LAB :: PGP (Pretty Good Privacy)

GnuPG : GnuPG forms the heart of Gpg4win – the actual encryption software.
Kleopatra : The central certificate administration of Gpg4win, which ensures uniform user navigation for all cryptographic operations.

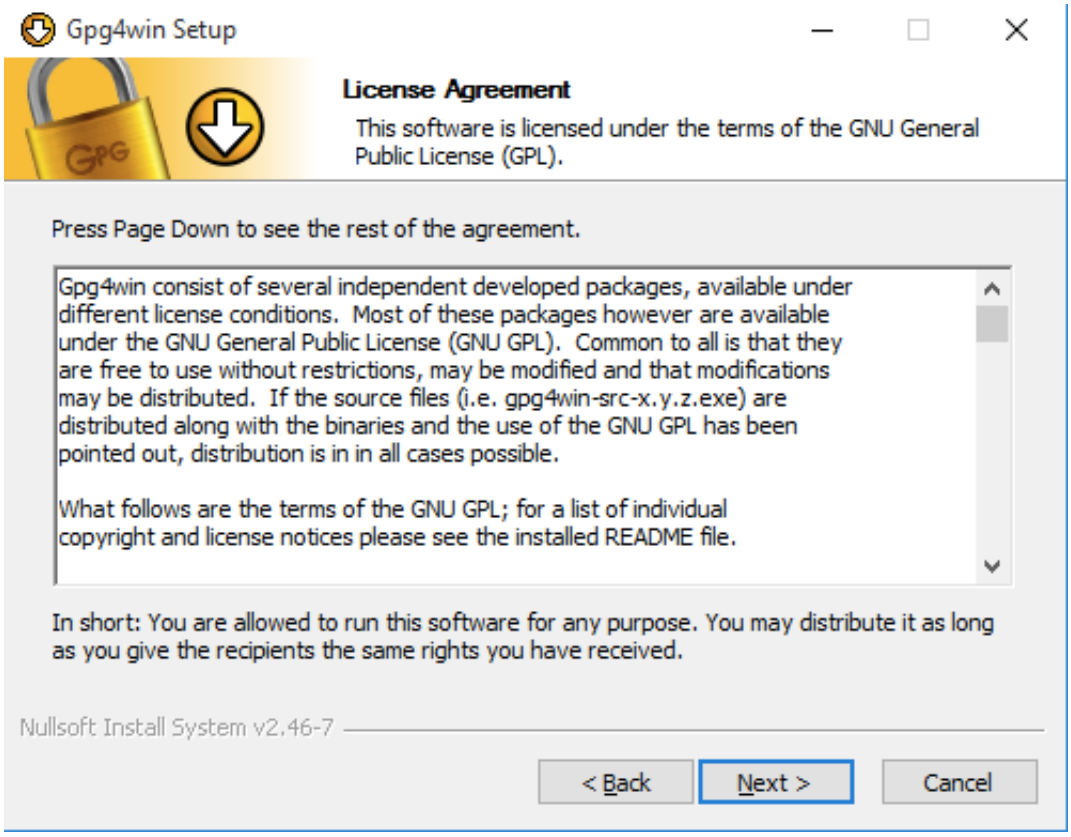
Download Gpg4win (GNU Privacy Guard for Windows) from https://www.gpg4win.org/index.html

Install GnuPG & Related application

1. The installation assistant will start and you will see this welcome dialog:

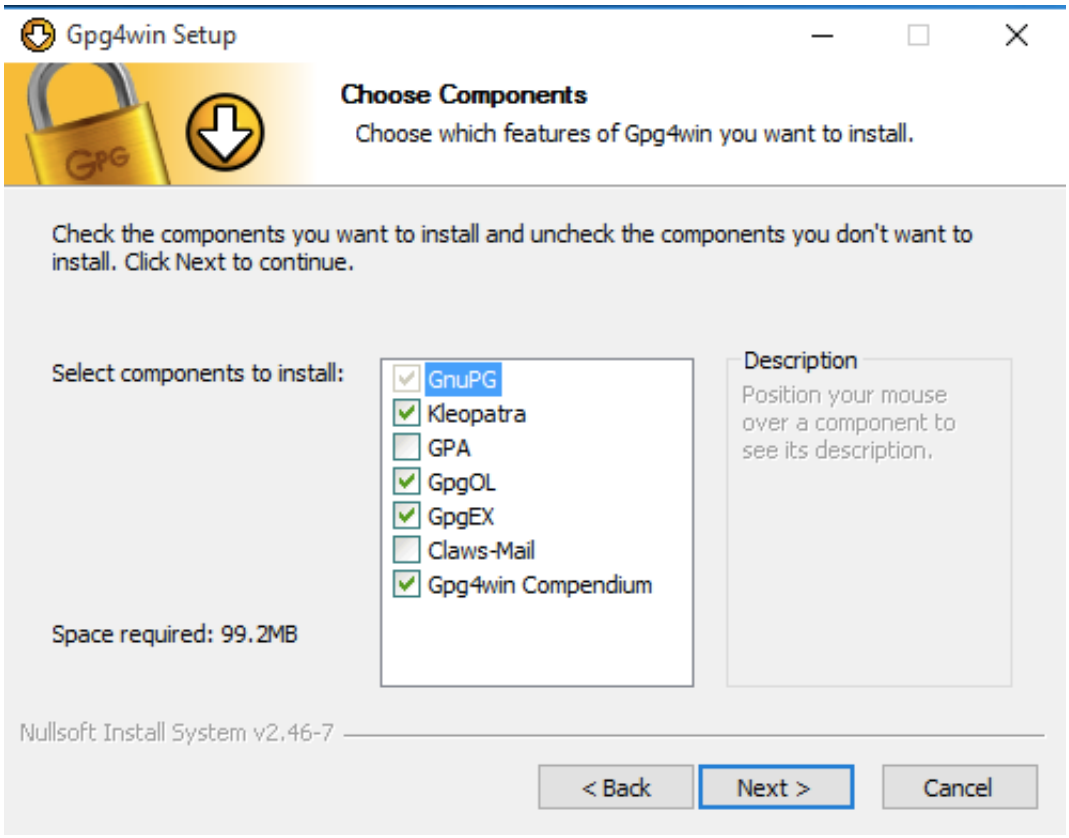
2. Close all programs that are running on your computer and click on `[ Next ]`

3. The next page displays the licensing agreement – it is only important if you wish to modify or forward Gpg4win. If you only want to use the software, you can do this right away – without reading the license.



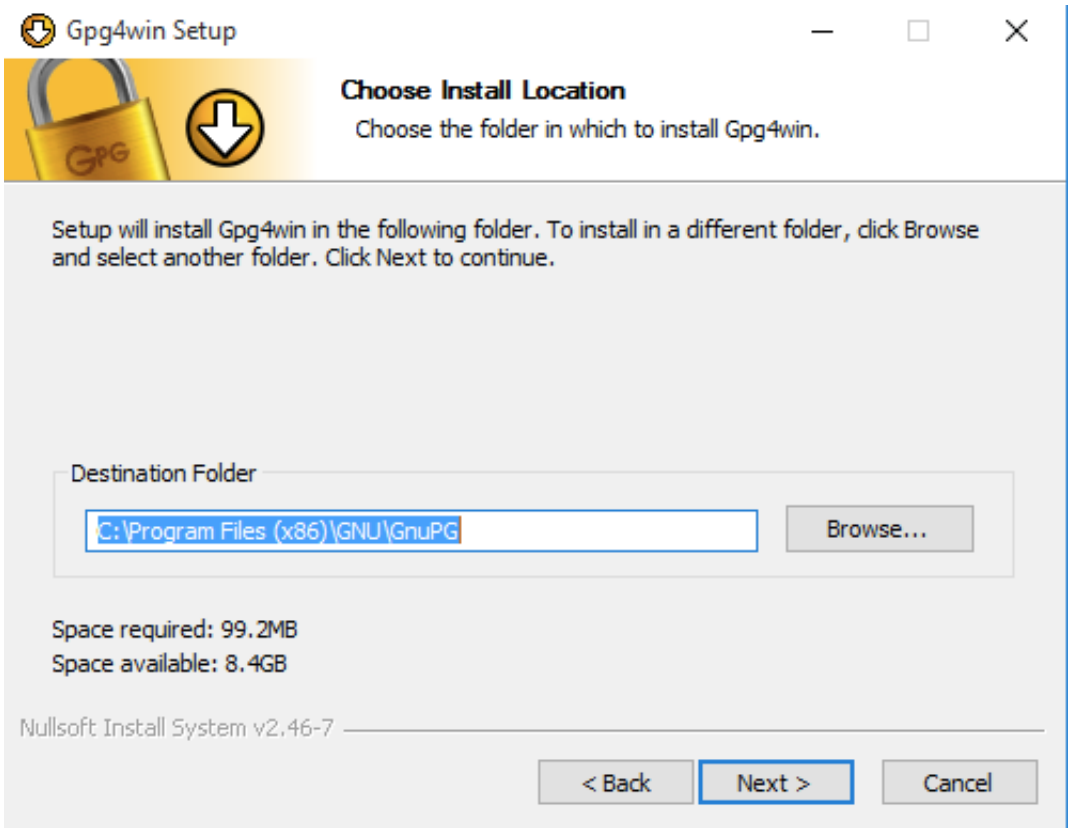
Click on `[ Next ]`

4. On the page that contains the selection of components you can decide which programs you want to install. A default selection has already been made for you. You can also install individual components at a later time. Moving your mouse cursor over a component will display a brief description. Another useful feature is the display of required hard drive space for all selected components. Bellow are the application and there fucntion:
   a. GnuPG: Gnu Privacy Guard
   b. Kleopatra: Keymanager for OpenPGP
   c. GPA: GNU Privacy Assistant
   d. GpgOL: GnuPG for Outlook
   e. GpgEX: GnuPG Shell Extension
   f. Claws-Mail: Claws Mail user client
   g. Gpg4win Compedium: The Gpg4Win documentation



Click on `[ Next ]`

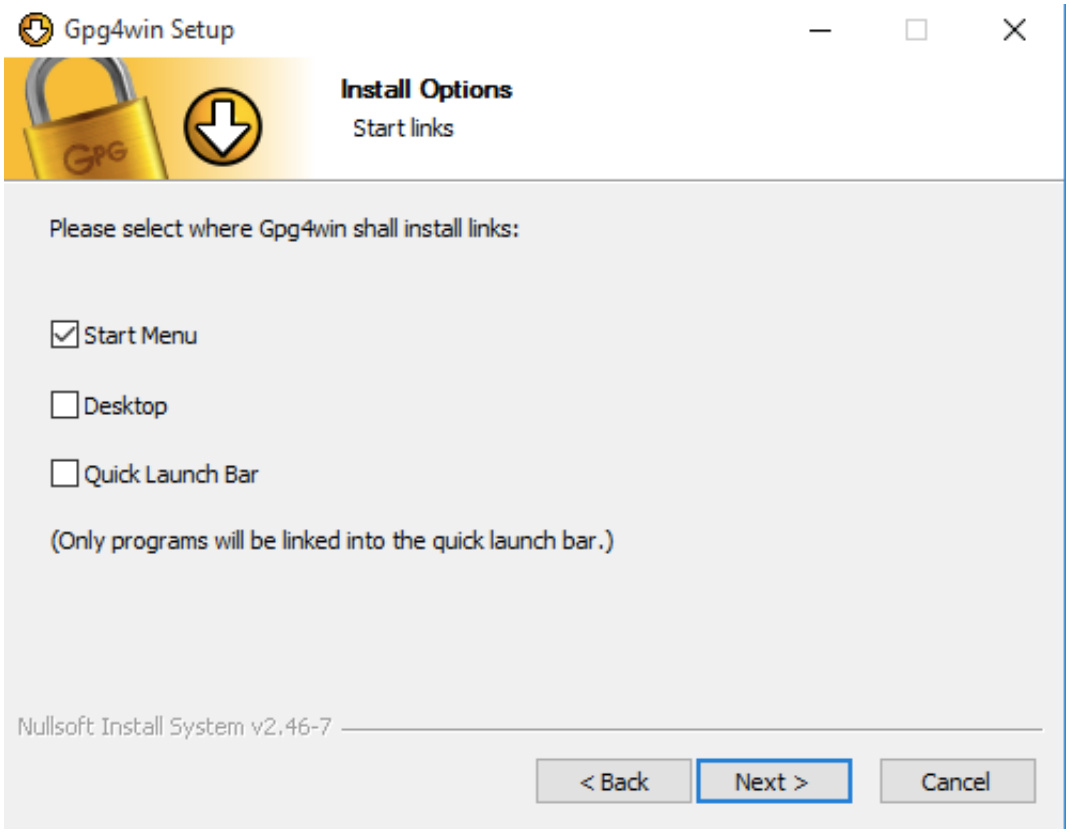
5. The system will suggest a folder for the installation, e.g.: C:\Programme Files (x86)\GNU\GnuPG You can accept the suggestion or select a different folder for installing Gpg4win.



Then click on `[ Next ]`

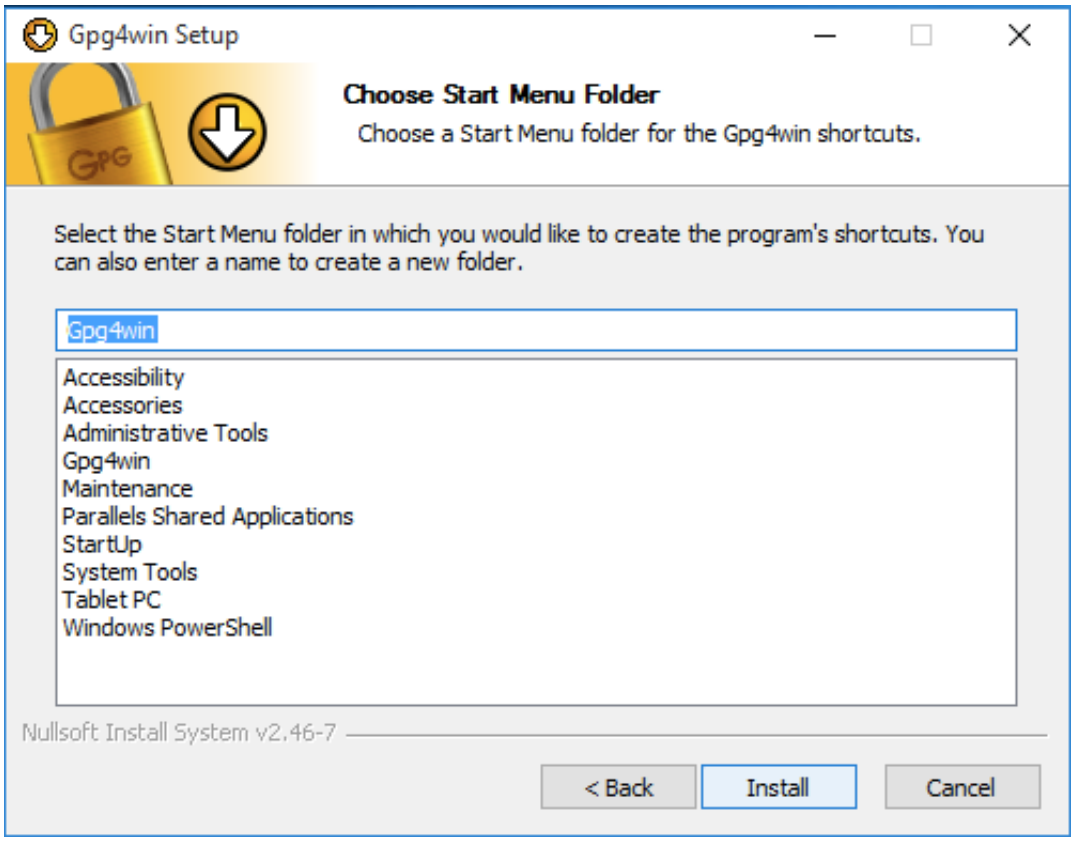
6. Now you can decide which links should be installed – the system will automatically create a link with

the start menu. You can change this link later on using the Windows dashboard settings.



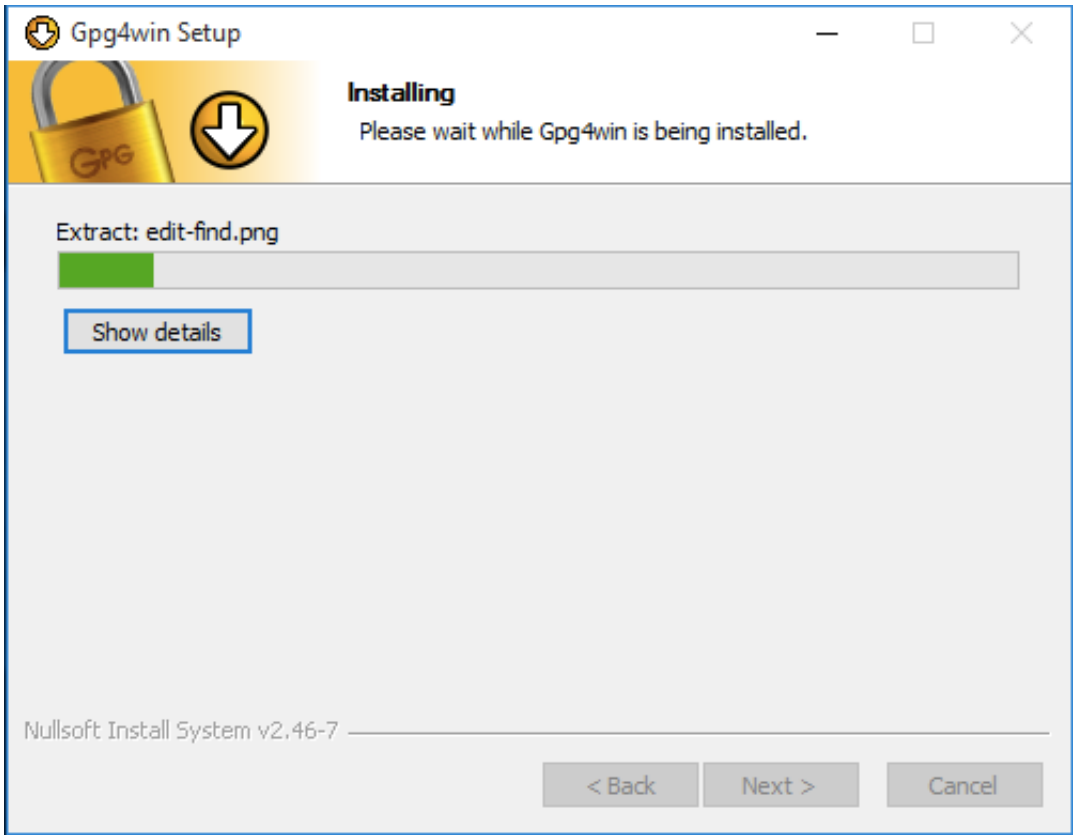
Then click on `[ Next ]`

7. If you have selected the default setting – link with start menu – you can define the name of this start menu on the next page or simply accept the name.



Then click on `[ Install ]`

8. During the installation process that follows, you will see a progress bar and information on which file is currently being installed. You can press `[ Show details ]` at any time to show the installation log.



Once you have completed the installation, please click on `[ Next ]`

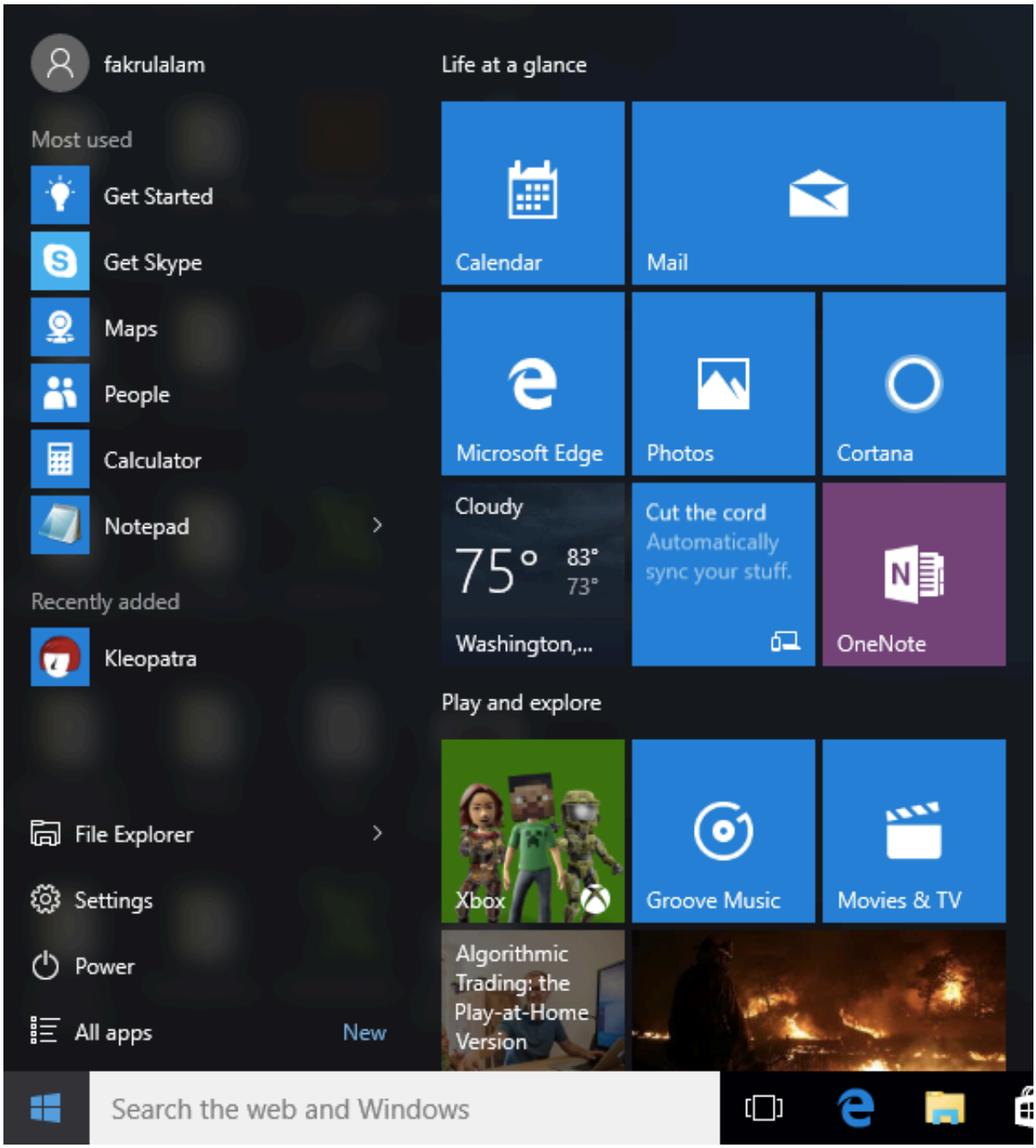
9. The last page of the installation process is shown once the installation has been successfully completed. In some cases you may have to restart Windows. In this case, you will see the following page:

10. Now you can decide whether Windows should be restarted immediately or manually at a later time. Click on `[ Finish ]`

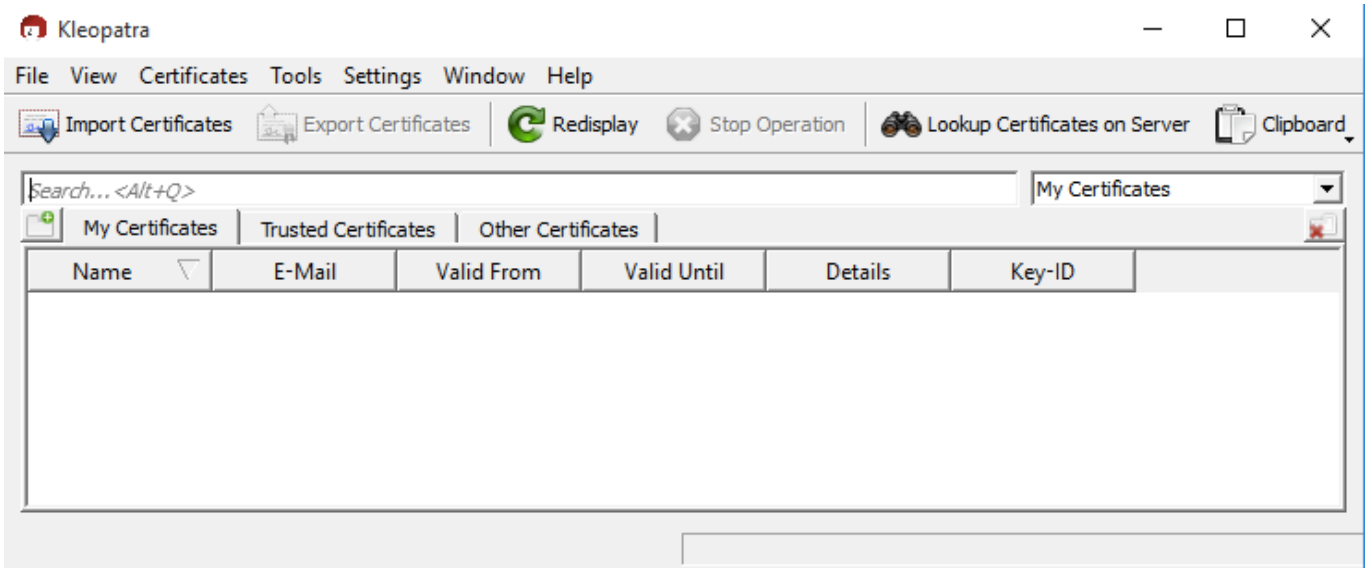
And that's it!
You have successfully installed Gpg4win and are ready to work with the program.

Create Certificate

1. Open Kleopatra using the Windows start menu:

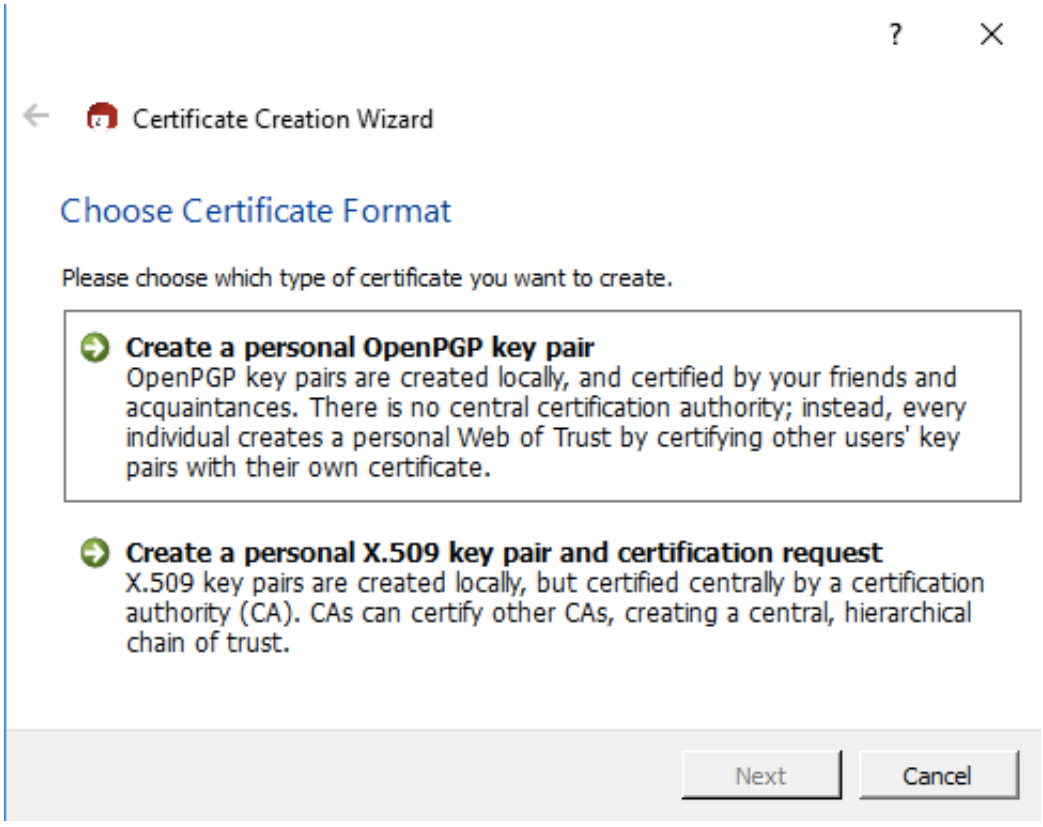


2. You will see the main Kleopatra screen – the certificate administration:



3. At the beginning, this overview will be empty, since you have not created or imported any certificates yet.
   Click on `File→New Certificate` .

4. In the following dialog you select the format for the certificate. You can choose from the following: OpenPGP (PGP/MIME) or X.509 (S/MIME).

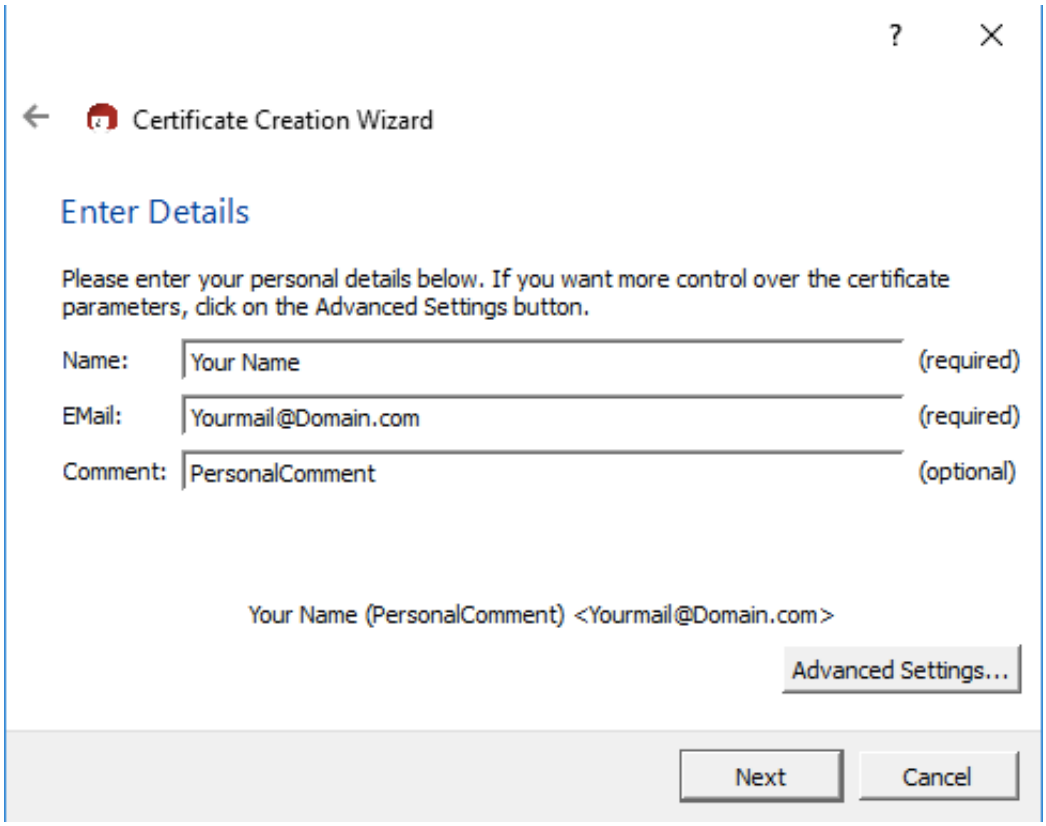


   click on `[ Create personal OpenPGP key pair ]` .

5. Now enter your e-mail address and your name in the following window. Name and e-mail address will be made publicly visible later.

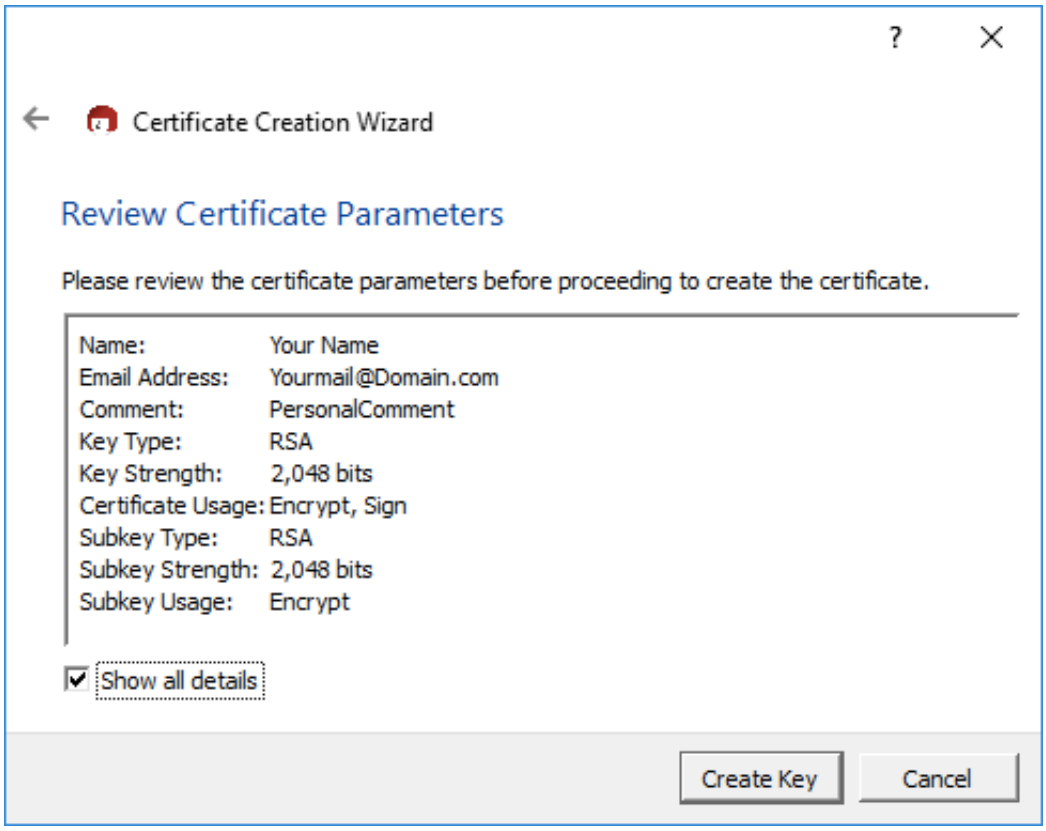
6. You also have the option of adding a comment for the key pair. Usually this field stays empty, but if you

are creating a key for test purposes, you should enter "test" so you do not forget it is a test key. This comment becomes part of your login name, and will become public just like your name and e-mail address.



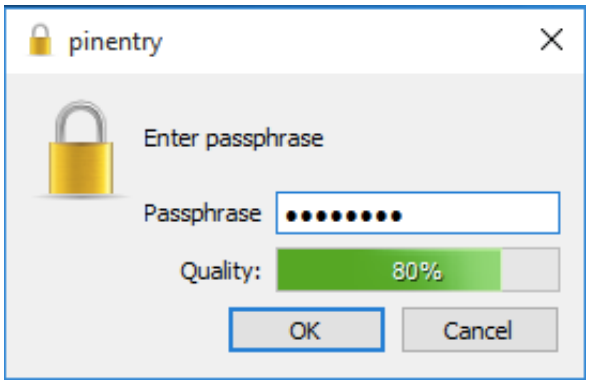
If you first wish to test your OpenPGP key pair, you can simply enter any name and fictional e-mail address, e.g.:
`Your Name` and `YourName@Domain.com`
Click on `[ Next ]`

7. You will see a list of all of the main entries and settings for review purposes. If you are interested in the (default) expert settings, you can view these via the All details option.



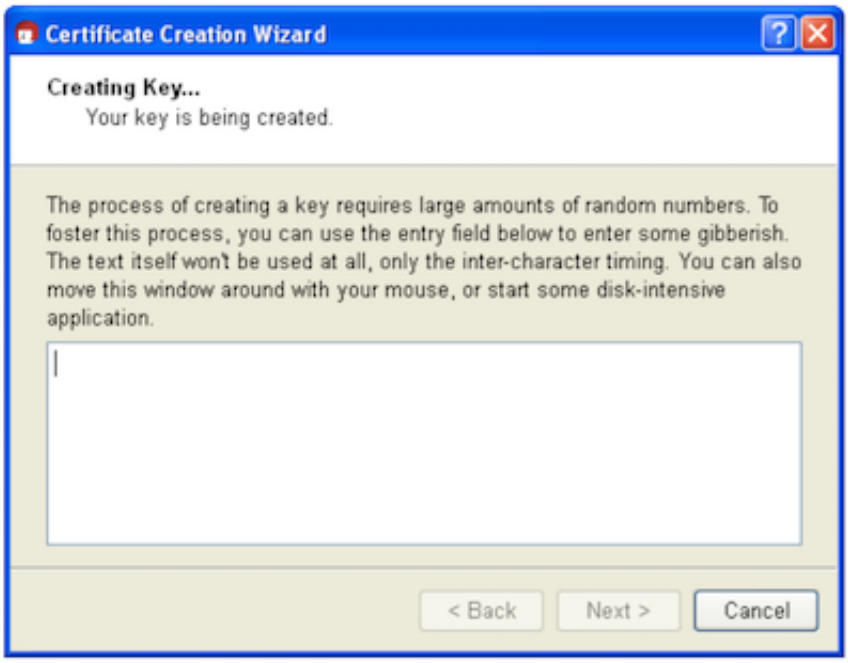
If everything is correct, click on `[ Create key ]`.

8. Now to the most important part: entering your **passphrase**!
   To create a key pair, you must enter your personal passphrase:



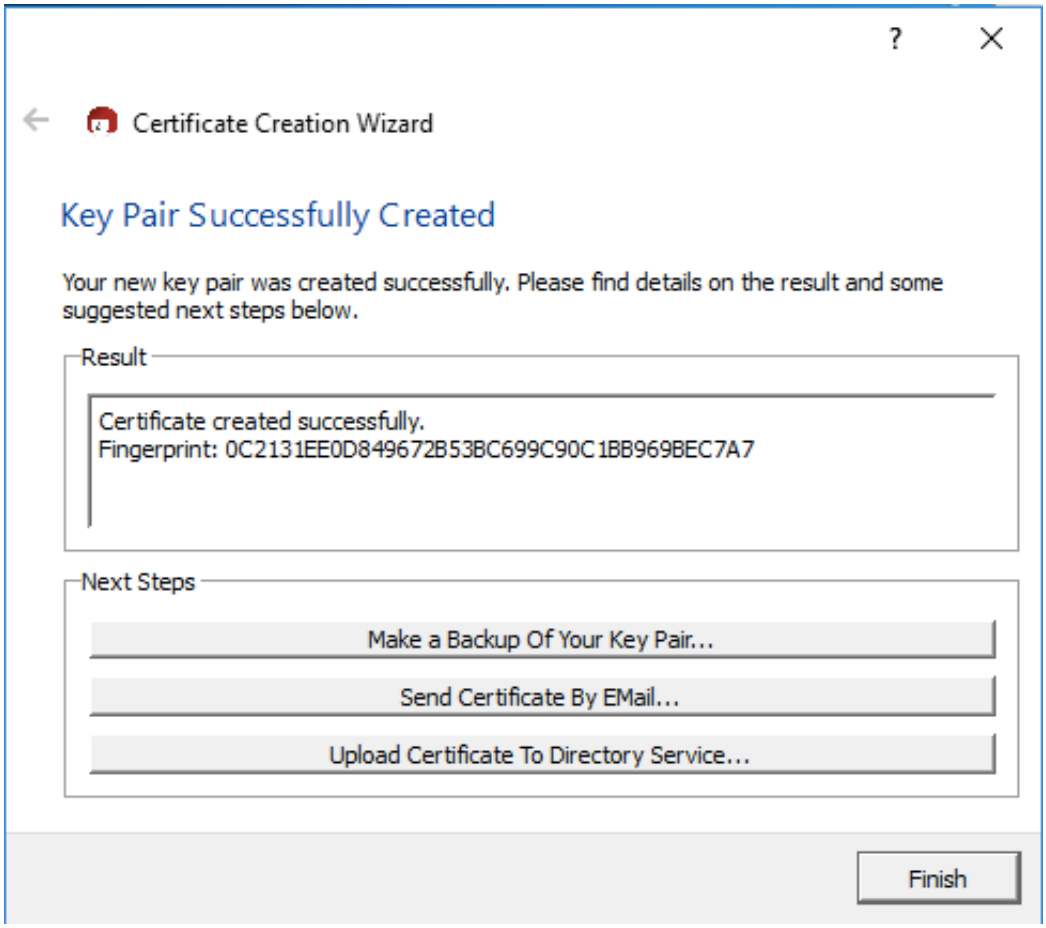
9. Choose passphrase which is easy-to-remember but hard to break secret passphrase.
   To make sure that you did not make any typing errors, the system will prompt you to enter your passphrase twice. Always confirm your entry with `[ OK ]`.

10. Now your OpenPGP key pair is being created:



This may take a couple of minutes. You can assist the creation of the required random numbers by entering information in the lower input field. It does not matter what you type, as the characters will not be used, only the time period between each key stroke. You can also continue working with another application on your computer, which will also slightly increase the quality of the new key pair.

11. As soon as the key pair creation has been successful, you will see the following dialog:



The 40-digit “fingerprint” of your newly generated OpenPGP certificate is displayed in the results text field. This fingerprint is unique anywhere in the world, i.e. no other person will have a certificate with

the same fingerprint. Actually, even at 8 digits it would already be quite unlikely that the same sequence would occur twice anywhere in world. For this reason, it is often only the last 8 digits of a fingerprint which are used or shown, and which are described as the key ID. This fingerprint identifies the identity of the certificate as well as the fingerprint of a person.

12. However, you do not need to remember or write down the fingerprint. You can also display it later in Kleopatra's certificate details.

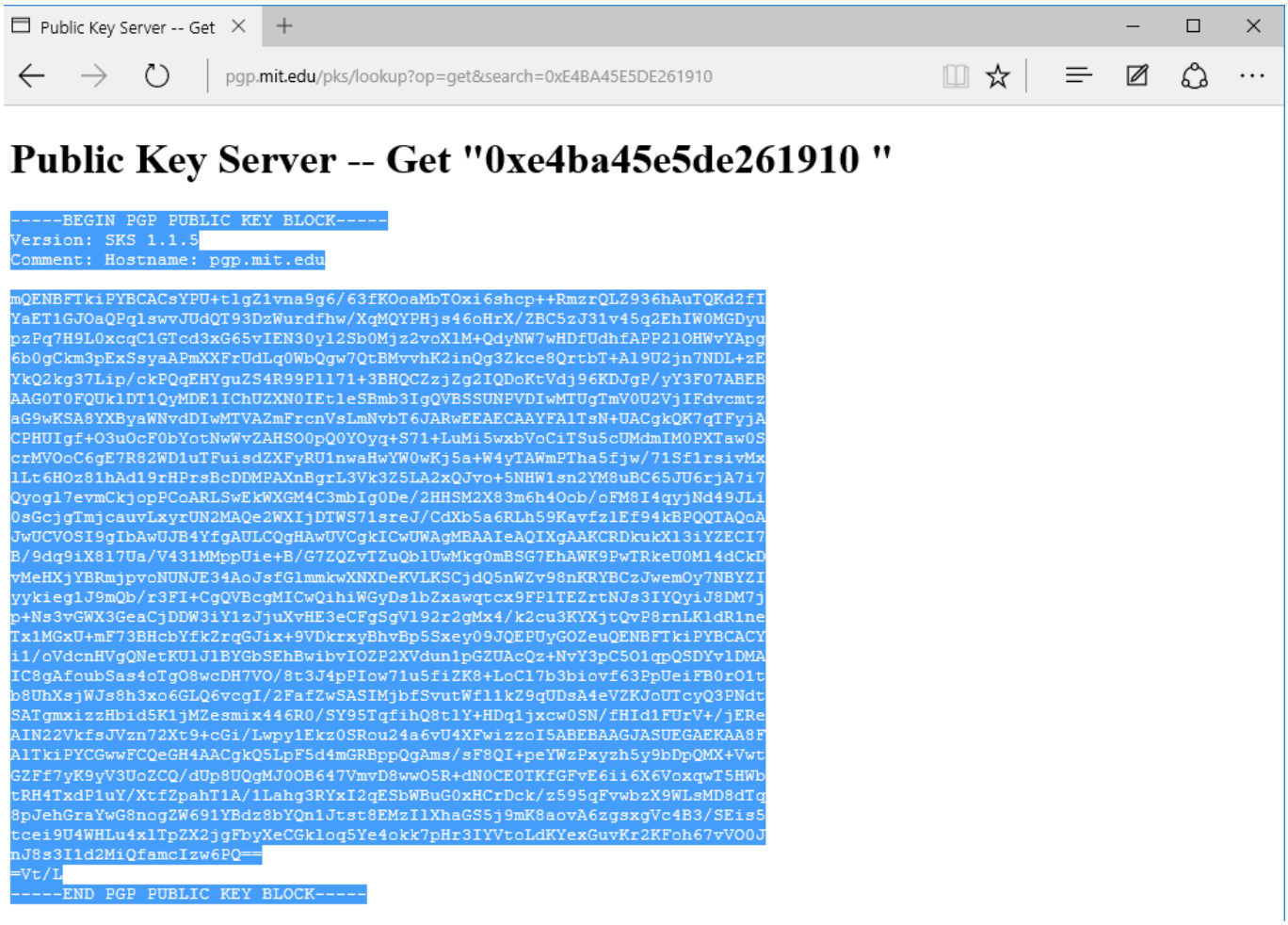
To send eccrypted mail you need to have receiver public key

To decrypt mail you need to upload your key to keyserver or send your public key to the sender

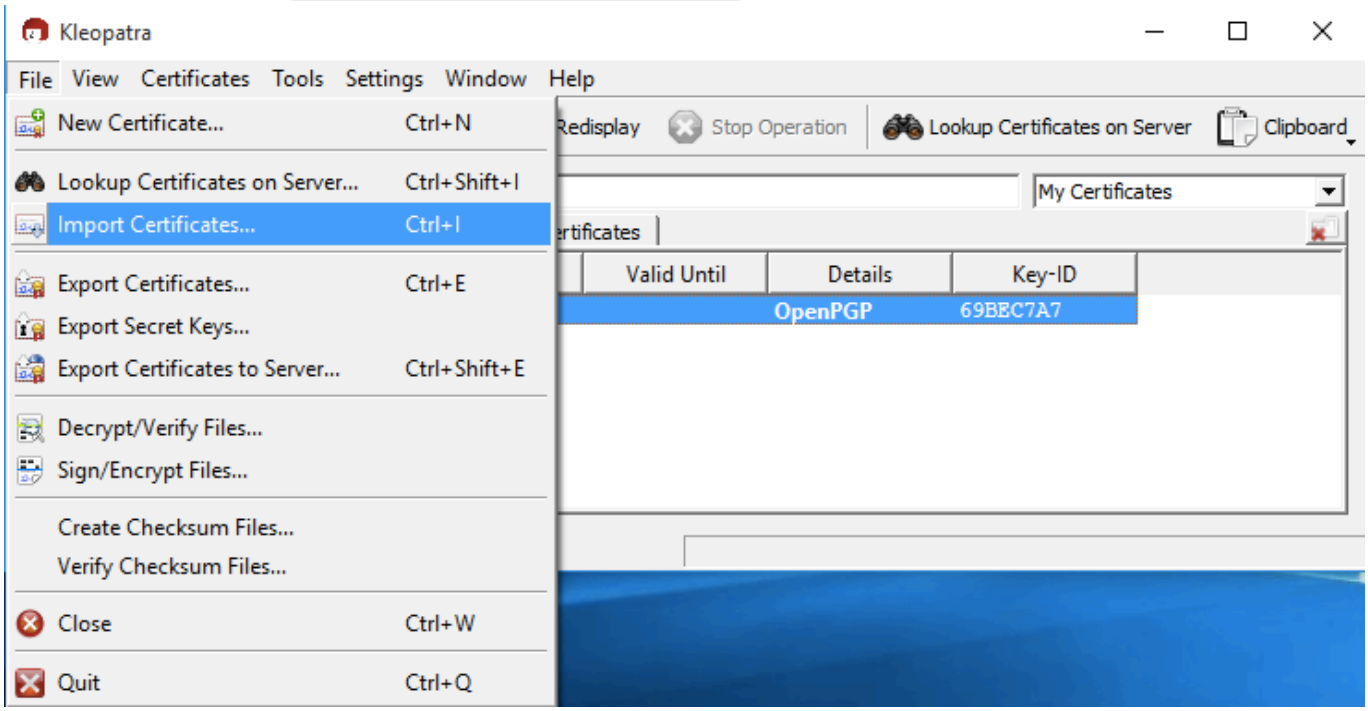
---

Import Public Key from Key Server

1. Open any browser and go to `http://pgp.mit.edu/`
2. In `Search String` field type email address for the correspondence public key and click `Do the search!`
3. You will get the list of key/keys with KeyID. KeyID is the last 8 digit of fingerprint.
4. Click on KeyID.
5. Copy from `-----BEGIN PGP PUBLIC KEY BLOCK-----` till `-----END PGP PUBLIC KEY BLOCK-----`. Save it in a file.

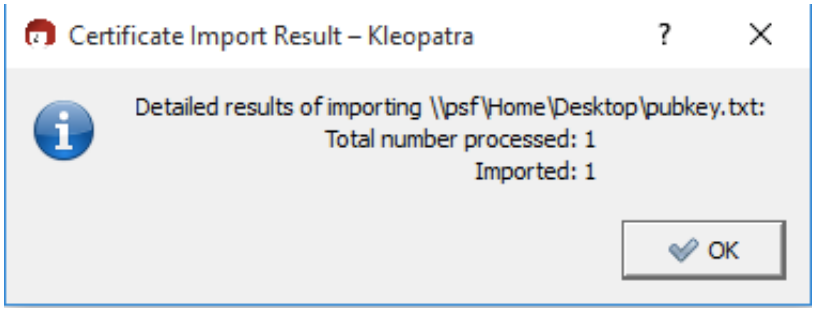


6. Now go to Kleopatra `File->Import Certificate`



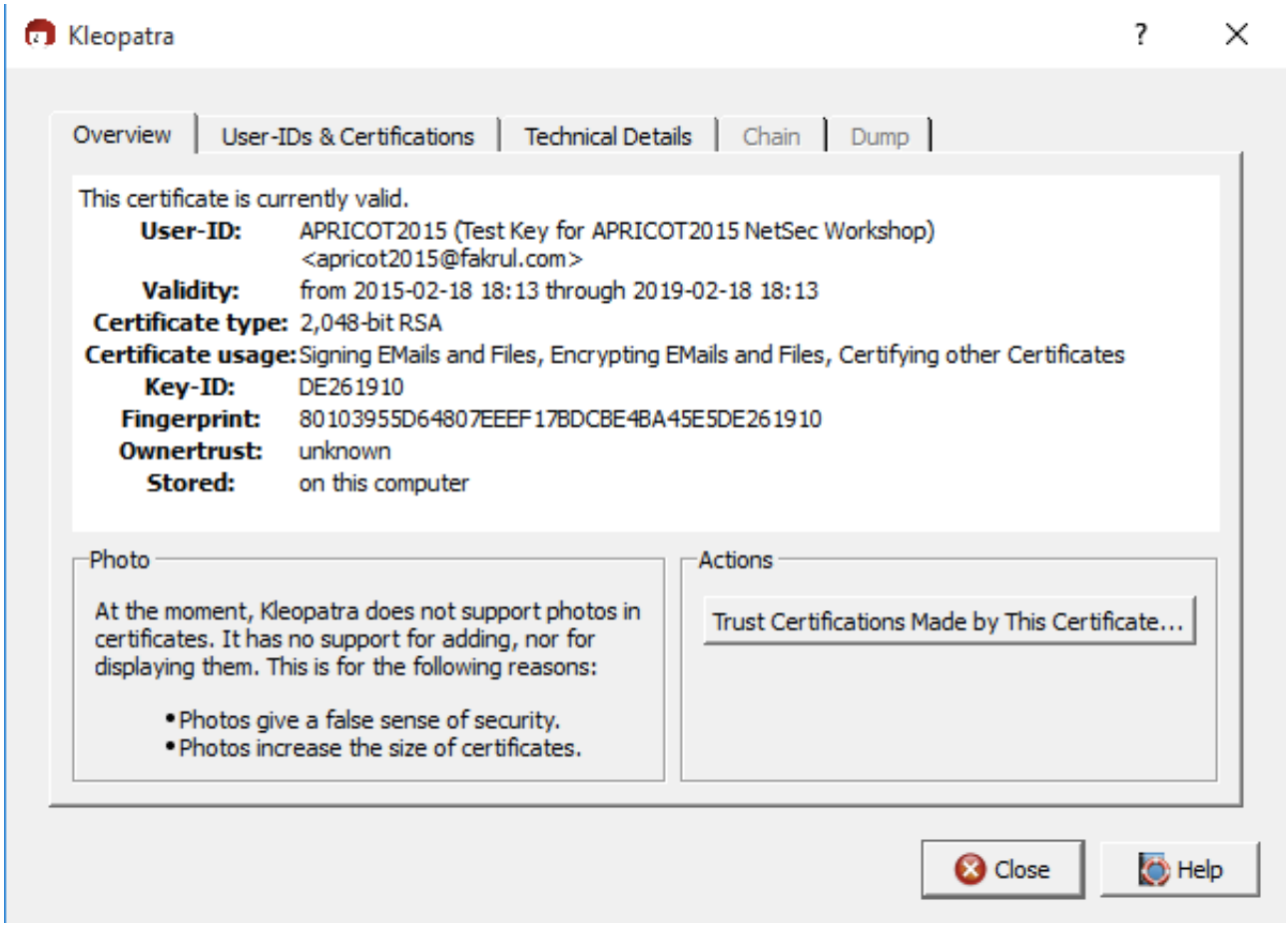
7. Browse the previoulsy saved public key and import it.

8. After successful inport it will show following message:



9. You will get those imported public key under `Imported Certificate` tab.

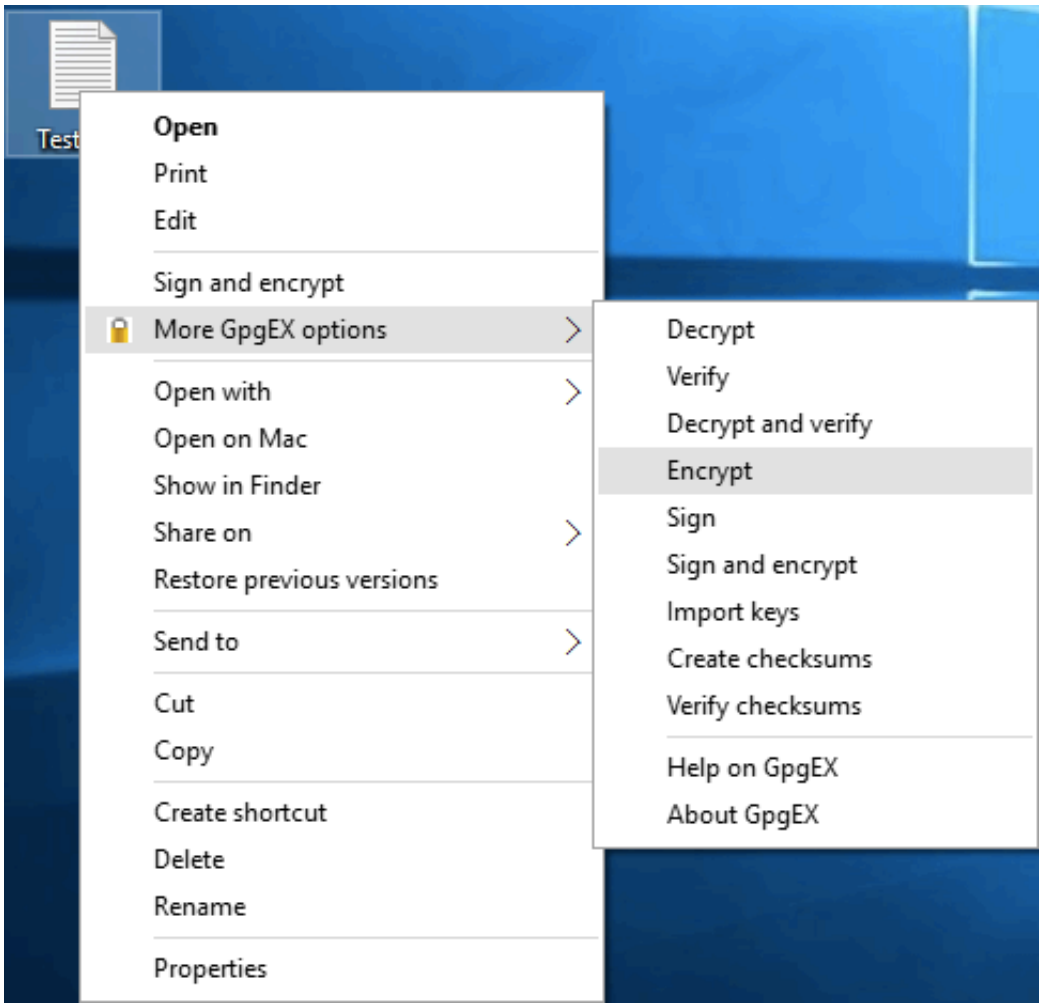
10. Double click on any key will open new window and show the key details which include Validity and Fingerprint.



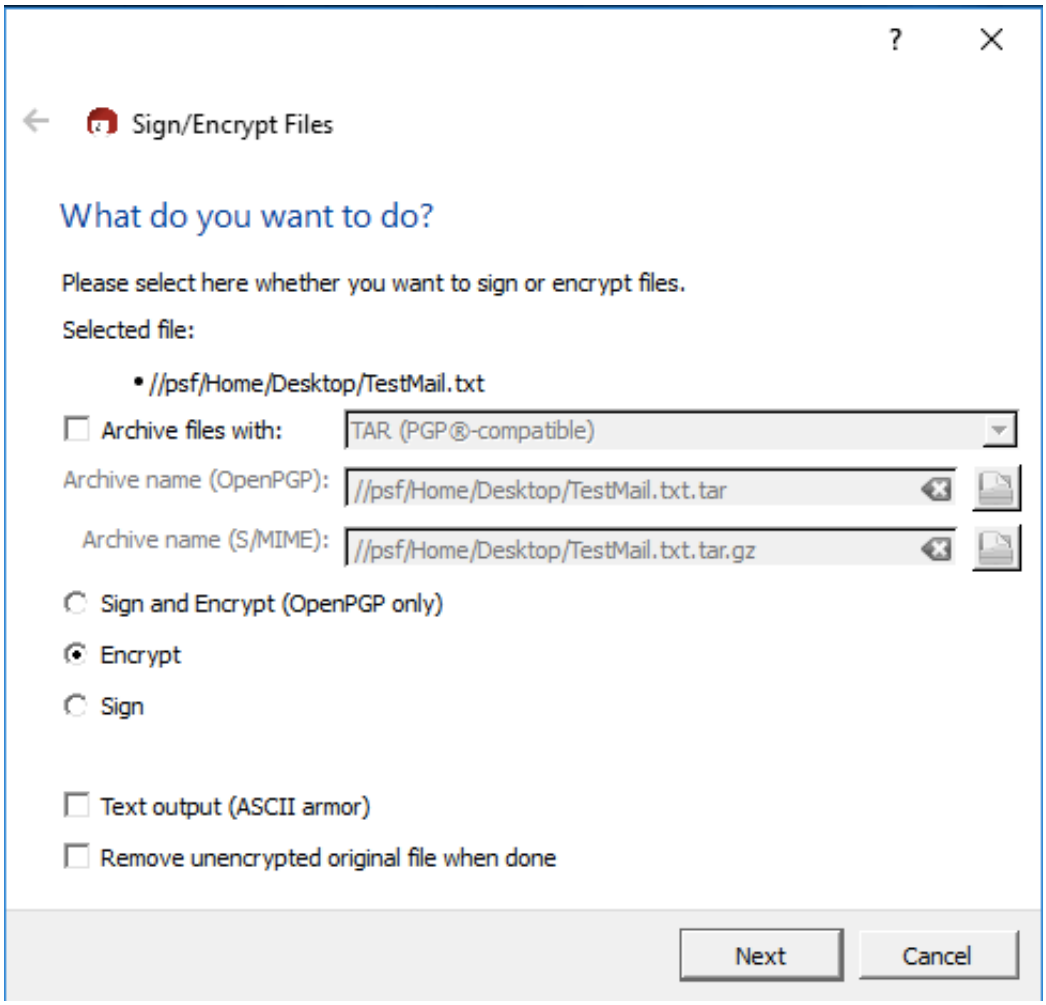
Encrypt Message

1. Create one new text file and type some message.

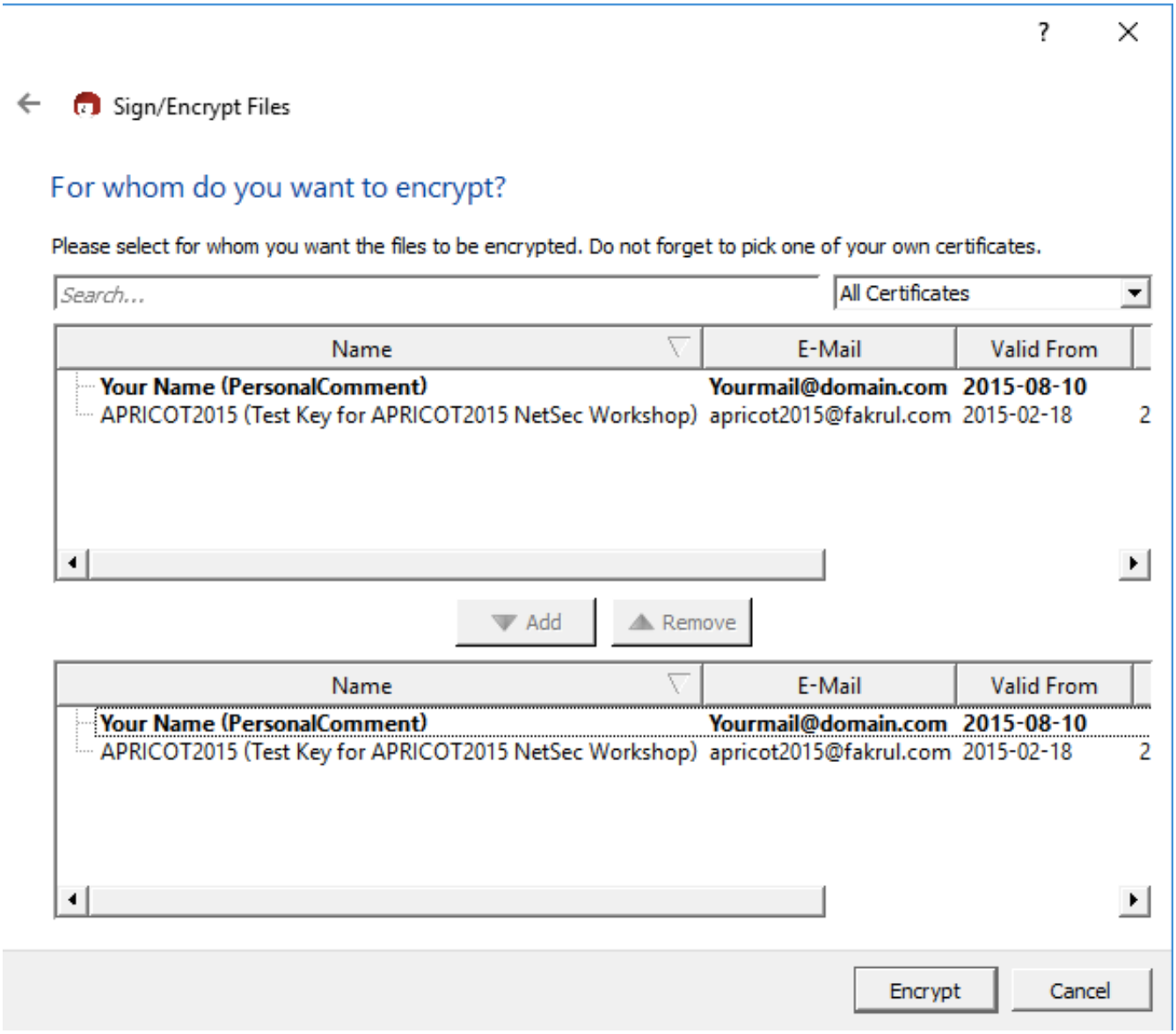
2. Select file; right mouse click and choose `More GpgEX Options -> Encrypt`



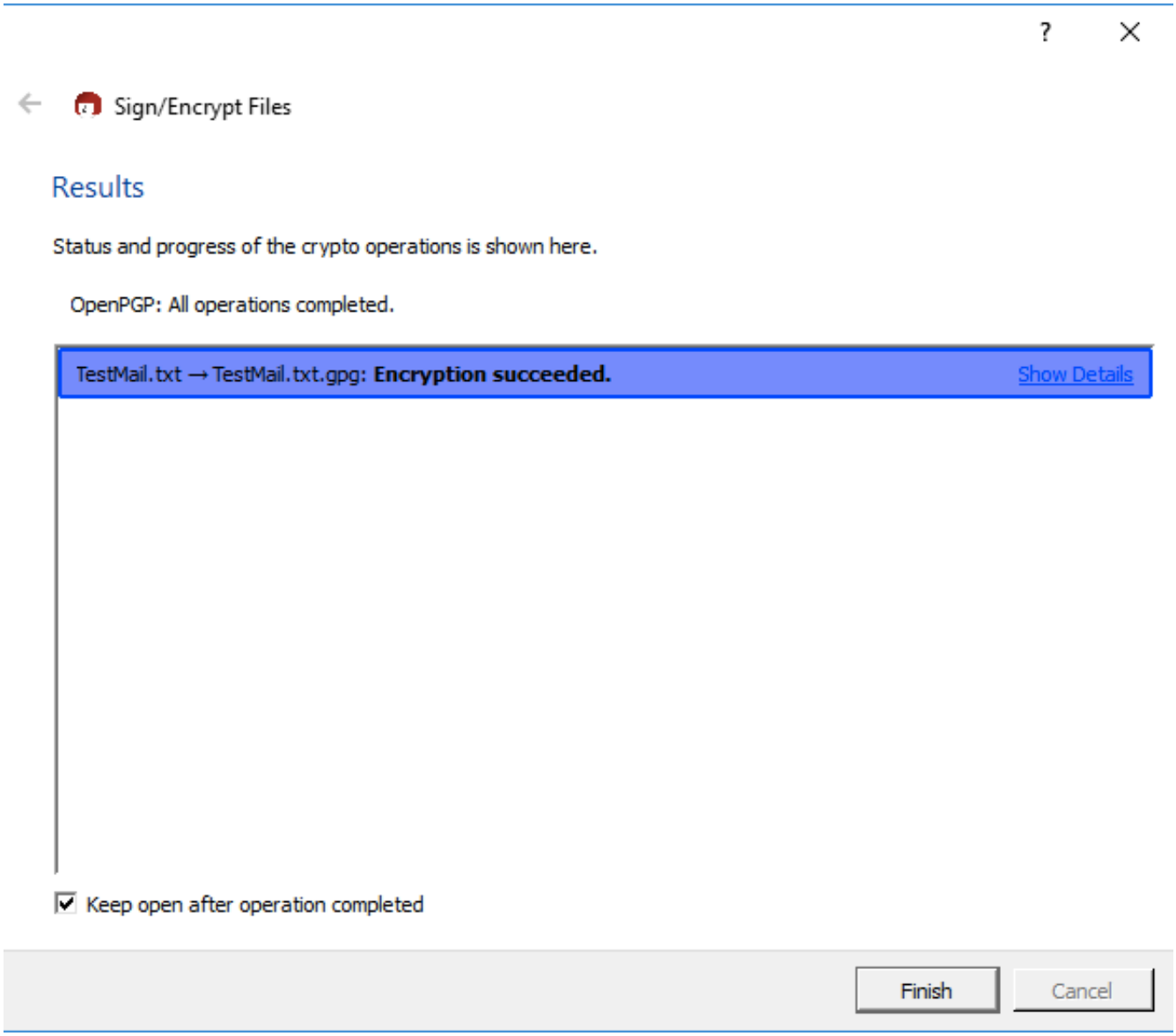
3. Next window will give you some extra option; we will procede with `Next`



4. Choose correspondence public key and choose `Add` and click `Encrypt`



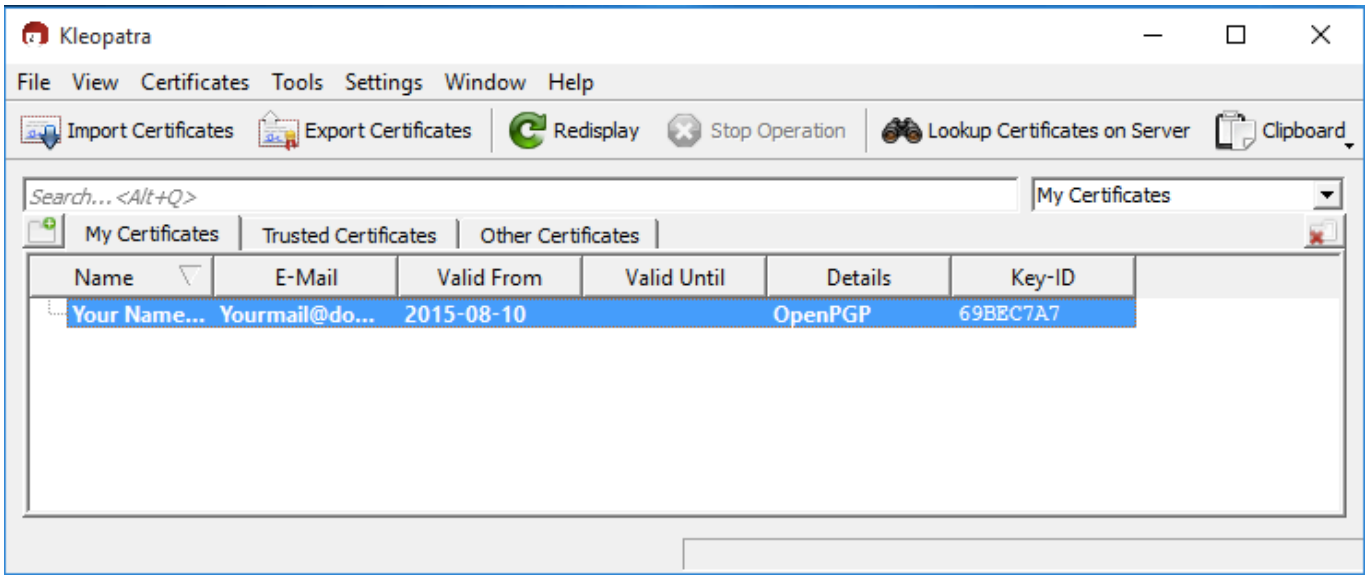
5. After encryption you will get `Encryption succeeded` message. This will also create another new file in same location with the extension of `.gpg`



6. Attach this file as email attachment and send it to the receiver.

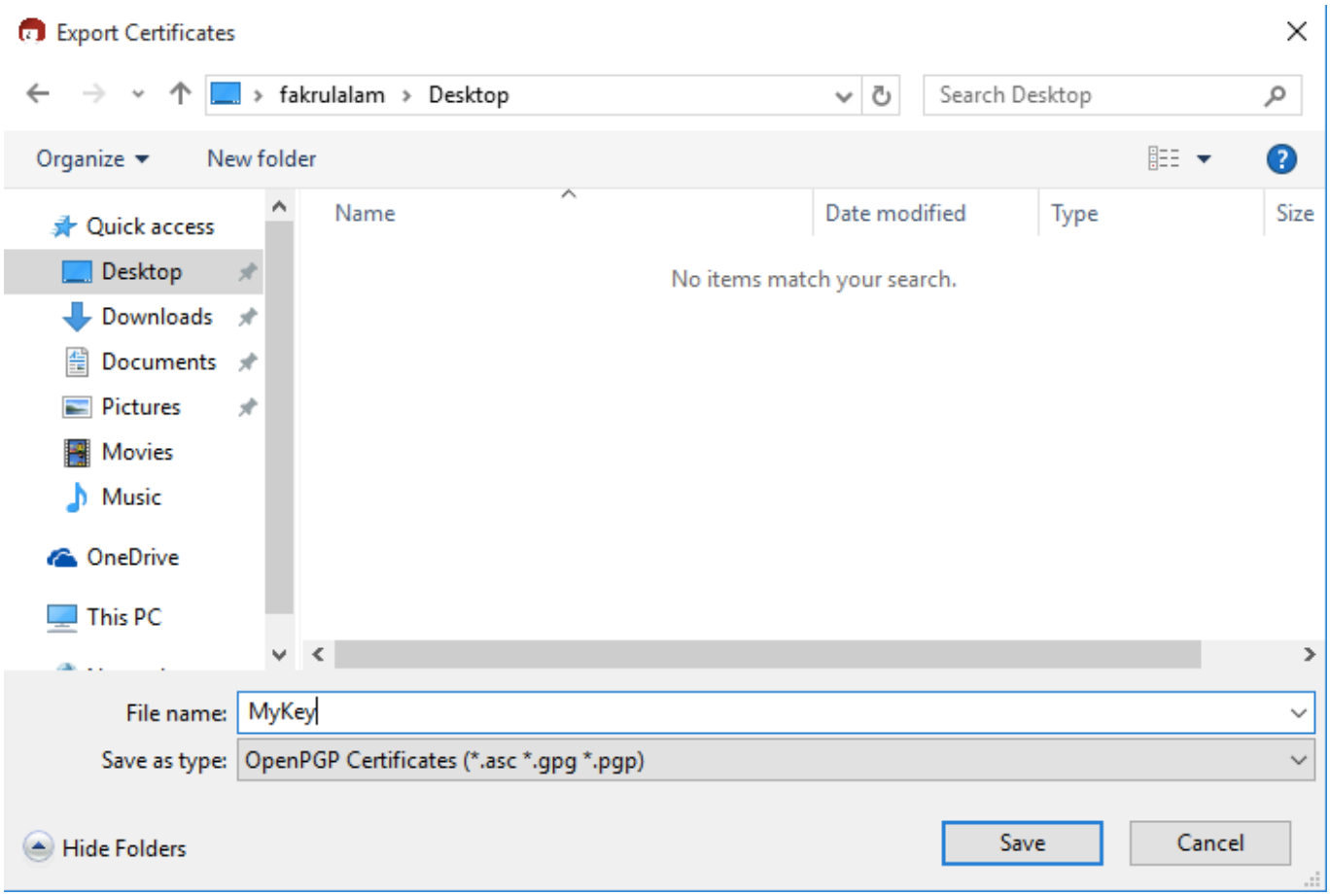
Export certificate (public key):

1. Open Kleopatra or if it's running you will see your key under My Certificates dashboad:

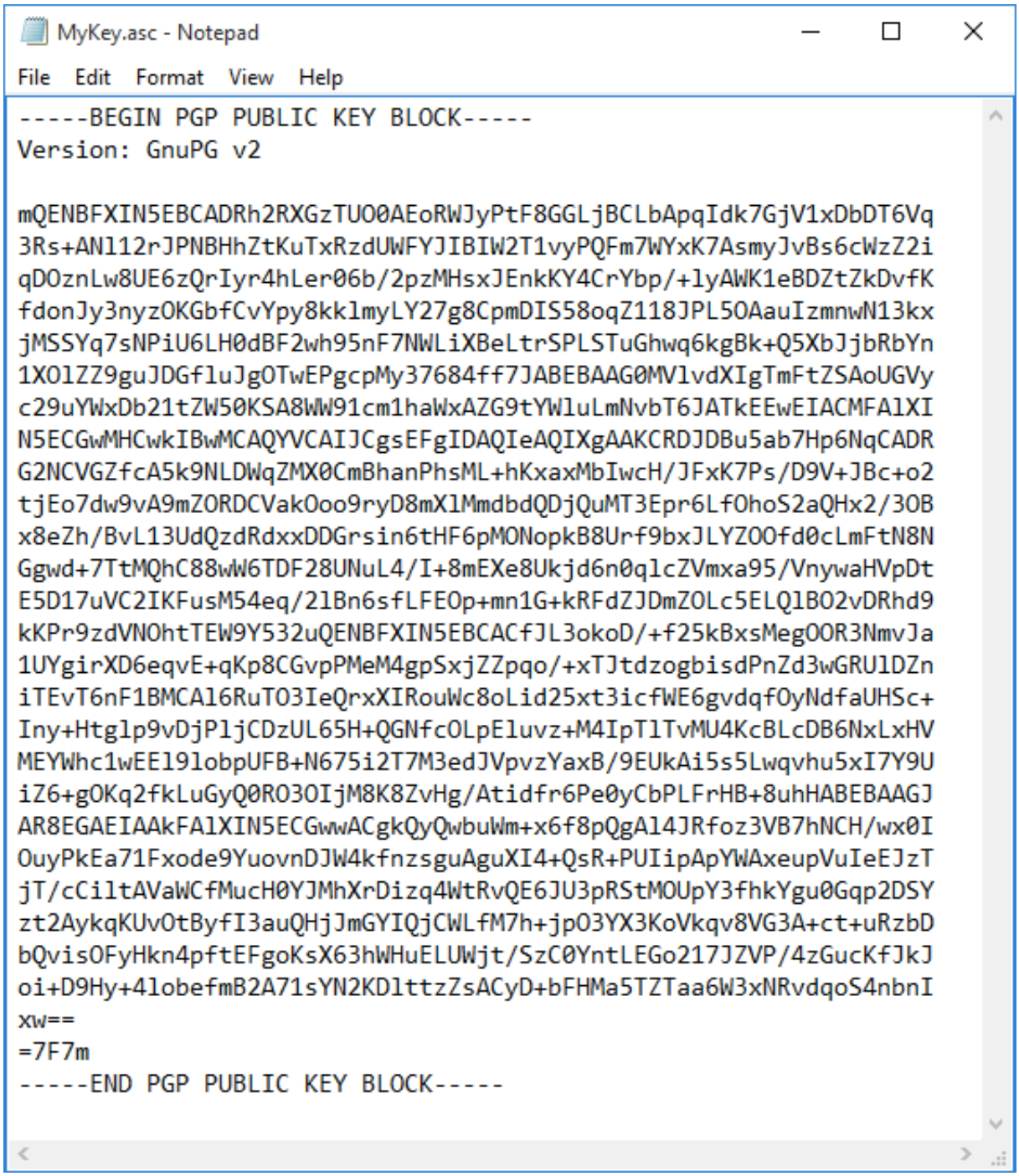


Right mouse click on your key and choose `Export Certificate` .

2. Choose your prefered location and name it with your key and save.



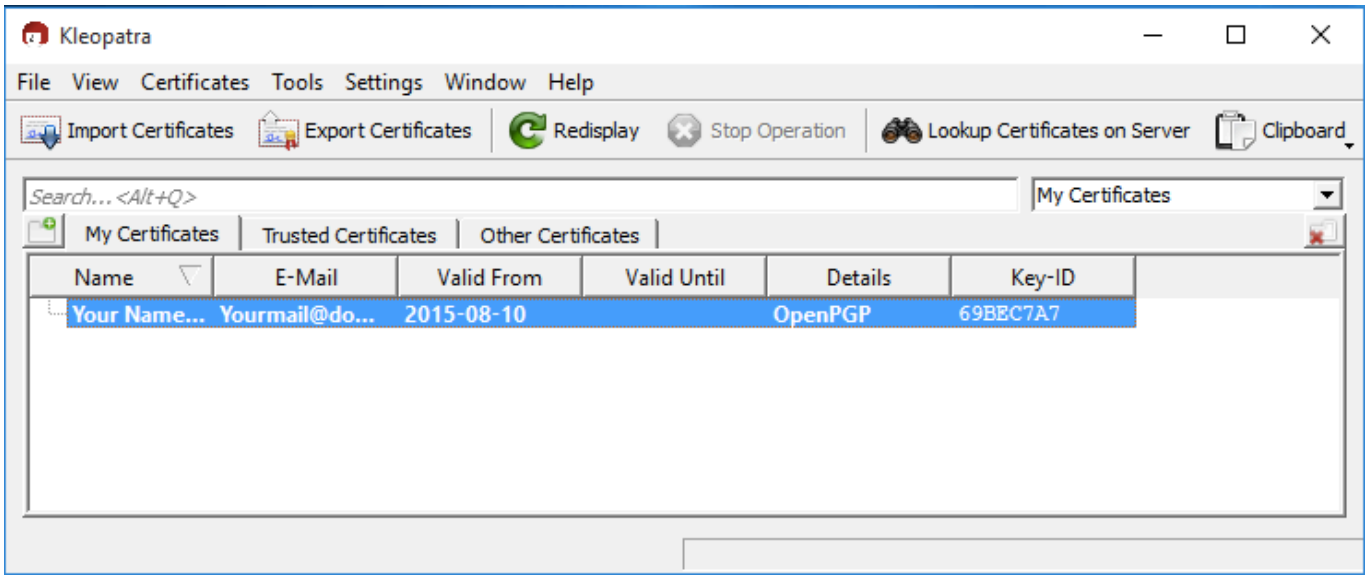
3. You can open it in notepad and look like:



This is your public key. You can share this key with outher via email or upload it to key server.

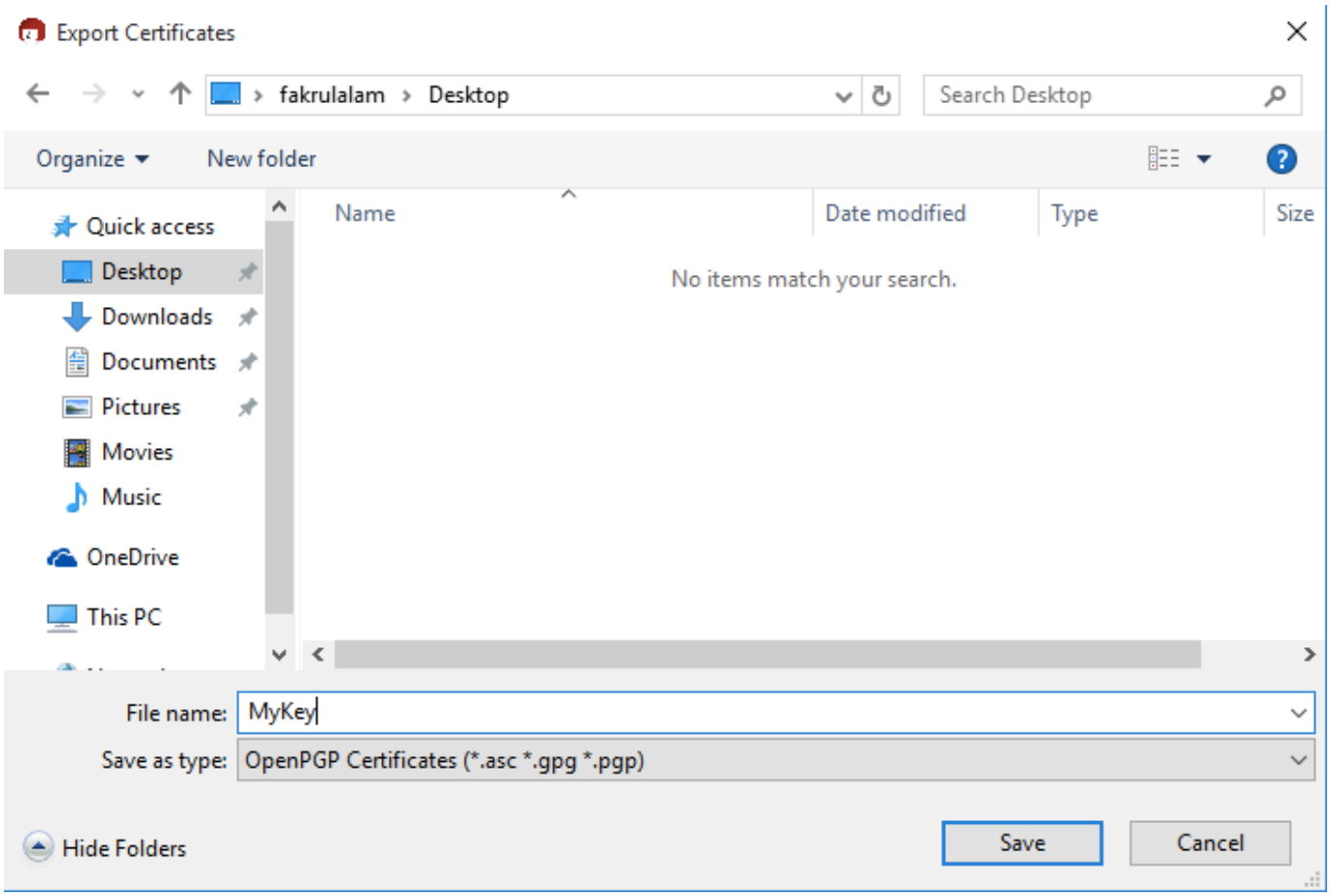
Export certificate (public key):

1. Open Kleopatra or if it’s running you will see your key under My Certificates dashboad:

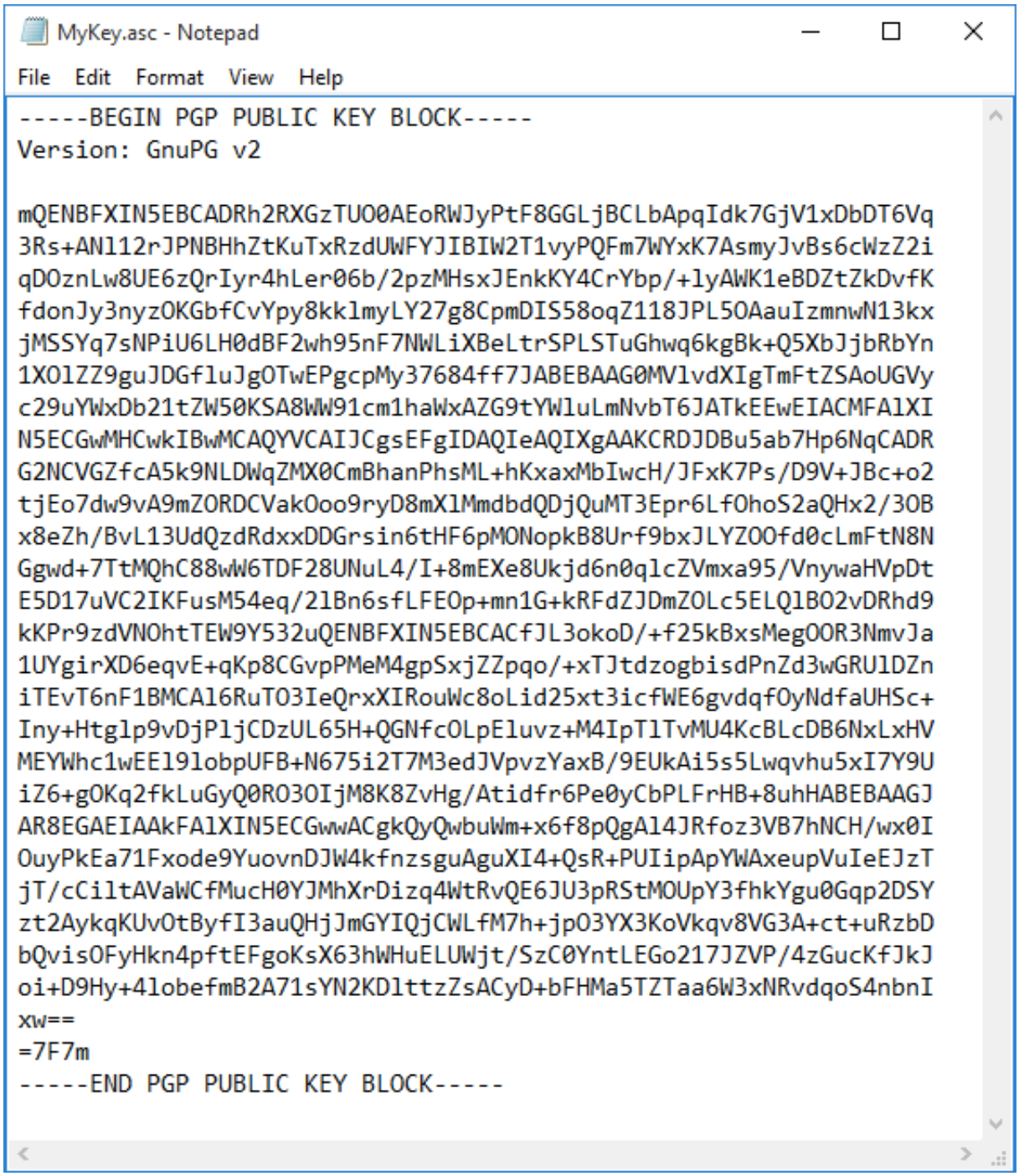


Right mouse click on your key and choose `Export Certificate` .

2. Choose your prefered location and name it with your key and save.



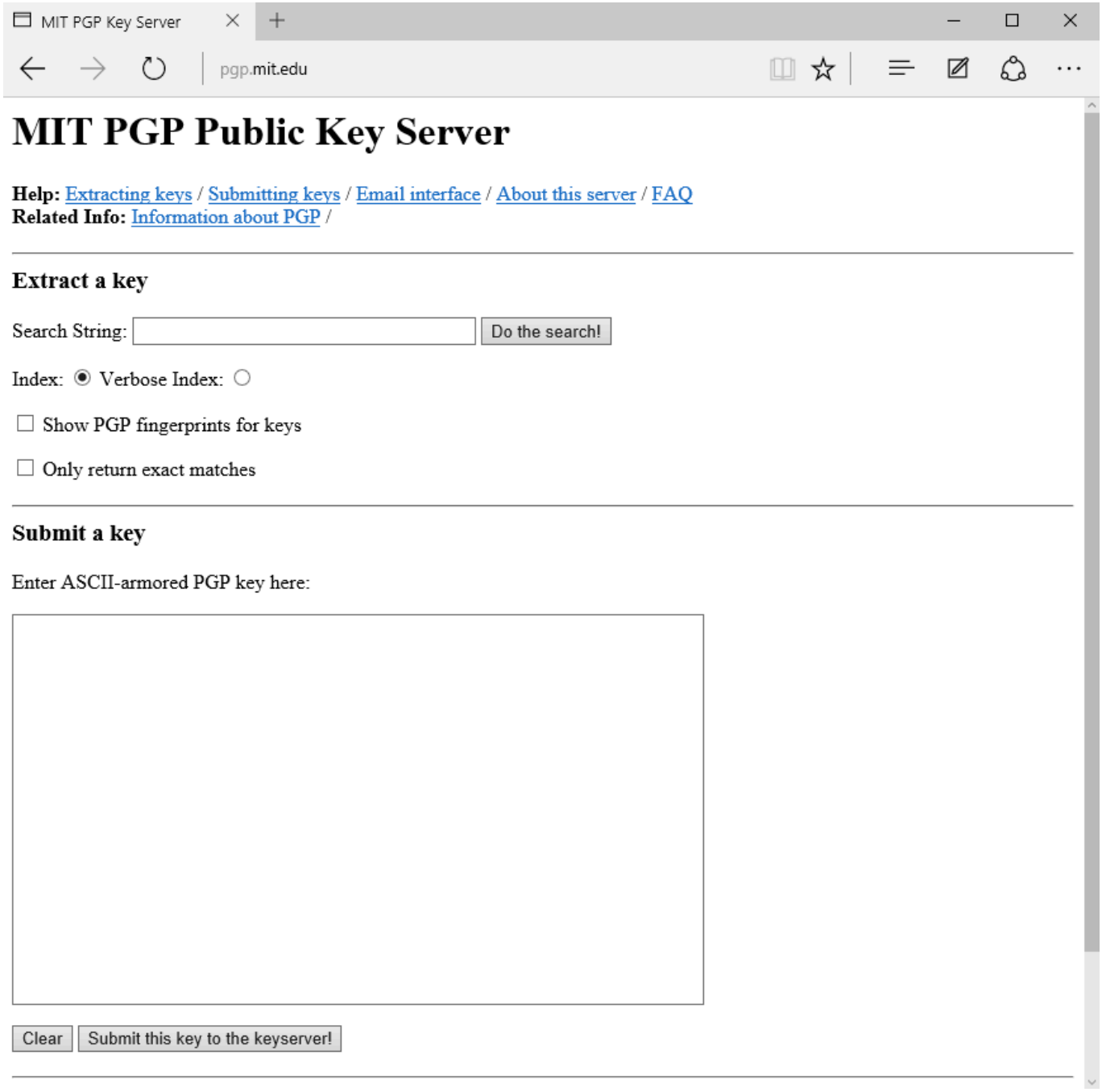
3. You can open it in notepad and look like:



This is your public key. You can share this key with outher via email or upload it to key server.

Upload key to Key Server

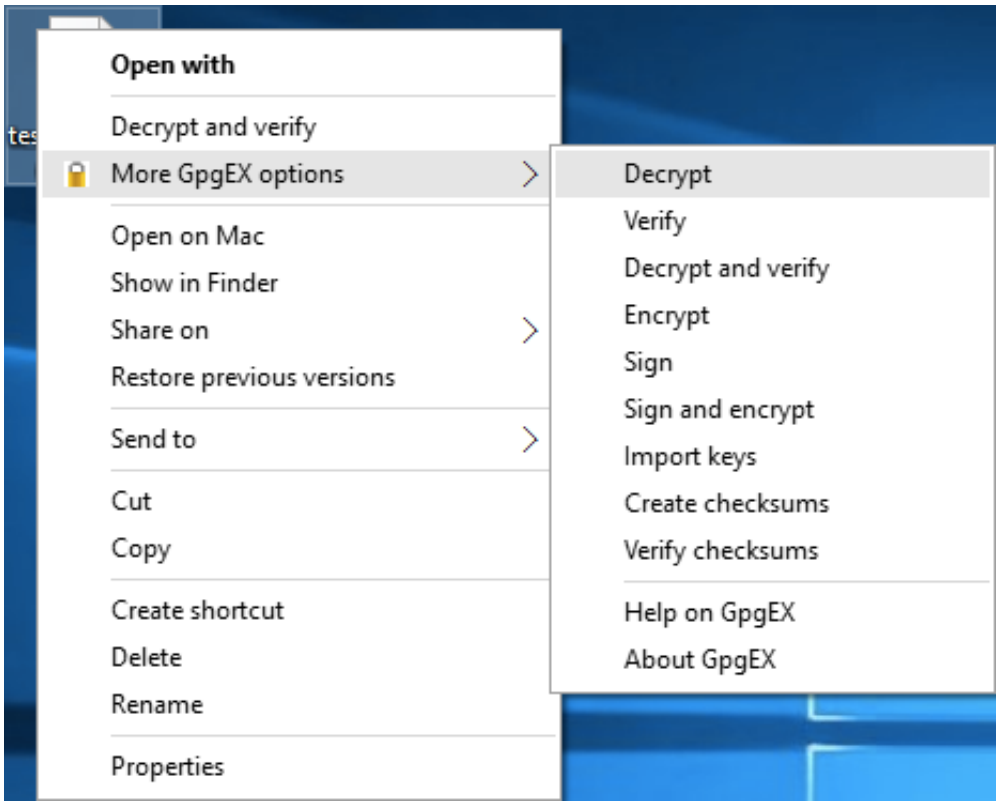
1. Open your previously saved public key using notepad. Copy the full text.
2. Open any browser and go to `http://pgp.mit.edu/`
3. Past your key in `Submit a key` and click `Submit this key to the keyserver!`



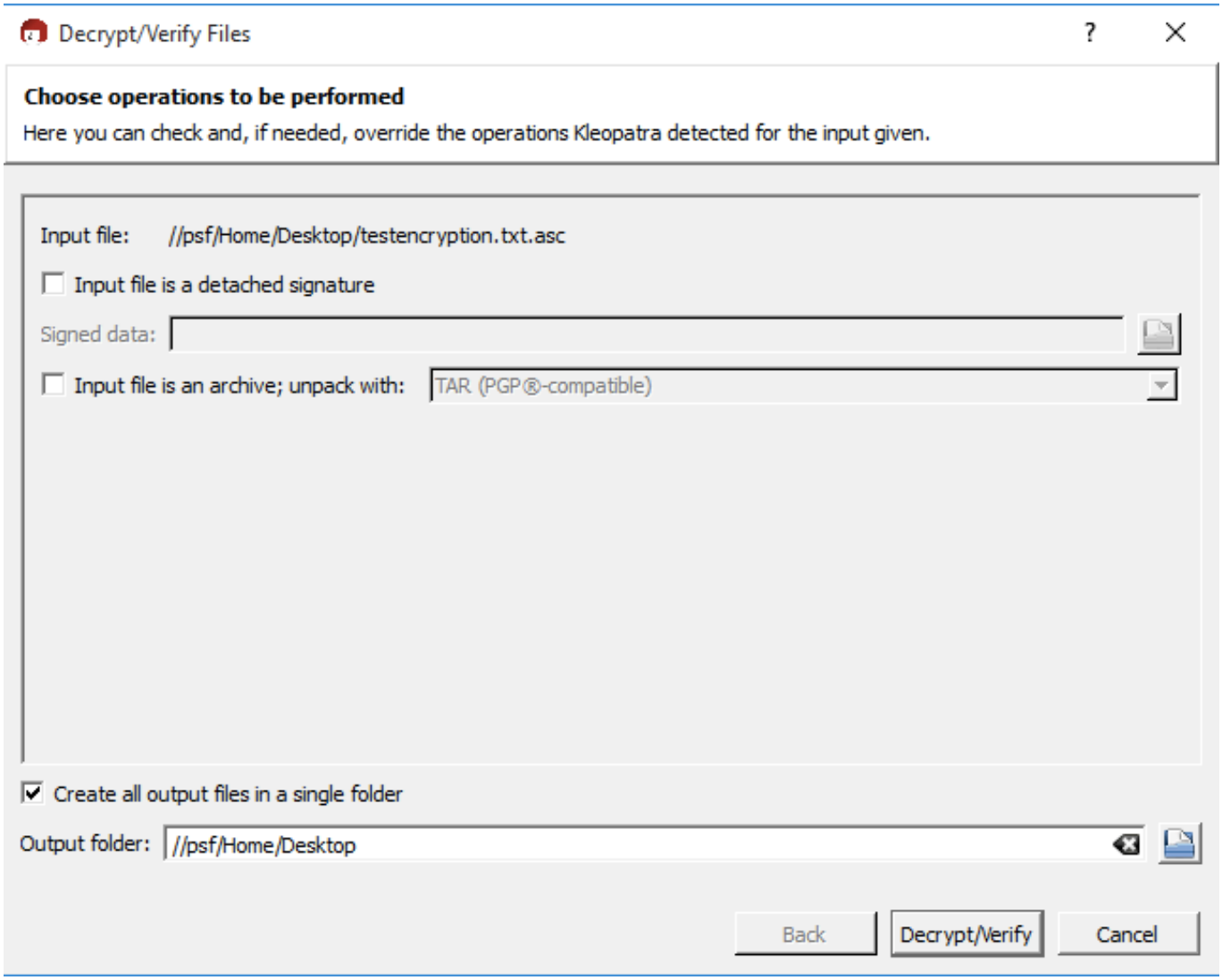
4. From `http://pgp.mit.edu/` you can search for you key or any other uploaded key.
5. Please note that you can't delete/remove any uploaded public key from key server. You can only revoke them.

Decrypt Message

1. Save the encrypted file.
2. Right mouse click choose `More GpgEX Options -> Decrypt`

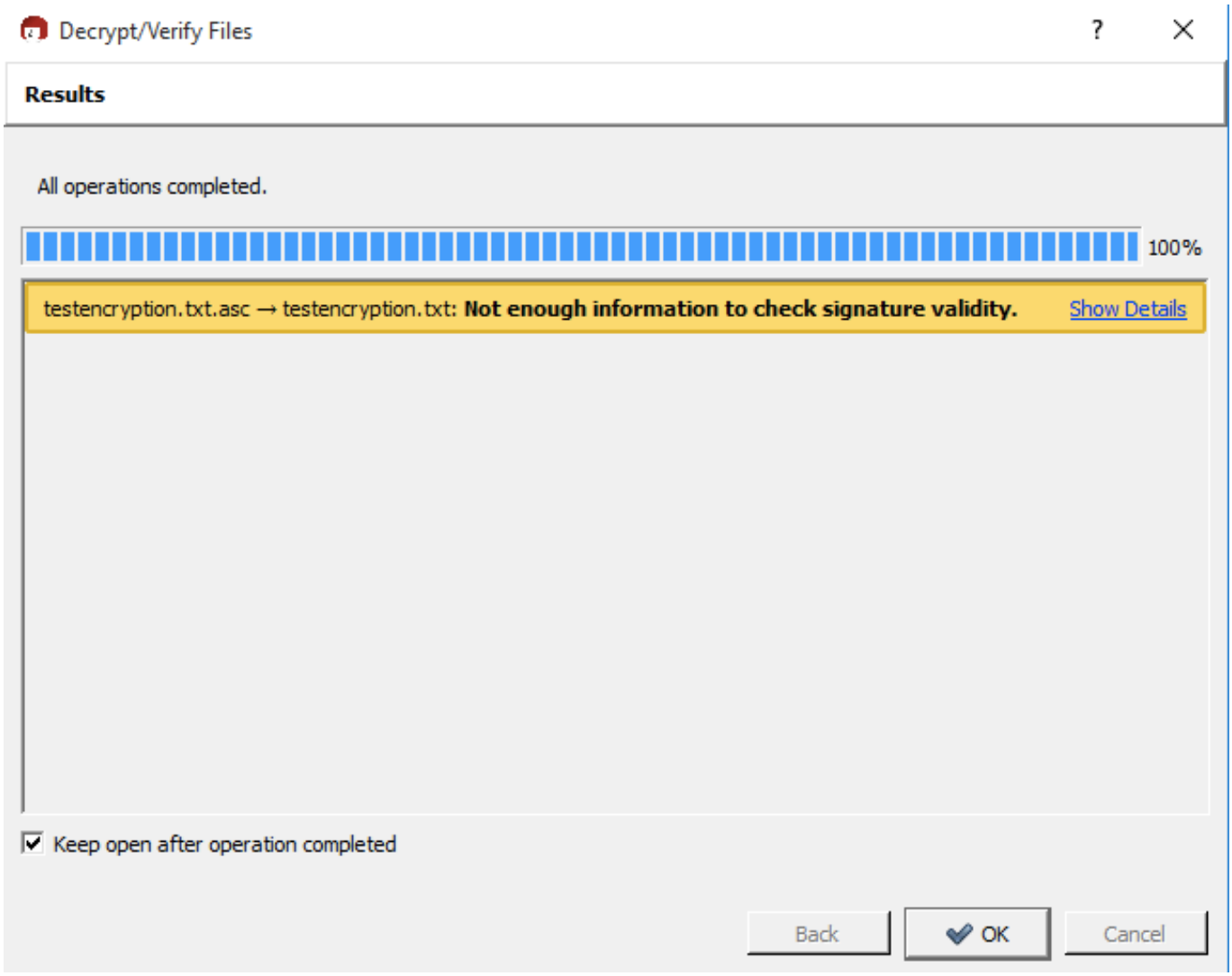


3. Next window will give you some infomation regarding input file location and output file location.



4. You will be asked for passphrase.

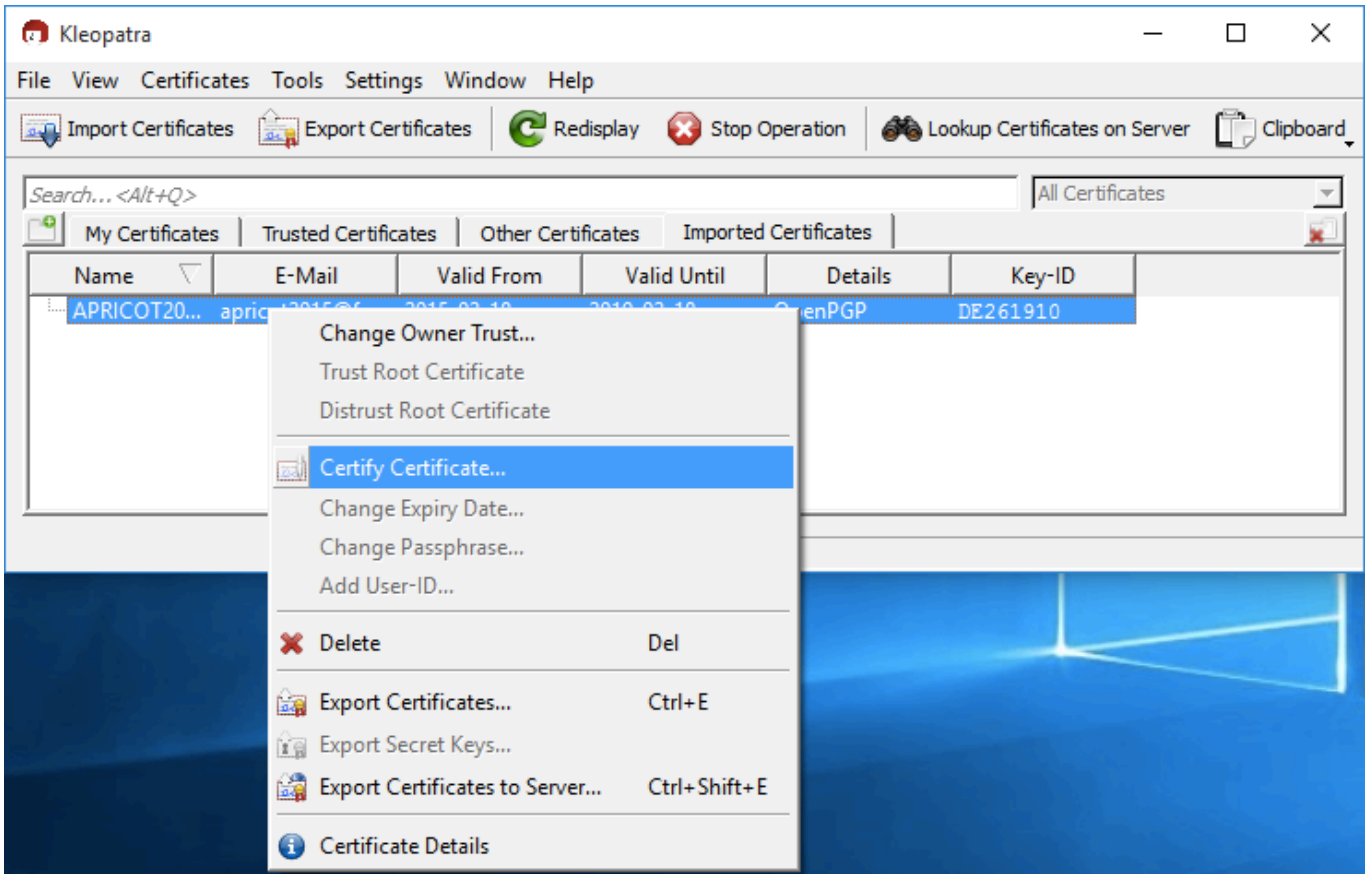
5. If your private key passphrase match; it will decrypt the file and you will get following confirmation:



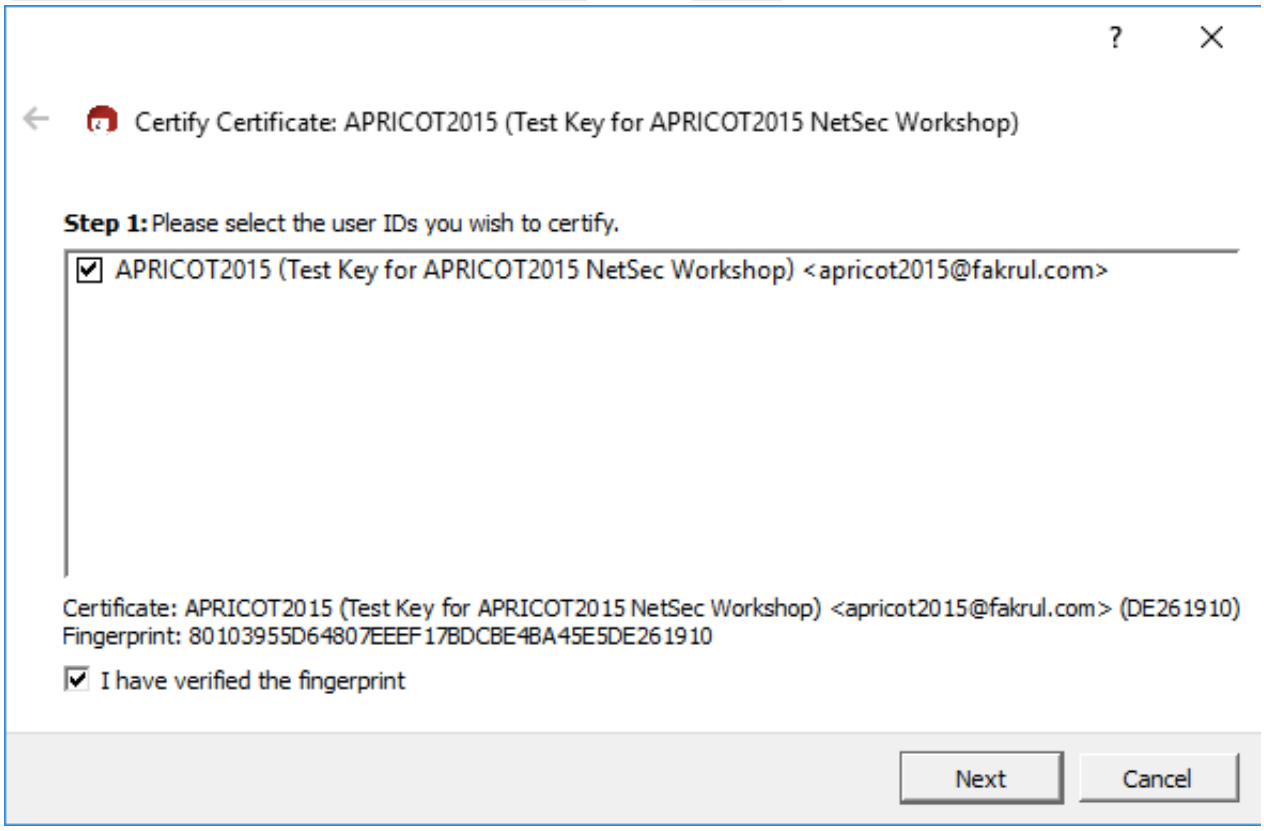
6. Now you get the plain text; open it using any text editor.

Sign other Public Key

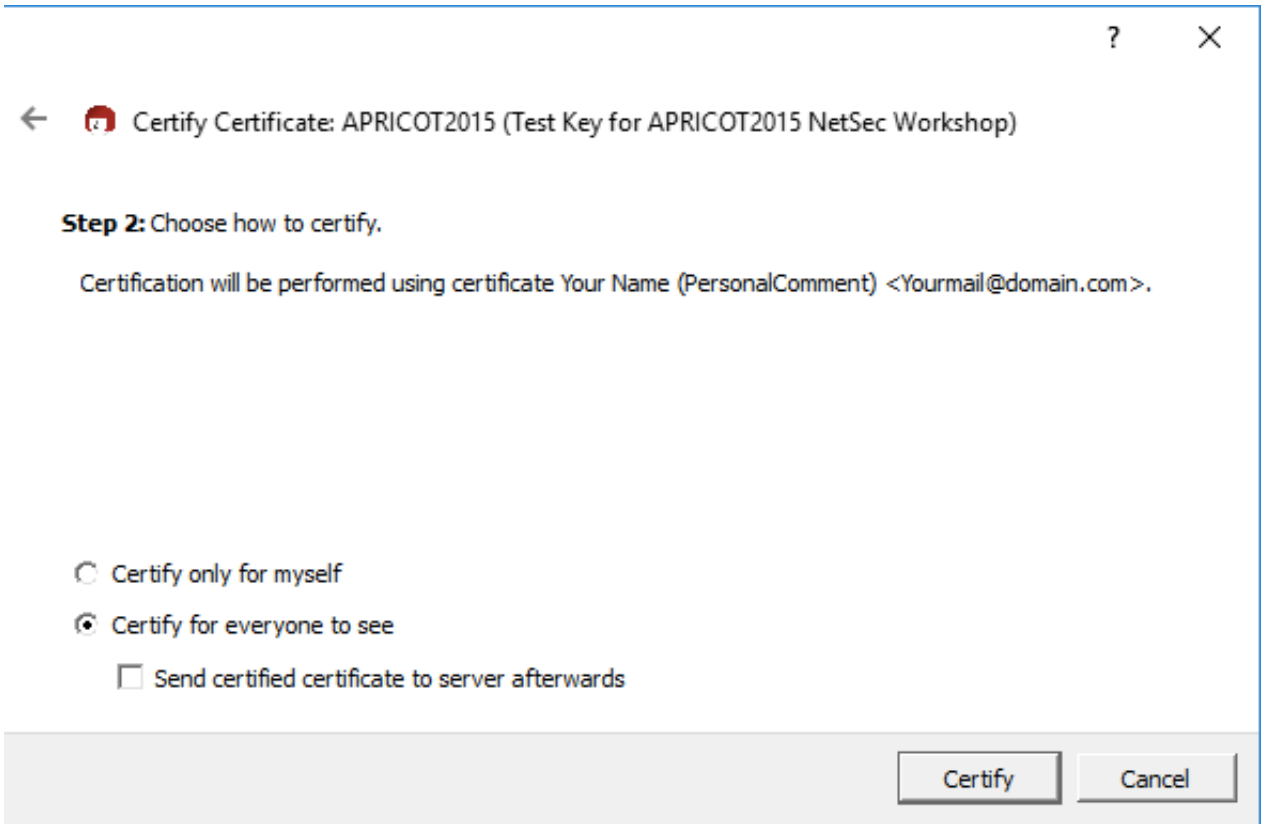
1. Go to `Imported Certificates` tab of Kleopatra.
2. Right mouse click and choose `Certify Certificate` for the key which you want to sign.



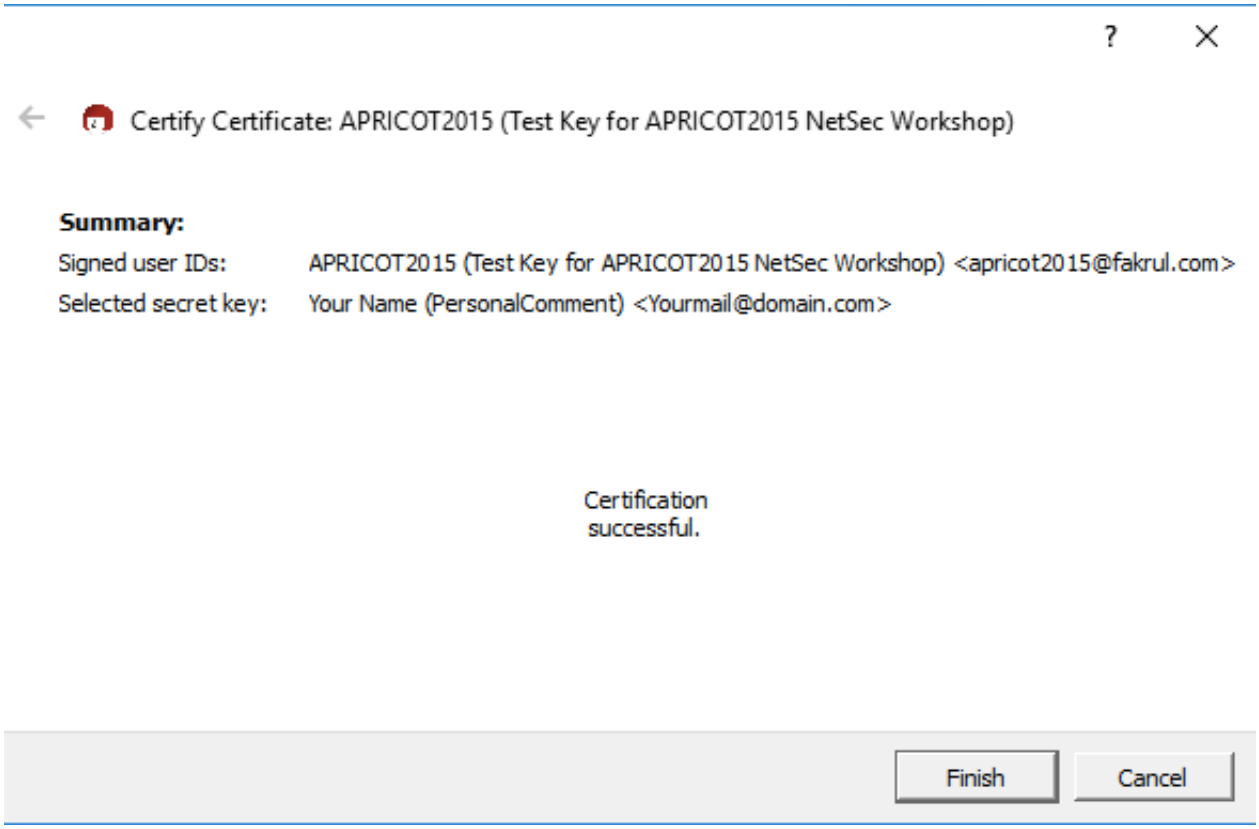
3. Choose the Key you want to certifiy. Carefully check the fingerprint and click `I have verified the fingerprint`. Click `Next`



4. Choose the option `Certify for everyone to see` option. You can disable `Send certified certificate to server afterwards`. Click `Next`.



5. You will be aksed for passphrase of your Pricate Key.
6. After successfuly sing; it will show confirmation message. Click `Finish` .



7. Now you can export this publc key and upload it to key server.

Few Reference Link:

How to: Use PGP for Windows PC (GPG4Win; Mozilla Thunderbird; Enigmail)
https://ssd.eff.org/en/module/how-use-pgp-windows-pc

```
***END OF EXERCISE***
```