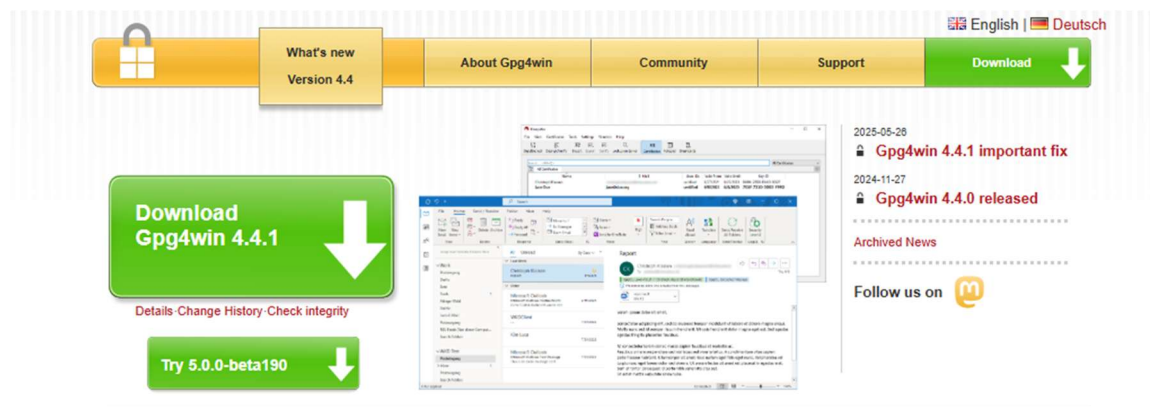


Manuale Operativo: Cifratura e Decifratura File con Gpg4win / Kleopatra (OpenPGP)

Installazione di Gpg4win

1. Scarica Gpg4win dal sito ufficiale: <https://www.gpg4win.org>



Gpg4win - a secure solution...

... for file and email encryption. Gpg4win (GNU Privacy Guard for Windows) is Free Software and can be installed with just a few mouse clicks.

Discover Gpg4win

Learn what Gpg4win is and read more about the features of our solution!

[About Gpg4win »](#)

Getting started

We help you to use Gpg4win. Learn the basics about Gpg4win and get in the world of cryptography. The best point to start is with the illustrative Gpg4win Compendium.

[Go to the Gpg4win Compendium »](#)

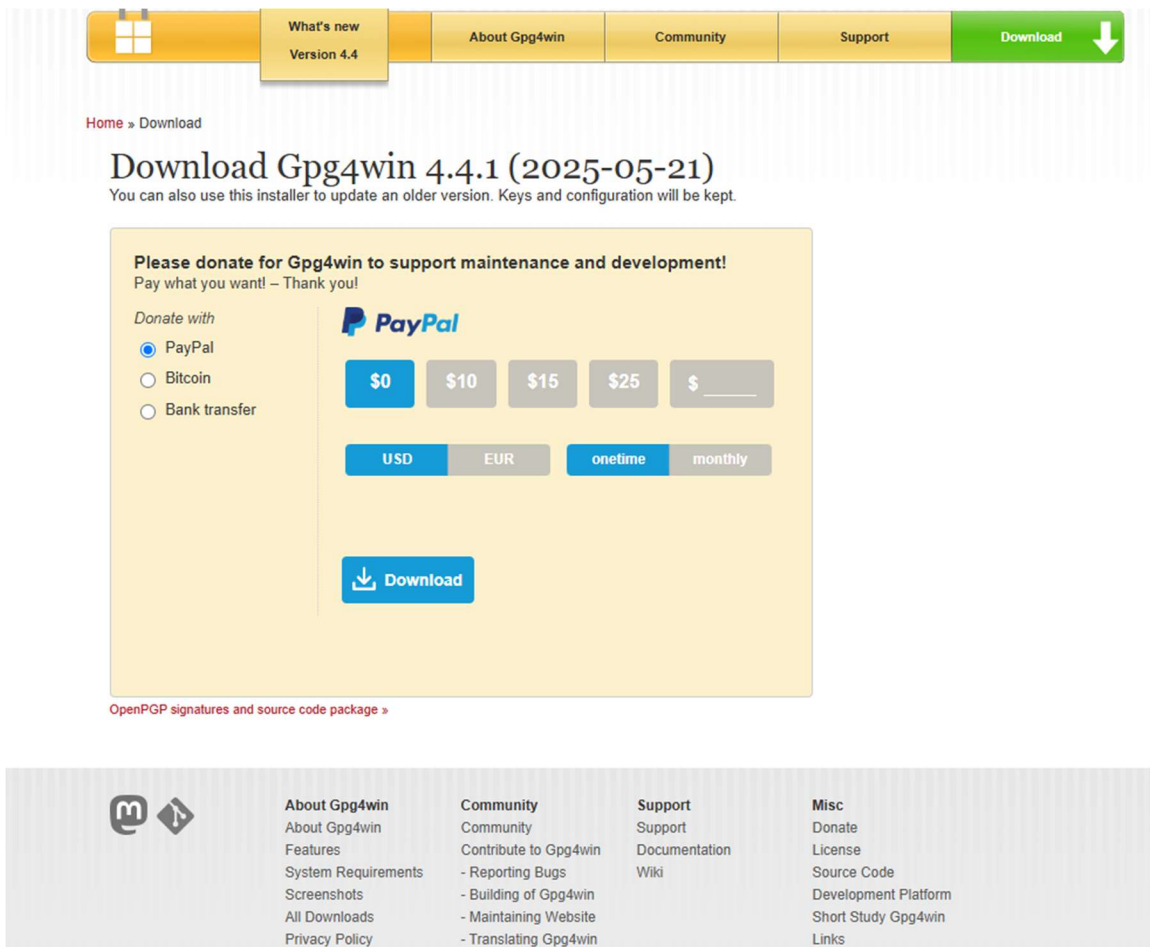
Join the community

Gpg4win is Free Software. Join the community! We recommend subscribing to the [Gpg4win announcement mailing list](#) to be automatically informed about new releases and other important Gpg4win news.

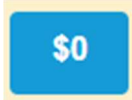
[Go to the community »](#)

	About Gpg4win About Gpg4win Features System Requirements Screenshots All Downloads Privacy Policy	Community Community Contribute to Gpg4win - Reporting Bugs - Building of Gpg4win - Maintaining Website - Translating Gpg4win	Support Support Documentation Wiki	Misc Donate License Source Code Development Platform Short Study Gpg4win Links Contributors
---	--	---	--	---

2. Clicca sul pulsante verde **Download**, si aprirà la seguente pagina web:

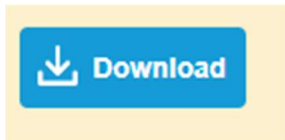


3. Per procedere senza effettuare una donazione, clicca sul link “\$0” (opzione per il download gratuito senza donazione).



4. A questo punto comparirà un pulsante blu con la scritta “Download”.

Cliccalo per avviare lo scaricamento del file di installazione (es. gpg4win-4.x.x.exe).



5. Una volta scaricato il file, esegilo per avviare l’installazione.

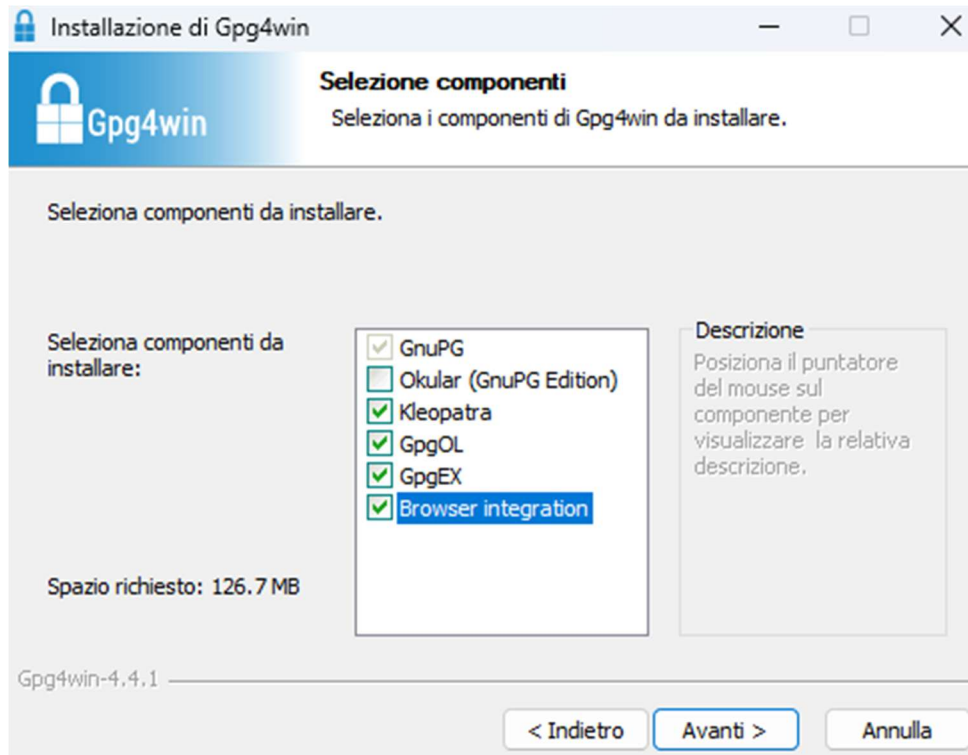
6. Si aprirà la seguente finestra, clicca su Avanti

7. Se viene richiesto “Installare senza diritti di amministratore?” clicca su Sì per procedere



8. Durante l'installazione, assicurati che siano selezionati:

- Kleopatra (programma che andrà a cifrare/decifrare file)
- GnuPG
- GpgEX
- **Browser integration**

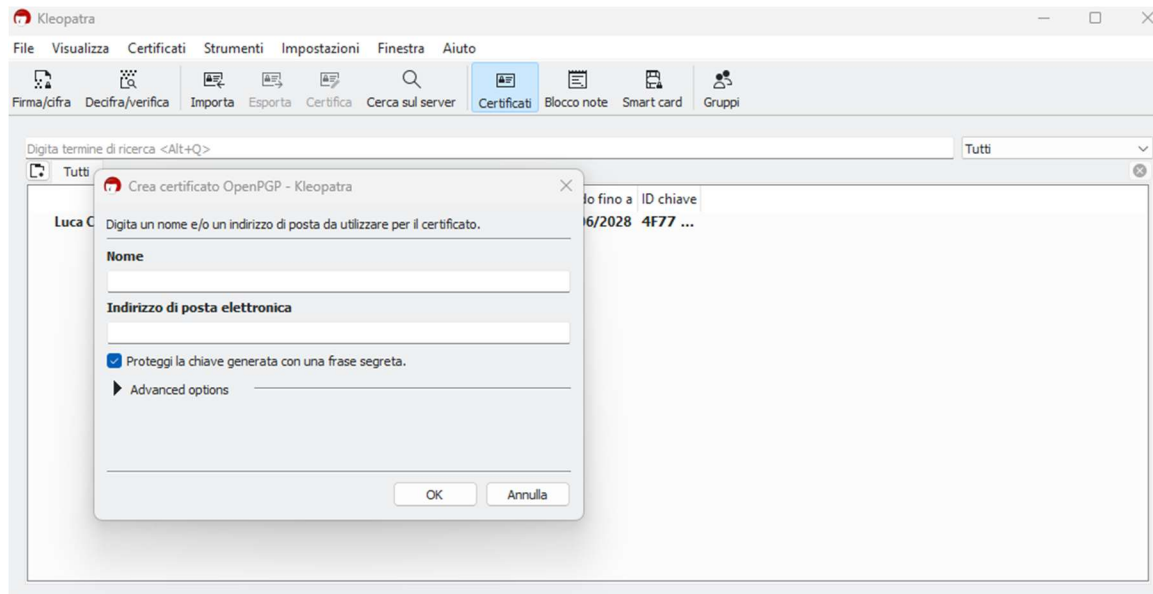


7. Clicca su “Avanti” poi su “Installa” per completare l'installazione.

8. Completata l'installazione, clicca su Avanti e poi su Chiudi.

Generazione di una coppia di chiavi OpenPGP

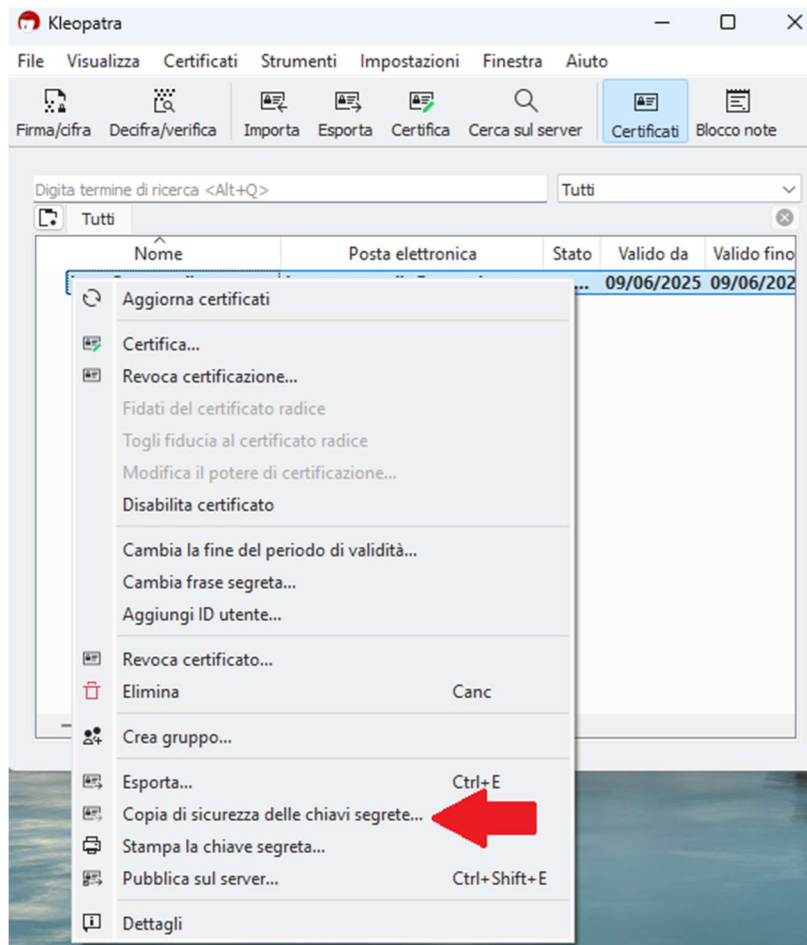
1. Avvia Kleopatra
2. Vai su "File" → "Nuova coppia di chiavi"
3. Si aprirà la seguente schermata. **Assicurati che sia selezionato “Proteggi la chiave generata con una frase segreta”**, inserisci nome ed e-mail e fai clic su OK



4. Clicca su ok, quindi si aprirà una schermata dove viene richiesto di impostare una passphrase. Imposta una passphrase robusta, **la stessa verrà richiesta successivamente per altre operazioni che vedremo in seguito.**

Copia di sicurezza chiave privata

1. Fai clic con il tasto destro sulla chiave appena generata nell'elenco di Kleopatra e seleziona l'opzione "copia di sicurezza delle chiavi segrete".

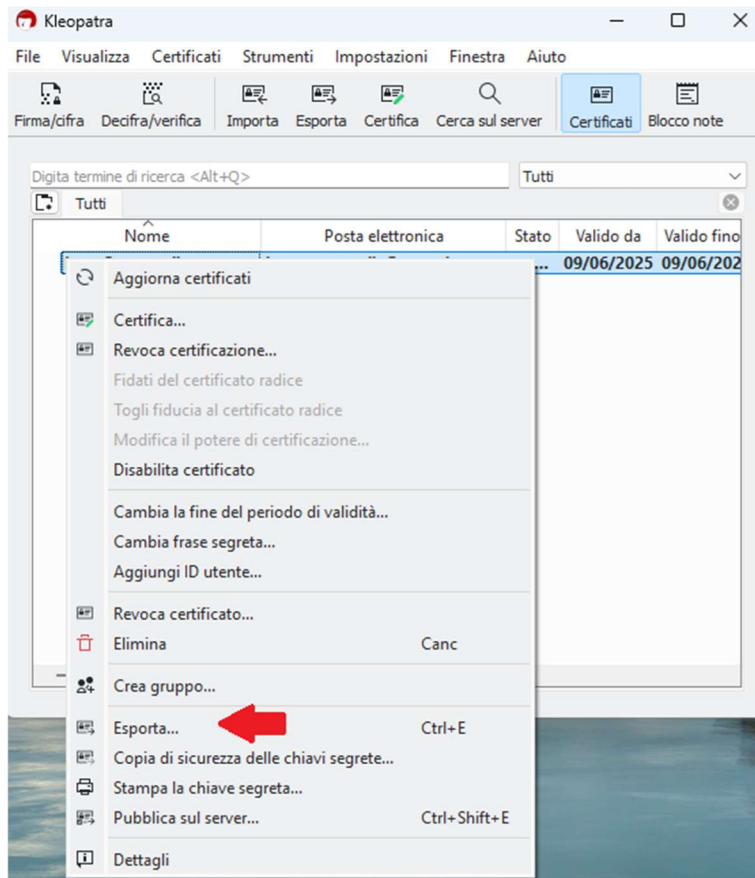


2. Apparirà una finestra dove sarà richiesto di scegliere il percorso di salvataggio. Il nome del file terminerà con "_SECRET".
3. Una volta scelto il percorso fai clic su Salva.
4. Se richiesto, inserisci la tua passphrase e clicca su OK

È fondamentale conservare ogni chiave privata generata in modo sicuro e strettamente confidenziale, proteggendola con una passphrase robusta e garantendone il backup sicuro. Le chiavi private non dovranno MAI essere condivise o trasmesse all'esterno di ciascuna Struttura o tra unità operative diverse, se non strettamente necessario e con adeguate misure di sicurezza.

Esportazione chiave pubblica

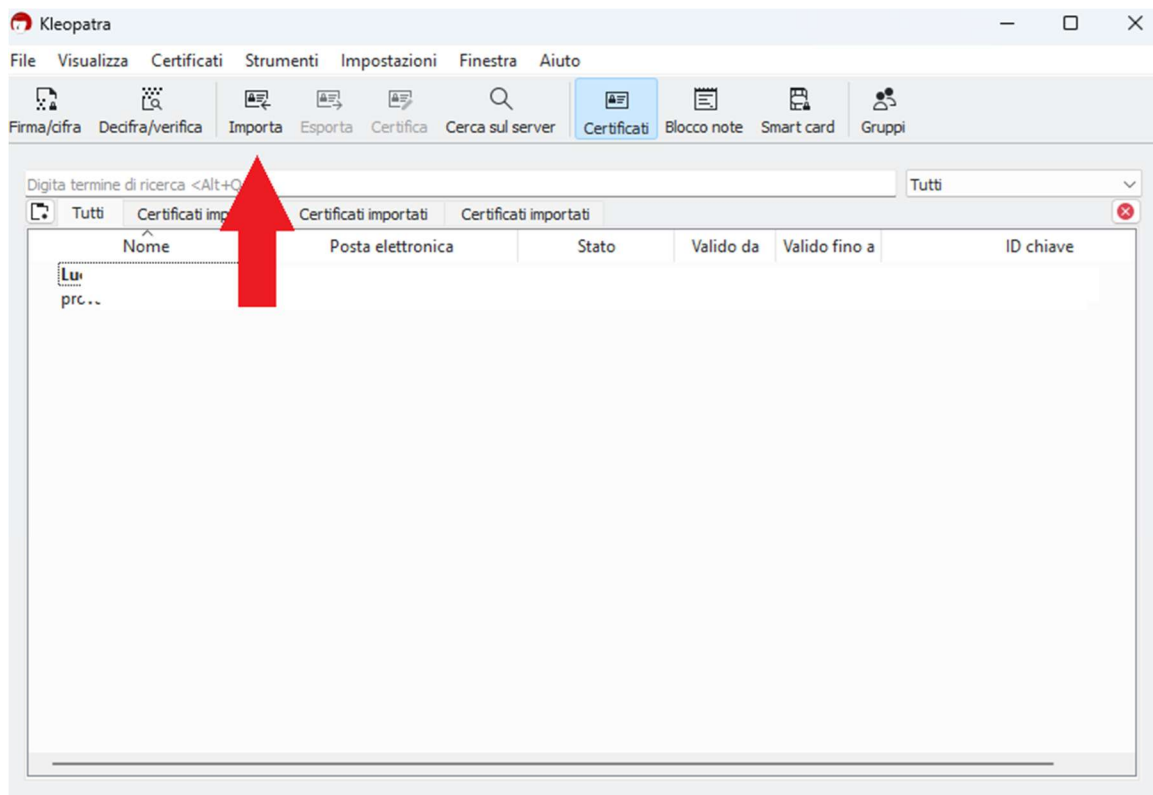
1. Fai clic con il tasto destro sulla chiave appena generata nell'elenco di Kleopatra e seleziona l'opzione "Esporta"



2. Seleziona il percorso e fai clic su Salva.
3. Una volta esportata la chiave pubblica in formato .asc, è fondamentale condividerla in modo sicuro con le controparti con cui si desidera stabilire una comunicazione cifrata. La chiave pubblica consente ai destinatari di cifrare i messaggi o i file destinati al proprietario della chiave privata corrispondente.
4. Ogni destinatario dovrà avere la chiave pubblica del mittente.

Importazione della chiave pubblica del destinatario

1. Ricevi la chiave pubblica dal destinatario (via mail, usb, ecc.) e salvala in una cartella apposita dove si andranno a inserire eventuali chiavi pubbliche ricevute da altri soggetti
2. In Kleopatra clic su Importa



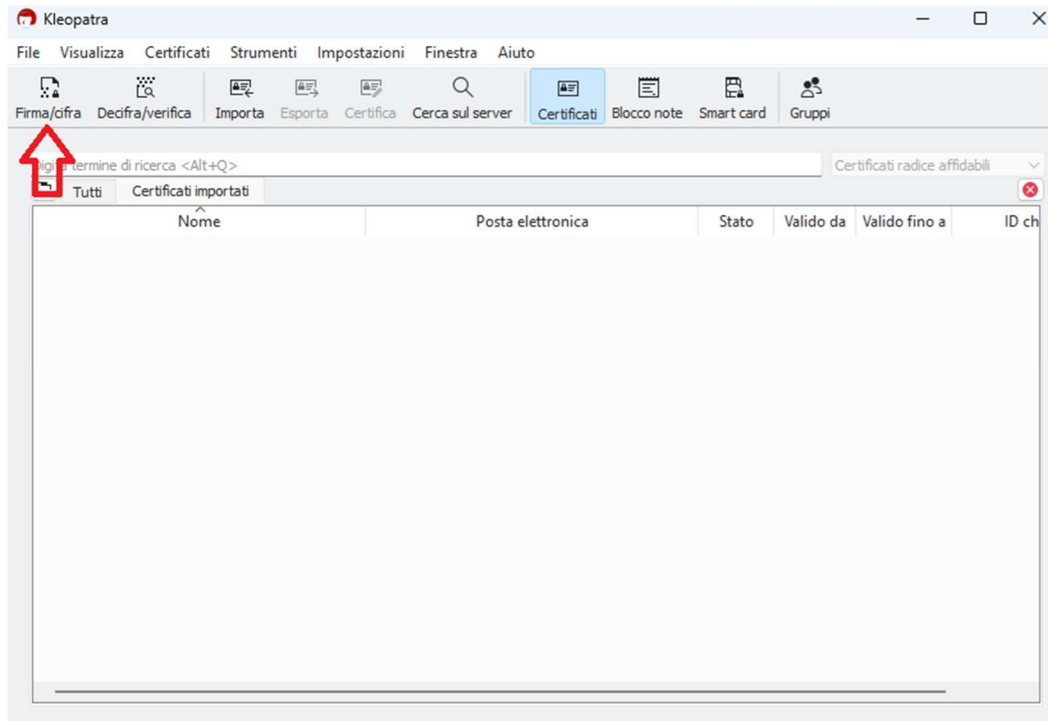
3. Seleziona il file della chiave pubblica del destinatario (file .asc da importare)
4. Clic su Apri, poi su Certifica.
5. Se richiesto, inserisci la tua passphrase.

Cifratura di un file

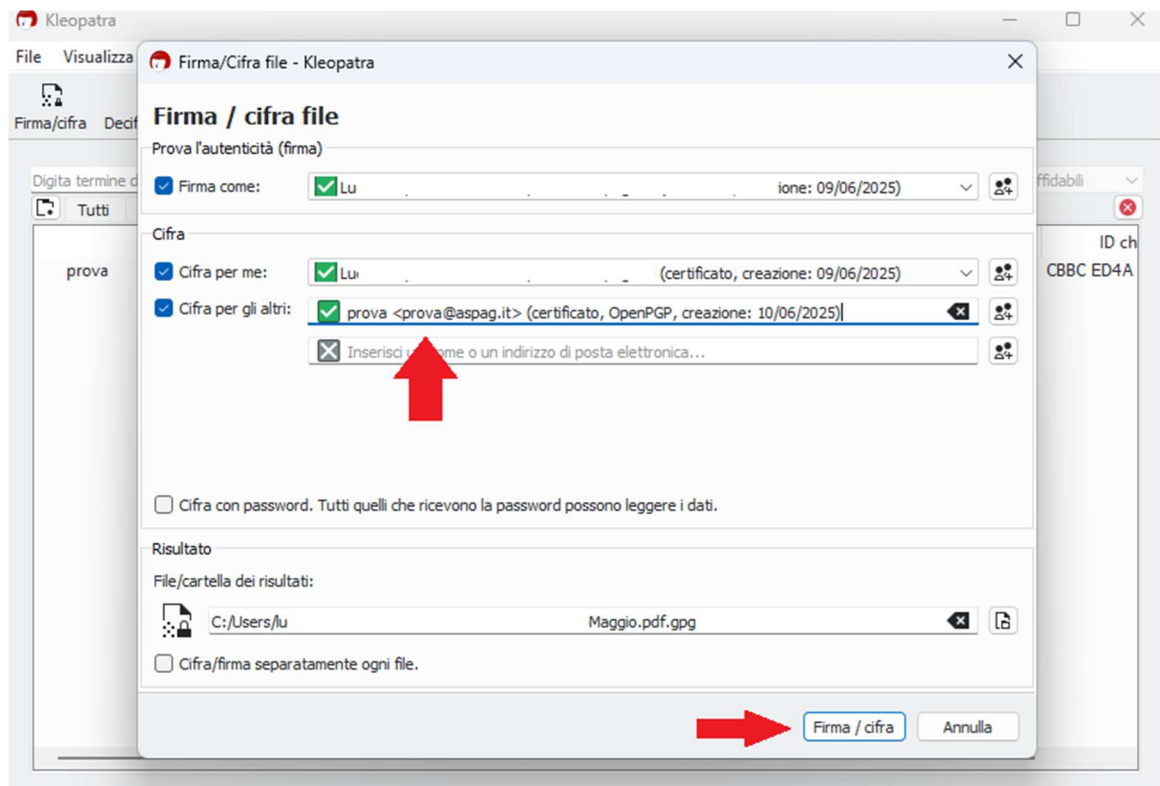
Una volta che entrambi i soggetti avranno le chiavi pubbliche, potranno scambiarsi file cifrati.

Da Kleopatra

1. File → "Firma/Cifra"



2. Seleziona il file da cifrare
3. Apparirà la seguente finestra:

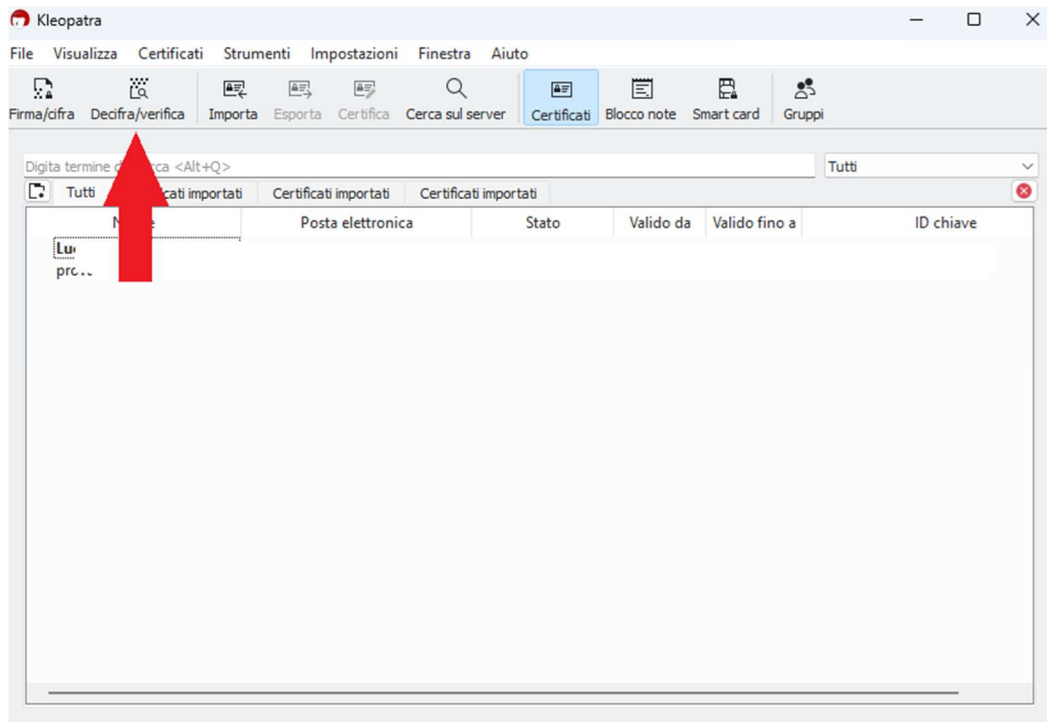


4. Nella casella “Cifra per gli altri” (4), scrivi l’indirizzo e-mail del destinatario. Seleziona il destinatario tra quelli suggeriti e conferma.
5. Una volta inserito il destinatario, fai clic su Firma/Cifra (5). Il file sarà salvato nella stessa posizione del file originale, con estensione .gpg
6. **Se richiesto, inserisci la tua passphrase e clicca su OK**

Decifratura di un file

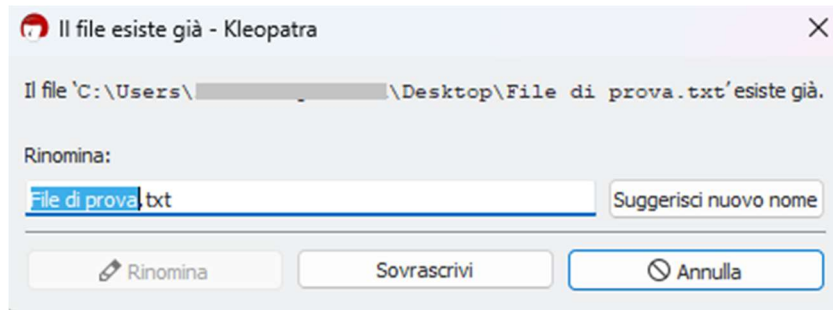
Da Kleopatra

1. File → "Decifra/Verifica file" → **seleziona file .pgp** da decifrare e fai clic su Apri



2. Se richiesto, inserisci la tua passphrase (che è la stessa password che viene usata per tutte le operazioni) e fai clic su OK.

3. Fai clic su **“Salva Tutti”** per salvare il file decifrato.
4. Se compare la seguente finestra, rinomina il file e fai clic su **“Rinomina”**. Il file decifrato sarà salvato nello stesso percorso.



IN SINTESI:

1. Scarica e installa Kleopatra (Gpg4win)

2. Crea la tua coppia di chiavi (pubblica e privata)

All'avvio di Kleopatra, crea una nuova coppia di chiavi. Inserisci nome, e-mail e **scegli una passphrase sicura**, ovvero una password robusta che servirà a proteggere la tua chiave privata.

Questa passphrase ti verrà chiesta ogni volta che userai la chiave.

3. Genera una copia di sicurezza della chiave privata e non condividerla con nessuno.

4. Condividi solo la tua chiave pubblica

Le chiavi pubbliche al contrario verranno **scambiate** tra mittente e destinatario **una volta sola** ed usate all'occorrenza per criptare i file da inviare. **Esporta la tua chiave pubblica** (non la privata!) da Kleopatra e inviala al destinatario (via e-mail, USB, ecc.).

Allo stesso modo, ricevi la chiave pubblica dell'altra persona e **importala** in Kleopatra.

5. Scambia file cifrati

Una volta che entrambi i soggetti avranno le chiavi pubbliche, potranno scambiarsi file cifrati. **Quando vuoi inviare un file protetto, lo cifri usando la chiave pubblica del destinatario (così solo lui potrà leggerlo).**