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

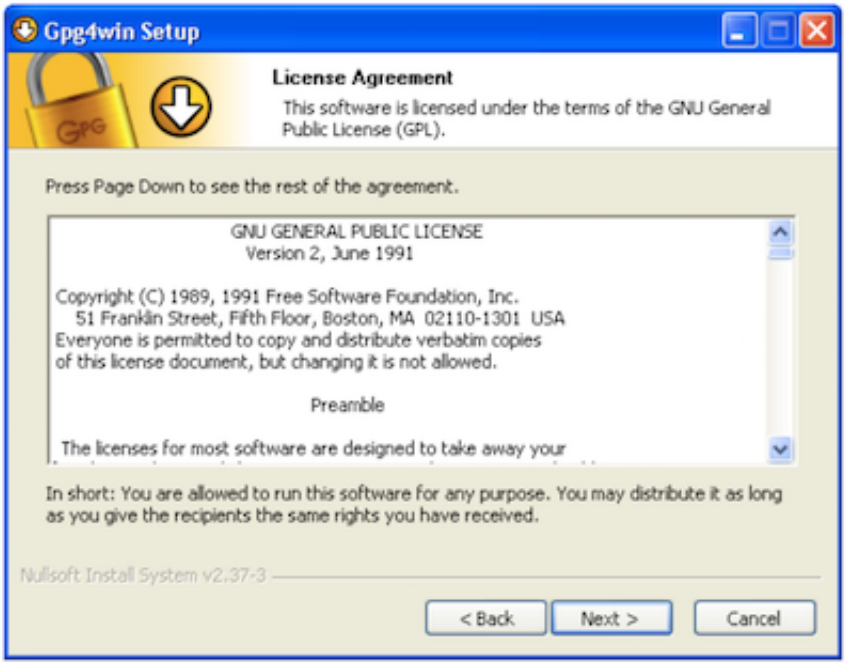
Install GnuPG & Related application

The installation assistant will start and ask you for the language to be used with the installation process:

Confirm your language selection with `[ OK ]`
Afterwards you will see this welcome dialog:

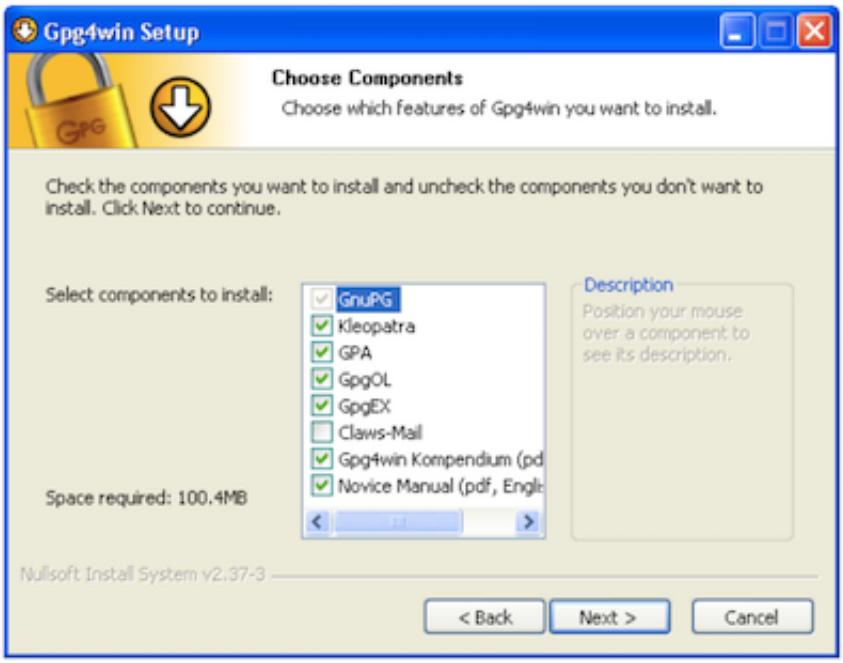
Close all programs that are running on your computer and click on `[ Next ]`

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.



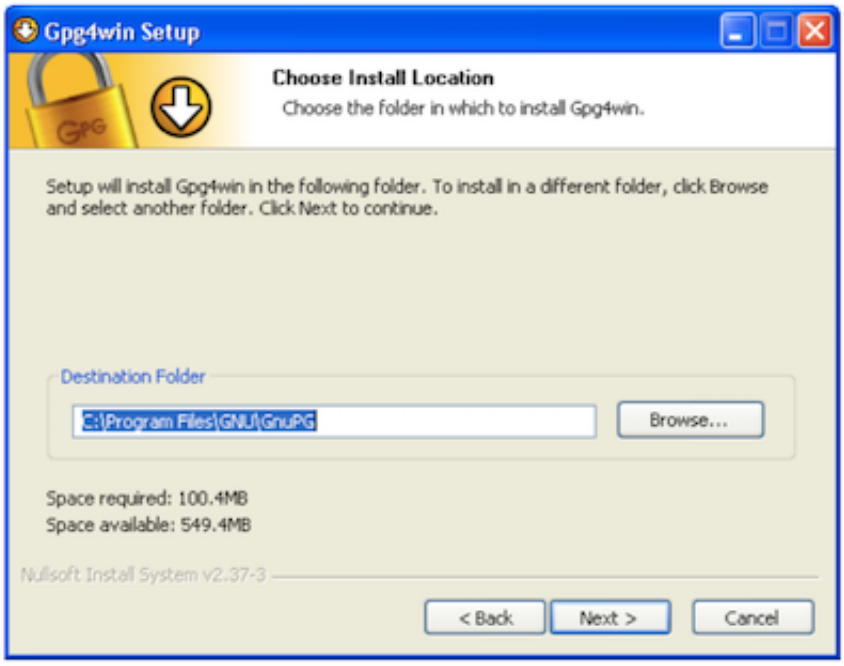
Click on `[ Next ]`

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. Yo 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.



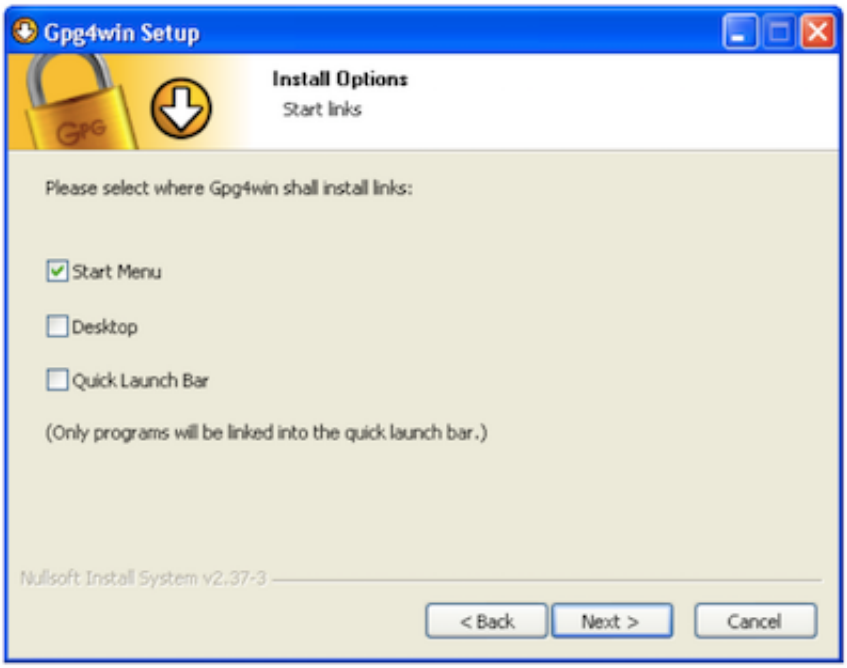
Click on `[ Next ]`

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



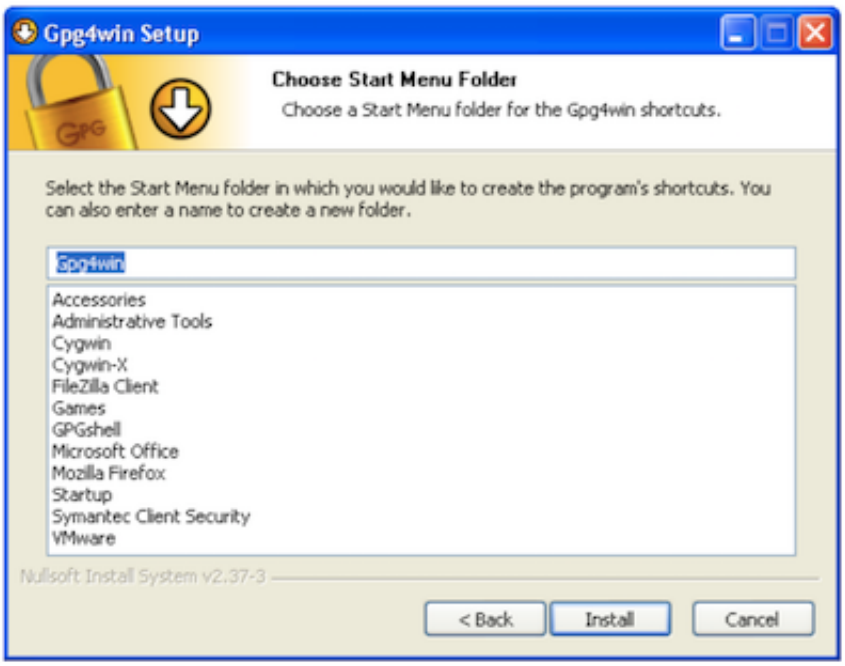
Then click on `[ Next ]`

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.



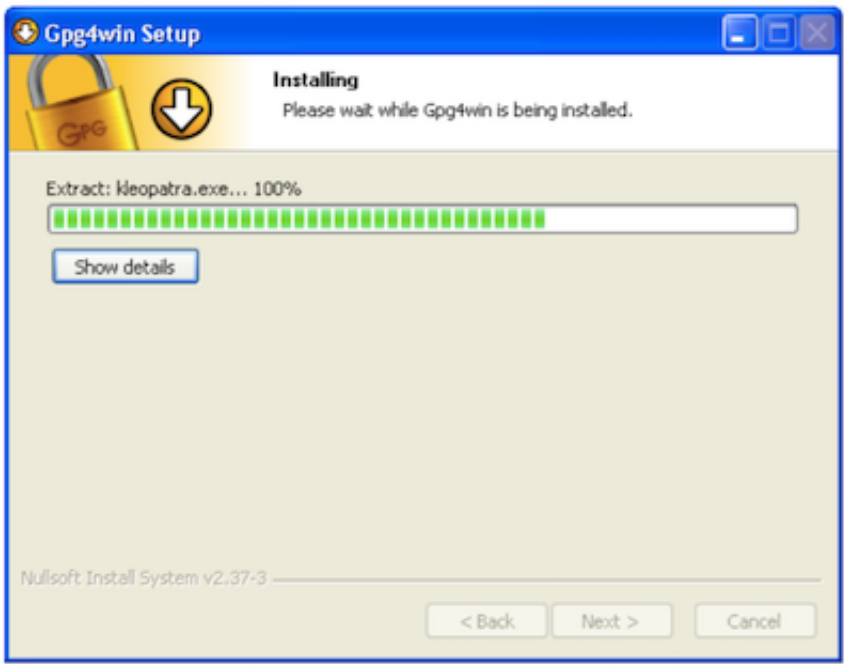
Then click on `[ Next ]`

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 ]`

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 ]`

The last page of the installation process is shown once the installation has been successfully completed:

You have the option of displaying the README file, which contains important information on the Gpg4win version you have just installed. If you do not wish to view this file, deactivate this option. Then click on `[ Finish ]`

In some cases you may have to restart Windows. In this case, you will see the following page:

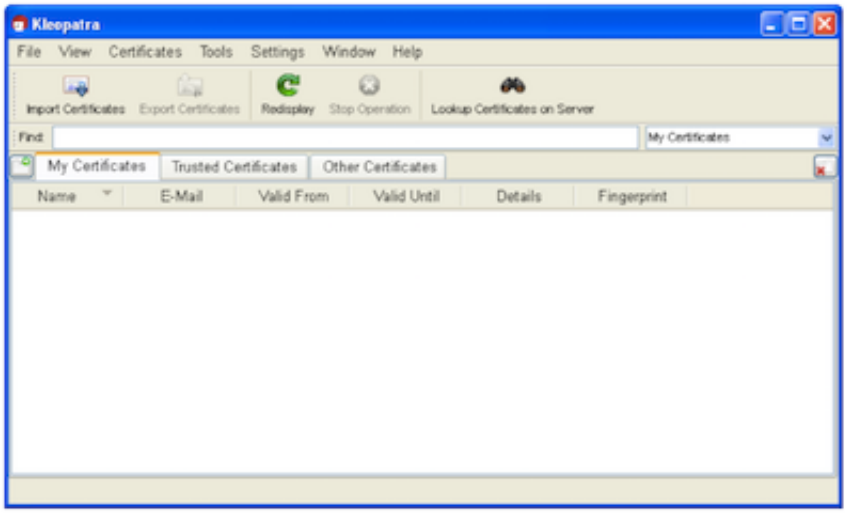
Now you can decide whether Windows should be restarted immediately or manually at a later time. Click on `[ Finish ]`

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

Create Certificate

Open Kleopatra using the Windows start menu:

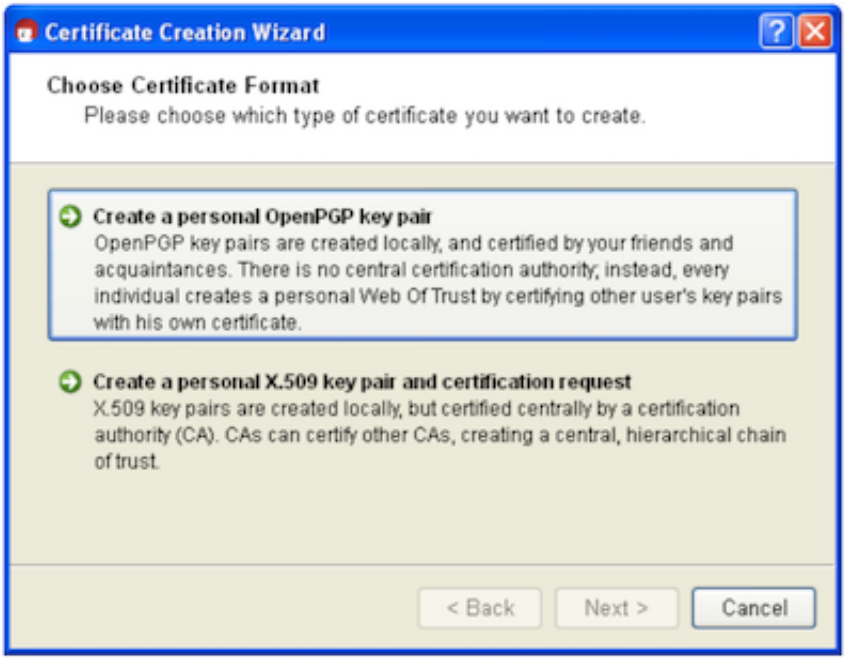
You will see the main Kleopatra screen – the certificate administration:



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).

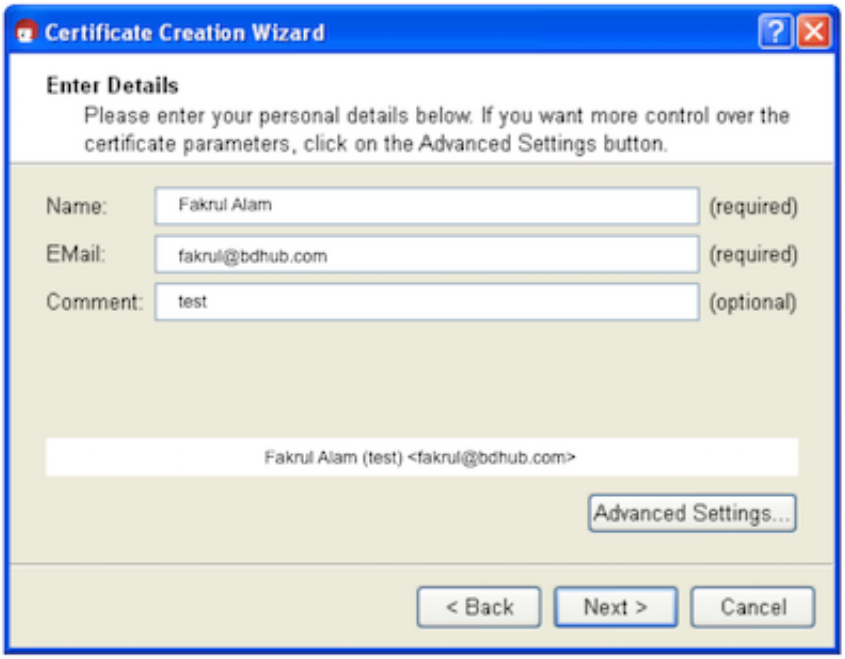


click on `[ Create personal OpenPGP key pair ]`.

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

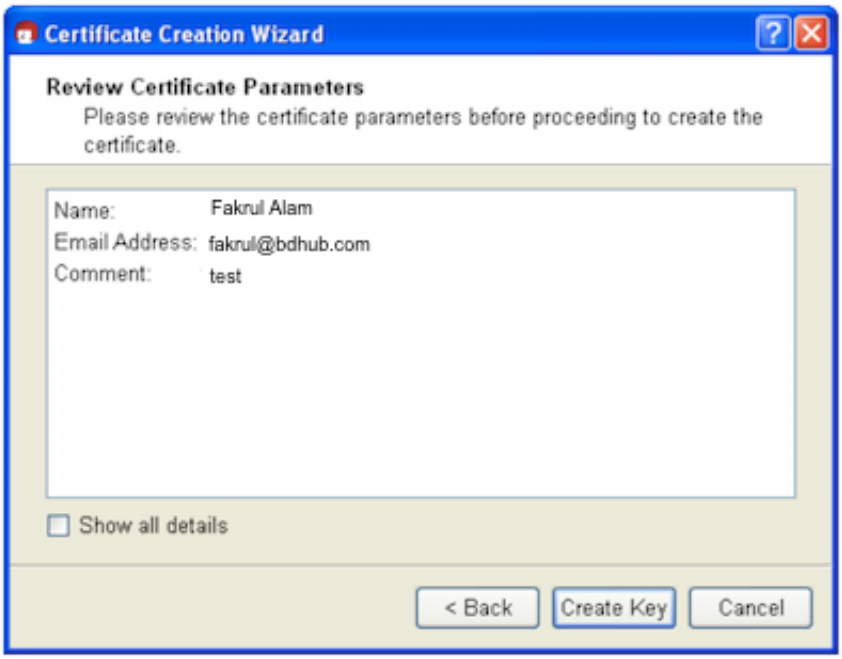
You also have the option of adding a comment for the key pair. Usually this field stays empty, but if you are creating a key for test purposes, you should enter "test" so you do not forget it is a test key. This comment becomes part of your login name, and will become public just like your name and e-mail

address.



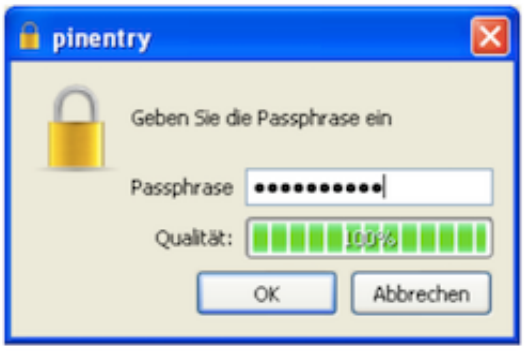
If you first wish to test your OpenPGP key pair, you can simply enter any name and fictional e-mail address, e.g.:
`Fakrul Alam` and `fakrul@bdhub.com`
Click on `[ Next ]`

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.



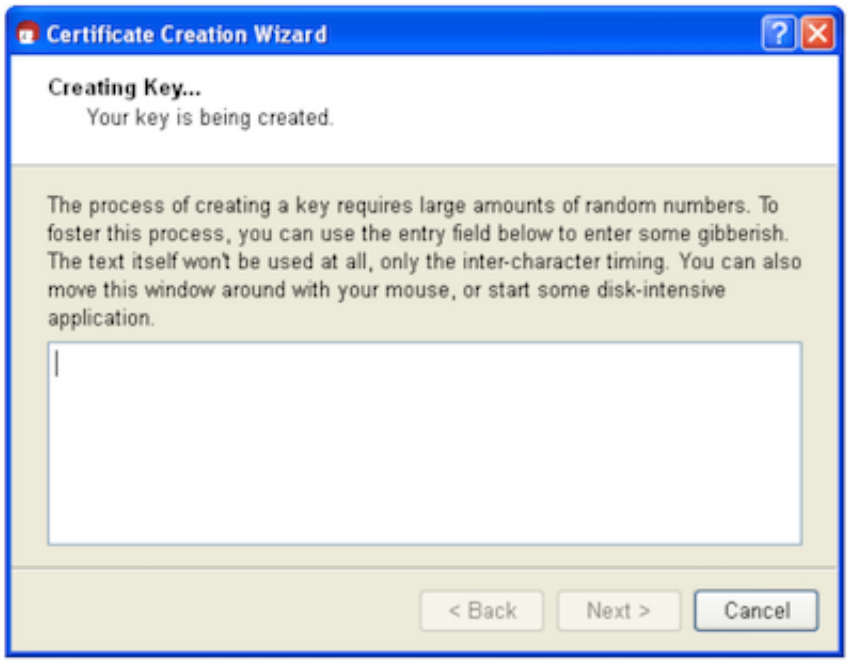
If everything is correct, click on `[ Create key ]`.

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



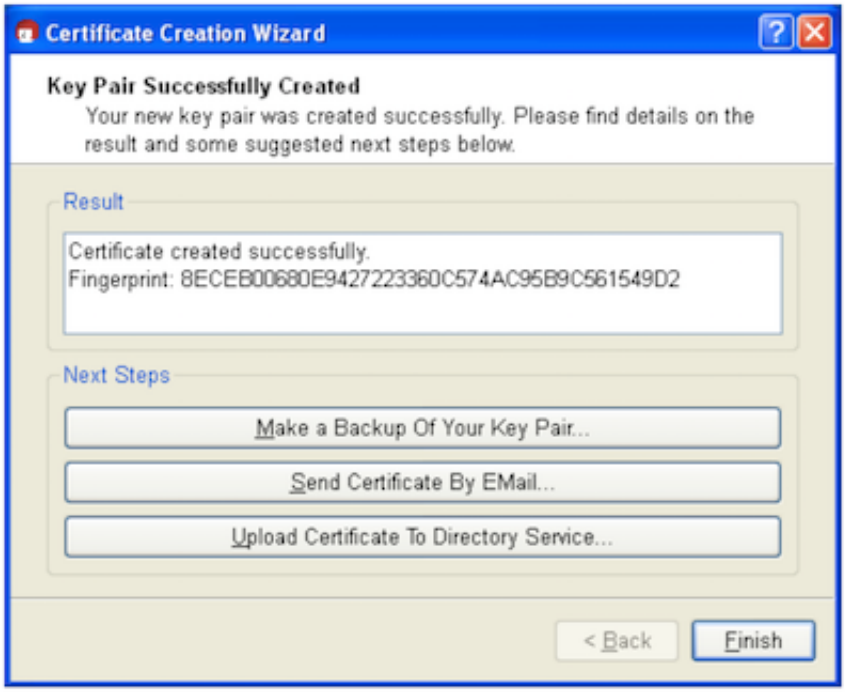
Choose passphrase which is easy-to-remember but hard to break secret passphrase.
To make sure that you did not make any typing errors, the system will prompt you to enter your passphrase twice. Always confirm your entry with `[ OK ]`.

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.

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

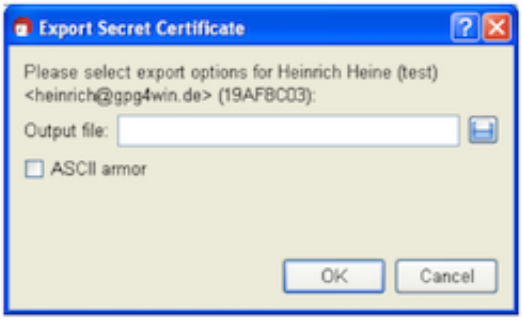


The 40-digit “fingerprint” of your newly generated OpenPGP certificate is displayed in the results text field. This fingerprint is unique anywhere in the world, i.e. no other person will have a certificate with the same fingerprint. Actually, even at 8 digits it would already be quite unlikely that the 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.

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

Next, you can activate one or more of the following three buttons:

1. Creating a backup copy of your (private) certificate...
Enter the path under which your full certificate (which contains your new key pair, hence the private and public key) should be exported:



Kleopatra will automatically select the file type and store your certificate as an .asc or.gpg file – depending on whether you activate or deactivate the ASCII armor option.

For export, click on `[ OK ]`.

You can also create a back-up copy later; to do this, select the following from the Kleopatra main menu: File→Export private certificate

2. Sending a certificate via e-mail ...

Clicking on this button should create a new onee-mail – with your new public certificate in the attachment. Your secret Open PGP key will of course not be sent. Enter a recipient e-mail address; you can also add more text to the prepared text for this e-mail.

3. Sending certificates to certificate servers...
Your certificate will be uploaded to public key server.

Signing message

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