

# 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.

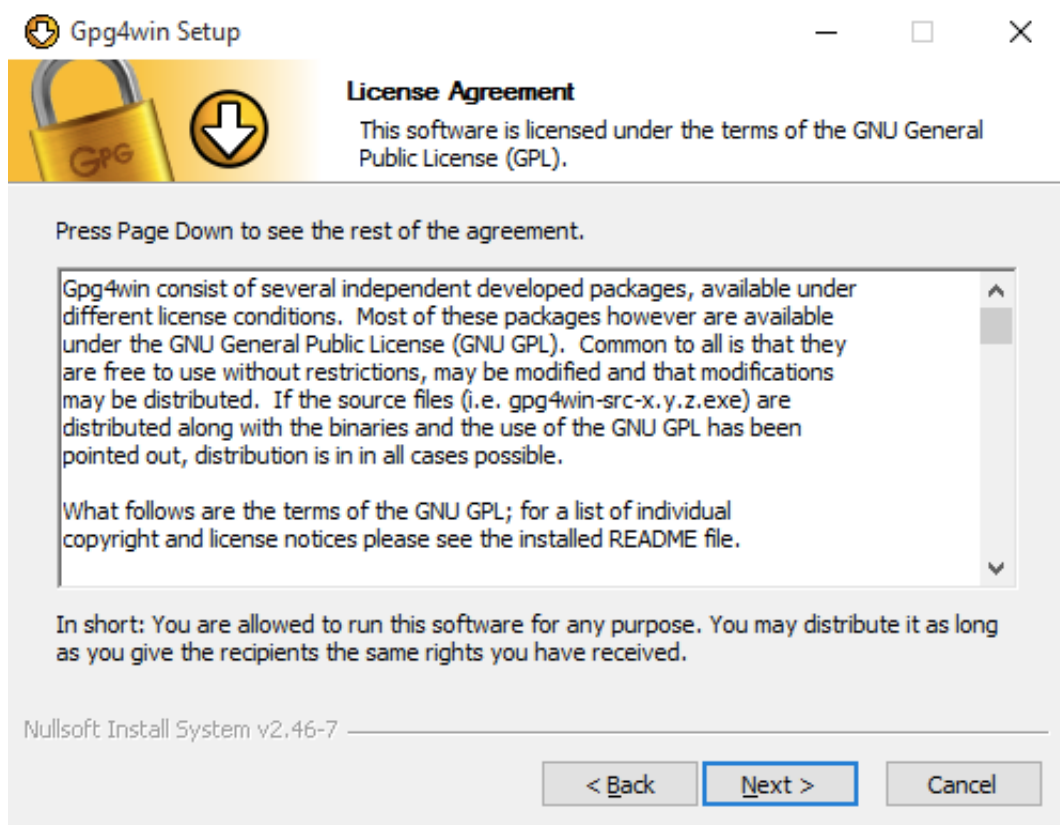
Download Gpg4win (GNU Privacy Guard for Windows) from <https://www.gpg4win.org/index.html>

## Install GnuPG & Related application

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

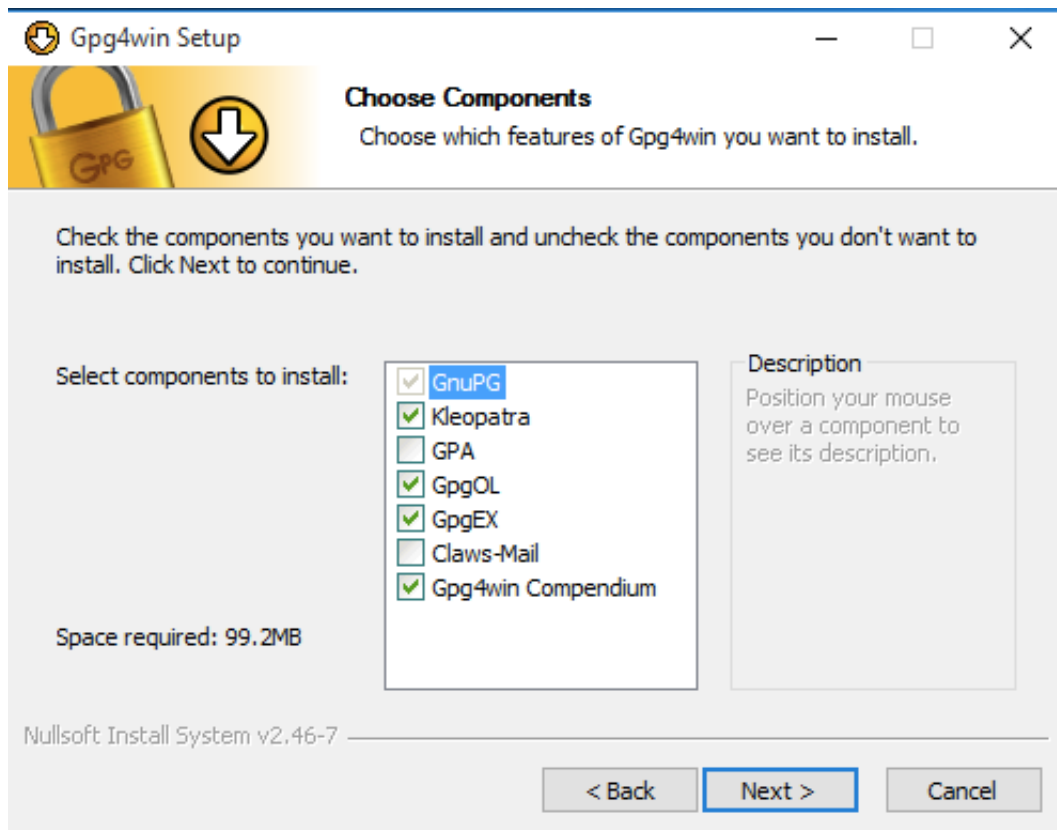


2. Close all programs that are running on your computer and click on [ Next ]
3. The next page displays the licensing agreement – it is only important if you wish to modify or forward Gpg4win. If you only want to use the software, you can do this right away – without reading the license.



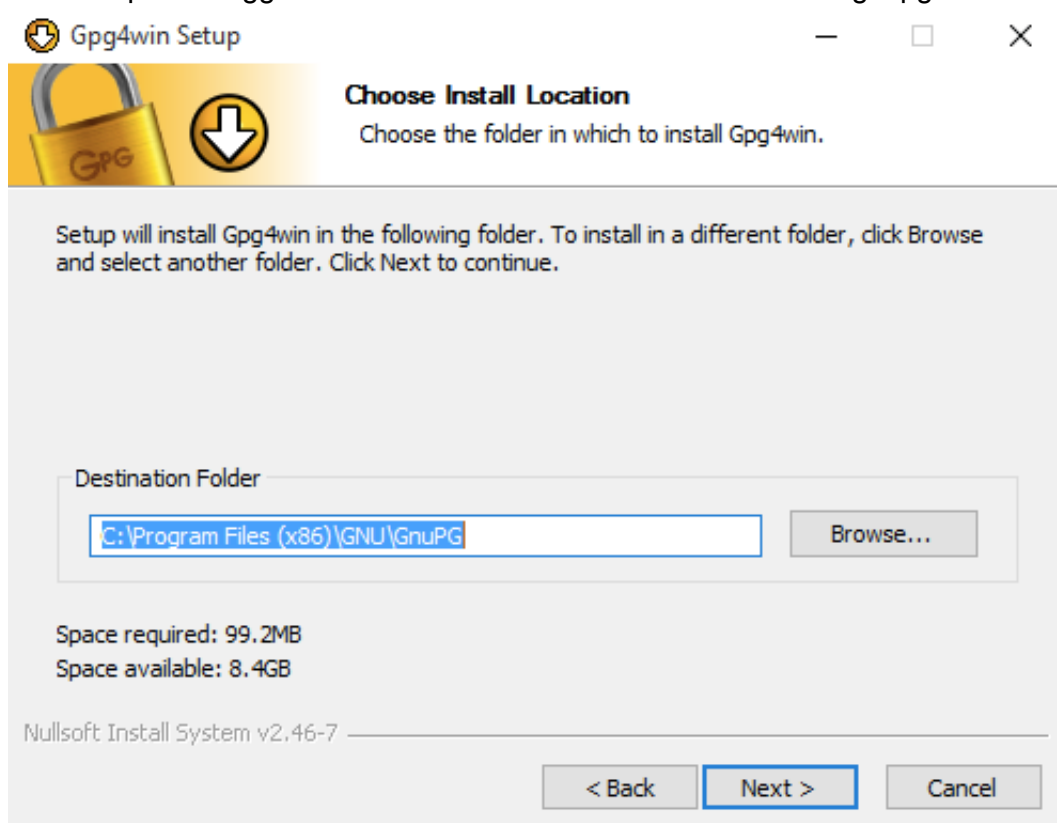
Click on [ Next ]

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. Below are the application and their function:
  - 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 Compendium: The Gpg4Win documentation



Click on [ Next ]

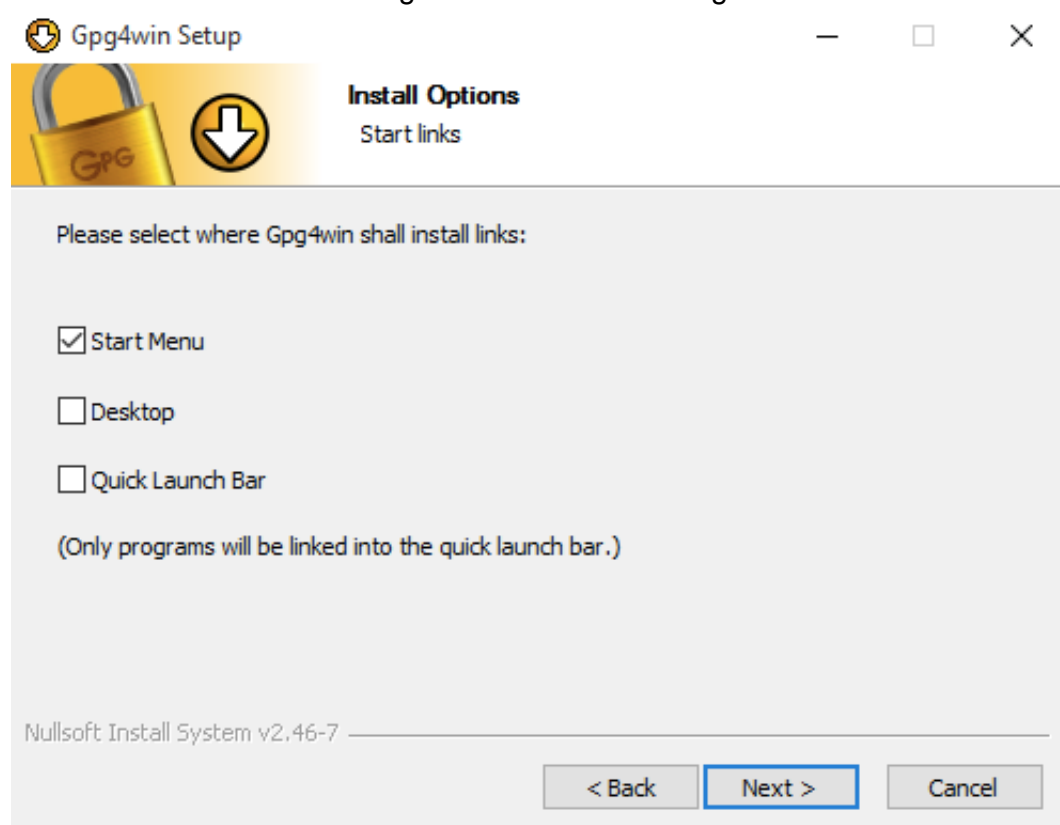
5. The system will suggest a folder for the installation, e.g.: C:\Programme Files (x86)\GNU\GnuPG You can accept the suggestion or select a different folder for installing Gpg4win.



Then click on [ Next ]

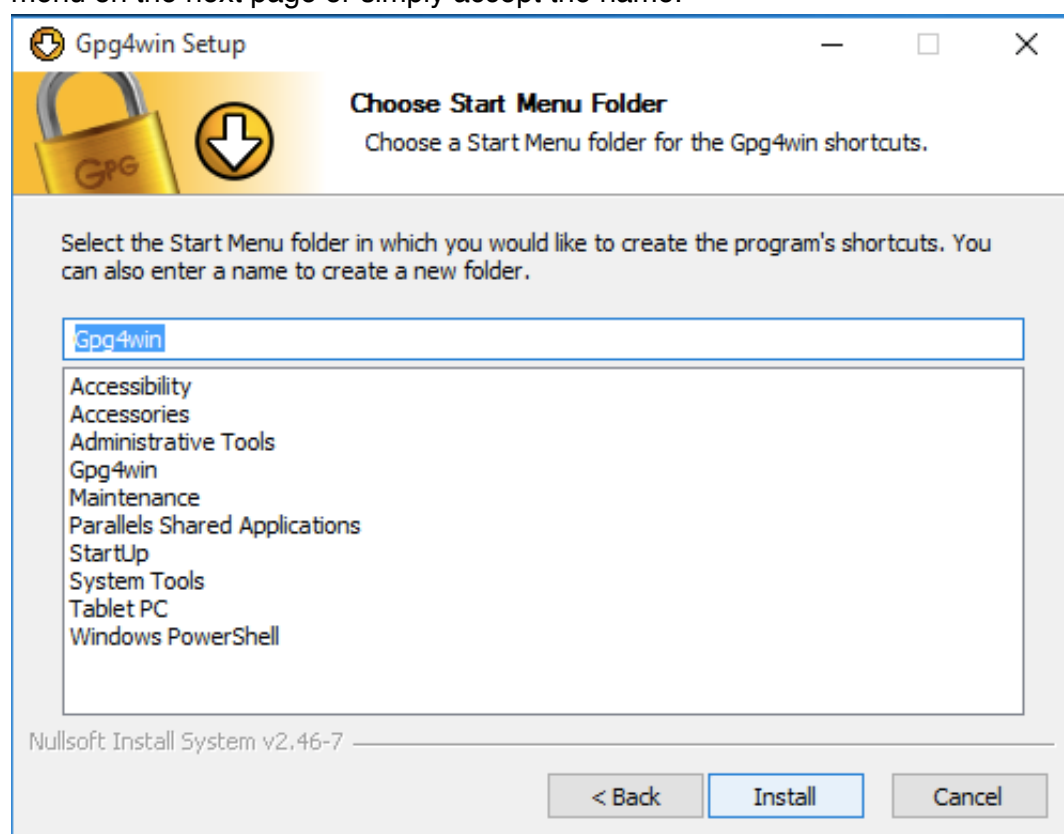
6. Now you can decide which links should be installed – the system will automatically create a link with

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



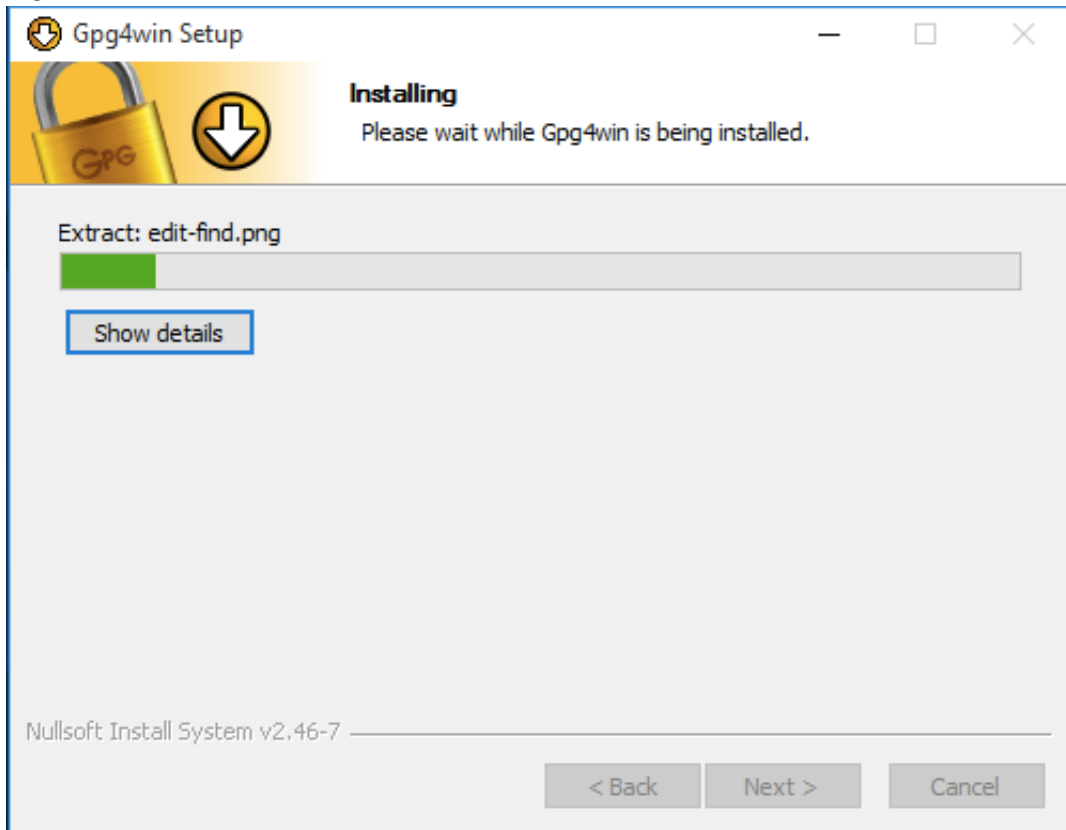
Then click on [ Next ]

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.

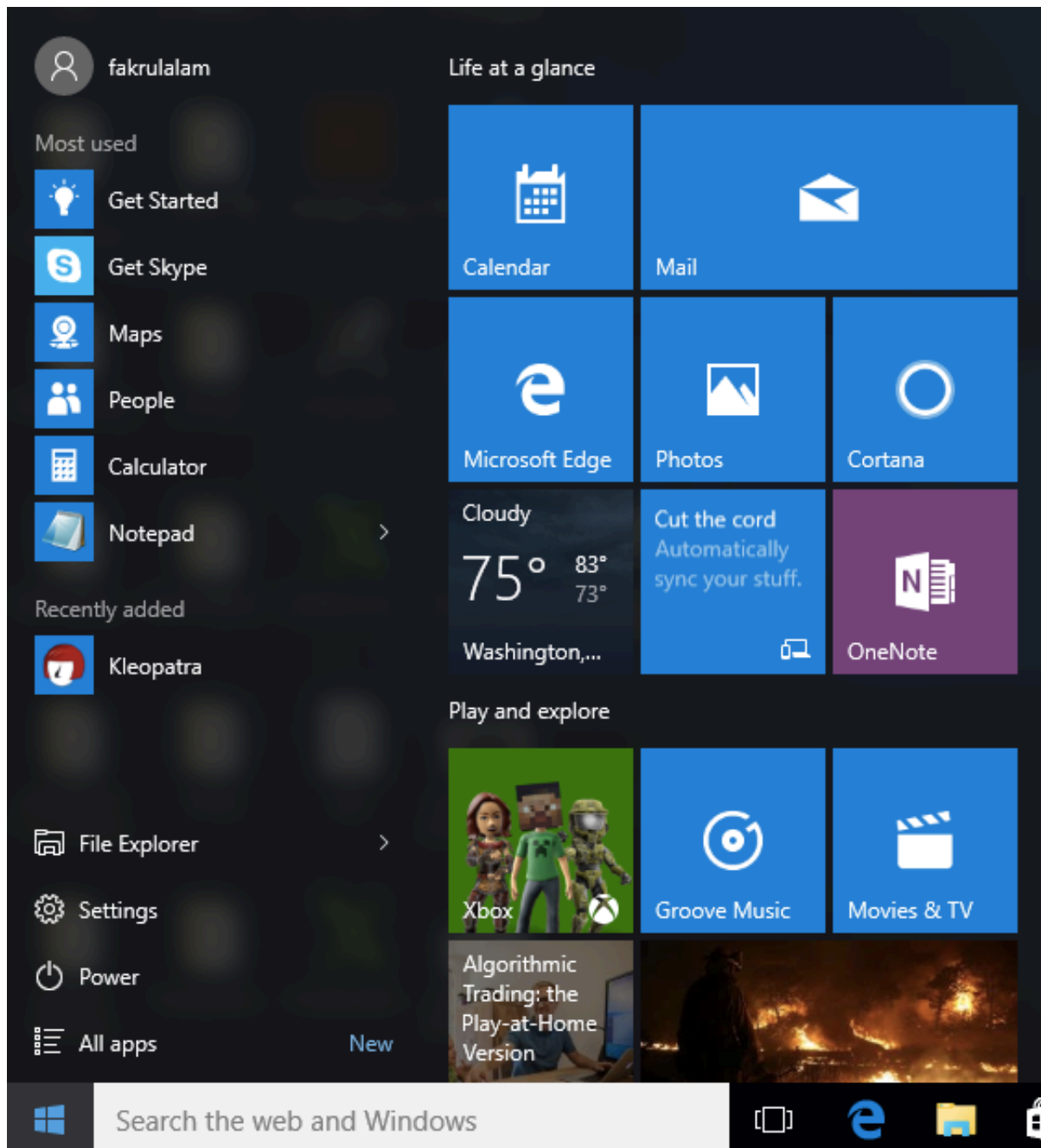
Click on [ Finish ]

And that's it!

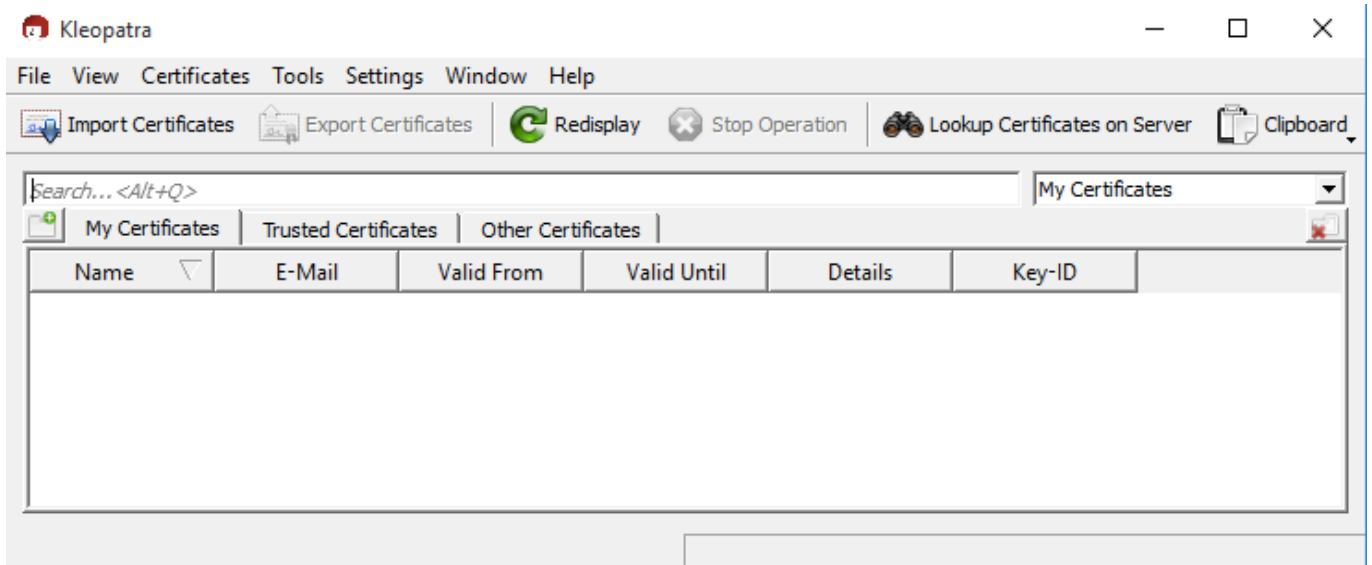
You have successfully installed Gpg4win and are ready to work with the program.

## Create Certificate

1. Open Kleopatra using the Windows start menu:



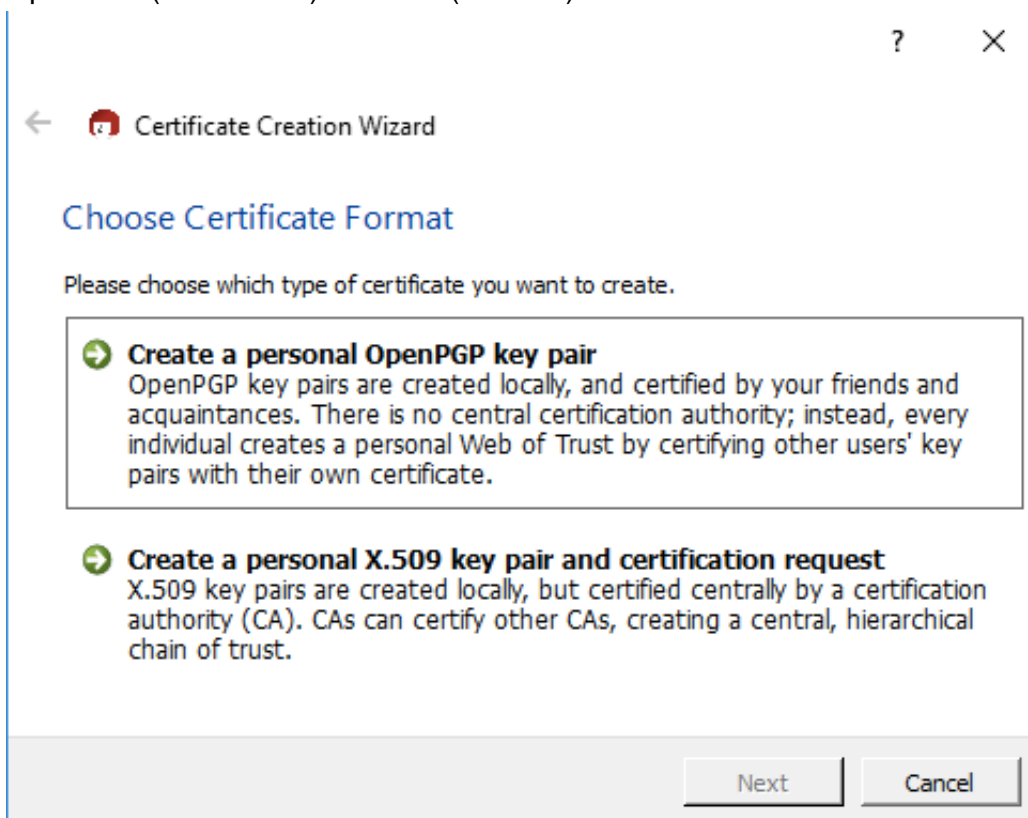
2. You will see the main Kleopatra screen – the certificate administration:



- At the beginning, this overview will be empty, since you have not created or imported any certificates yet.

Click on `File→New Certificate`.

- 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).

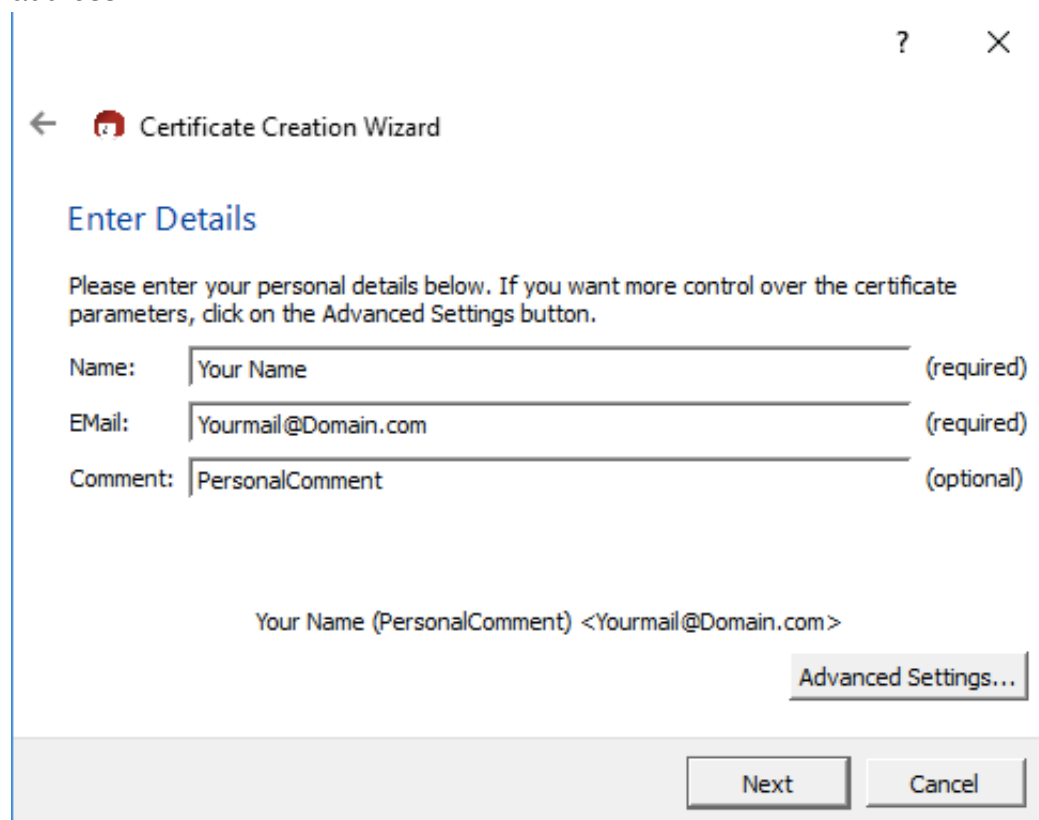


click on `[ Create personal OpenPGP key pair ]`.

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



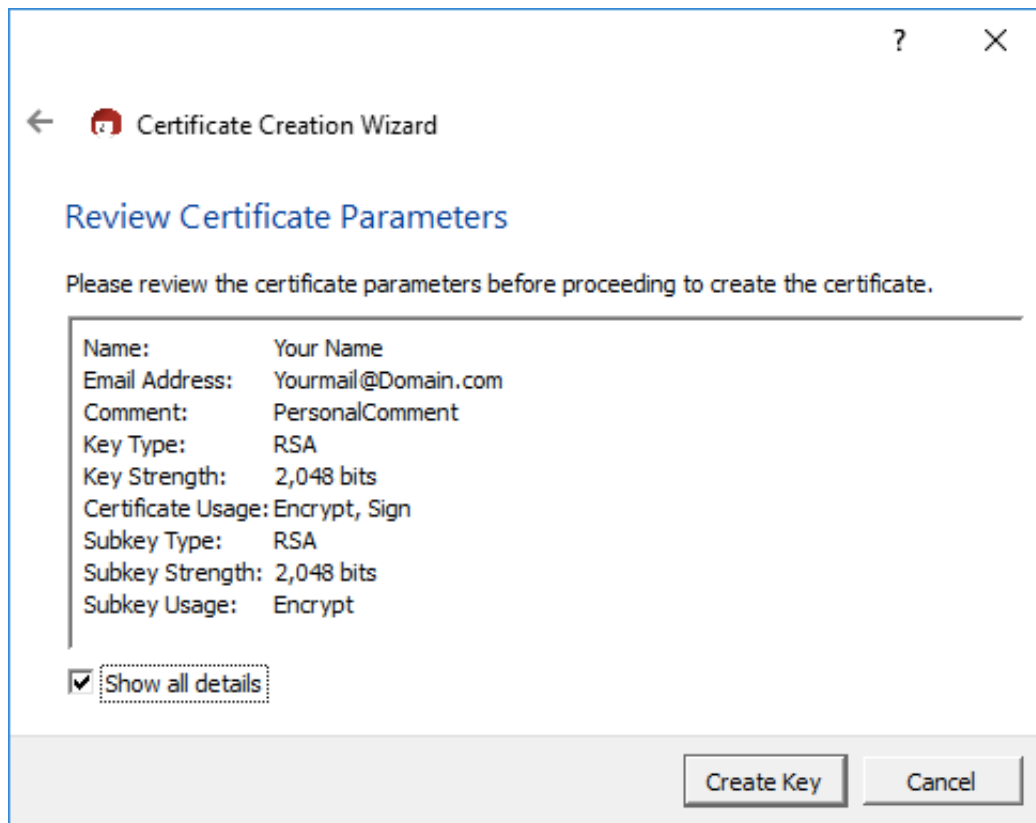
The screenshot shows a window titled "Certificate Creation Wizard" with a back arrow and a red key icon. The window has a title bar with a question mark and a close button. The main content area is titled "Enter Details" and contains the following text: "Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button." Below this text are three input fields: "Name:" with the value "Your Name" and "(required)" to its right; "EMail:" with the value "Yourmail@Domain.com" and "(required)" to its right; and "Comment:" with the value "PersonalComment" and "(optional)" to its right. Below the input fields, the text "Your Name (PersonalComment) <Yourmail@Domain.com>" is displayed. To the right of this text is a button labeled "Advanced Settings...". At the bottom of the window are two buttons: "Next" and "Cancel".

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 ]`

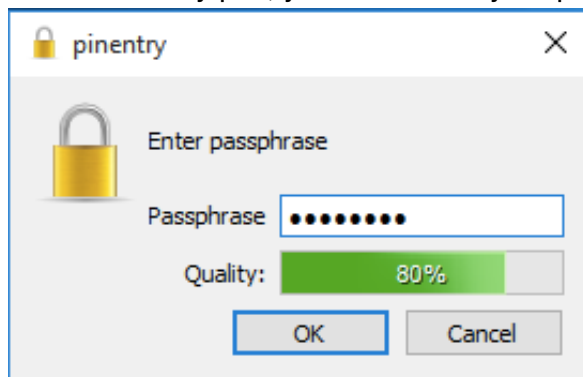
7. You will see a list of all of the main entries and settings for review purposes. If you are interested in the (default) expert settings, you can view these via the All details option.



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

8. Now to the most important part: entering your **passphrase**!

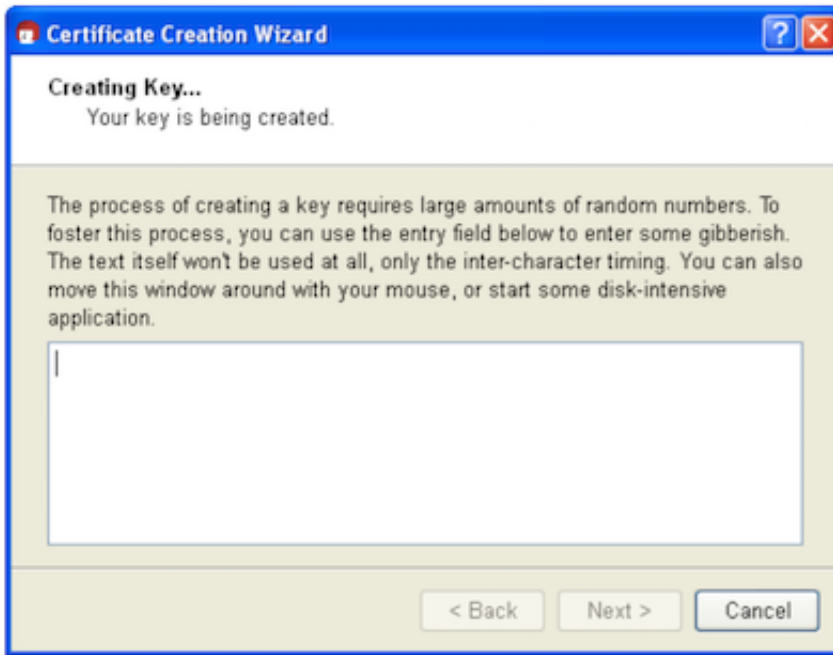
To create a key pair, you must enter your personal passphrase:



9. Choose passphrase which is easy-to-remember but hard to break secret passphrase.

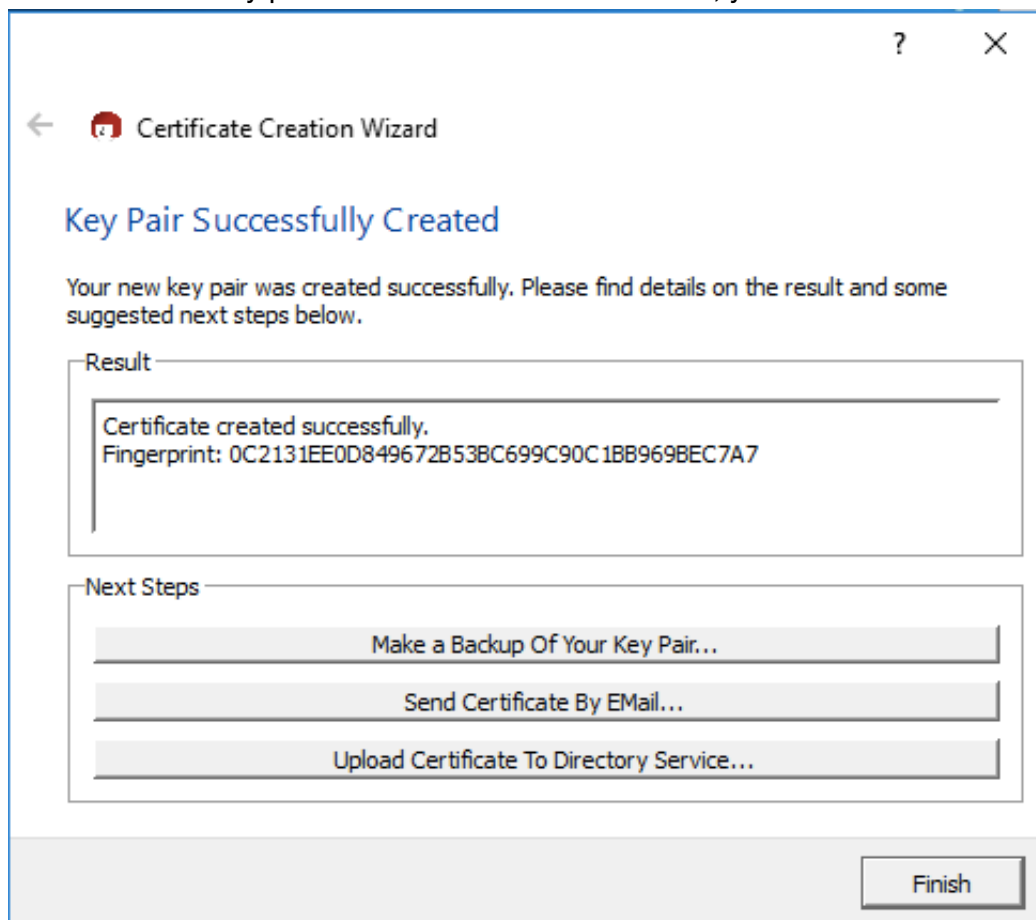
To make sure that you did not make any typing errors, the system will prompt you to enter your passphrase twice. Always confirm your entry with [ OK ].

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:



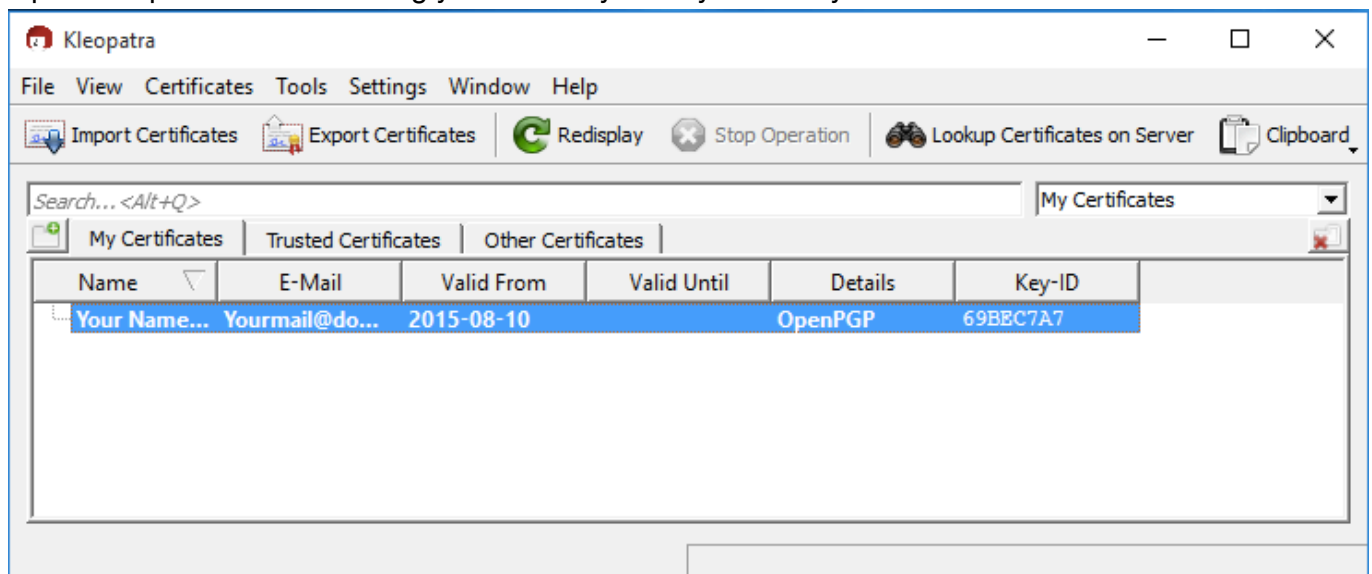
The 40-digit “fingerprint” of your newly generated OpenPGP certificate is displayed in the results text field. This fingerprint is unique anywhere in the world, i.e. no other person will have a certificate with

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.

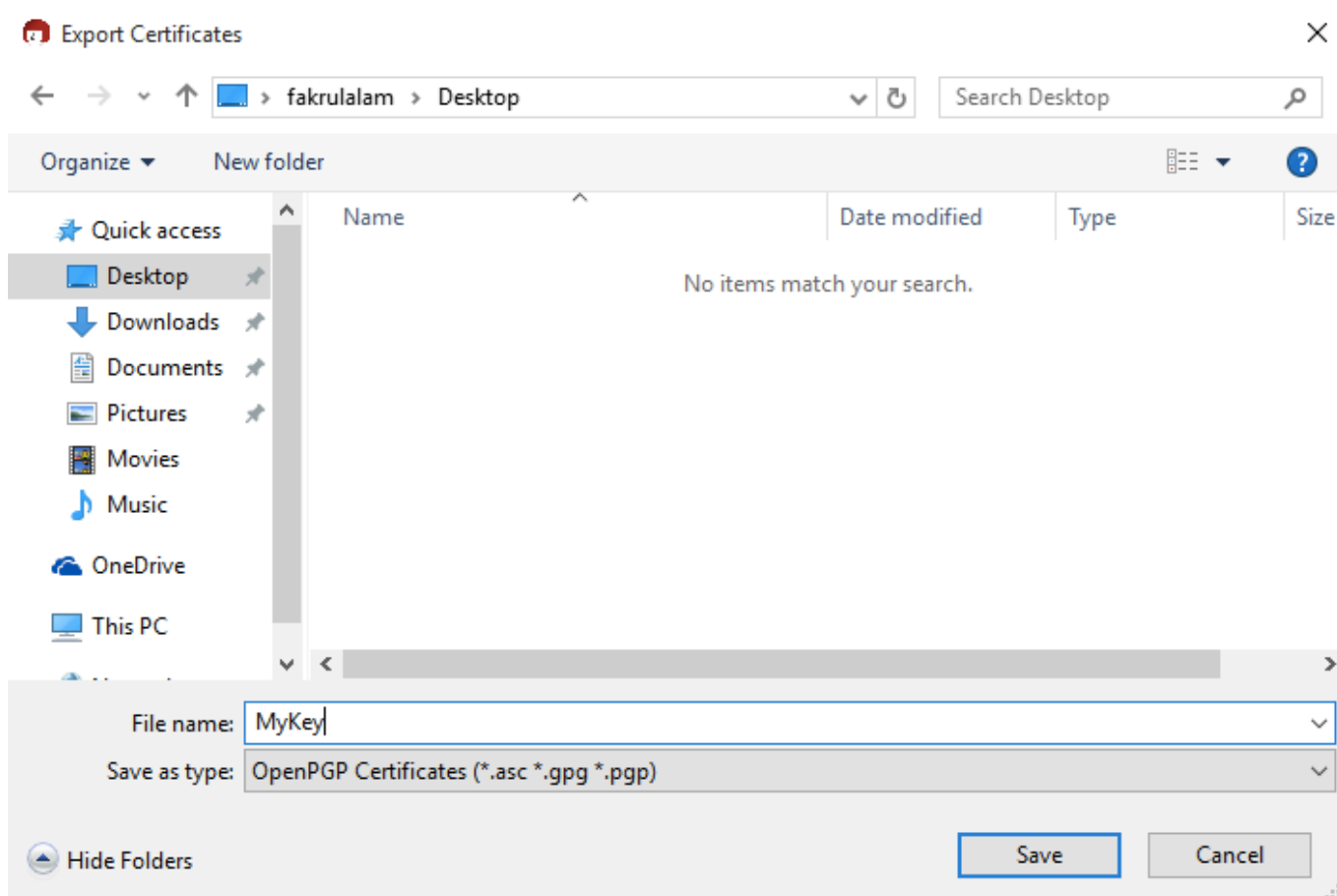
## Next, Export certificate (public key):

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



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

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



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

```
MyKey.asc - Notepad
File Edit Format View Help

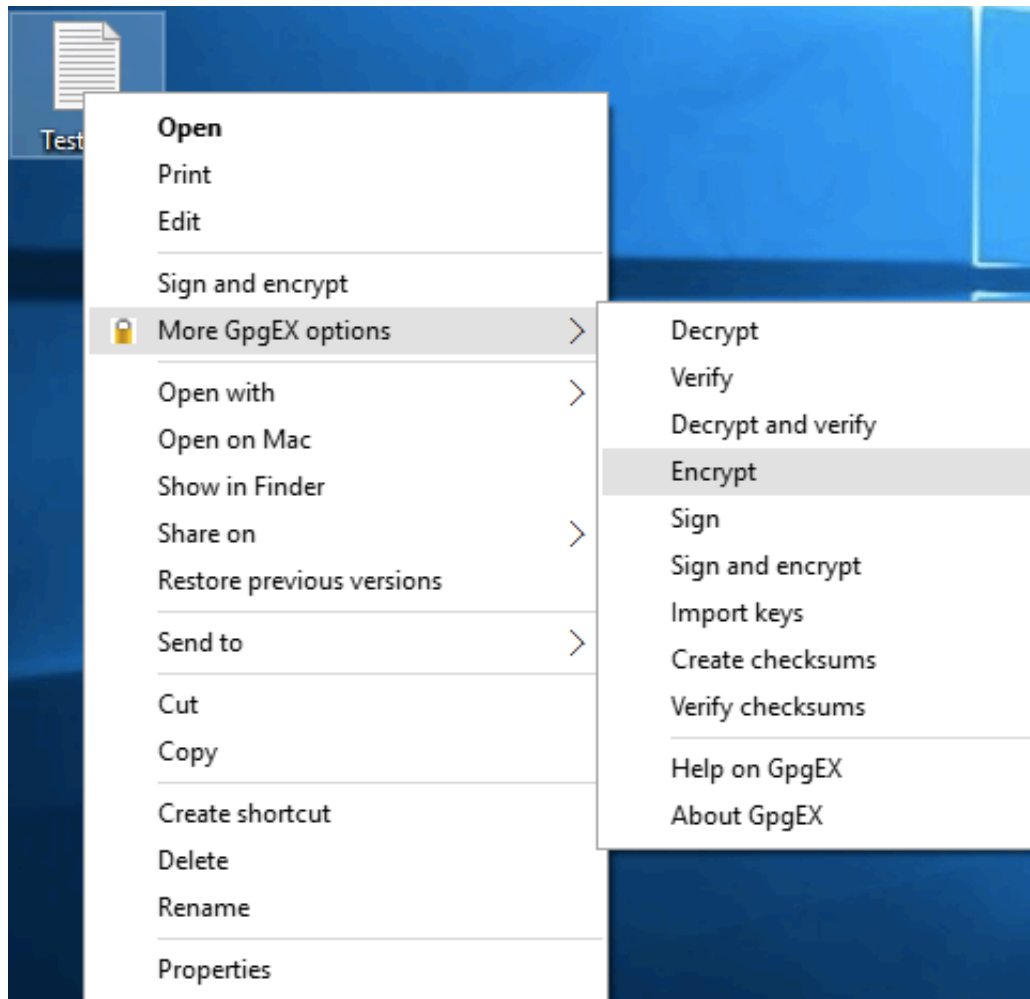
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFXIN5EBCADRh2RXGzTU00AEoRWJyPtF8GGLjBCLbApqIdk7GjV1xDbDT6Vq
3Rs+AN112rJPNBHhZtKuTxRzdUWFYJIBIW2T1vyPQFm7WYxK7AsmyJvBs6cWzZ2i
qD0znLw8UE6zQrIyr4hLer06b/2pzMHsxJEnkKY4CrYbp/+lyAWK1eBDZtZkDvfK
fdonJy3nyzOKGbfCvYpy8kk1myLY27g8CpmDIS58oqZ118JPL50AauIzmnwN13kx
jMSSYq7sNPiU6LH0dBF2wh95nF7NWLIXBeLtrSPLSTuGhwq6kgBk+Q5XbJjbRbYn
1X01ZZ9guJDGf1uJgOTwEPgcpMy37684ff7JABEBAAG0MV1vdXIgTmFtZSAoUGVy
c29uYWxDb21tZW50KSA8WW91cm1haWwAZG9tYW1uLmNvbT6JATkEEwEIACMFA1XI
N5ECGwMHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRDJDBu5ab7Hp6NqCADR
G2NCVGZfcA5k9NLDWqZMX0CmBhanPhsML+hKxaxMbIwch/JFxK7Ps/D9V+JBc+o2
tjEo7dw9vA9mZORDCVakOoo9ryD8mX1MmddbQDjQuMT3Epr6Lf0hoS2aQHx2/30B
x8eZh/BvL13UdQzdRdxxDDGrsin6tHF6pMONopk8B8Ur9bxJLYZ00fd0cLmFtN8N
Ggwd+7TtMQhC88wW6TDF28UNuL4/I+8mEXe8Ukj6n0qlcZVmx95/VnywaHVPdt
E5D17uVC2IKFusM54eq/21Bn6sflFE0p+mn1G+kRFdZJDmZOLc5ELQ1B02vDRhd9
kKPr9zdVNOhtTEW9Y532uQENBFXIN5EBCACfJL3okoD/+f25kBxsMeg00R3NmvJa
1UYgirXD6eqvE+qKp8CGvpPMem4gpSxjZZpgo/+xTJtdzogbisdpNzd3wGRU1DZn
iTEvT6nF1BMCA16RuT03IeQrxXIRouWc8oLid25xt3icfWE6gvdqf0yNdfaUHSc+
Iny+Htg1p9vDjPljCDzUL65H+QGNfcOLpEluvz+M4IpT1TvMU4KcBLcDB6NXLxHV
MEYWhc1wEE19lobpUFB+N675i2T7M3edJVpvzYaxB/9EUKAi5s5Lwqvhu5xI7Y9U
iZ6+gOKq2fkLuGyQ0R03OIjM8K8ZvHg/Atidfr6Pe0yCbPLFrHB+8uhHABEBAAGJ
AR8EGAEIAAkFA1XIN5ECGwwACgkQyQwbuWm+x6f8pQgA14JRfoz3VB7hNCH/wx0I
OuyPkEa71Fxode9YuovnDJW4kfnzsguAguXI4+QsR+PUIipApYWAxeupVuIeEJzT
jT/cCiltAVaWCFMucH0YJMHXrDizq4WtRvQE6JU3pRStMOUpY3fhkYgu0Gqp2DSY
zt2AykqKUv0tByfI3auQHjJmGYIQjCWLfM7h+jp03YX3KoVkv8VG3A+ct+uRzbD
bQvisOFyHkn4pftEFgoKsX63hWHuELUWjt/SzC0YntLEGo217JZVP/4zGucKfJkI
oi+D9Hy+4lobefmB2A71sYN2KD1ttzZsACyD+bFhMa5TZTaa6W3xNRvdqoS4nbnI
xw==
=7F7m
-----END PGP PUBLIC KEY BLOCK-----
```

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

## 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](#)

?

×

←  Sign/Encrypt Files

What do you want to do?

Please select here whether you want to sign or encrypt files.

Selected file:

- //psf/Home/Desktop/TestMail.txt

☐ Archive files with: 

TAR (PGP®-compatible)

Archive name (OpenPGP): 

//psf/Home/Desktop/TestMail.txt.tar

Archive name (S/MIME): 

//psf/Home/Desktop/TestMail.txt.tar.gz

☐ Sign and Encrypt (OpenPGP only)

☒ Encrypt

☐ Sign

☐ Text output (ASCII armor)

☐ Remove unencrypted original file when done

Next

Cancel

4. Choose correspondence public key and choose 

Add


 and click 

Encrypt



?

×

←  Sign/Encrypt Files

For whom do you want to encrypt?

Please select for whom you want the files to be encrypted. Do not forget to pick one of your own certificates.

Search...

All Certificates

Name	E-Mail	Valid From
<div><div>Your Name (PersonalComment)</div><div>APRICOT2015 (Test Key for APRICOT2015 NetSec Workshop)</div></div>	<div>Yourmail@domain.com</div> <div>apricot2015@fakrul.com</div>	<div>2015-08-10</div> <div>2015-02-18</div>

▼ Add

▲ Remove

Name	E-Mail	Valid From
<div><div>Your Name (PersonalComment)</div><div>APRICOT2015 (Test Key for APRICOT2015 NetSec Workshop)</div></div>	<div>Yourmail@domain.com</div> <div>apricot2015@fakrul.com</div>	<div>2015-08-10</div> <div>2015-02-18</div>

Encrypt

Cancel

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

←  Sign/Encrypt Files

## Results

Status and progress of the crypto operations is shown here.

OpenPGP: All operations completed.

TestMail.txt → TestMail.txt.gpg: **Encryption succeeded.**

[Show Details](#)

☒ Keep open after operation completed

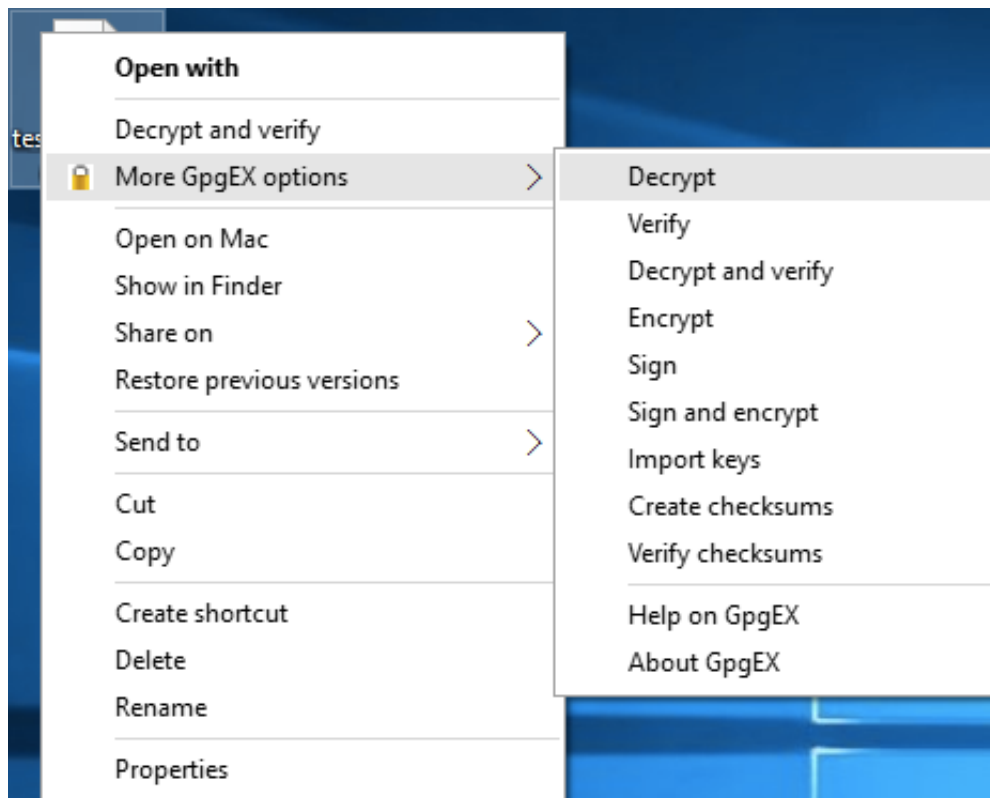
Finish

Cancel

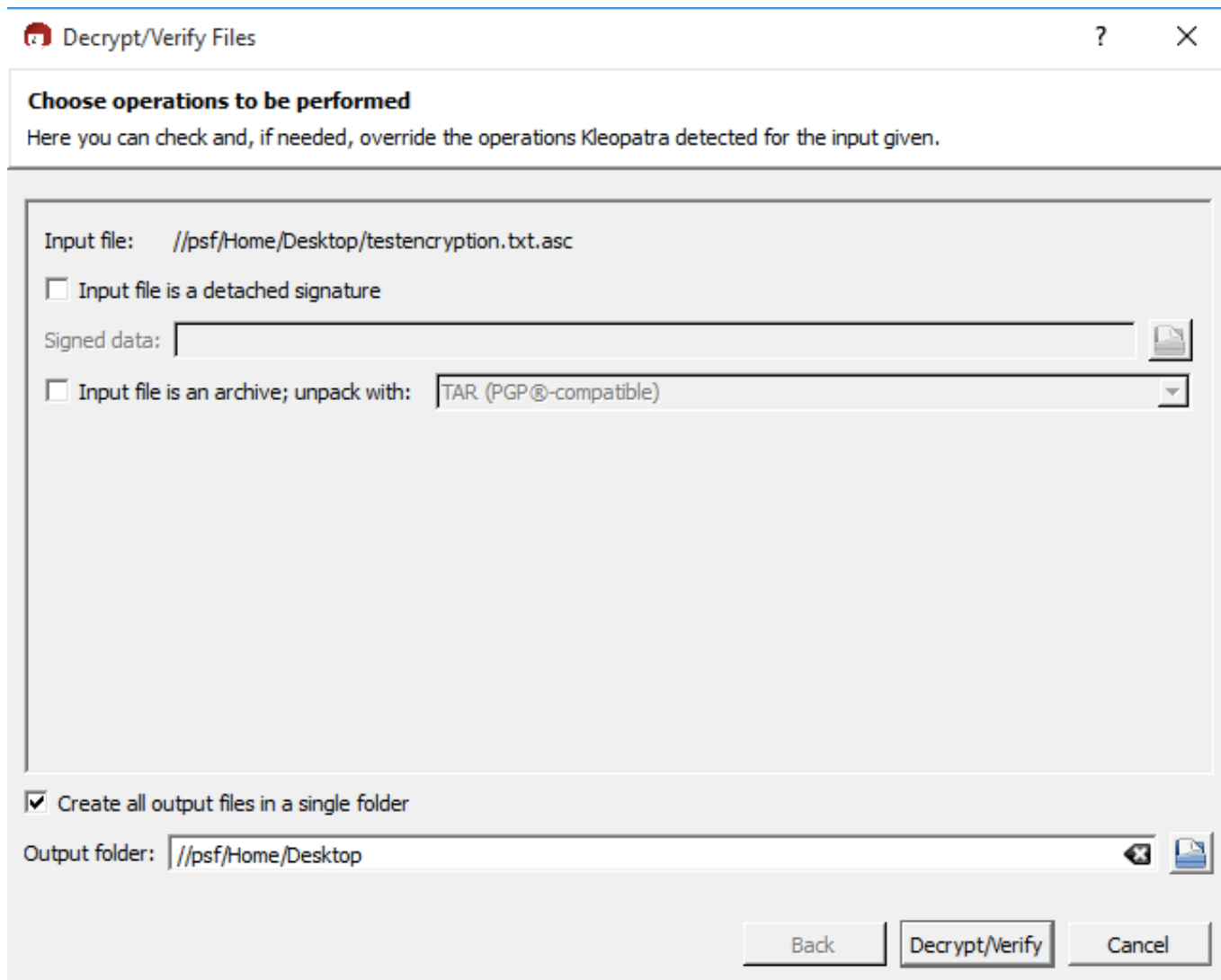
6. Attach this file as email attachment and send it to the receiver.

## Decrypt Message

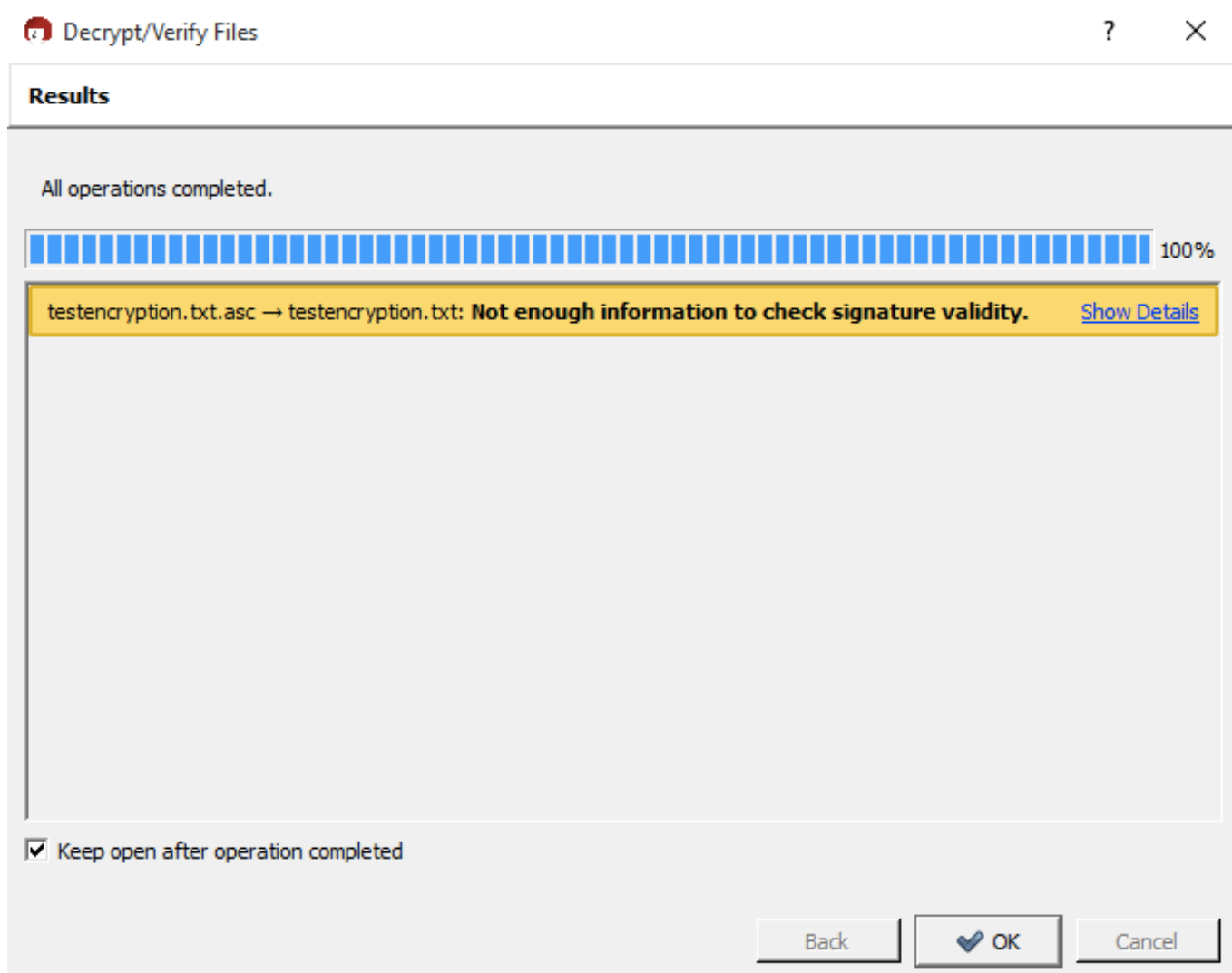
1. Save the encrypted file.
2. Right mouse click choose `More GpgEX Options -> Decrypt`



3. Next window will give you some information 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.

## 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!`

The screenshot shows a web browser window with the address bar displaying 'pgp.mit.edu'. The page title is 'MIT PGP Public Key Server'. Below the title, there are links for 'Help' (Extracting keys, Submitting keys, Email interface, About this server, FAQ) and 'Related Info' (Information about PGP). The main content area is divided into two sections: 'Extract a key' and 'Submit a key'. The 'Extract a key' section has a 'Search String' input field, a 'Do the search!' button, and radio buttons for 'Index' and 'Verbose Index'. There are also checkboxes for 'Show PGP fingerprints for keys' and 'Only return exact matches'. The 'Submit a key' section has a text input field for 'Enter ASCII-armored PGP key here:' and buttons for 'Clear' and 'Submit this key to the keyserver!'.

MIT PGP Key Server

pgp.mit.edu

# MIT PGP Public Key Server

Help: [Extracting keys](#) / [Submitting keys](#) / [Email interface](#) / [About this server](#) / [FAQ](#)  
Related Info: [Information about PGP](#) /

---

## Extract a key

Search String:

Index: ☒ Verbose Index: ☐

☐ Show PGP fingerprints for keys  
☐ Only return exact matches

---

## Submit a key

Enter ASCII-armored PGP key here:

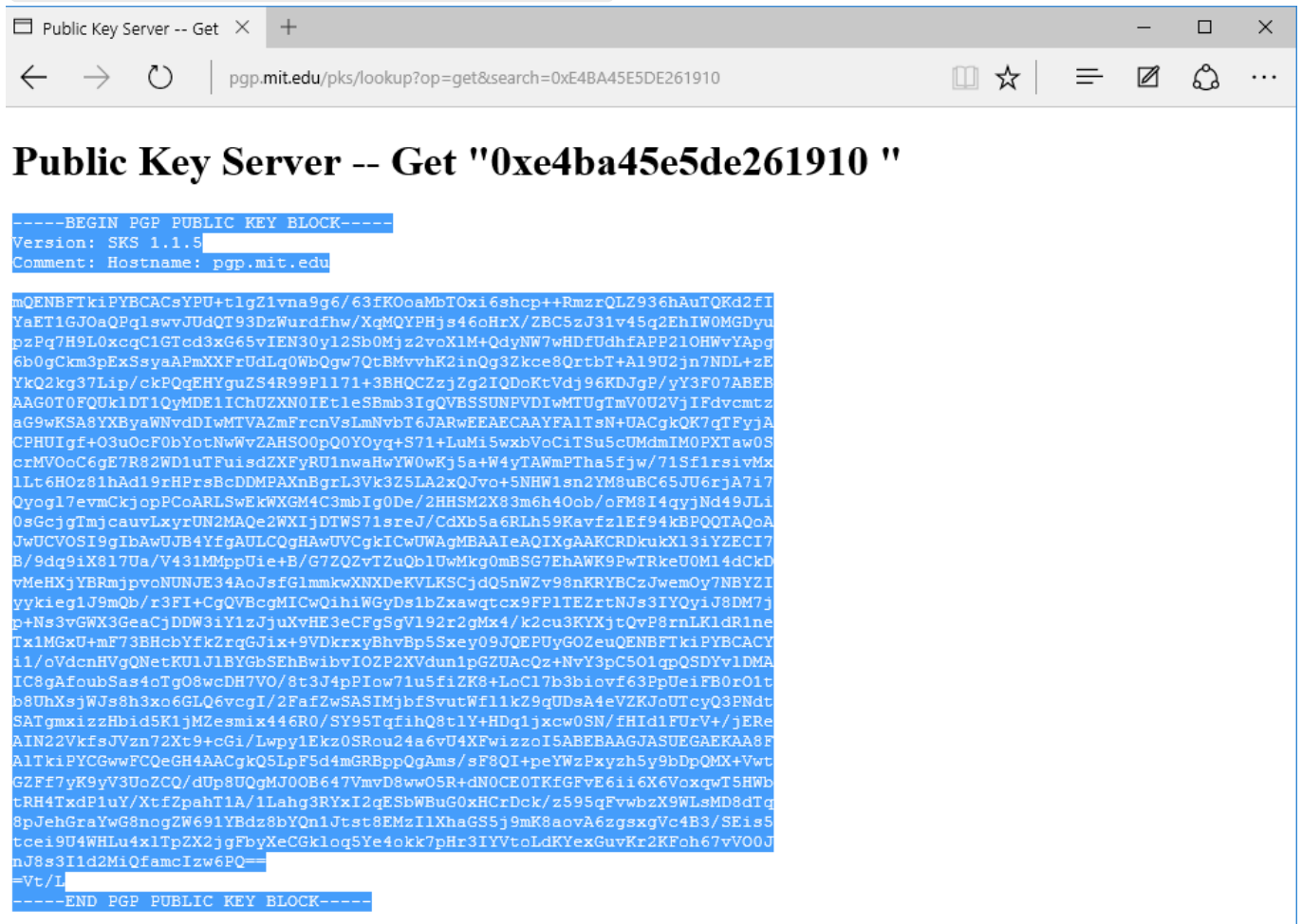
- From `http://pgp.mit.edu/` you can search for you key or any other uploaded key.
- Please note that you can't delete/remove any uploaded public key from key server. You can only revoke them.

## Import Public Key from Key Server

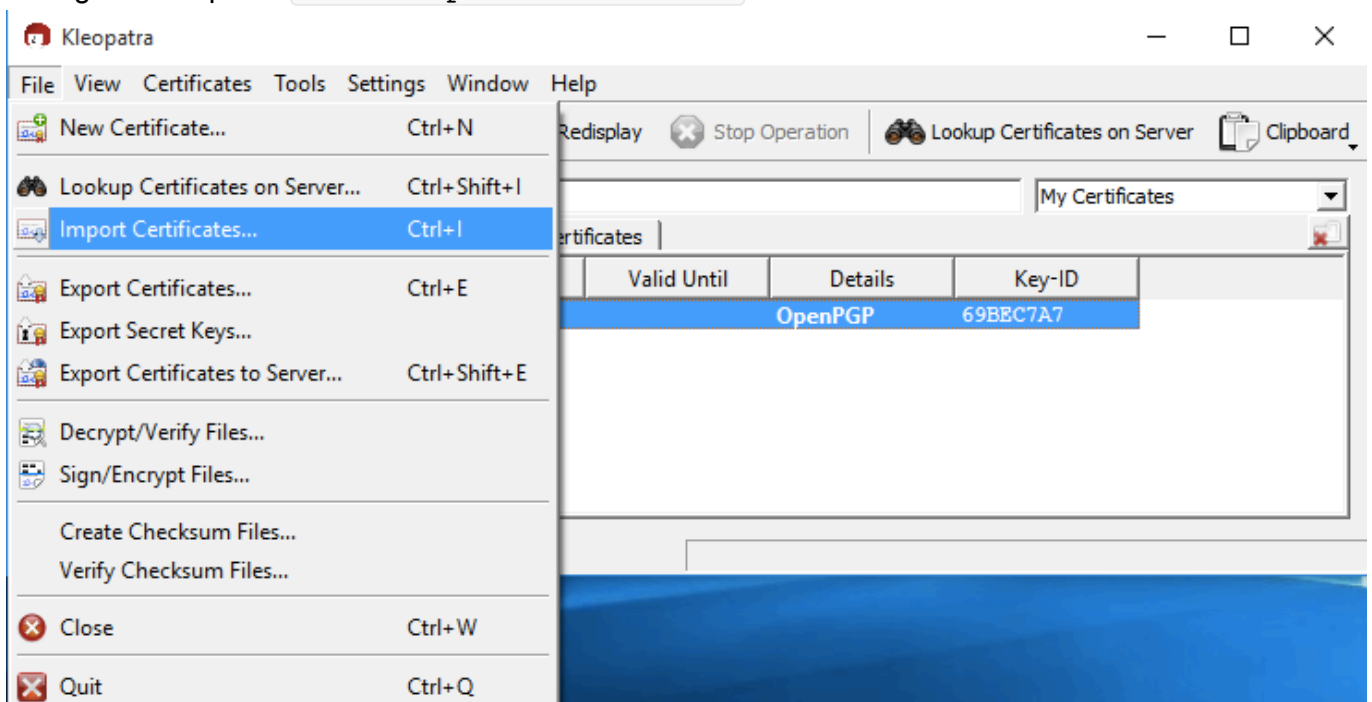
- Open any browser and go to `http://pgp.mit.edu/`
- In `Search String` field type email address for the correspondence public key and click `Do the search!`
- You will get the list of key/keys with KeyID. KeyID is the last 8 digit of fingerprint.

4. Click on KeyID.

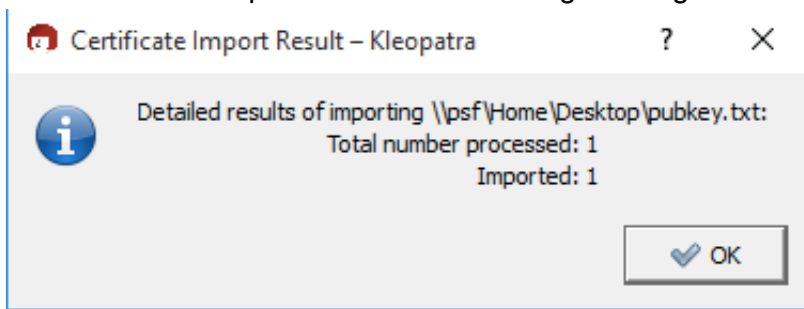
5. Copy from -----BEGIN PGP PUBLIC KEY BLOCK----- till -----END PGP PUBLIC KEY BLOCK----- . Save it in a file.



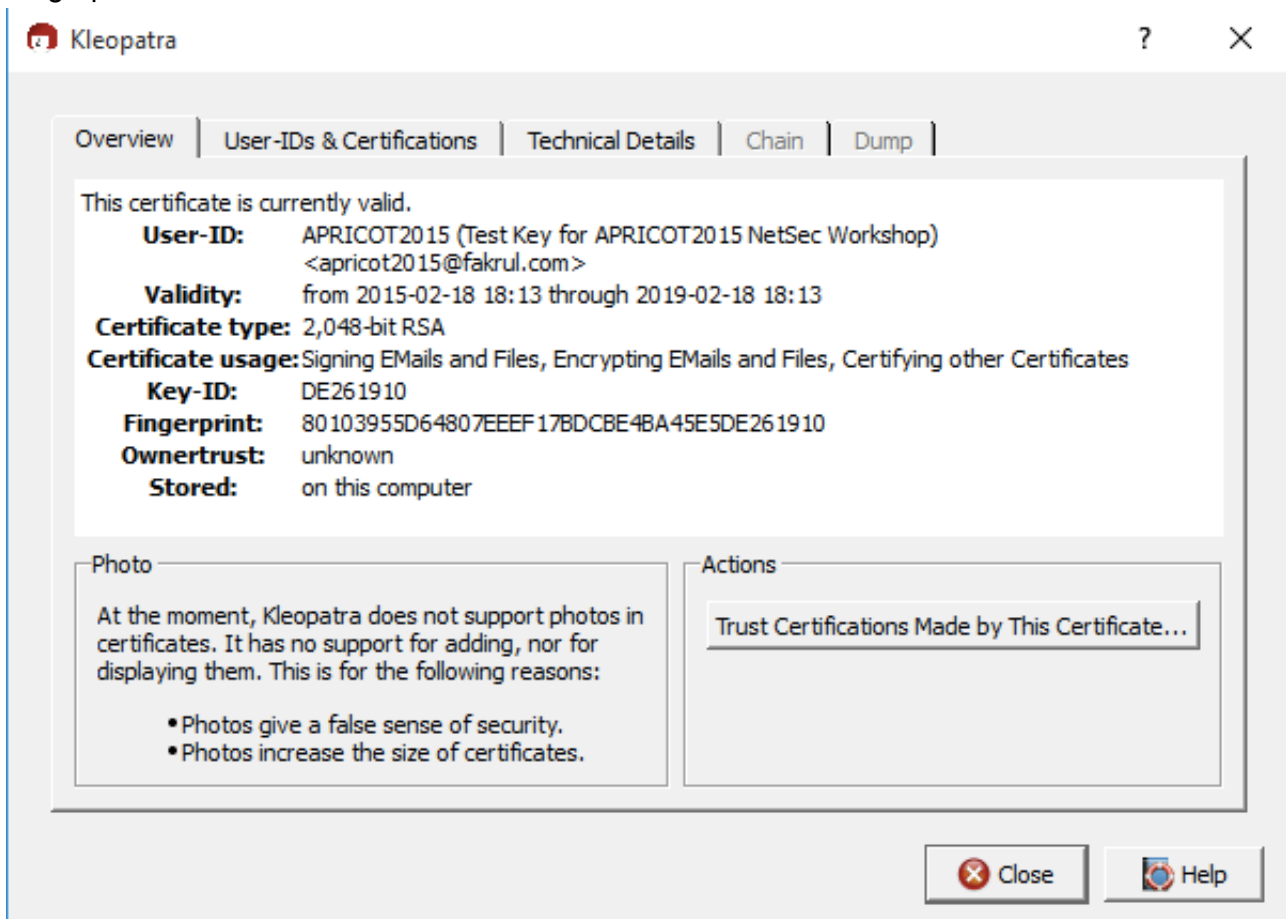
6. Now go to Kleopatra File->Import Certificate



7. Browse the previously saved public key and import it.
8. After successful import it will show following message:



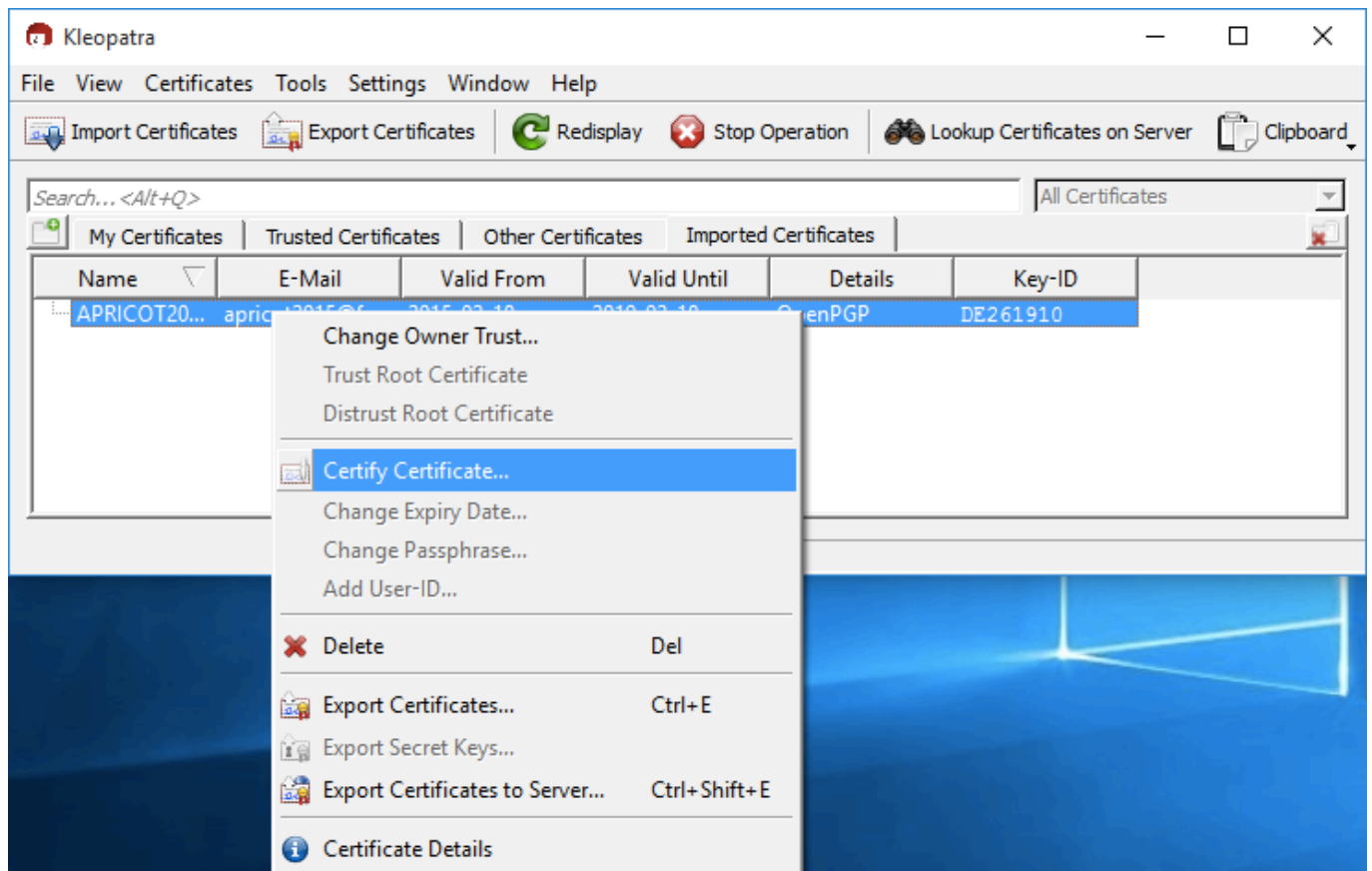
9. You will get those imported public key under **Imported Certificate** tab.
10. Double click on any key will open new window and show the key details which include Validity and Fingerprint.



## Sign other Public Key

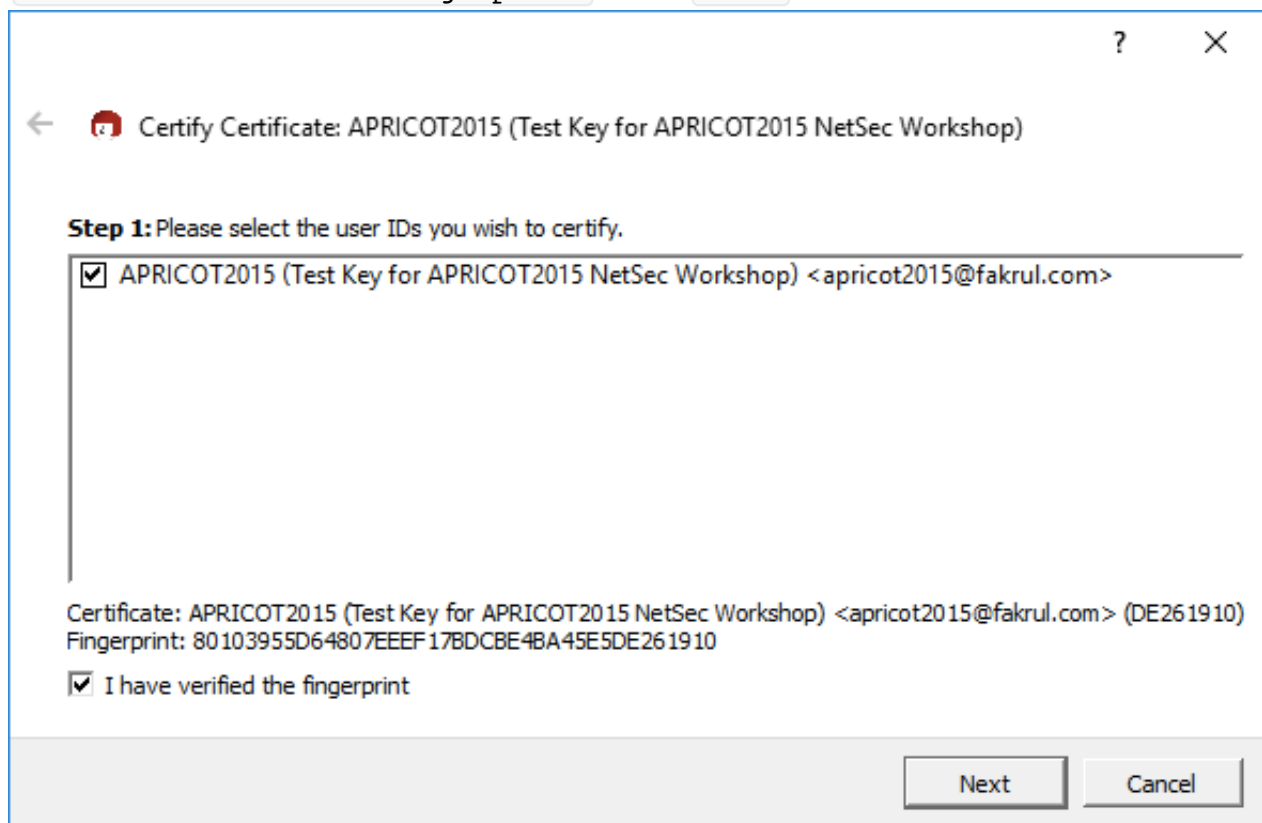
1. Go to **Imported Certificates** tab of Kleopatra.
2. Right mouse click and choose **Certify Certificate** for the key which you want to sign.





3. Choose the Key you want to certify. 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** .

?

×

←  Certify Certificate: APRICOT2015 (Test Key for APRICOT2015 NetSec Workshop)

**Step 2:** Choose how to certify.

Certification will be performed using certificate Your Name (PersonalComment) <Yourmail@domain.com>.

☐ Certify only for myself

☒ Certify for everyone to see

☐ Send certified certificate to server afterwards


Certify Cancel

5. You will be asked for passphrase of your Private Key.

6. After successfully signing, it will show confirmation message. Click **Finish**.

?

×

←  Certify Certificate: APRICOT2015 (Test Key for APRICOT2015 NetSec Workshop)

**Summary:**

Signed user IDs: APRICOT2015 (Test Key for APRICOT2015 NetSec Workshop) <apricot2015@fakrul.com>

Selected secret key: Your Name (PersonalComment) <Yourmail@domain.com>

Certification successful.

Finish Cancel

7. Now you can export this public 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\*\*\*