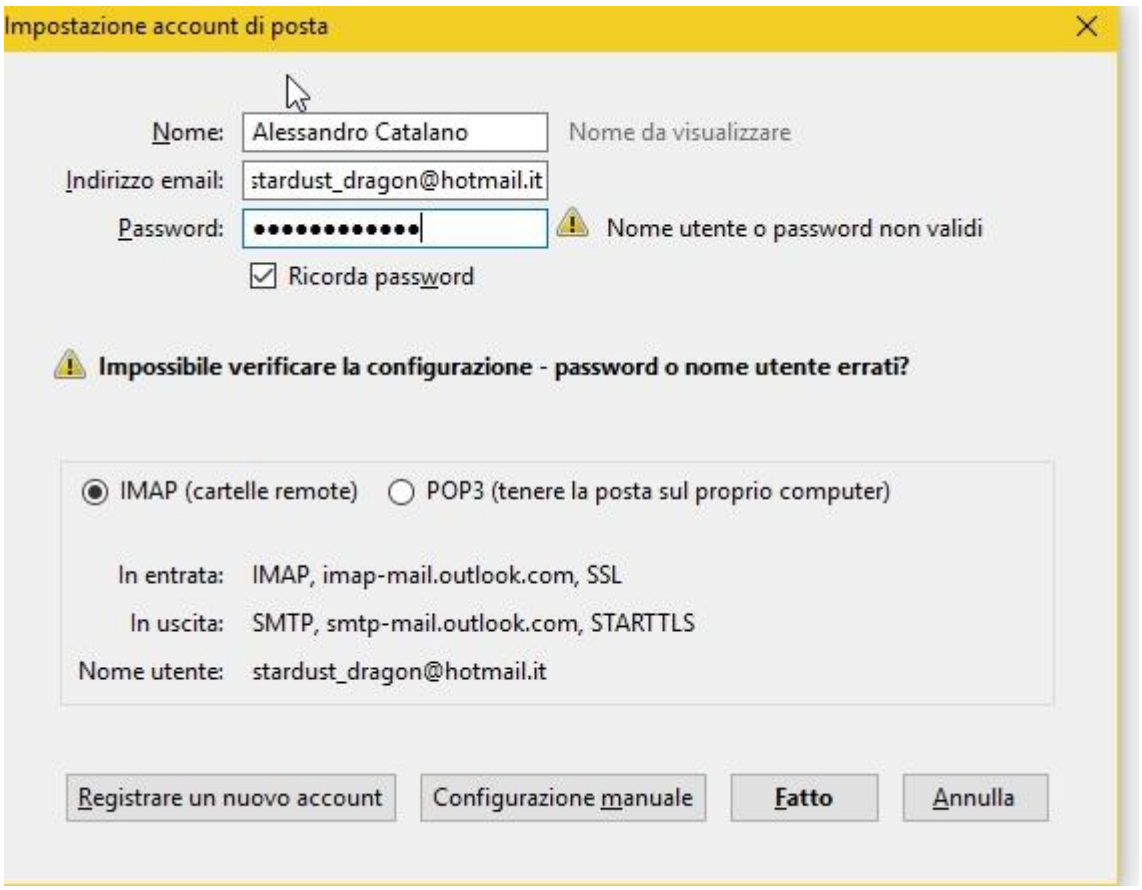
GP4WINDOWS

Cosa ho usato:

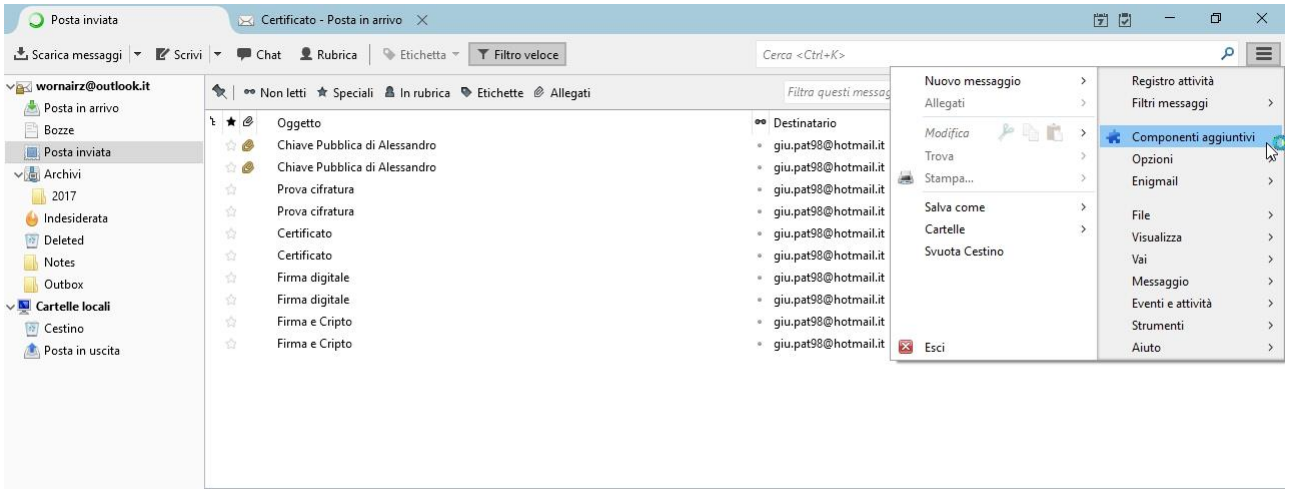
- L'ultima versione di **Gpg4win**
- **Mozilla Thunderbird** come client di posta
- **Enigmail**, una estensione di Thunderbird che permette di gestire i certificati (sostituisce Kleopatra e GpgOL)

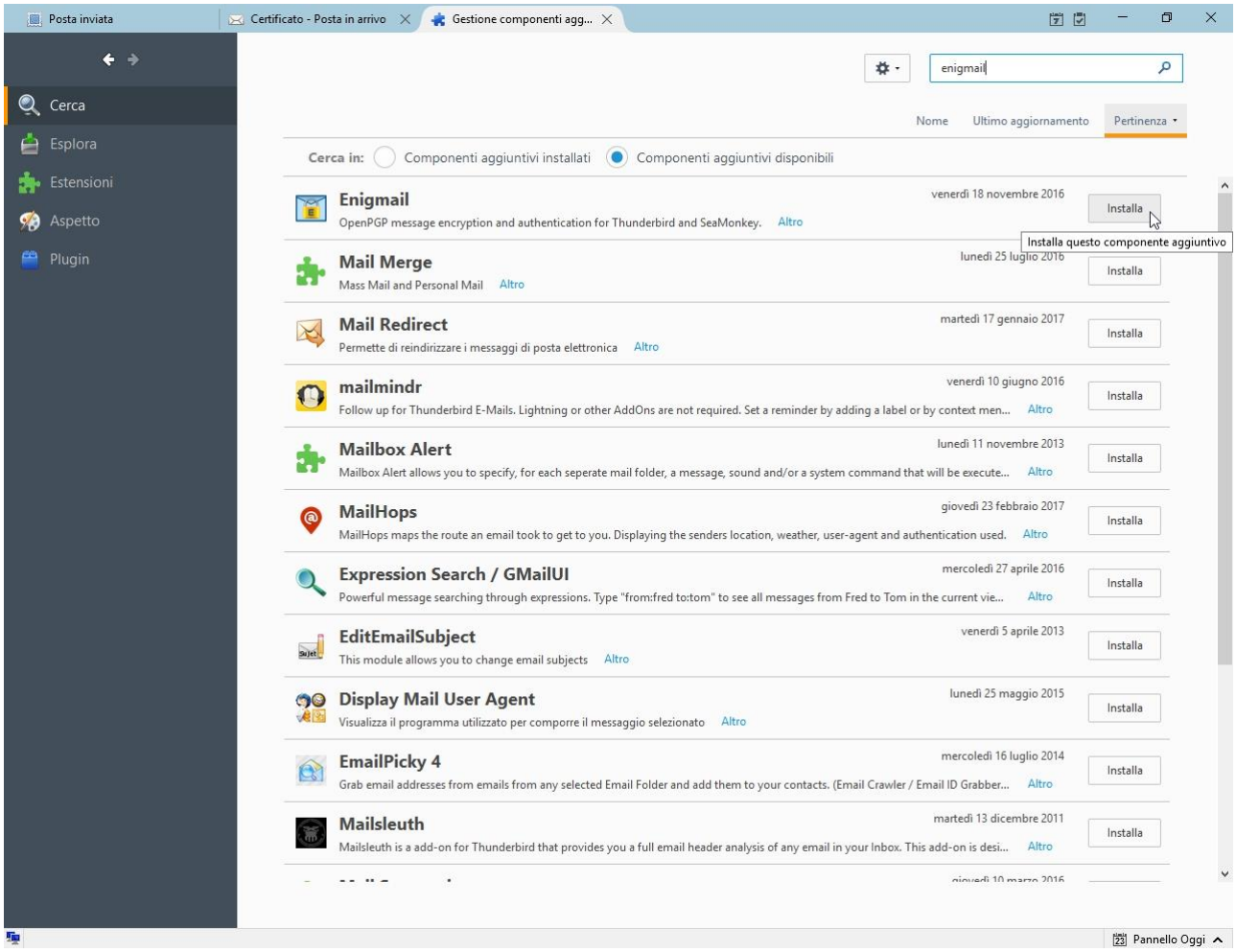
Primi passi: set-up di Thunderbird e generazione di chiavi e certificato con Enigmail

1) Aprire Thunderbird e configurare l'account di posta su cui ricevere le email

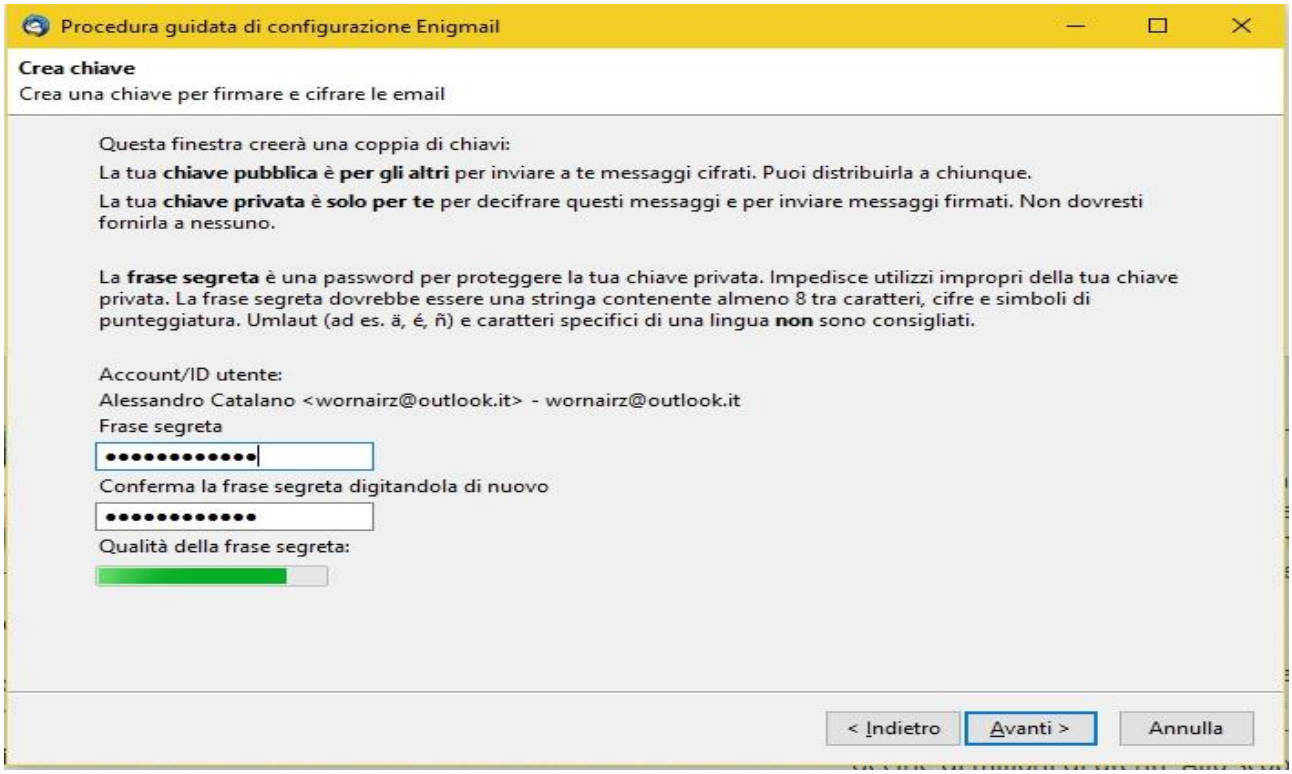


2) Installare l’estensione Enigmail

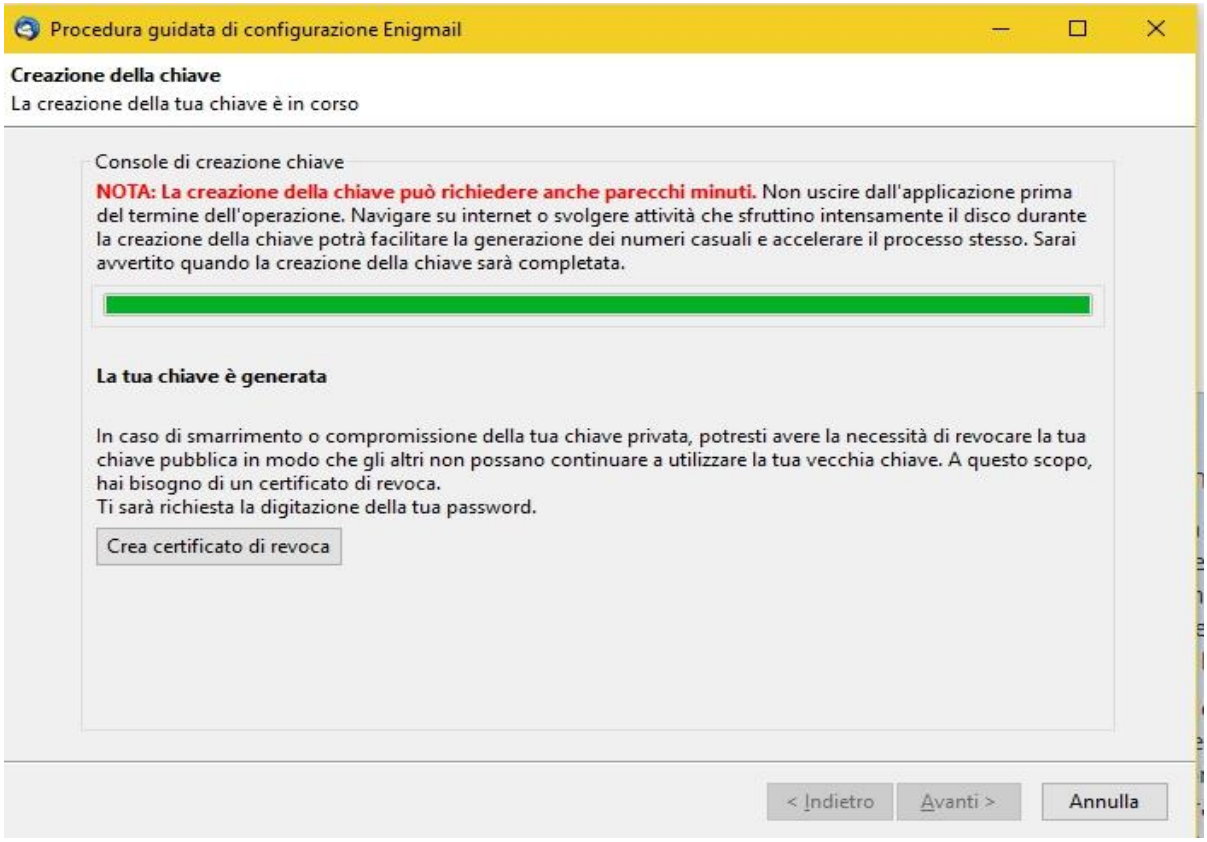




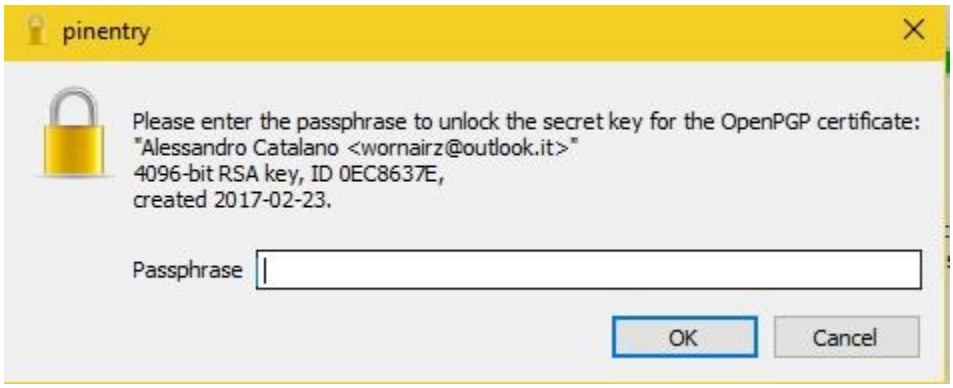
3) Seguire la configurazione guidata di Enigmail per la creazione di un certificato e della coppia di chiavi



Scegliere una passphrase a protezione della chiave privata, quindi sceglierne una difficile da ricordare per gli altri ma facile per noi



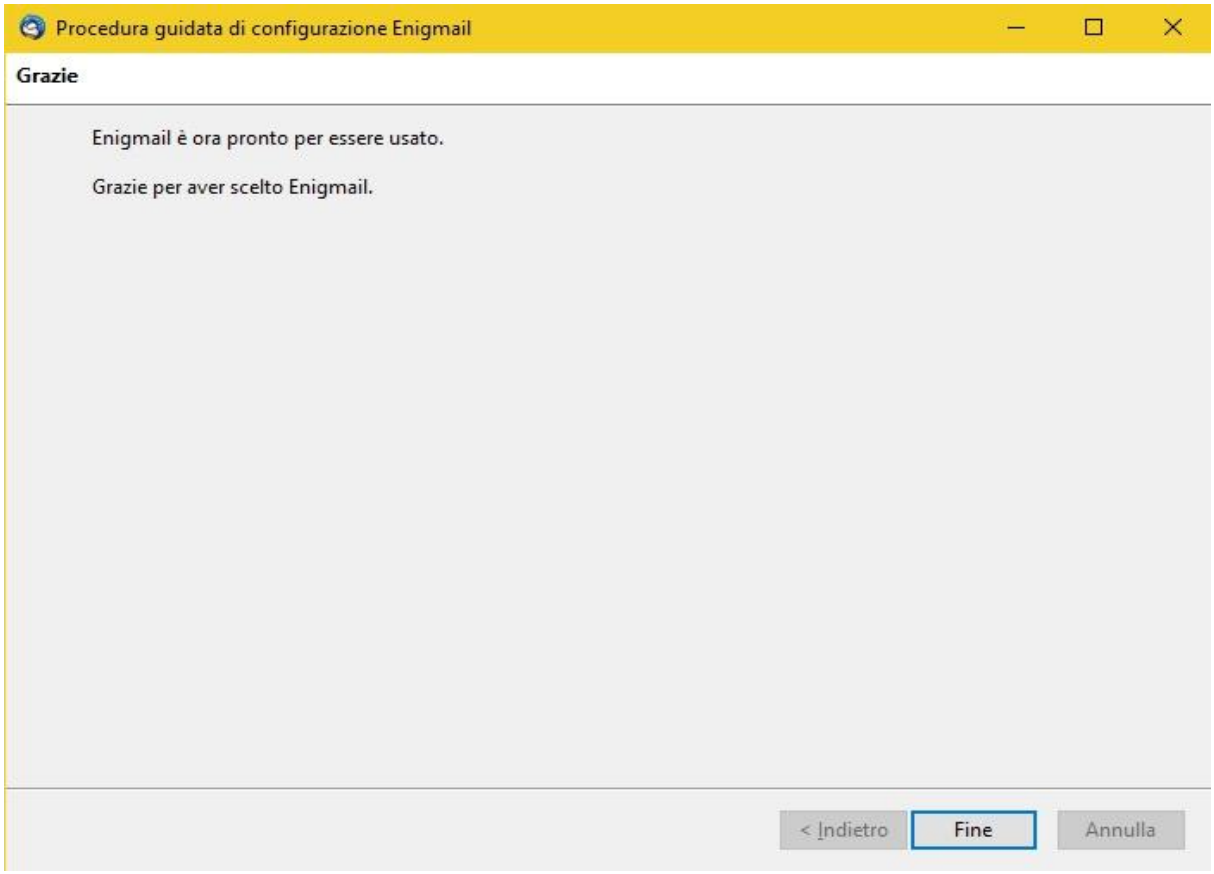
4) Dopo che la coppia di chiavi è stata generata, Enigmail ci chiede di creare un certificato di revoca in caso smarrissimo la nostra chiave privata.



Il certificato di revoca è firmato con la nostra chiave privata quindi necessita della nostra passphrase.

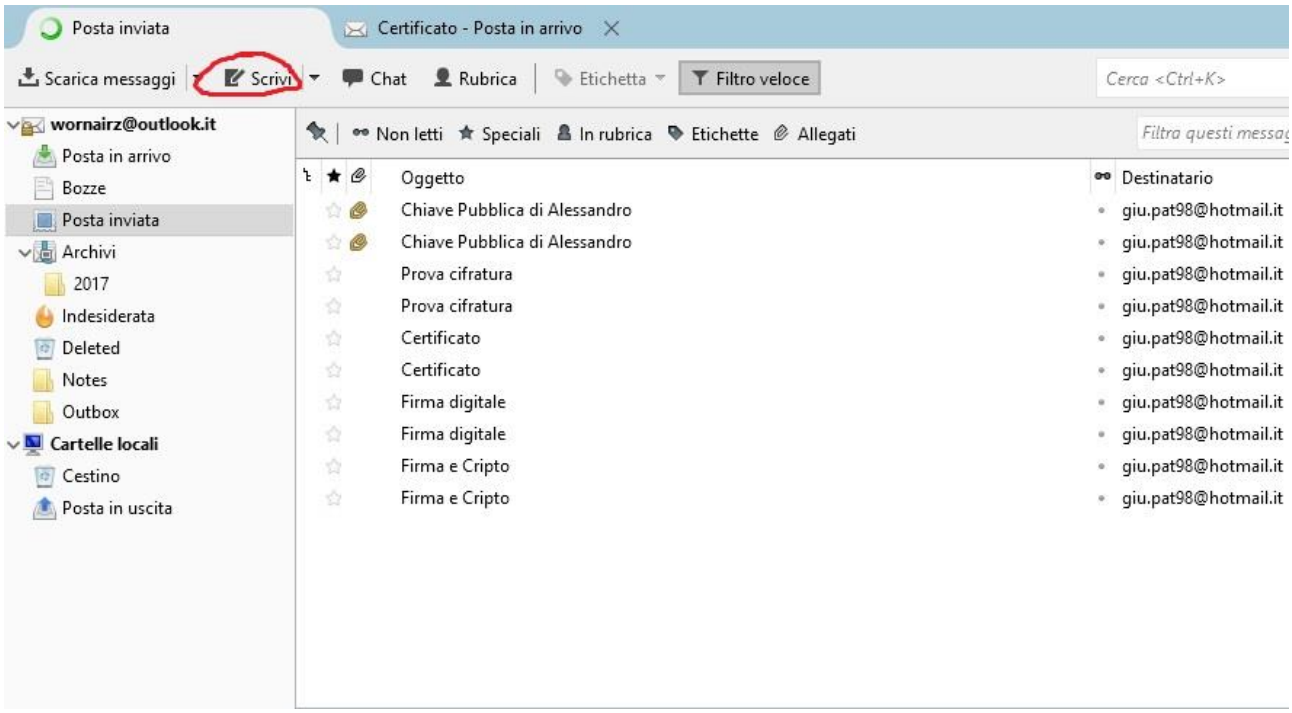
Salviamolo in un posto sicuro

Se tutto è andato a buon fine ci apparirà questa schermata



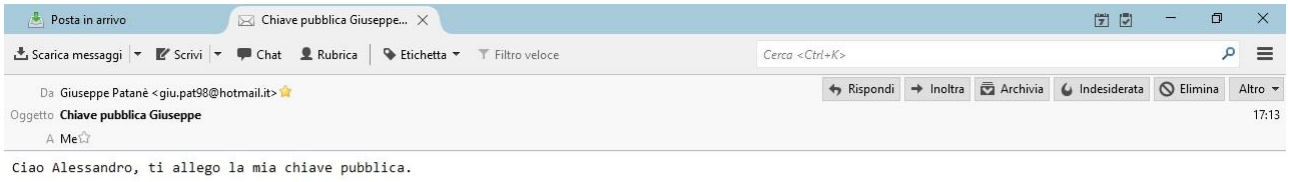
Adesso possiamo cominciare a crittografare le e-mail.

1) Scriviamo quindi un nuovo messaggio

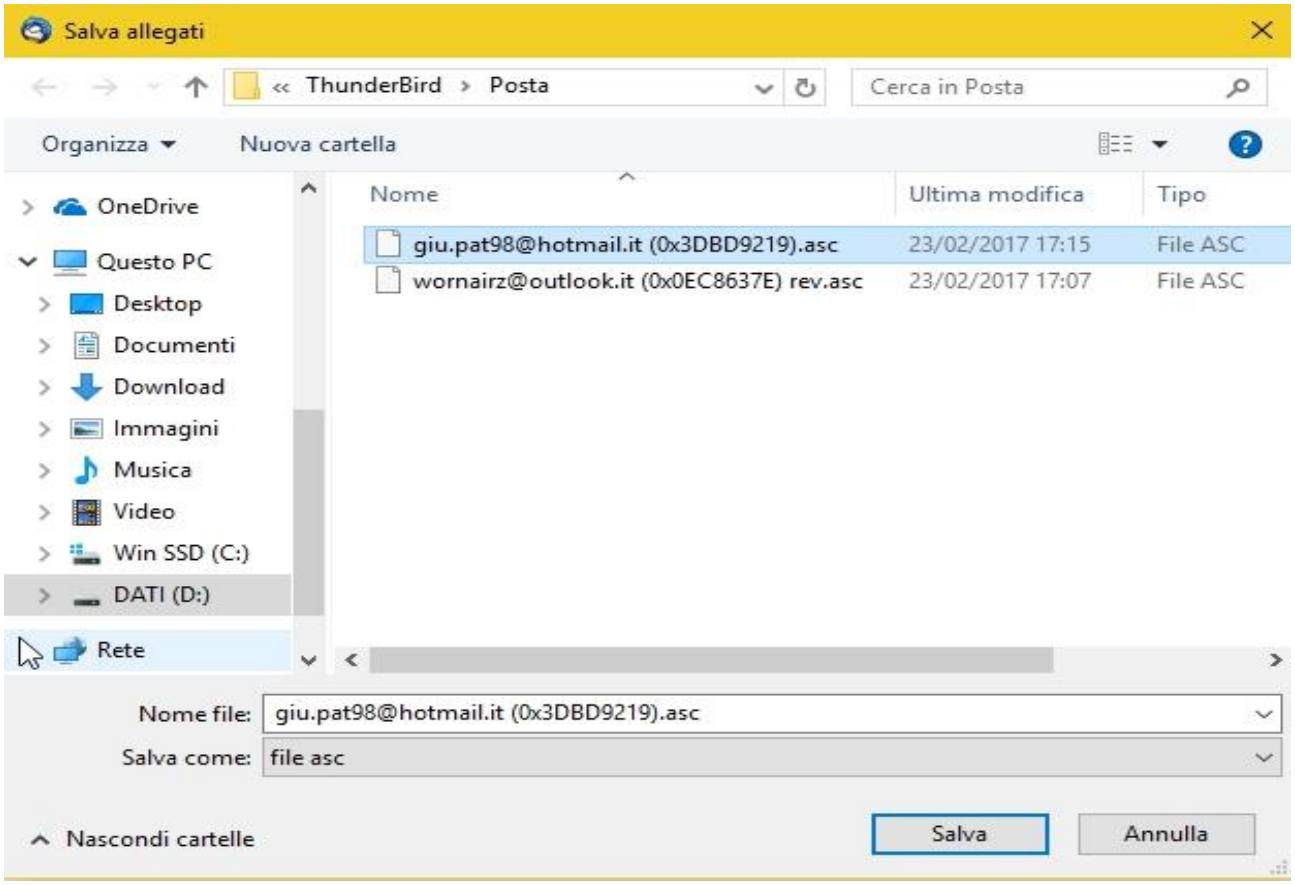


Adesso nel nuovo messaggio clicchiamo il bottone cerchiato in rosso per mandare la nostra chiave pubblica al destinatario come allegato, e clicchiamo invia per mandare la mail.

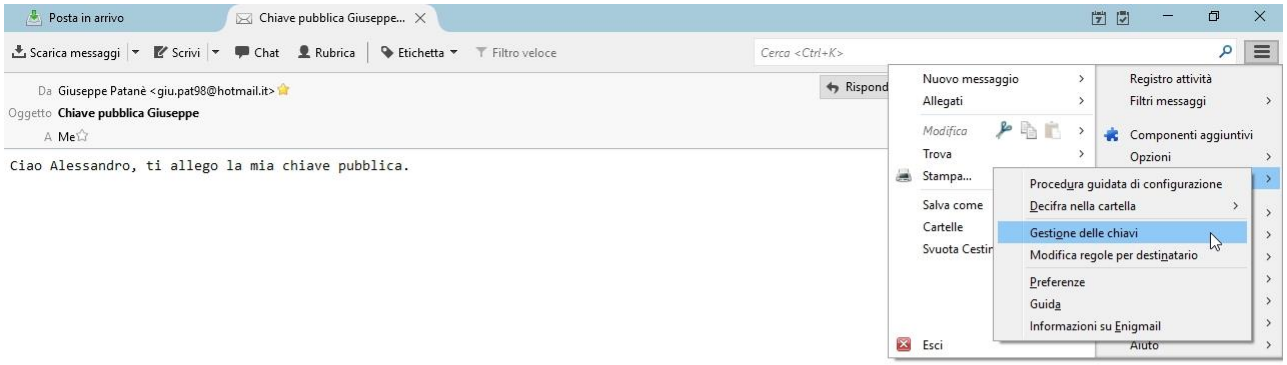
3) Il mio amico ha intanto mandato a me una mail contenente la sua chiave pubblica.



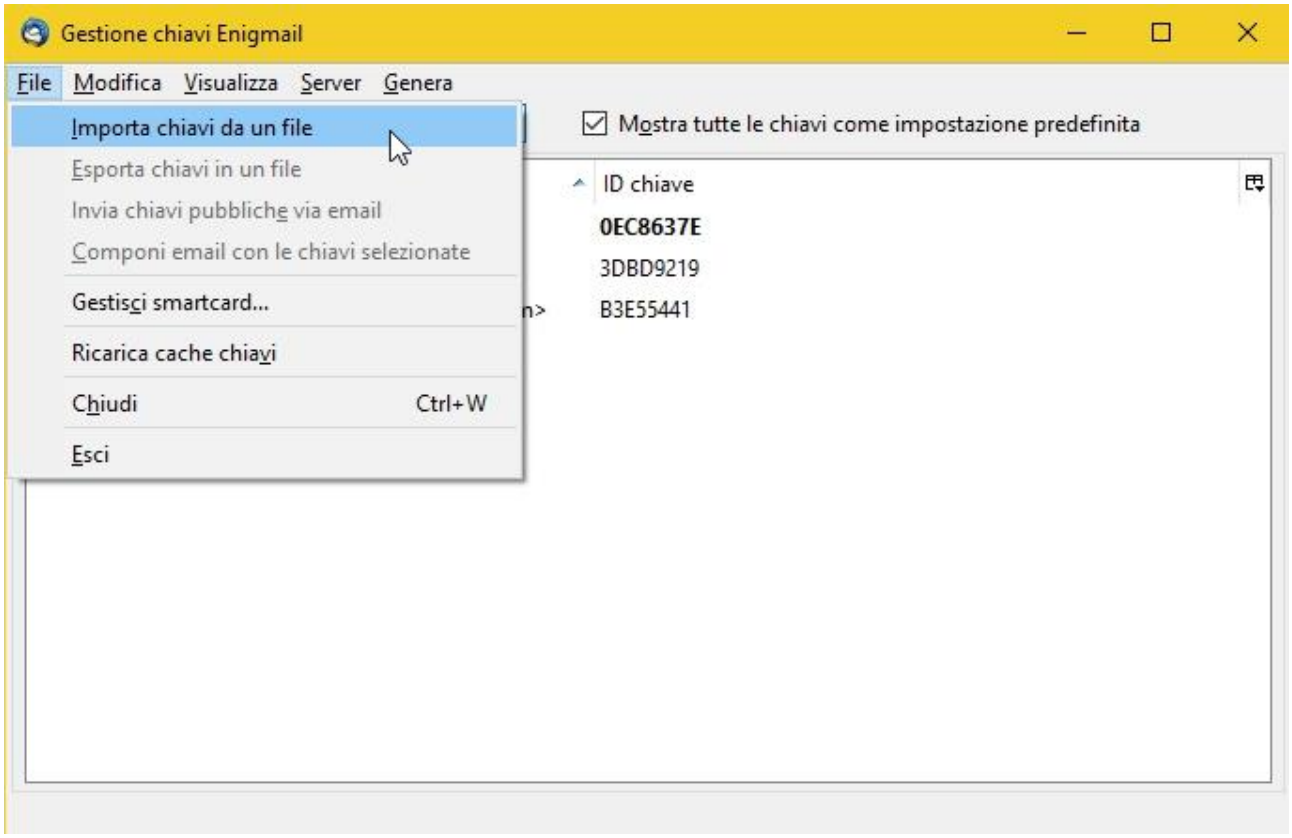
Clicchiamo sul pulsante Salva per salvarlo in locale.



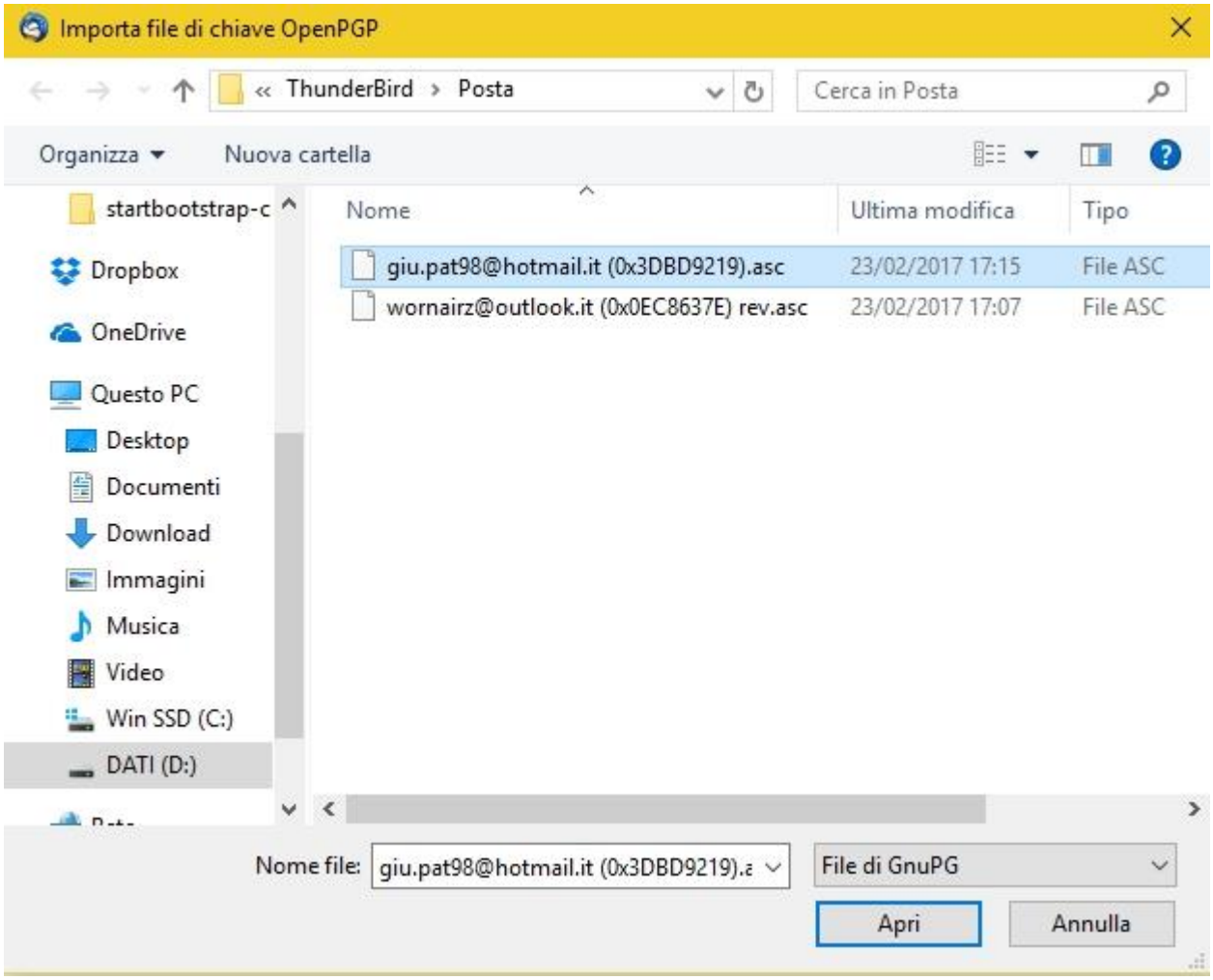
Per importare un certificato da un file, dobbiamo andare sul gestore delle chiavi di EnigMail



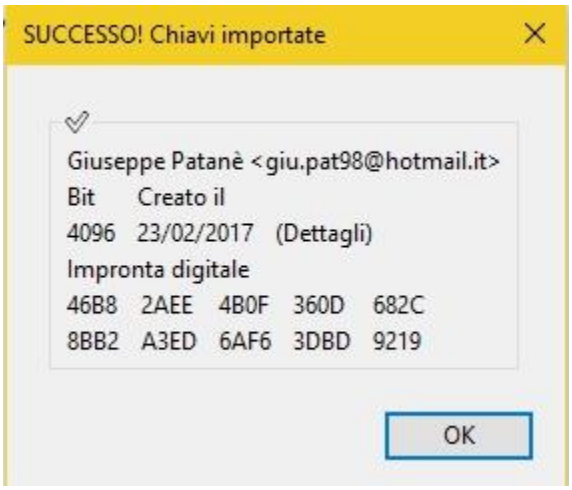
Poi andiamo su Importa chiavi da file


Gestione chiavi Enigmail
File
Modifica
Visualizza
Server
Genera
Importa chiavi da un file
Esporta chiavi in un file
Invia chiavi pubbliche via email
Componi email con le chiavi selezionate
Gestisci smartcard...
Ricarica cache chiavi
Chiudi
Ctrl+W
Esci
Mostra tutte le chiavi come impostazione predefinita
ID chiave
0EC8637E
3DBD9219
B3E55441

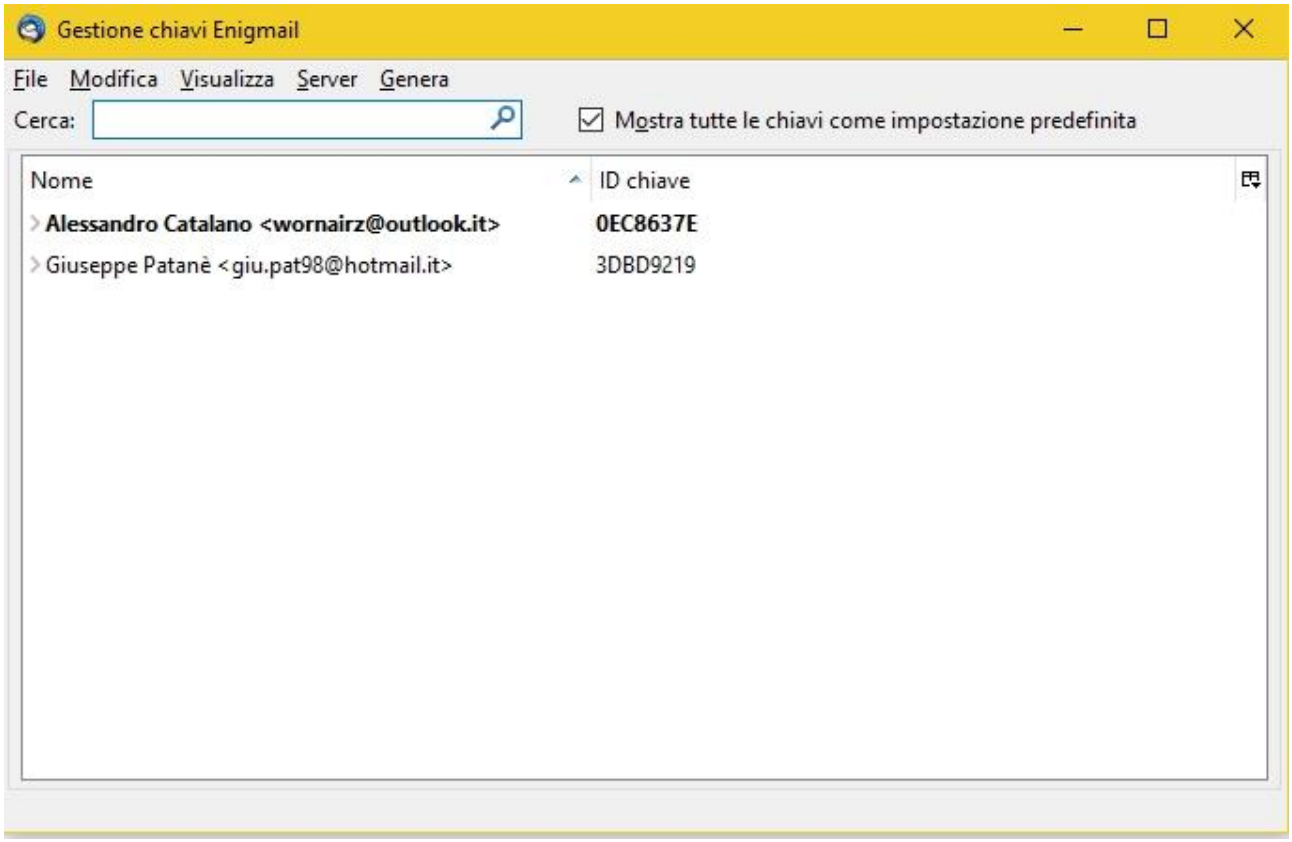
E selezioniamo il file che abbiamo in precedenza salvato



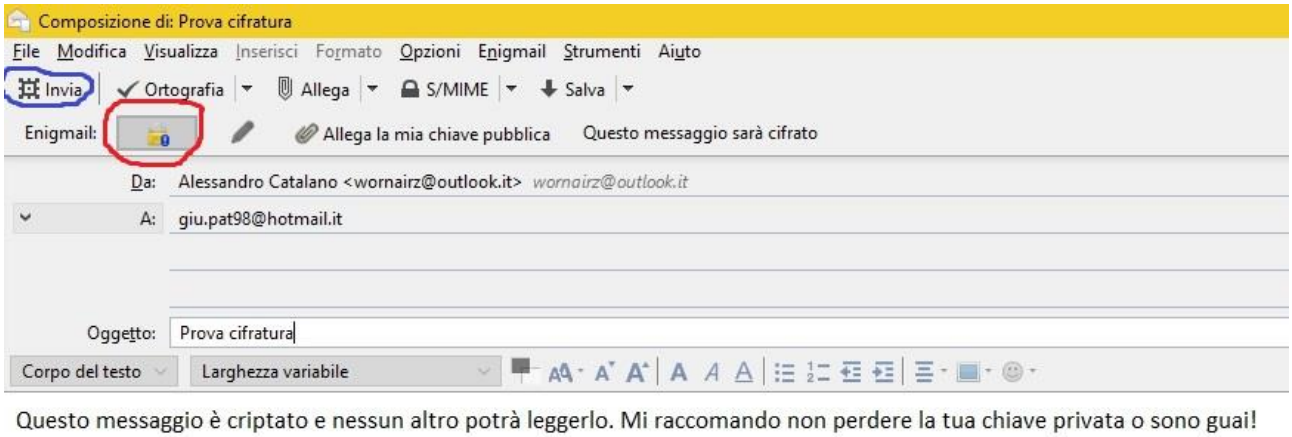
Se tutto è andato a buon fine avremo questa schermata ed il certificato del nostro amico sarà importato



Adesso insieme al nostro certificato, dovremmo vedere anche quello del nostro amico

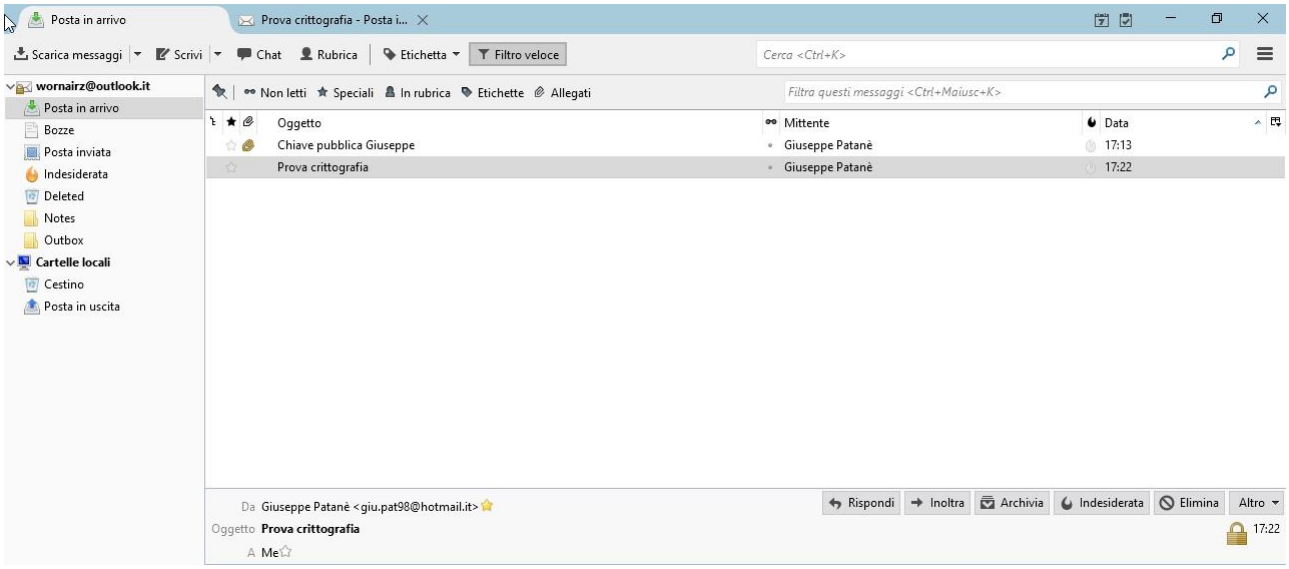


7) Adesso che abbiamo importato il certificato del nostro amico, possiamo inviargli delle mail criptate



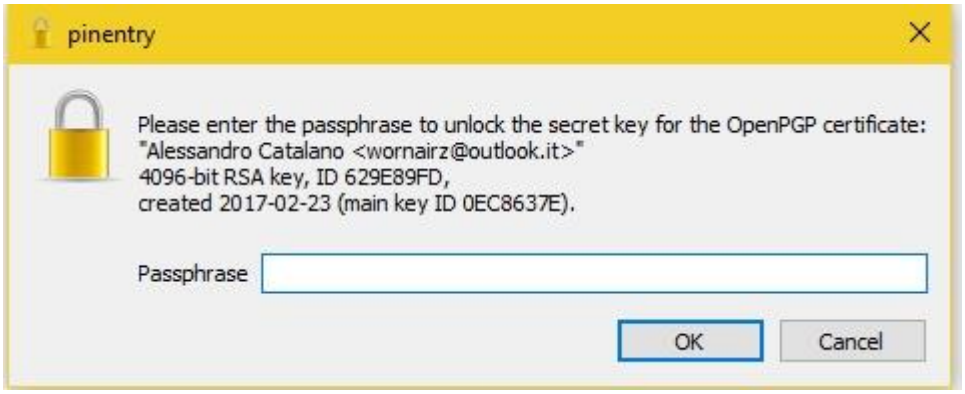
Cliccando sul bottone cerchiato in rosso, applicheremo la cifratura al documento. Enigmail riconoscerà in automatico il certificato associato al destinatario, crittografando il testo con la sua chiave pubblica.

5) Adesso proviamo a decriptare una mail crittografata.

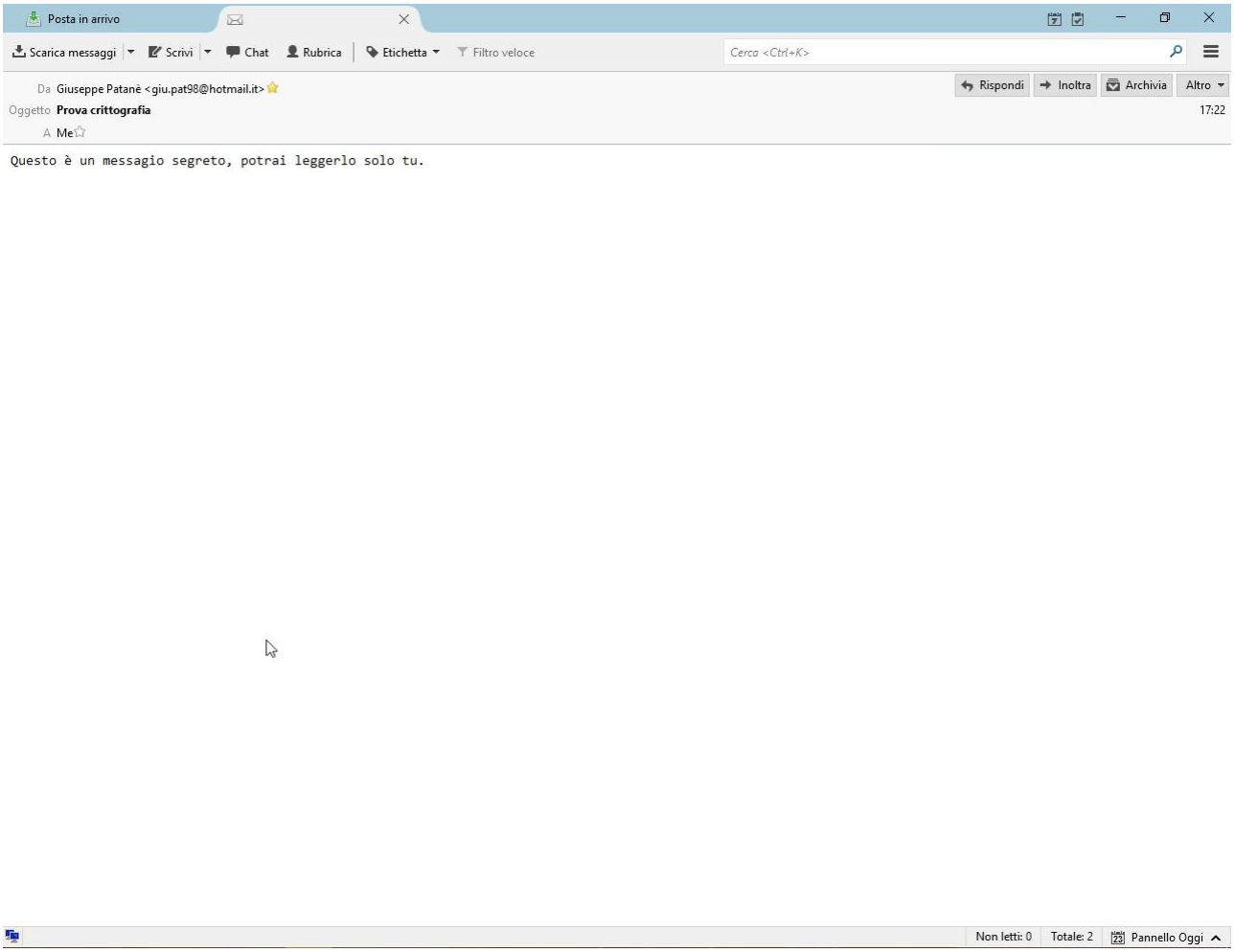


Facciamo doppio click sul messaggio e ci verrà chiesta la passphrase, in modo da sbloccare la nostra chiave privata da usare per decriptare il messaggio perché il mittente ha usato la nostra

chiave pubblica.

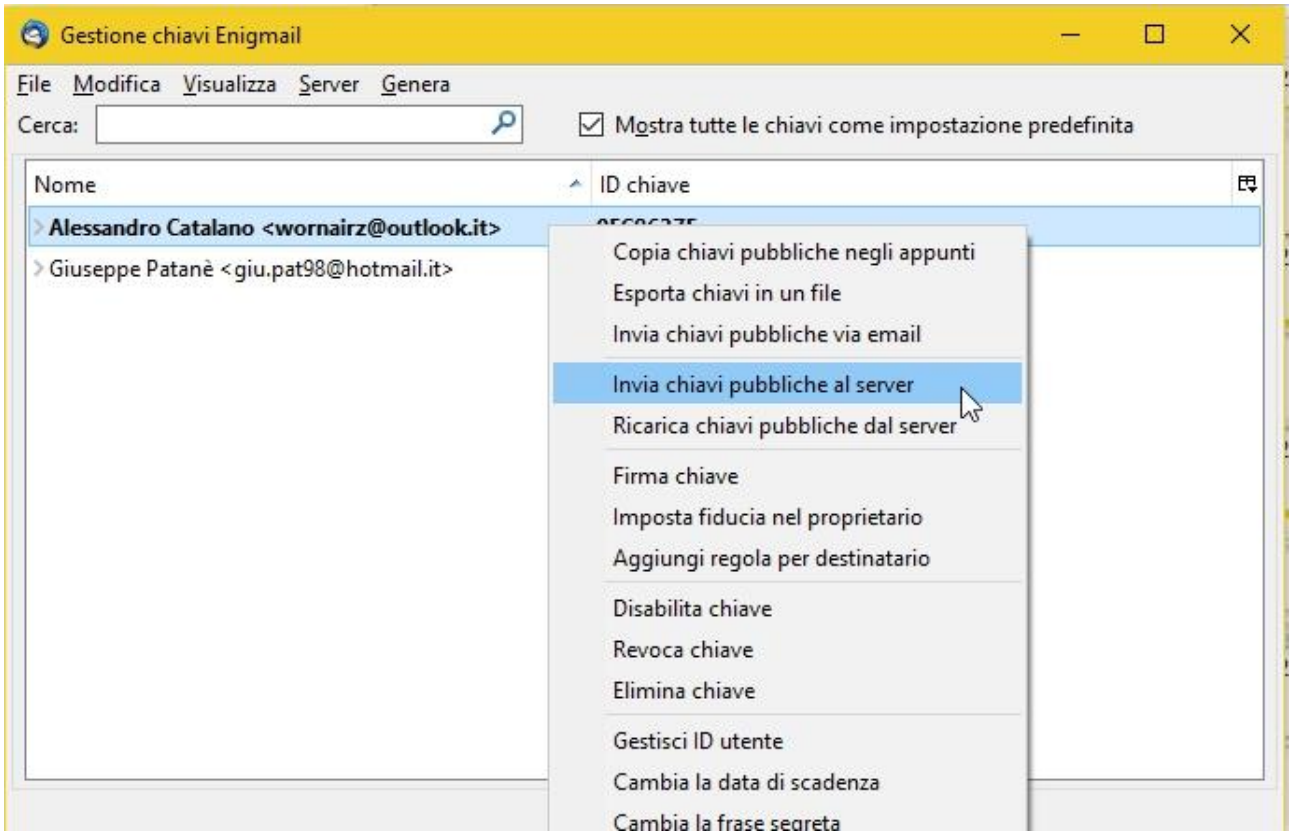


Dopo aver inserito la passphrase, potremo vedere il messaggio segreto

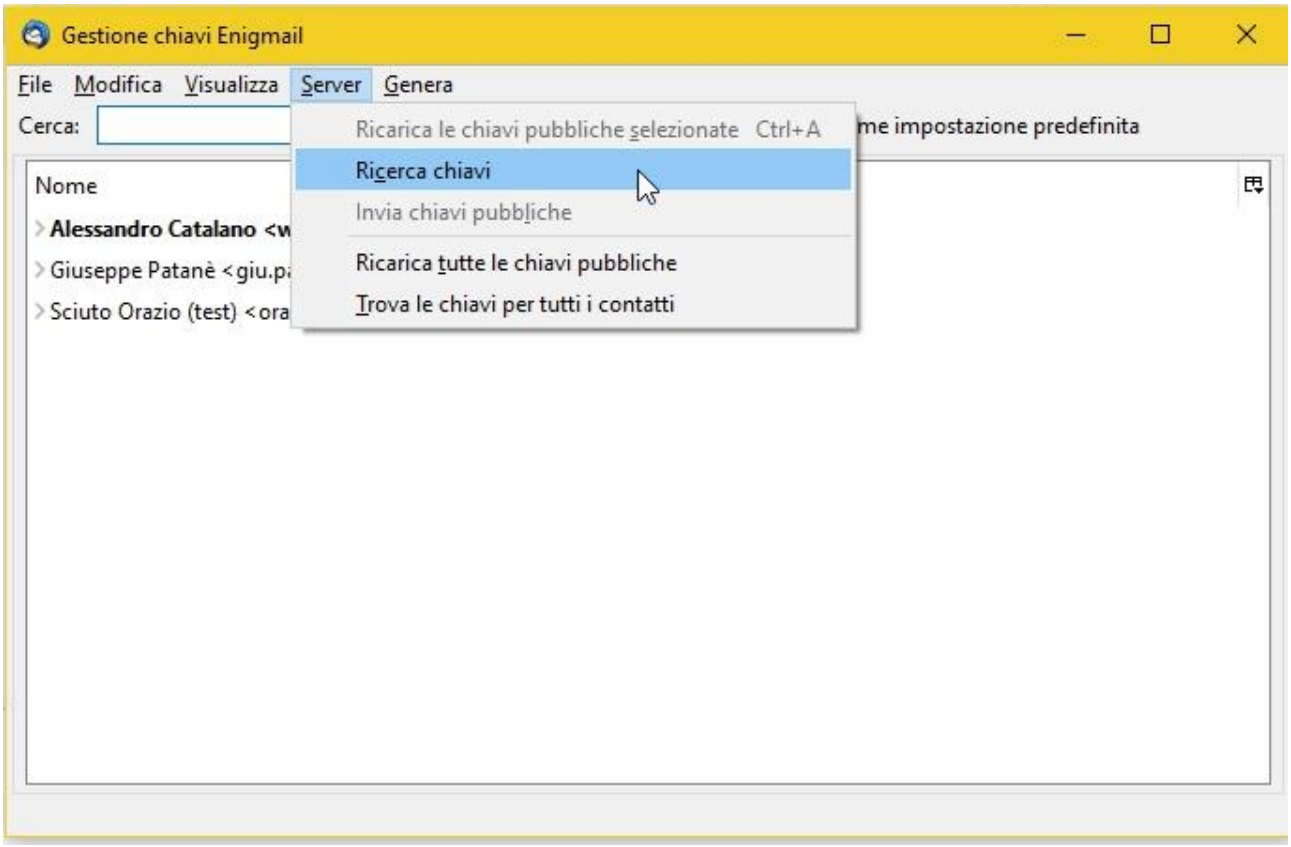


2) 4) In Enigmail il server OpenGPG di default è pool.sks-keyservers.net. Per importare il proprio certificato bisogna semplicemente selezionare il

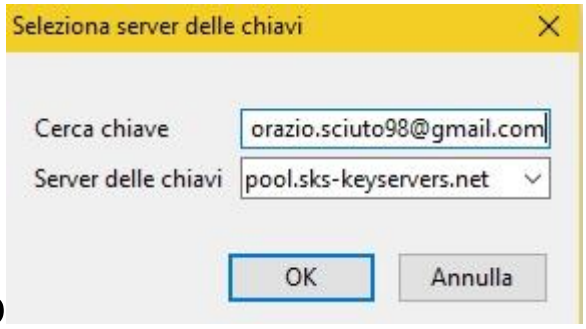
certificato, fare click con il tasto destro e spedirlo al server



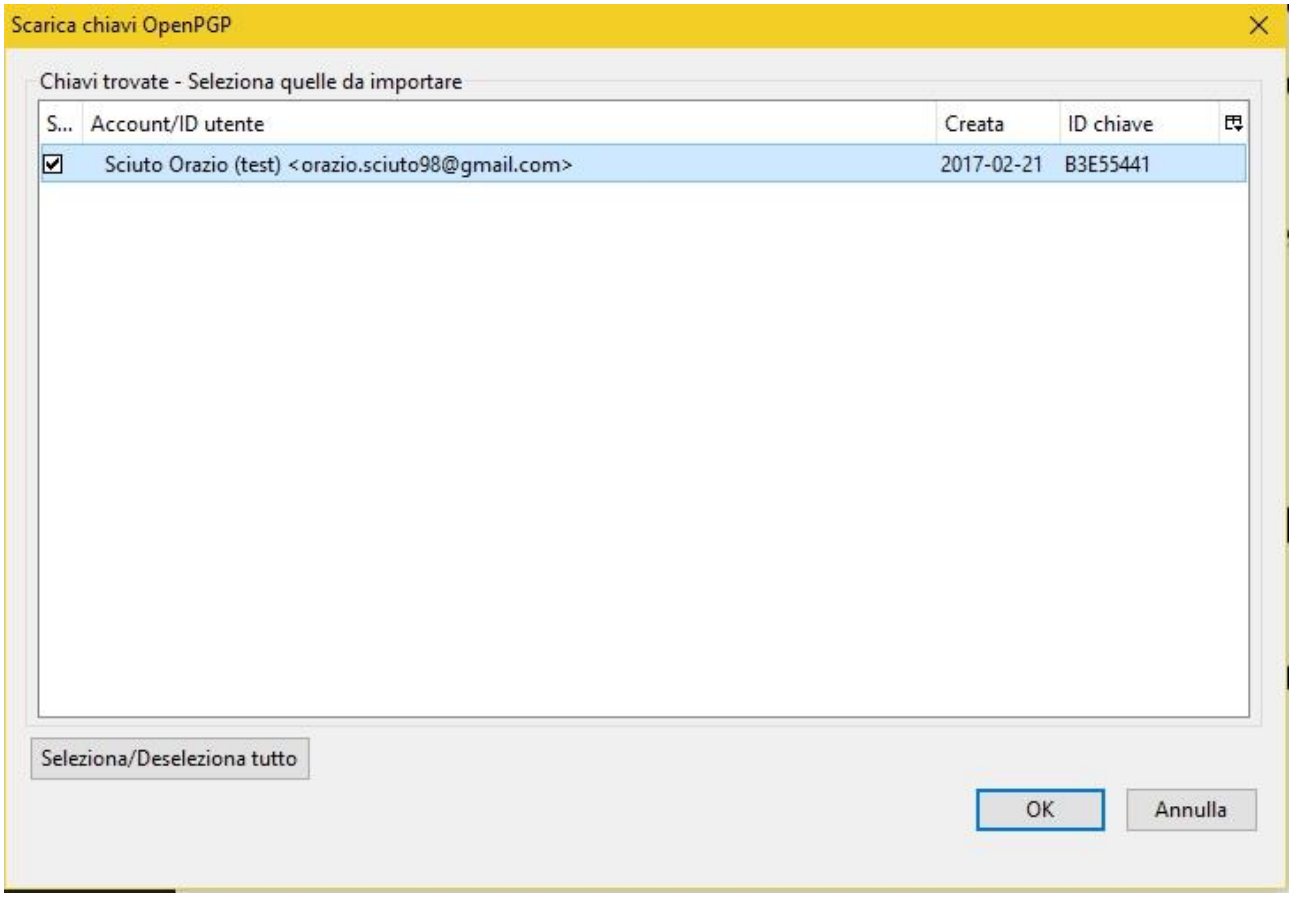
Per importare invece bisogna fare click su Server -> Ricerca chiavi



Ci apparirà un popup dove dovremo selezionare il server e la keyword per trovare il certificato. Ho usato la mail del mio compagno per trovare il suo certificato

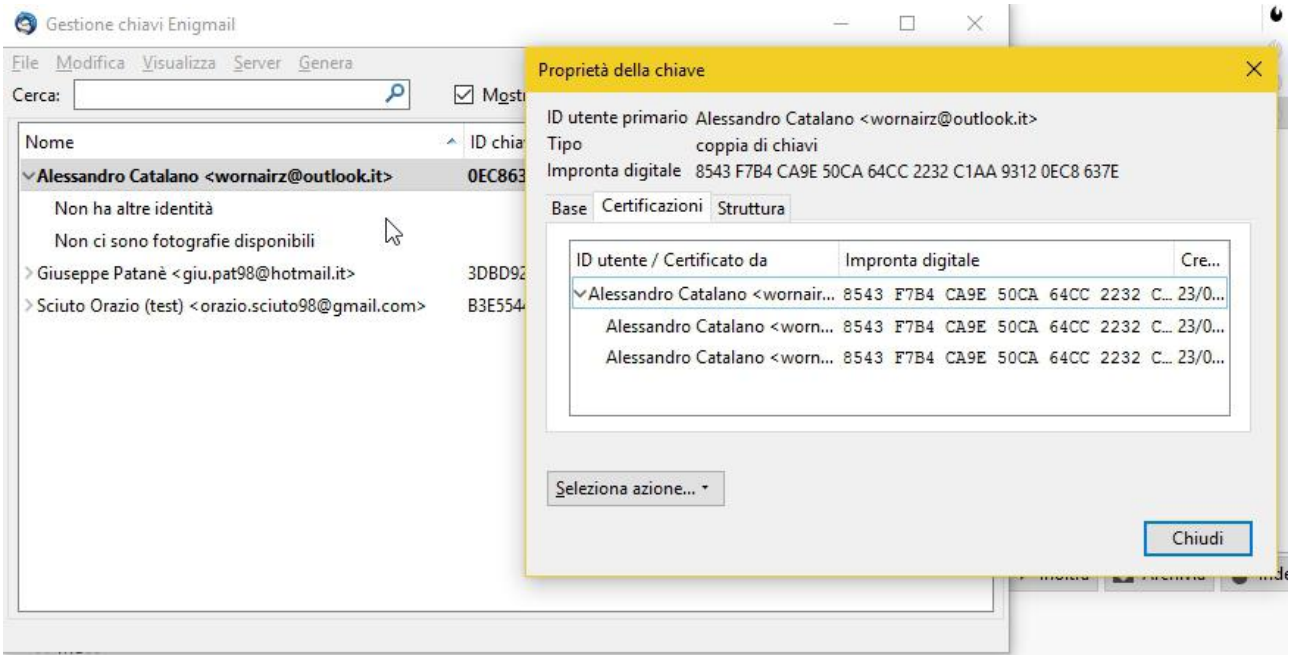


Abbiamo trovato una sola corrispondenza, quindi procediamo ad importare il certificato selezionandolo e premendo ok.



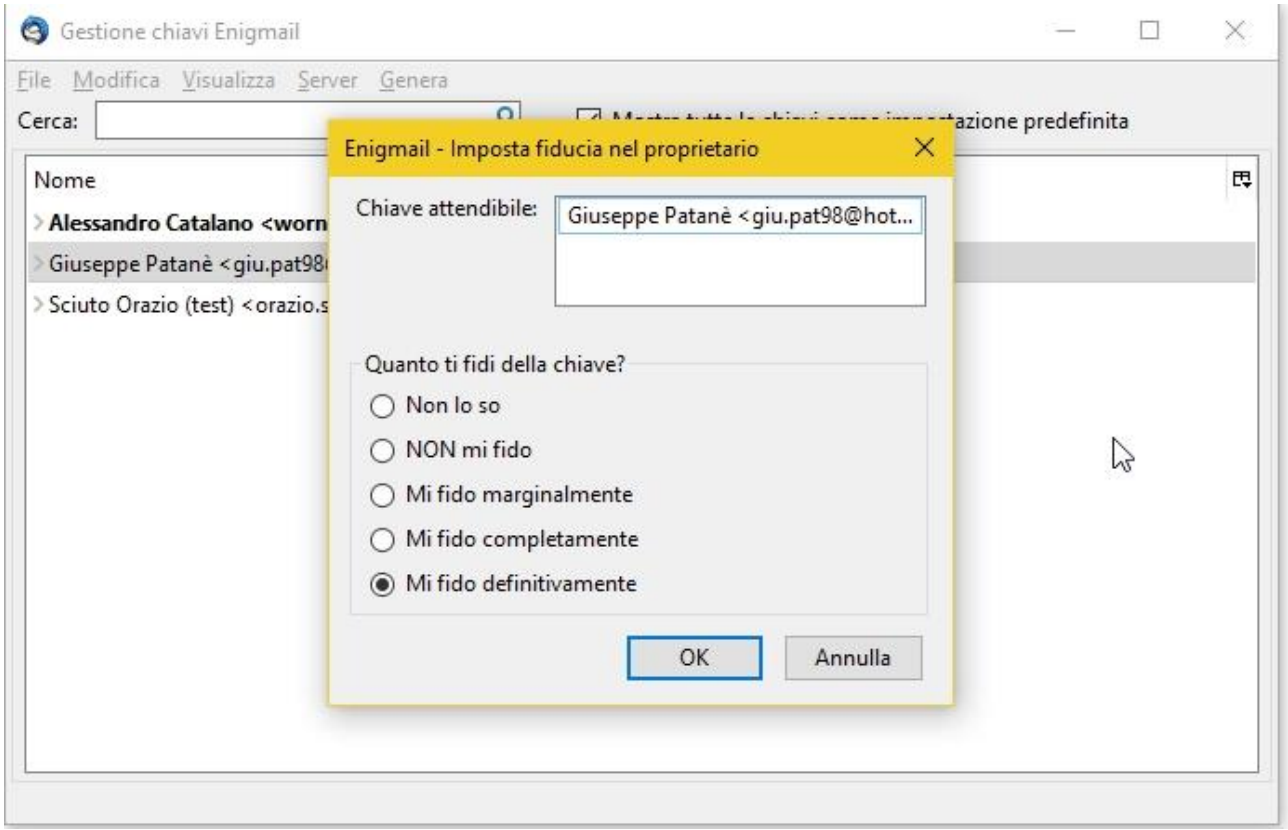
Se tutto è andato a buon fine, troveremo questa scritta

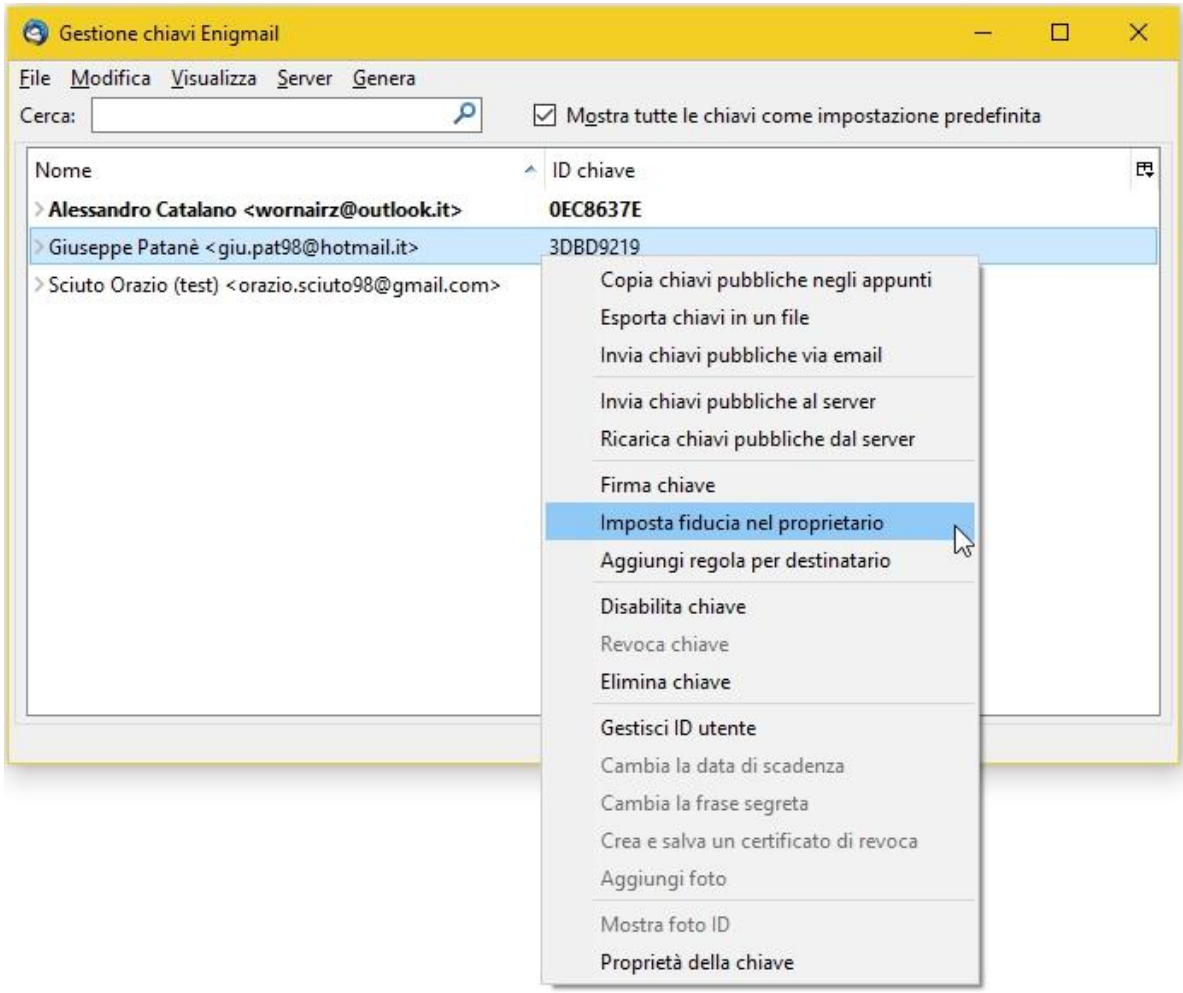
6) Il nostro certificato è attualmente firmato solo da noi stessi (self-signed)



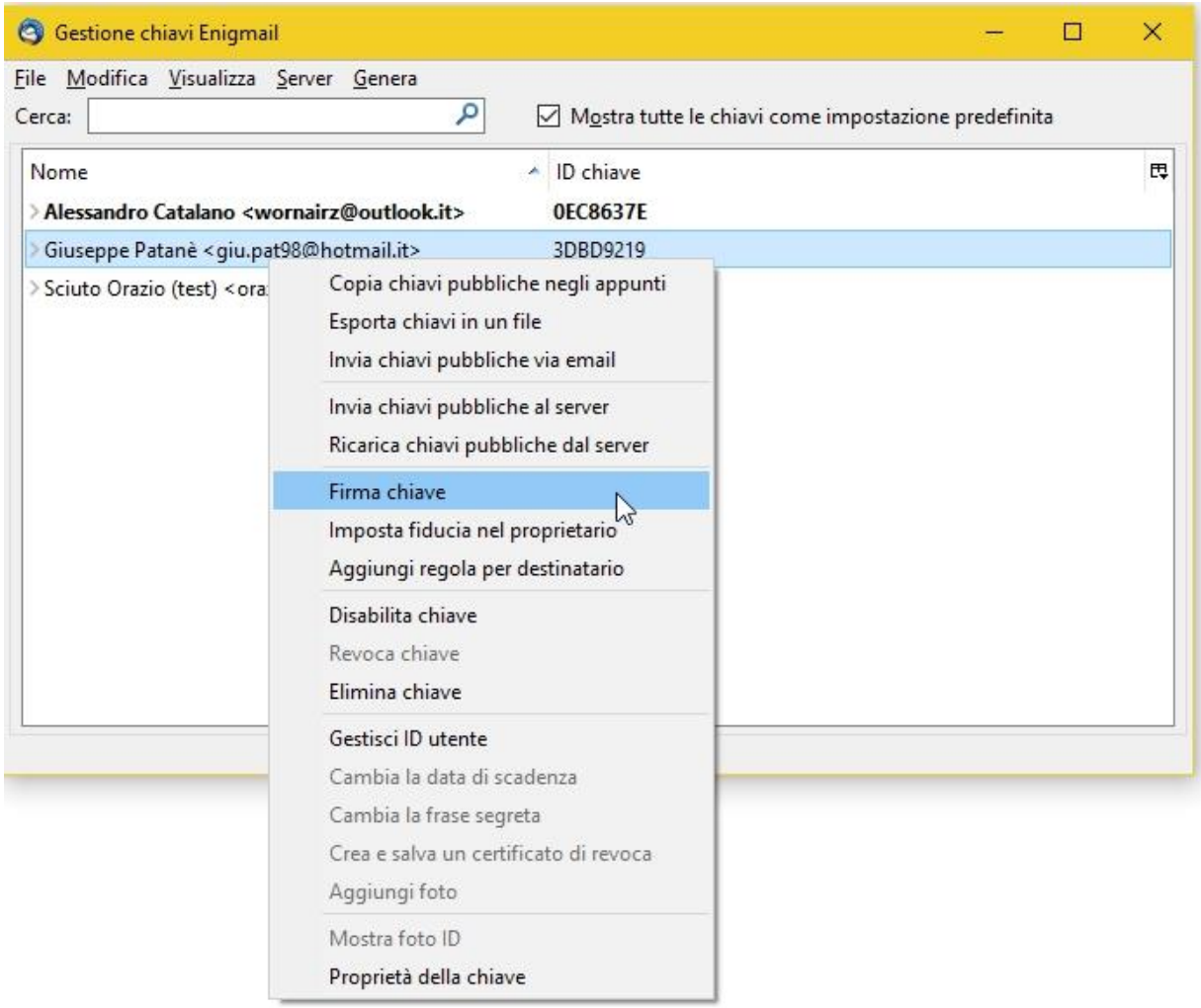
Provvediamo quindi a firmare il certificato del nostro amico, e lui farà lo stesso con noi.

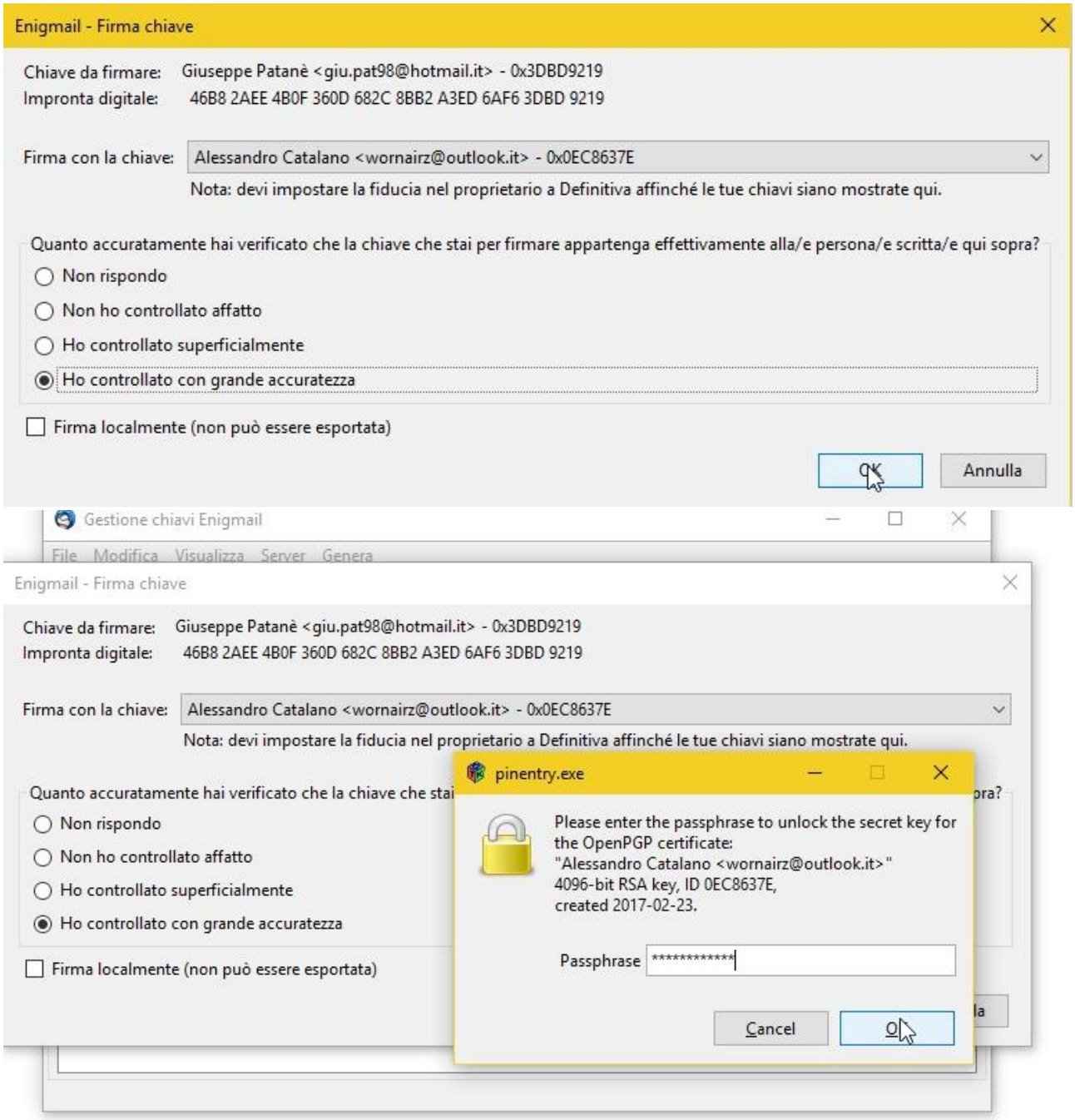
Iniziamo con l’impostare la nostra fiducia al proprietario di quel certificato


Gestione chiavi Enigmail
File Modifica Visualizza Server Genera
Cerca:
Nome
Alessandro Catalano <worn
Giuseppe Patanè <giu.pat98
Sciuto Orazio (test) <orazio.s
Enigmail - Imposta fiducia nel proprietario
Chiave attendibile:
Giuseppe Patanè <giu.pat98@hot...
Quanto ti fidi della chiave?
Non lo so
NON mi fido
Mi fido marginalmente
Mi fido completamente
Mi fido definitivamente
OK
Annulla


Gestione chiavi Enigmail
File Modifica Visualizza Server Genera
Cerca:
Mostra tutte le chiavi come impostazione predefinita
Nome
ID chiave
Alessandro Catalano <wornairz@outlook.it>
0EC8637E
Giuseppe Patanè <giu.pat98@hotmail.it>
3DBD9219
Sciuto Orazio (test) <orazio.sciuto98@gmail.com>
Copia chiavi pubbliche negli appunti
Esporta chiavi in un file
Invia chiavi pubbliche via email
Invia chiavi pubbliche al server
Ricarica chiavi pubbliche dal server
Firma chiave
Imposta fiducia nel proprietario
Aggiungi regola per destinatario
Disabilita chiave
Revoca chiave
Elimina chiave
Gestisci ID utente
Cambia la data di scadenza
Cambia la frase segreta
Crea e salva un certificato di revoca
Aggiungi foto
Mostra foto ID
Proprietà della chiave

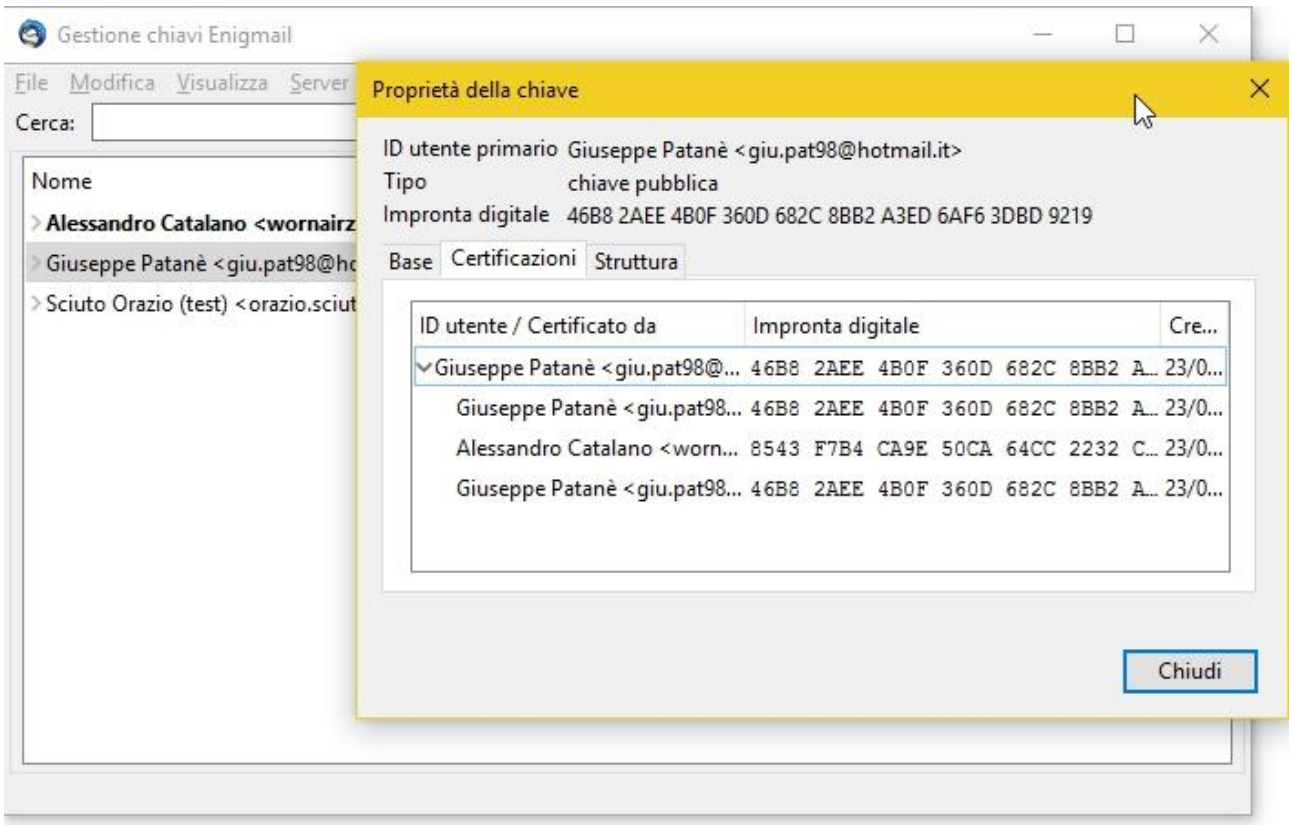
Solo adesso che ci fidiamo definitivamente del nostro amico, possiamo firmargli il certificato.



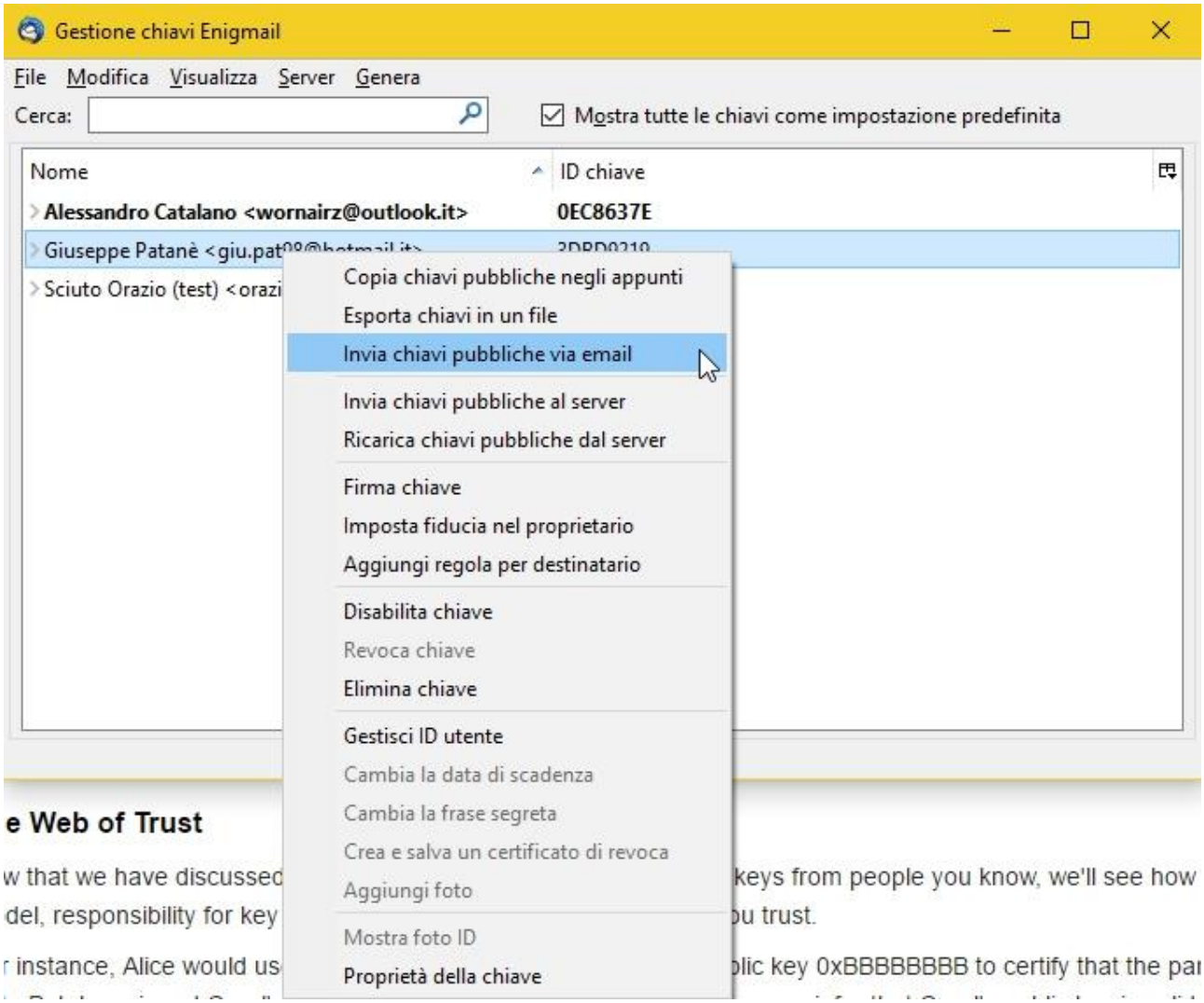


La passphrase è richiesta perché stiamo firmando il certificato con la nostra chiave privata in modo che chiunque, tramite la nostra chiave pubblica, può accertare della veridicità della nostra firma.

Adesso il suo certificato conterrà anche la nostra firma.

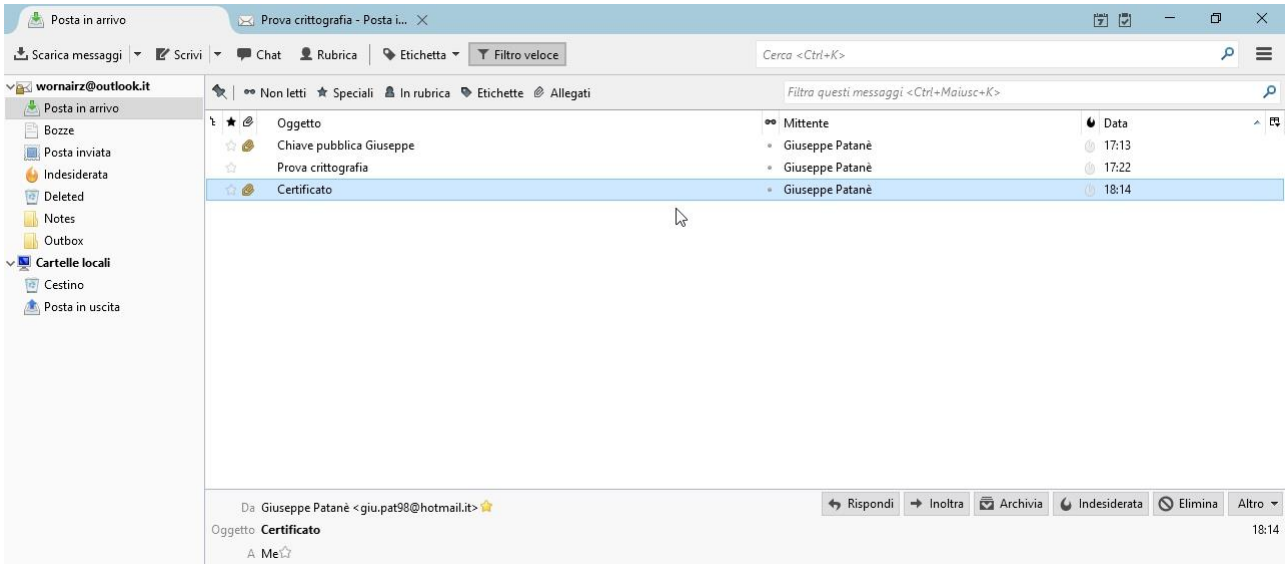


Adesso spediamoglielo via mail così lui potrà ricaricarlo sul server o mandarlo ad altre persone tramite email.

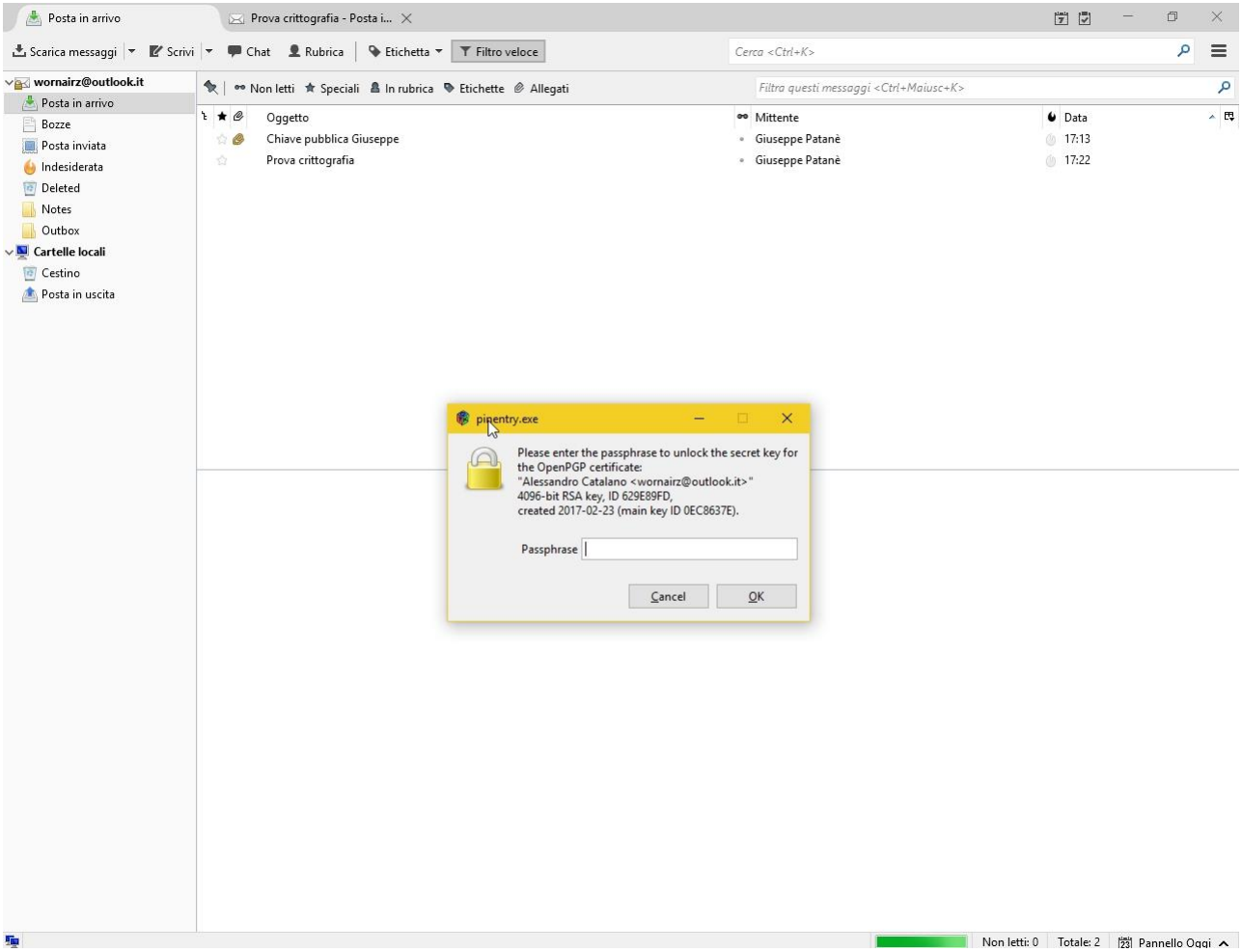


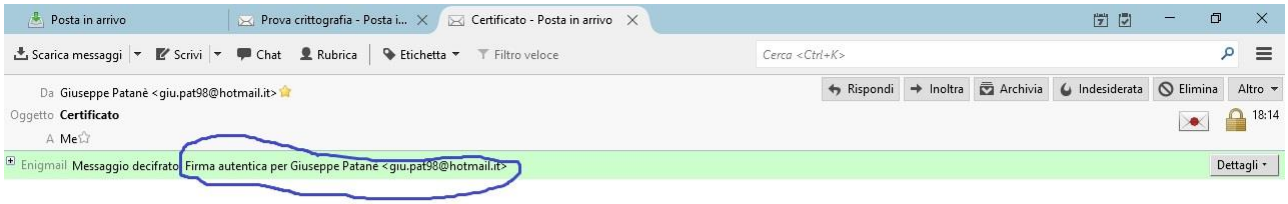
È una buona pratica crittografare il documento così nessuno si possa appropriare del certificato del nostro amico, ma soprattutto è decisamente consigliato firmare il documento applicando la firma digitale per far capire al destinatario che siamo davvero stati noi a firmarlo, non qualcuno che si spaccia per noi. La firma si applica tramite l'icona cerchiata in rosso.

Il nostro amico ci ha mandato una mail contente il nostro certificato firmato da lui.

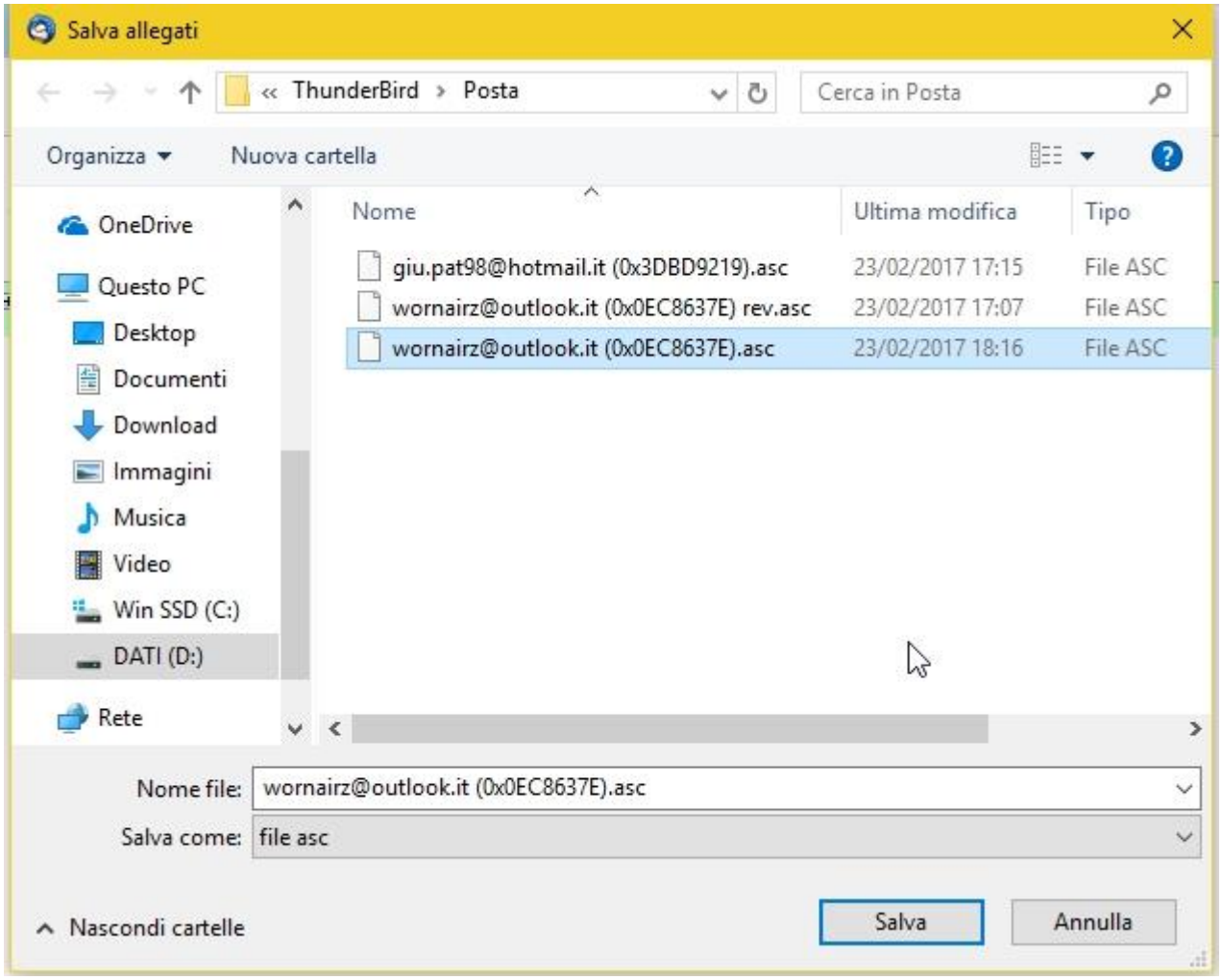


Anche lui ha mandato il documento crittografato, quindi ci viene richiesta la passphrase per poterlo decifrare

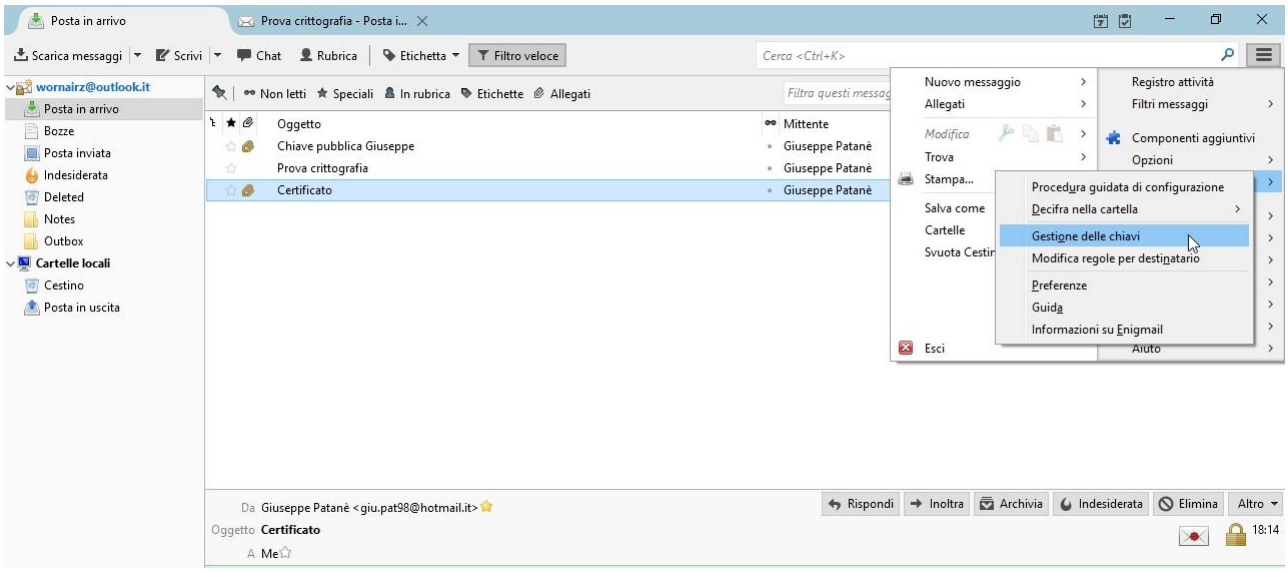




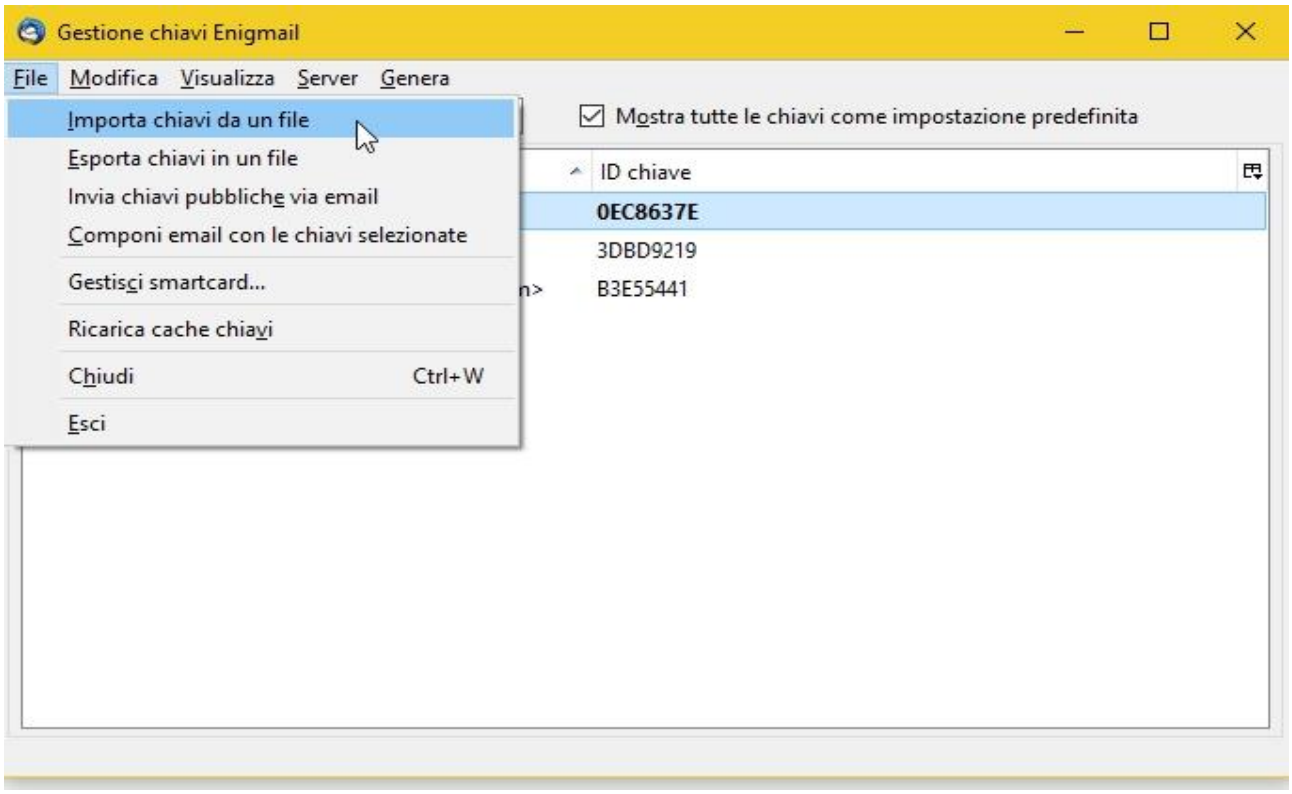
Cerchiato di blu, vediamo che Enigmail ha riconosciuto la firma autentica del nostro compagno. Cerchiato di rosso l'allegato contenente il nostro certificato firmato da lui. Scarichiamo l'allegato e salviamolo in un file.

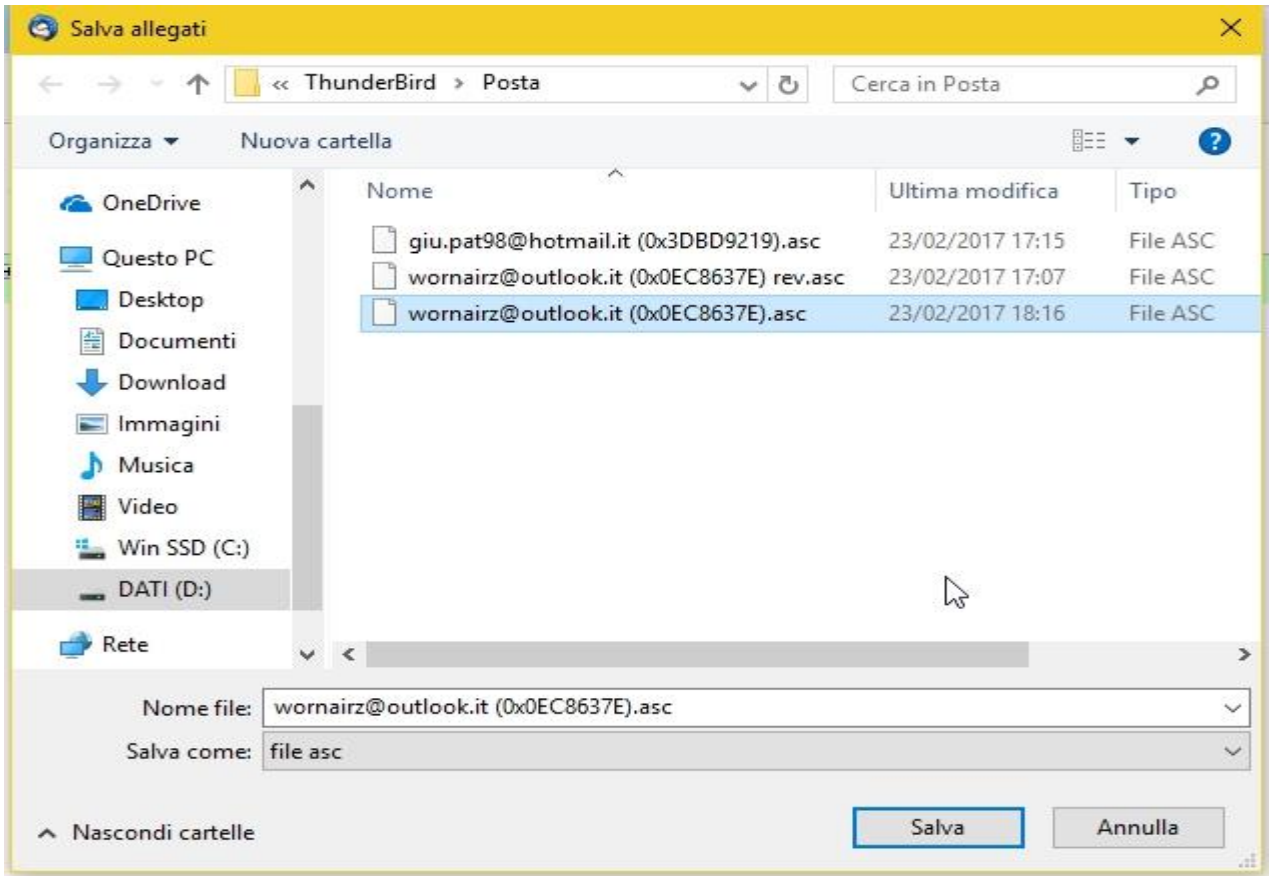


Torniamo al gestore delle chiavi

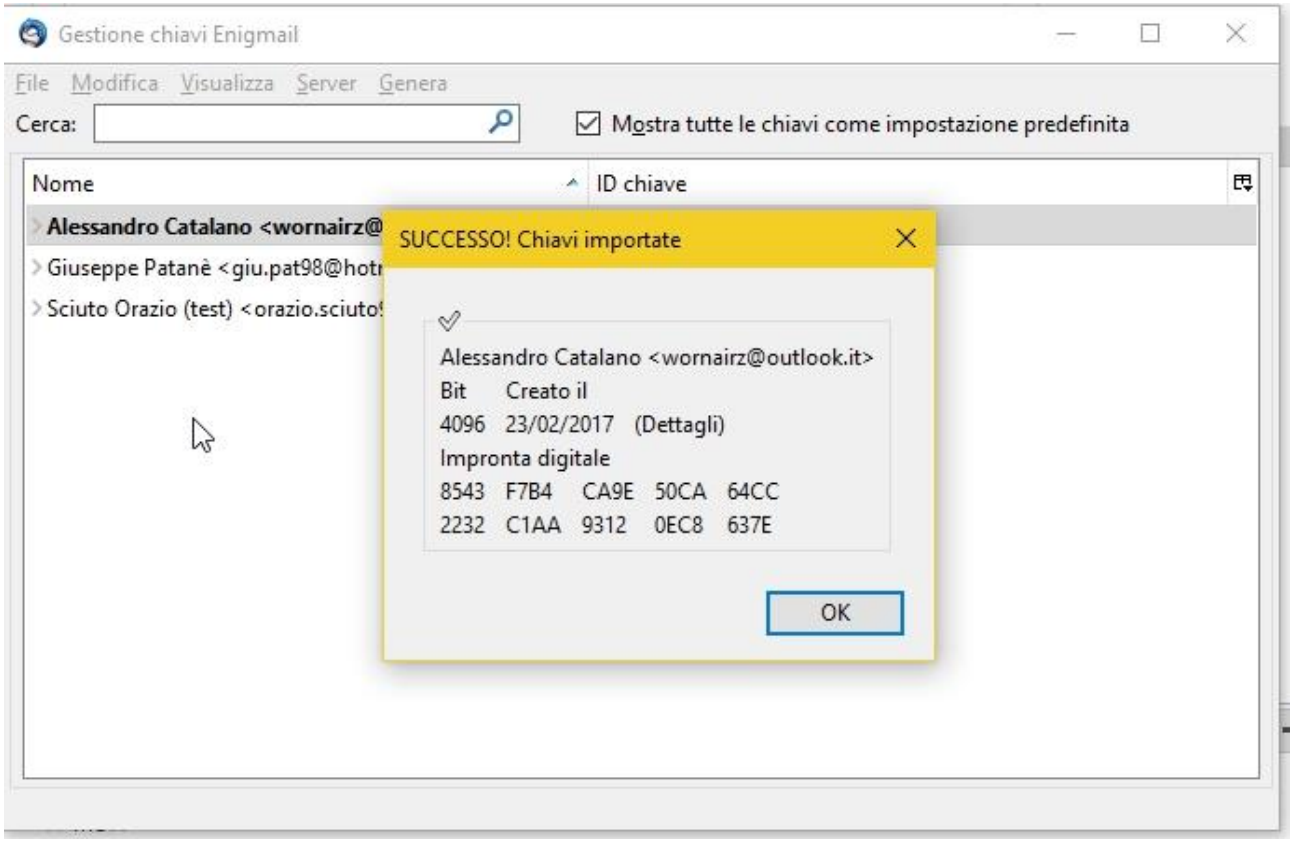


Premiamo File -> Importa chiavi da un file e selezioniamo il certificato che abbiamo ricevuto

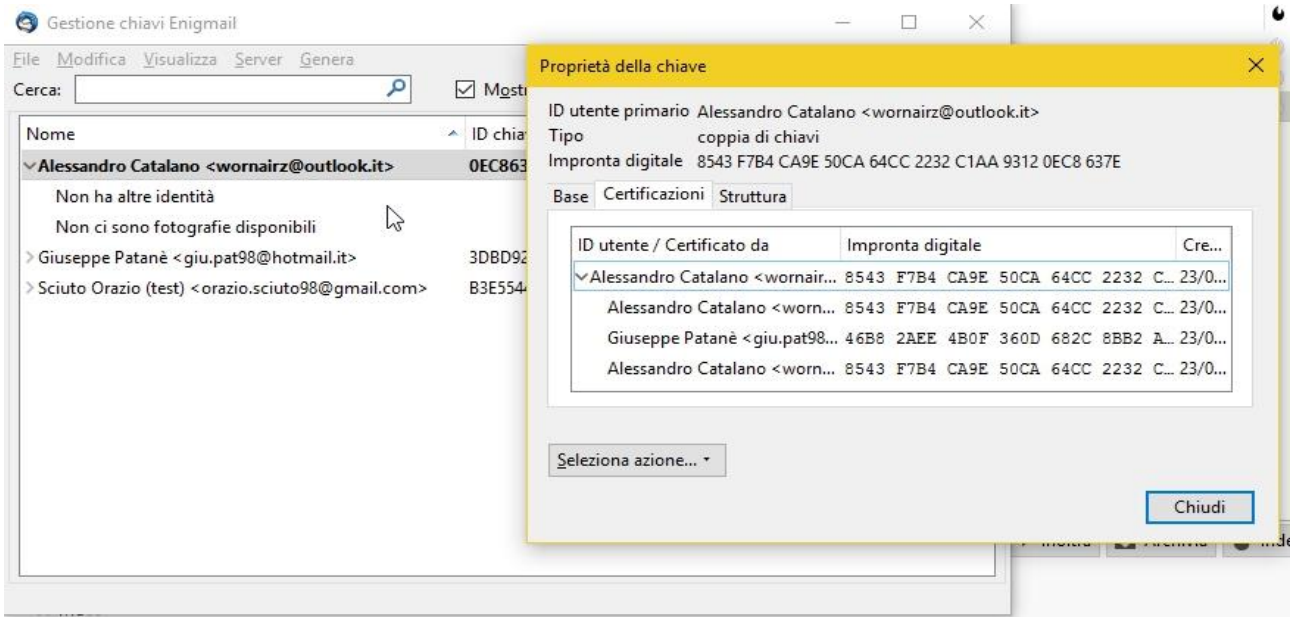

Gestione chiavi Enigmail
File
Modifica
Visualizza
Server
Genera
Importa chiavi da un file
Esporta chiavi in un file
Invia chiavi pubbliche via email
Componi email con le chiavi selezionate
Gestisci smartcard...
Ricarica cache chiavi
Chiudi
Ctrl+W
Esci
Mostra tutte le chiavi come impostazione predefinita
ID chiave
0EC8637E
3DBD9219
B3E55441


Salva allegati
ThunderBird
Posta
Cerca in Posta
Organizza
Nuova cartella
OneDrive
Questo PC
Desktop
Documenti
Download
Immagini
Musica
Video
Win SSD (C:)
DATI (D:)
Rete
Nome
Ultima modifica
Tipo
giu.pat98@hotmail.it (0x3DBD9219).asc
23/02/2017 17:15
File ASC
wornairz@outlook.it (0x0EC8637E) rev.asc
23/02/2017 17:07
File ASC
wornairz@outlook.it (0x0EC8637E).asc
23/02/2017 18:16
File ASC
Nome file:
wornairz@outlook.it (0x0EC8637E).asc
Salva come:
file asc
Nascondi cartelle
Salva
Annulla

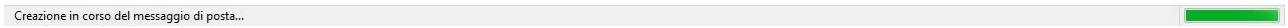
Se tutto è andato a buon fine apparirà questa scritta



Adesso, cliccando due volte sul nostro certificato e andando su Certificazioni, vedremo che il nostro certificato è stato firmato anche dal nostro amico

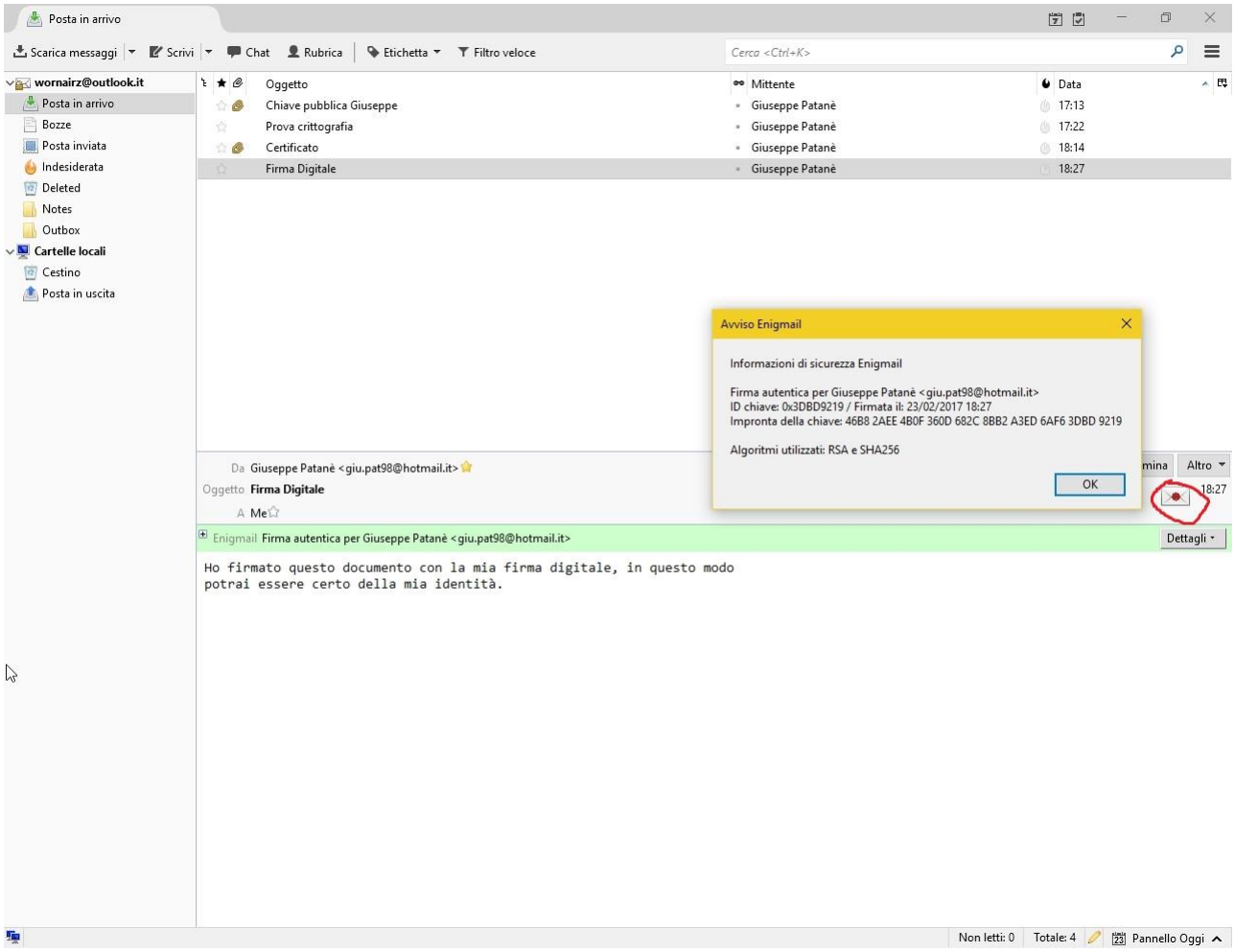


8) Per firmare digitalmente un documento, clicchiamo sull'icona cerchiata in rosso



La passphrase sarà richiesta perché dobbiamo usare la nostra chiave privata, in modo che chiunque possa accertarsi della nostra identità usando il nostro certificato pubblico disponibile in rete.

Quando riceviamo una mail firmata, Enigmail in automatico verifica l'autenticità di una firma digitale. Se vogliamo avere più dettagli sulla firma, basta cliccare l'icona cerchiata in rosso



9) Per applicare sia la firma che la crittografica, bisogna semplicemente cliccare entrambi i bottoni

Per riceve dei messaggi sia crittografati che firmati, bisogna intanto decifrarlo tramite la passphrase

La firma digitale è riconosciuta in automatico da Enigmail