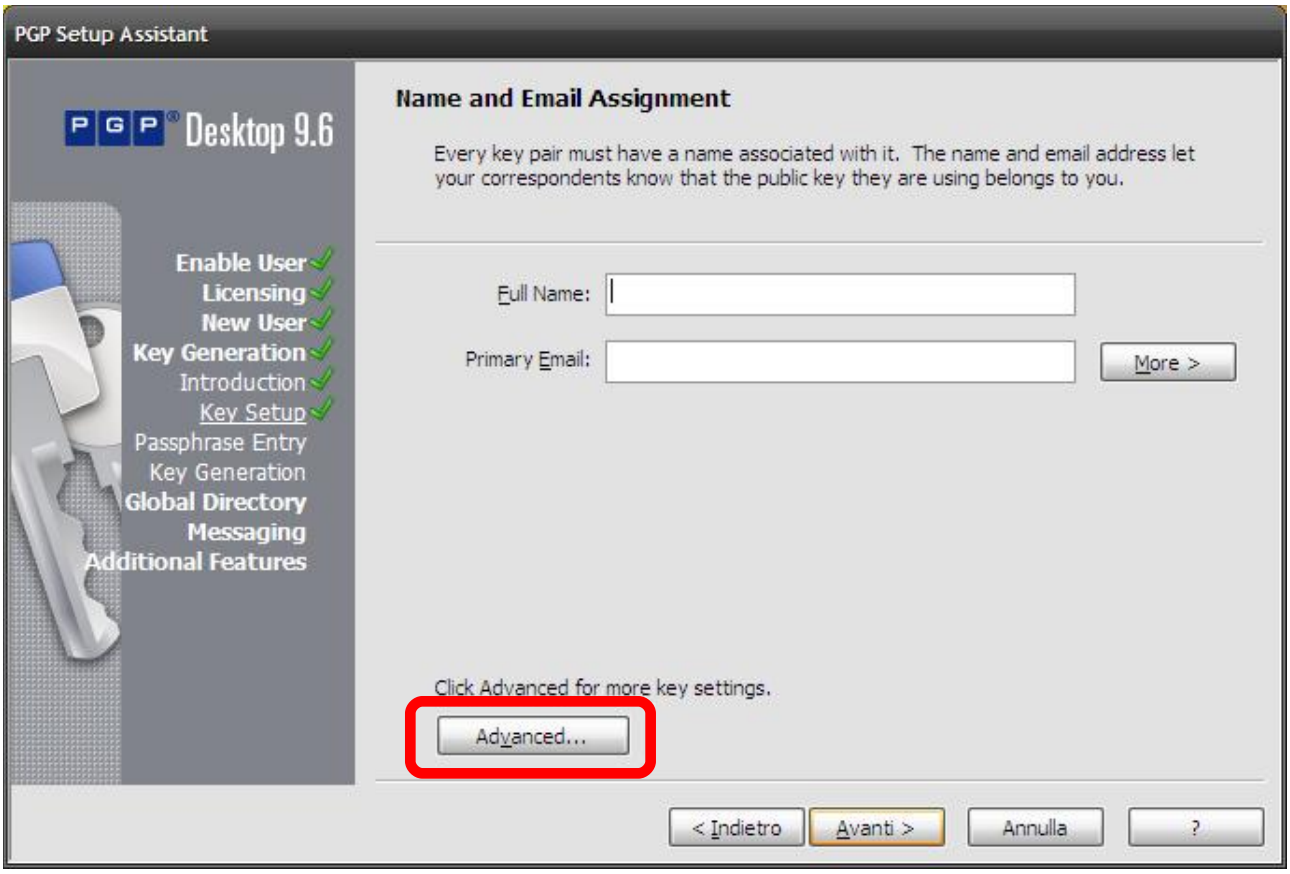
Il software utilizzato è PGP versione 9.6 per Windows e si tratta, come già accennato, di un programma freeware quindi non si riscontrano problemi né per il download né per la registrazione del prodotto che è possibile effettuare direttamente dal sito del produttore. In particolare, il software provato presenta varie operazioni possibili, eseguibili tramite i pacchetti inclusi quali:

- *Pgp Netshare che offre una gestione completa per il filesharing;*
- *Pgp Messaging che automaticamente cripta, decripta, emette firme digitali e verifica i messaggi in accordo con le impostazioni dell'utente;*
- *Pgp Zip che crea archivi sicuri criptati contenenti uno o più files, ma anche intere directory usando vari criteri di compressione;*
- *Pgp Virtual Disk che crea immagini criptate del disco e, quando non utilizzate, vengono protette da accessi non autorizzati;*
- *Pgp Whole Disk che offre le tecniche crittografiche per pc, portatile e dischi removibili, compresi file temporanei e file di scambio del sistema operativo.*

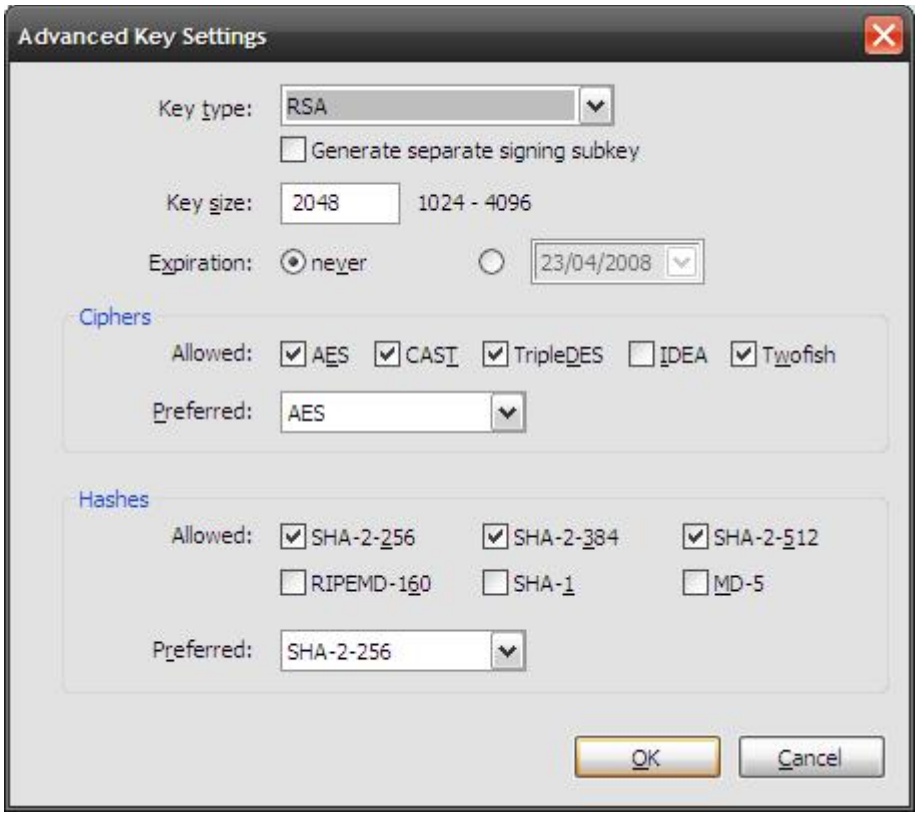
Primo passaggio: installazione

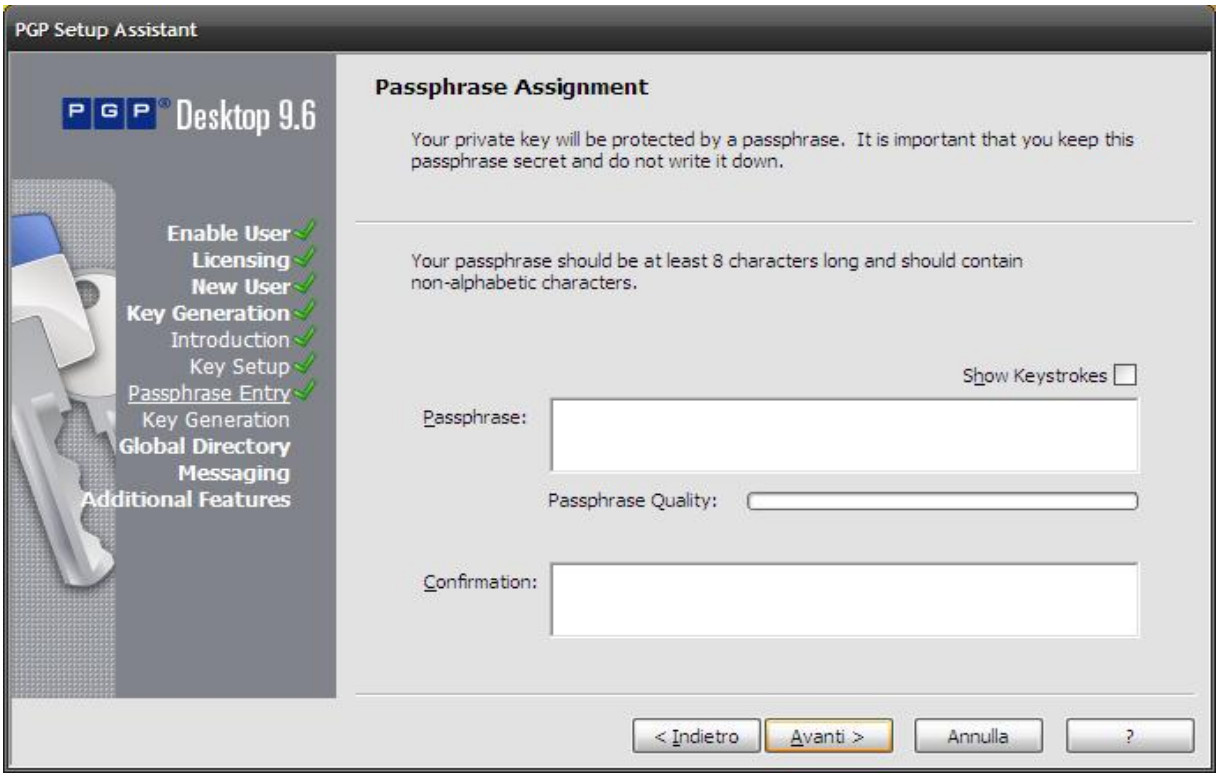


Secondo passaggio: acquisizione della licenza.
Il sito del produttore, assegnerà una licenza per il prodotto freeware
che sarà inviata direttamente al proprio account mail insieme ai dettagli per l'installazione corretta.

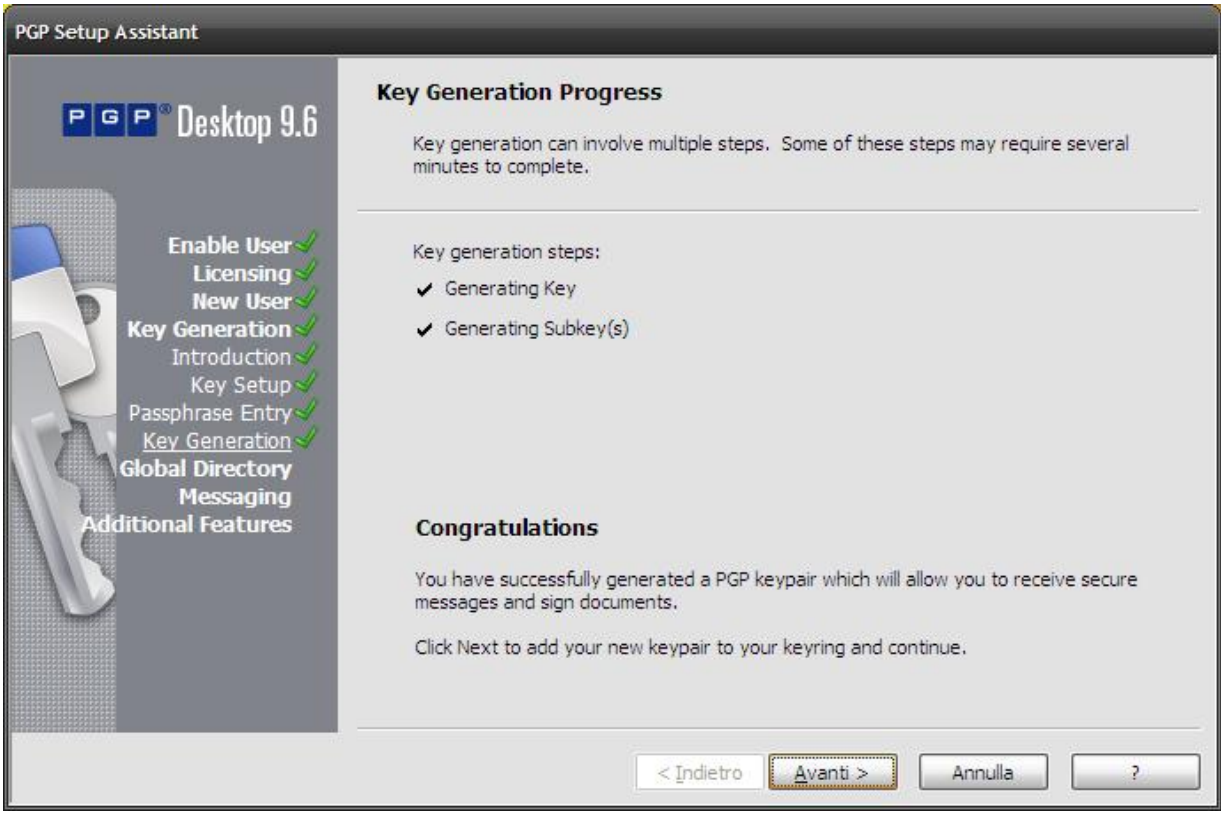


Terzo passaggio: acquisizione dei dettagli dell'utente per la successiva generazione delle chiavi personali. In particolare, cliccando su "Advanced…" potremo visualizzare quanto segue, ossia i dettagli delle impostazioni che il programma utilizzerà per la creazione delle chiavi.

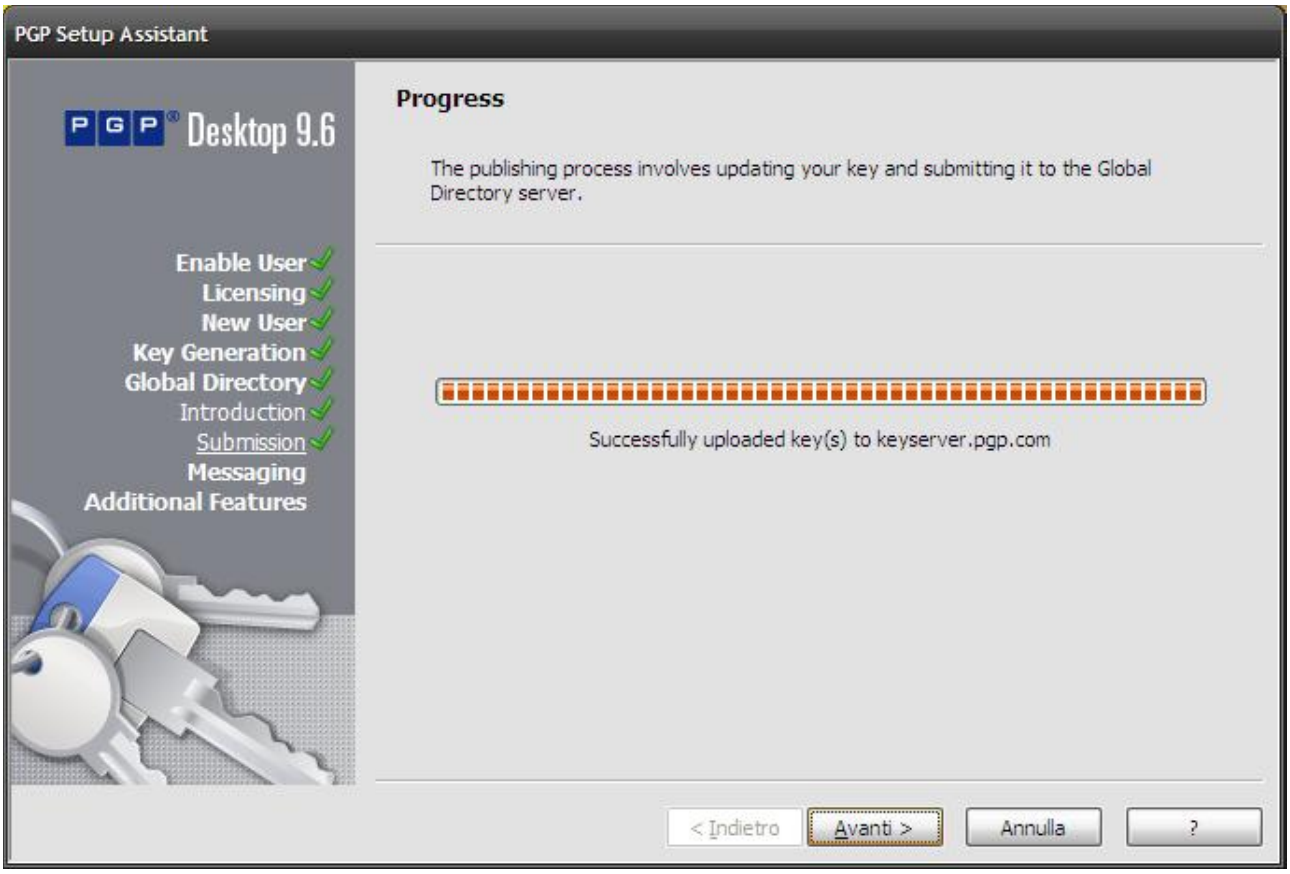




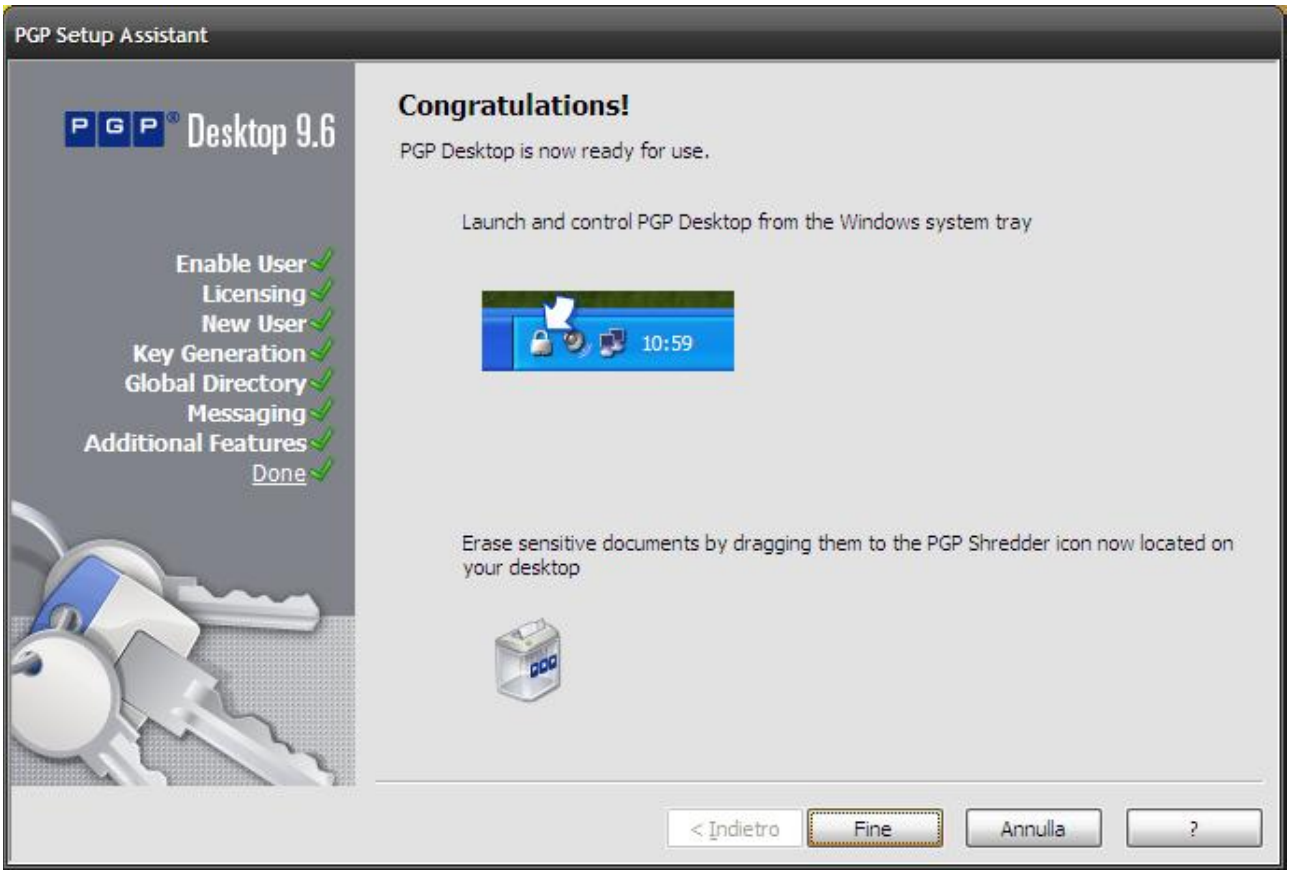
Quarto passaggio: assegnazione di una PassPhrase personale



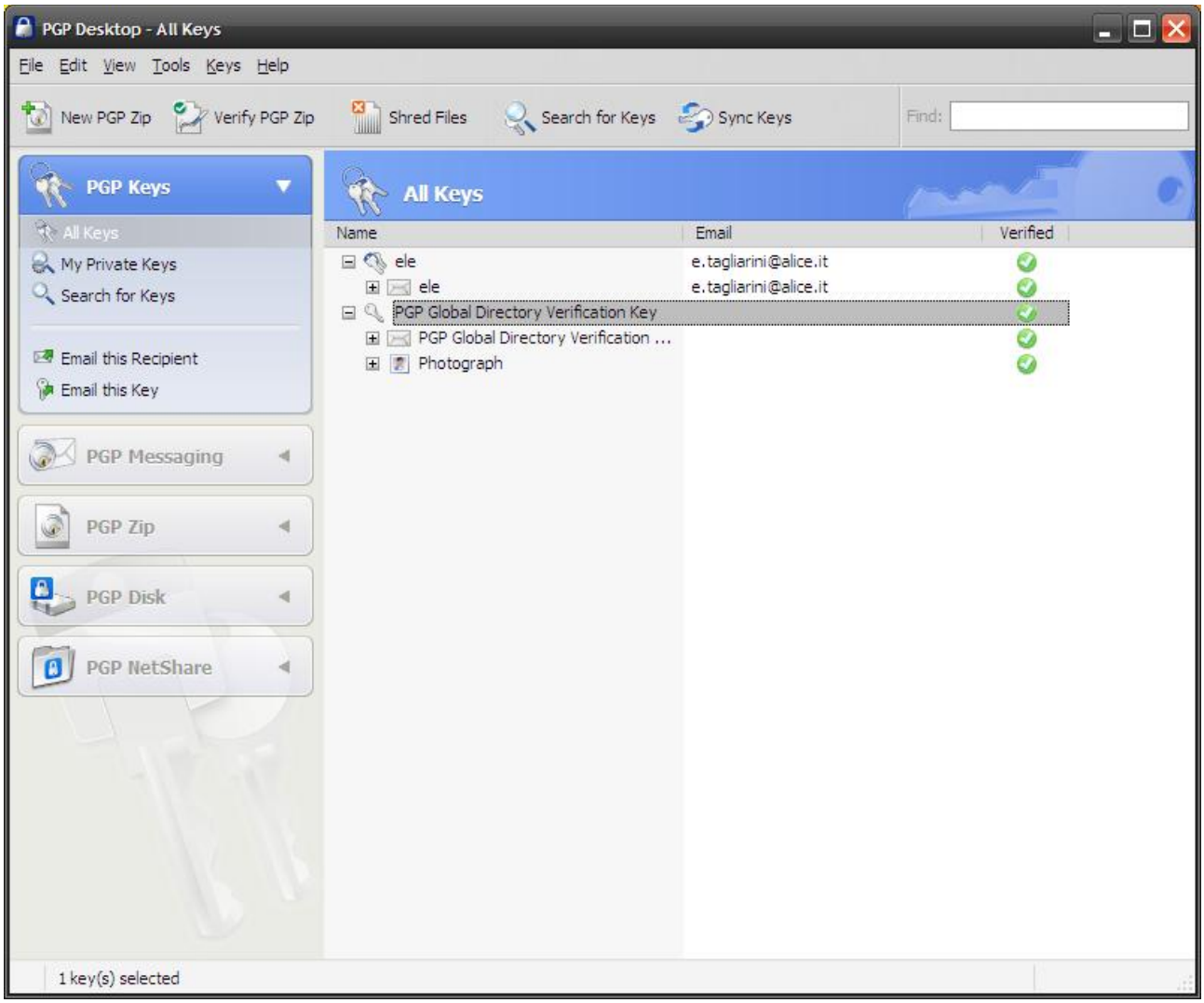
Esito della creazione delle chiavi



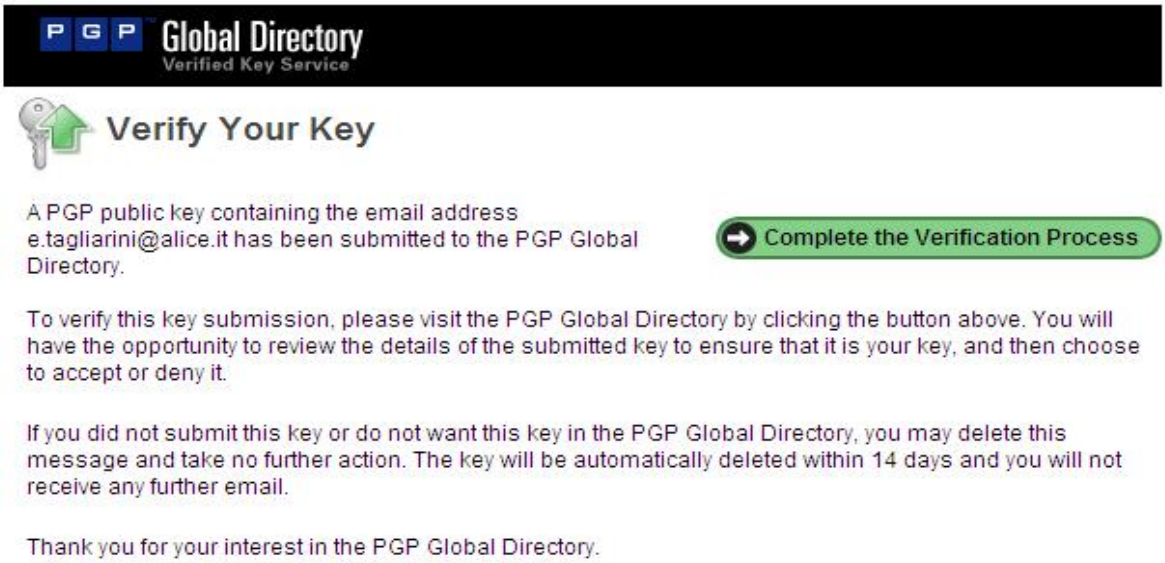
Quinto passaggio: aggiunta della chiave pubblica creata al Keyserver



Fine dell'installazione



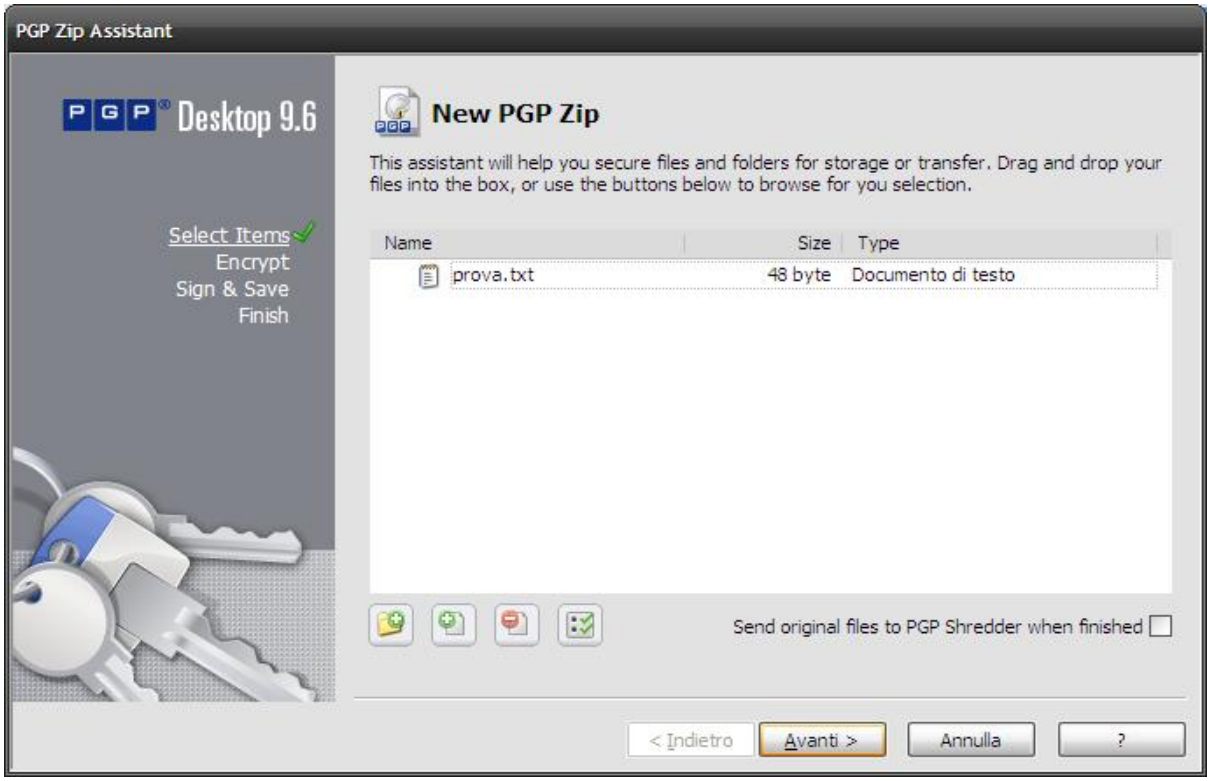
Programma pronto per l'uso. Dai pacchetti inclusi è possibile scegliere quale operazione svolgere.



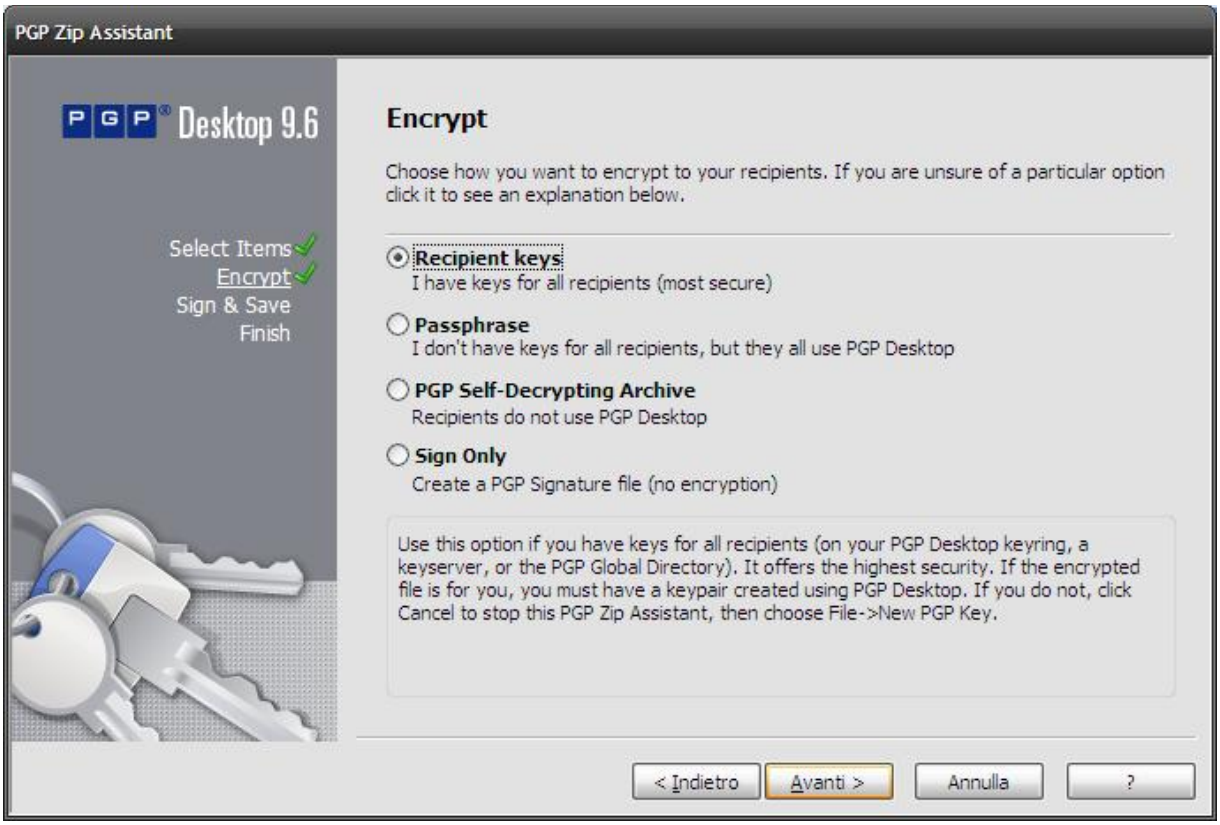
E-mail di verifica e conferma chiavi che perviene all'account immesso all'atto della registrazione; le informazioni verificate perverranno direttamente al Keyserver.

Le operazioni possibili col Keyserver saranno la ricerca di un utente, la modifica delle chiavi o la rimozione dal Keyserver della nostra chiave pubblica.

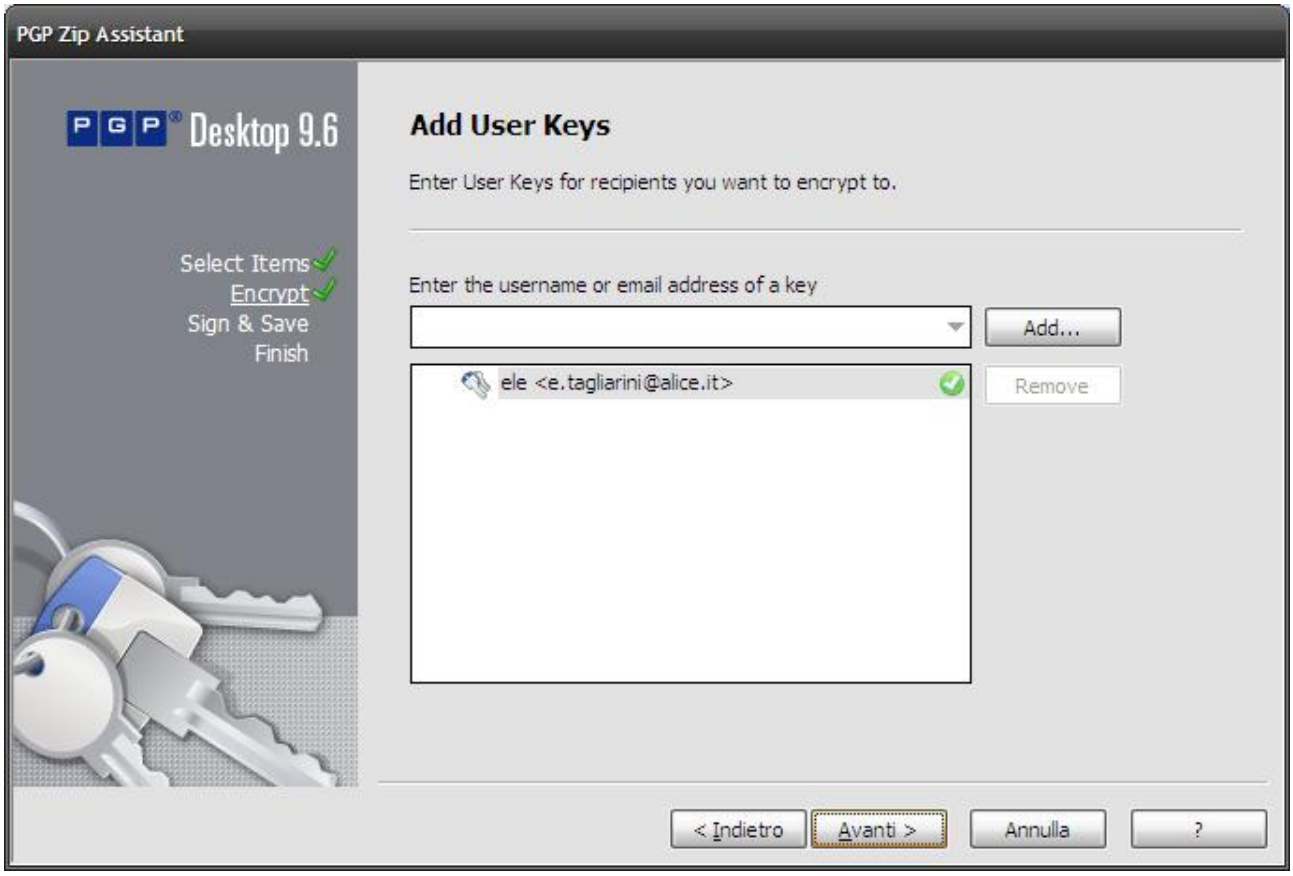
Si suppone ora, dopo aver installato e creato le chiavi correttamente, di effettuare un test al programma, sfruttando una delle funzioni permesse da PGP Zip, ossia, partendo un file di testo di prova, ottenere un perfetto archivio compresso e criptato. Seguono i passaggi.

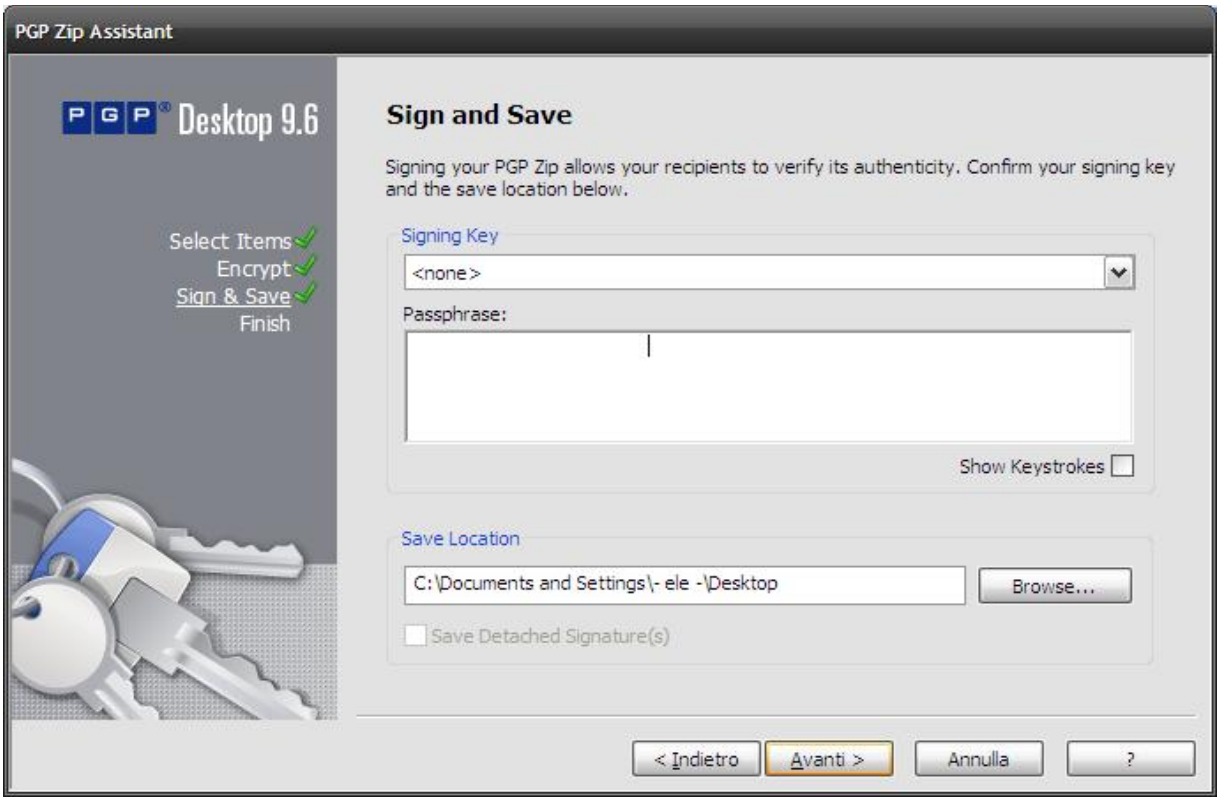


Selezione del file di partenza da cui si vuole ottenere l'archivio.

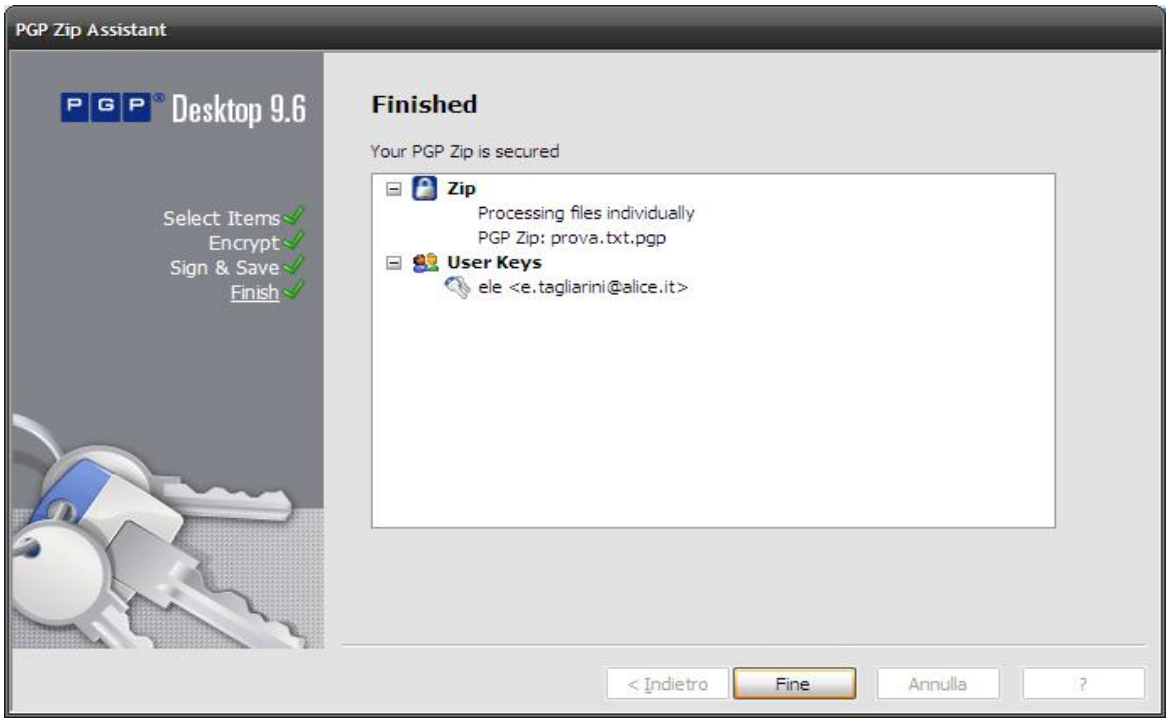


Selezione del modo per criptare il file e dell'account e-mail personale dal quale verrà inviato l'archivio





Aggiunta della firma digitale e inserimento della PassPhrase (viene richiesta per ogni operazione)



Passaggio finale: l'archivio è stato creato e presenta estensione .pgp

Keyservers

Si tratta di database automatici di chiavi pubbliche PGP, accessibili ed utilizzabili da tutti. Ogni Keyserver ha in pratica un enorme public ring, a cui tutti possono aggiungere la propria chiave pubblica e da cui e' possibile estrarre una chiave pubblica di cui si ha bisogno. Una sorta di elenco pubblico del telefono. Tutte le operazioni avvengono per e-mail in modo automatico. Di Keyservers ce ne sono diversi in tutto il mondo, e si aggiornano automaticamente tra di loro, quindi e' sufficiente utilizzarne uno qualunque.

Punto debole di PGP: la sicurezza delle chiavi pubbliche

La crittografia a chiave pubblica, avendo eliminato la necessità di trasmettere una chiave segreta, riduce praticamente il rischio che qualcuno si impadronisca della chiave segreta. Tuttavia, la gestione delle chiavi e' il punto debole anche di questo sistema di crittografia, perchè una chiave pubblica può non essere sicura.

Quando il destinatario riceve la chiave pubblica del mittente, non ha modo di essere sicuro che quella chiave:
- appartenga effettivamente al mittente conosciuto;
- non sia stata manipolata. E' possibile cioè ipotizzare che persone esterne attacchino questo tipo di sistema di crittografia sfruttando proprio la debolezza del sistema nel gestire le chiavi pubbliche al fine di introdursi nelle comunicazioni tra mittente e destinatario.

Tuttavia i problemi tra crittografia simmetrica e asimmetrica sono completamente diversi anche come ordine di grandezza:
- Il sistema convenzionale a chiave unica pone alla comunicazione per e-mail problemi di sicurezza tanto grossi da essere di fatto inutilizzabile. Non avrebbe infatti alcun senso pensare di inviare la chiave segreta sullo stesso canale non sicuro.
- Gli "attacchi", nel sistema a chiave pubblica sono azioni piuttosto complesse da effettuare, ed hanno quindi probabilità ridotte in circostanze normali. Inoltre essi sono, mediante una serie di norme di sicurezza, prevenibili.

Per potersi accertare dell'identità del mittente che scambia la chiave col destinatario, è raccomandabile uno scambio non attraverso e-mail o banche dati, ma possibilmente attraverso un incontro personale o tramite persone fidate o attraverso canali trasmissivi sicuri. Alternativa a ciò potrebbe essere l'invio della chiave "firmata" da un utente intermedio di cui il destinatario possiede una chiave sicura.

Conclusioni:

Il PGP, a seguito della prova di installazione, generazione delle chiavi e prova effettiva del programma, risulta essere molto semplice all'uso: presenta, come visualizzato, interfacce User-Friendly con le quali anche un utente poco esperto riesce velocemente ad orientarsi e capire i passaggi da effettuare per portare a termine una qualsiasi operazione. In questo modo, PGP risulta essere un software che unisce utilità, sicurezza dei propri messaggi/dati oltre che grande semplicità d'uso.