School of Computing
Diploma in Infocomm Security Management
ST2421 Infocomm Security and Network Fundamentals

Public Key Cryptography and Email Security

Objectives: By the end of this practical exercise, you should be able to:

- Install Gpg4win program
- Generate a pair of public and private keys
- Import and export of public key
- Sign and verify the digital signature

Instructions: Submit your files of the practical task in the submission portal on PoliteMall.

Part 1

A. Use Gpg4win for Signing E-mail Messages

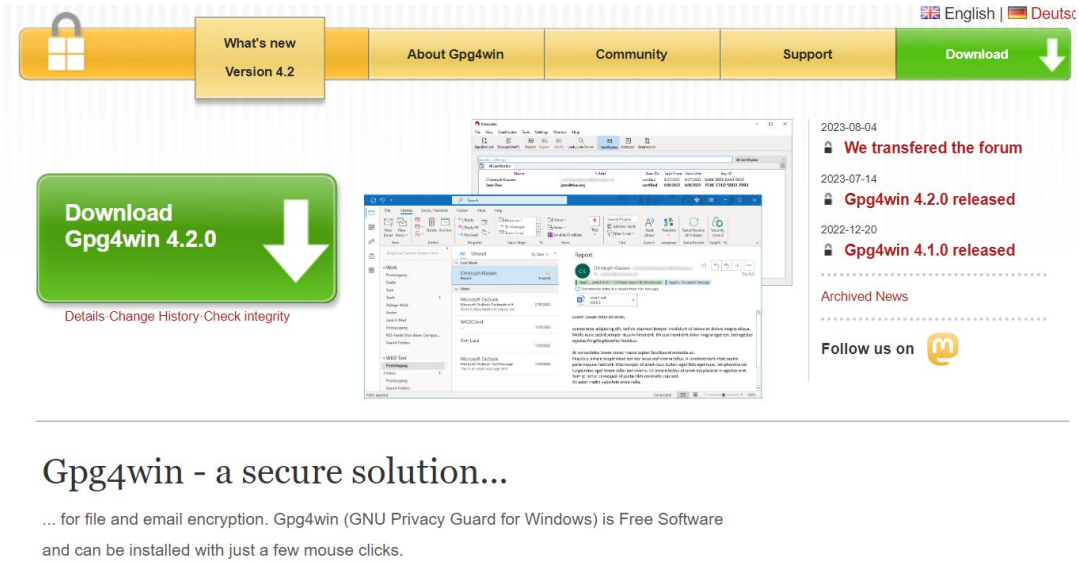
Gpg4win creates a set of public and private keys, which can be stored on a key ring. The public keys are distributed freely to others and may be used by them to encrypt material intended for your eyes only.

You then use your private key (which you must guard closely) to decipher the message. In a similar way, you can use your private key to digitally sign a document, the origin of which can then be confirmed by others using the corresponding public key.

Note: **You will be performing the following tasks to send a signed email to your partner.**

1. Open your Web browser and enter the URL **www.gpg4win.org**

Note: The location of content on the Internet such as this program may change without warning. If you are no longer able to access the program through the above URL, then use a search engine like Google (www.google.com) and search for "GnuPG".

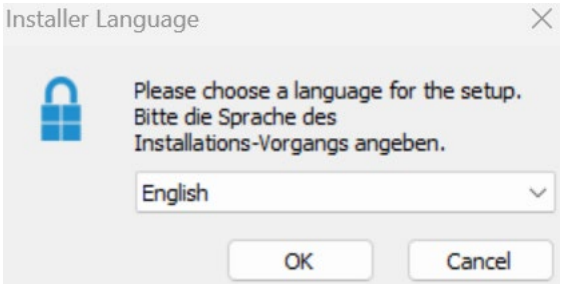


2. Click on **Download Gpg4win 4.2.0**.

3. Click **Save** and save the program to the desired location on your computer.

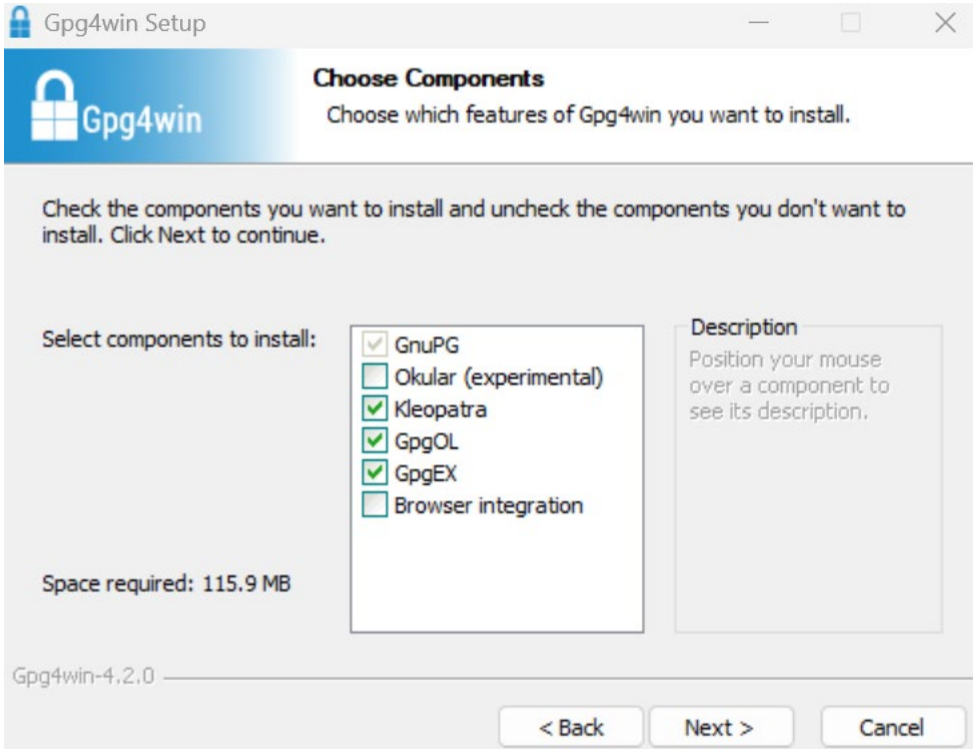
4. Alternatively, you can download the Gpg4win 4.2.0.zip file on Politemall and extract it onto your computer.

5. When the download completes, double-click on the executable file (gpg4win-4.2.0.exe) and follow the default installation instructions.

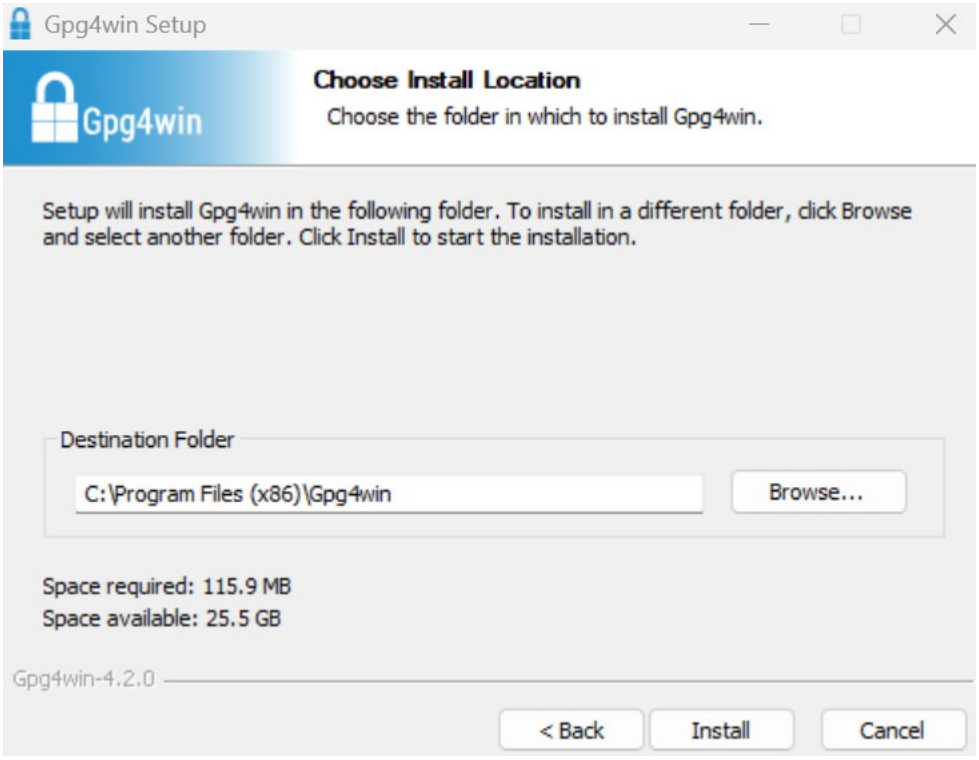


6. Click **OK** to continue and the following dialog box appears.

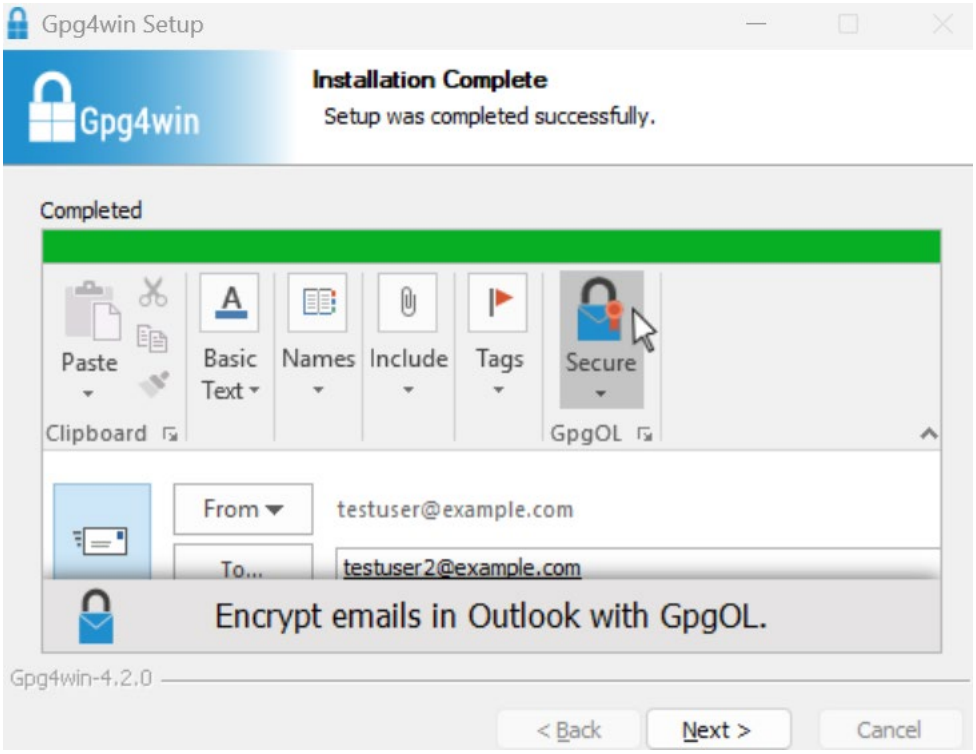
7. Click **Next >** to continue and the next dialog box appears.



8. Click **Next >** to accept the default settings.

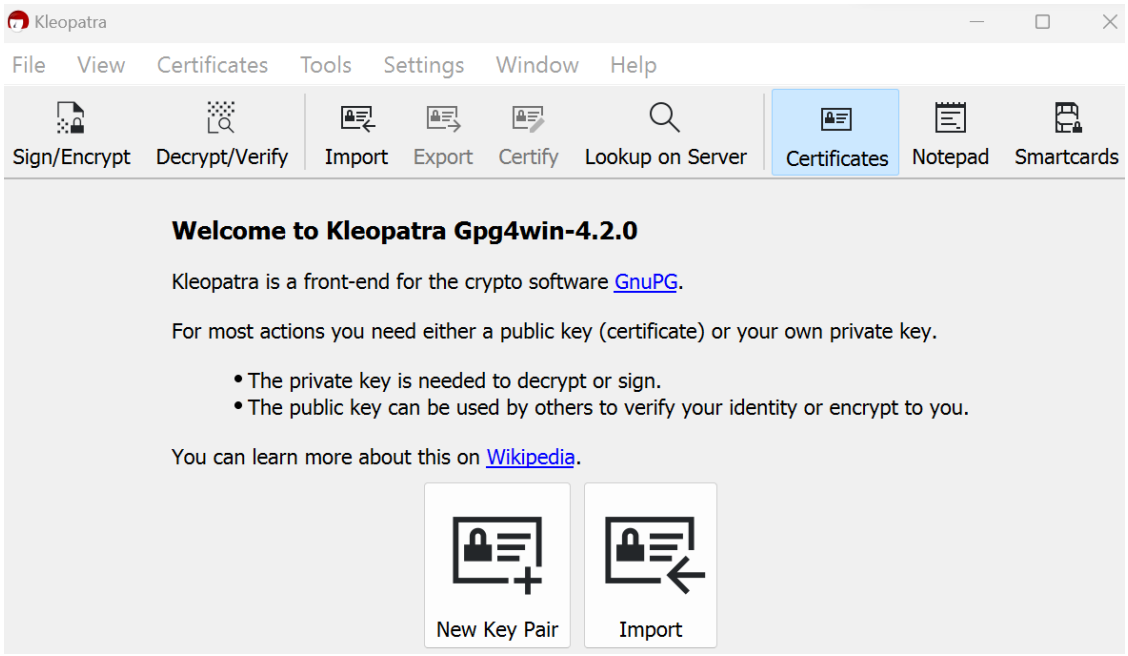


9. Click **Install** to begin the installation.

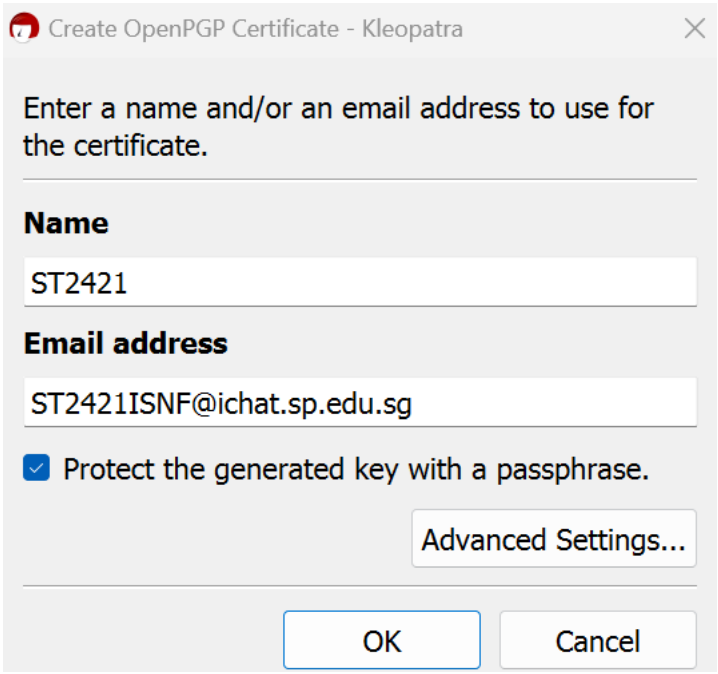


10. Click **Next >** to finish the installation.

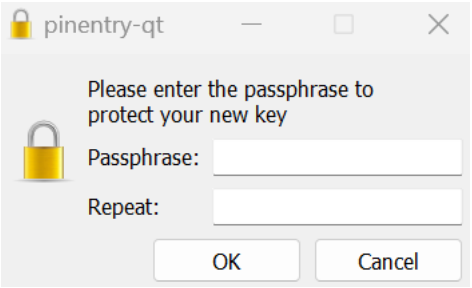
11. Leave **Run Kleopatra** checked as default. Click on **Finish**.



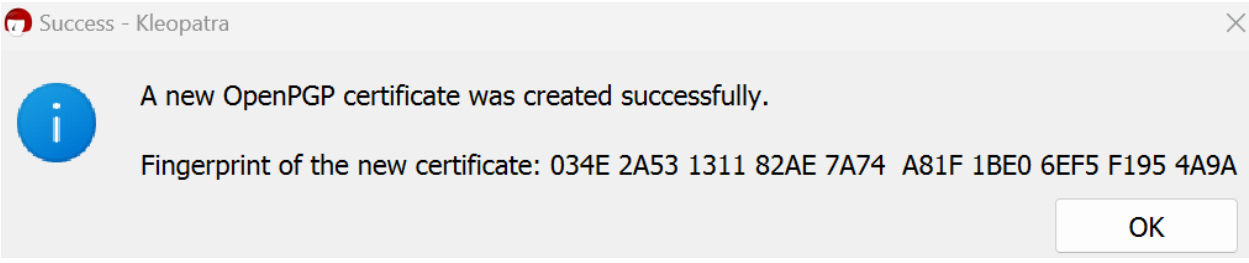
12. You will now see the **GUI** of Gpg4win-4.2.0, known as **Kleopatra**. Click on **New Key Pair** to start generating a new public key.



13. Enter your name and Email address in the dialog box. This should be a genuine email address, you can use your student email account. **Ensure to check/tick on** the **Protect the generated key with a passphrase.** Click **OK**.

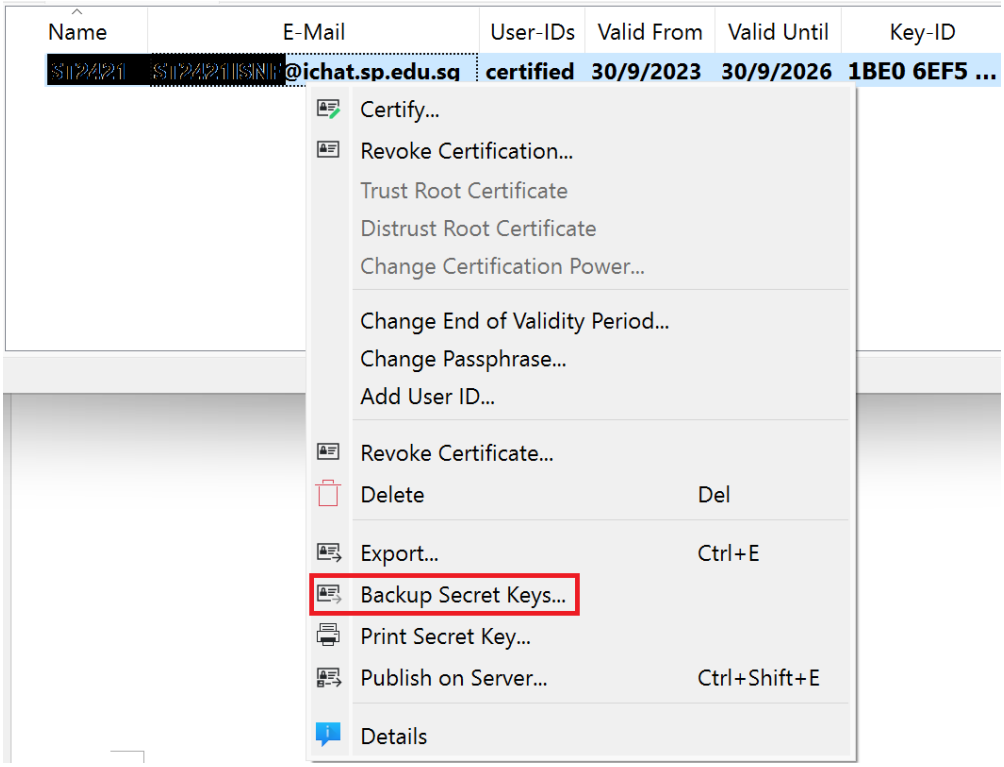


14. Enter your preferred passphrase in the box twice. You will need to ensure that the passphrase be at least 8 characters long. Else, select the **Take this one anyway** option. In a short while, the OpenPGP certificate will be shown as created successfully, along with the Fingerprint of the new certificate.

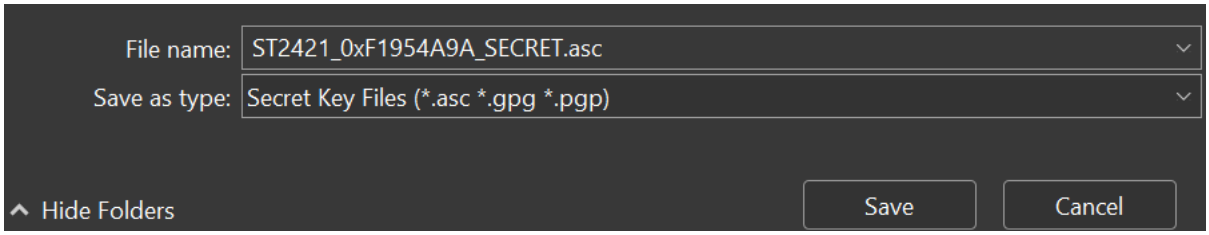


A fingerprint is a hash of a certificate, computed over all certificate data and its signature. Fingerprints are used as unique identifiers for certificates, in applications when making trust decisions, in configuration files, and displayed in interfaces.

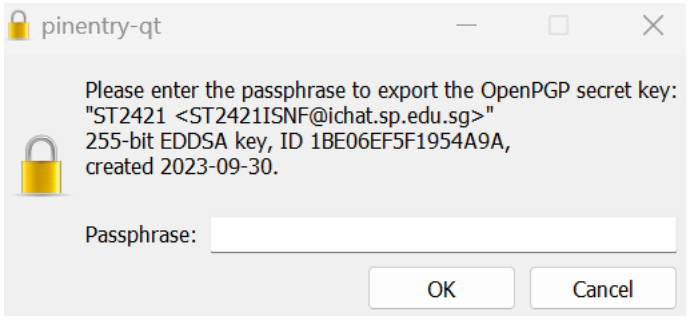
15. Click **OK** to continue.



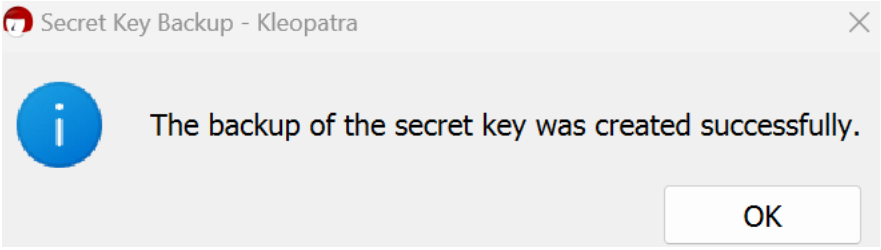
16. Save the secret key by right clicking on the newly created certificate (this is actually the private key associated with the generated public key).



17. Click **Save**.



18. Enter your Passphrase and click **OK**.



19. You will be greeted with a dialog box that says created successfully. Click **OK**.

Part 2

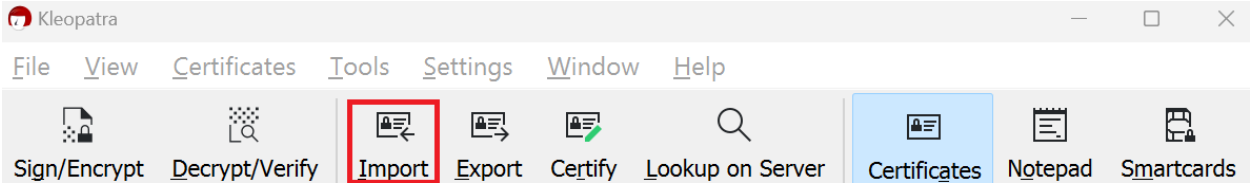
B. Export of Public Key

1. Click on the **Export** icon.

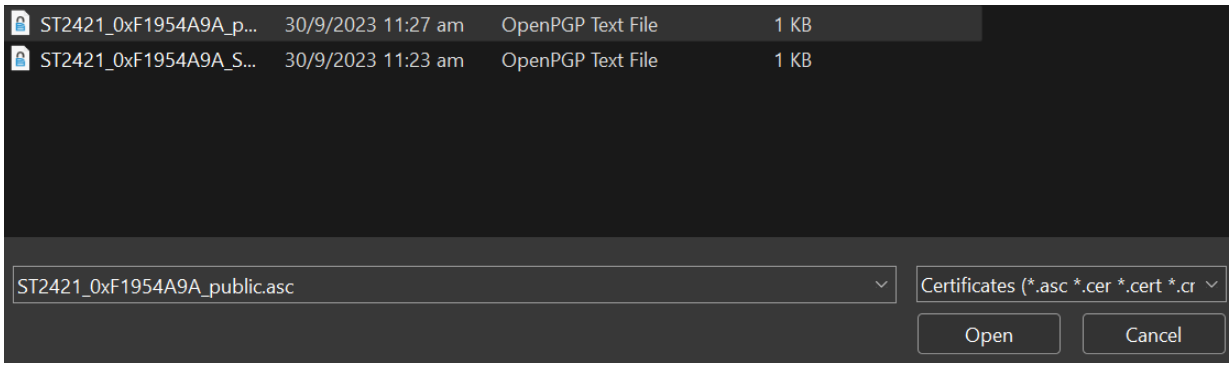
2. Leave the File name as it is, and click **Save**.

3. Send the file containing the public key to your partner. You may do so over a thumbdrive, email, social media, upload onto a cloud, etc.

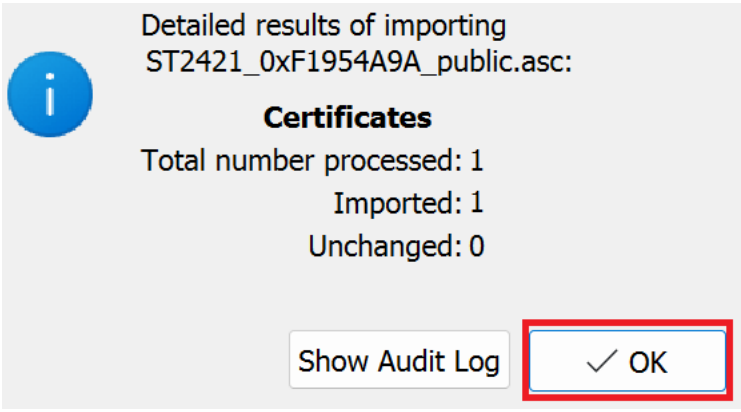
C. Import of Public Key



1. Click on the **Import** icon.



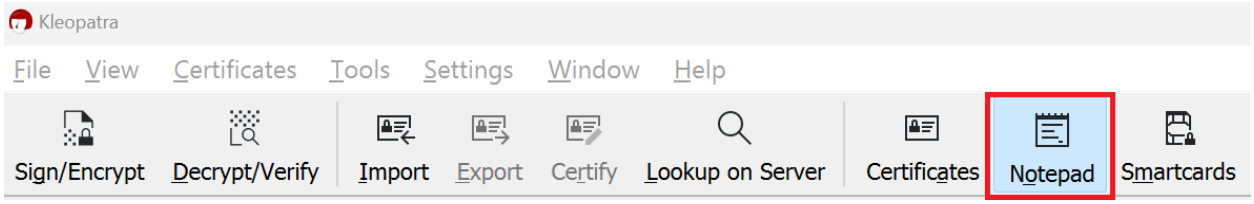
2. The following dialog box will appear, requiring you to select the public key that you send previously to your partner. Click **Open** to import the file.



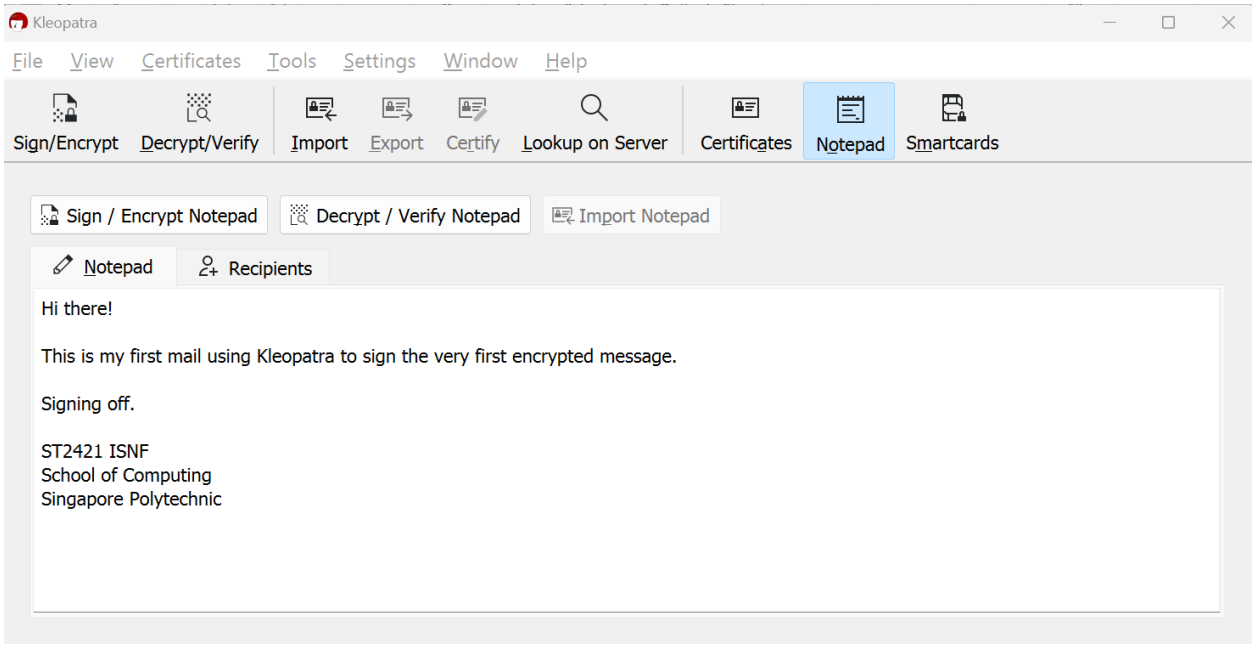
3. You will see a Detailed result of importing processed. You should see:
Total number processed: 1
Imported: 1
Unchanged: 0

Click **OK** to confirm.

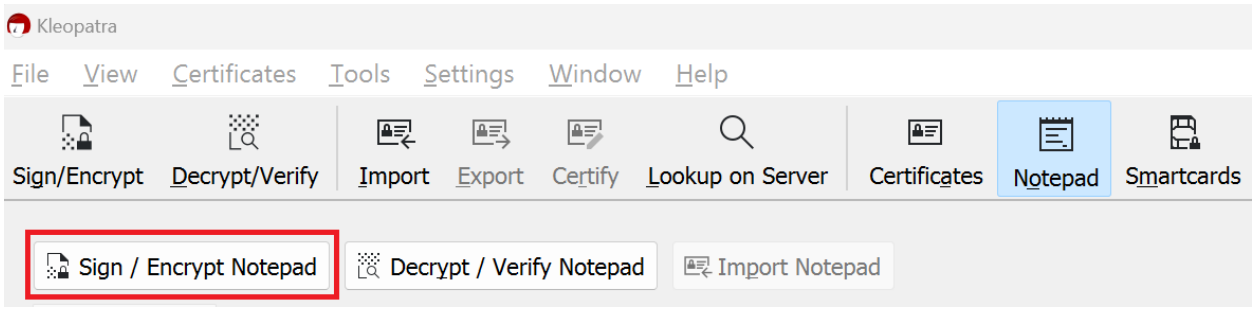
D. Signing of Email Messages



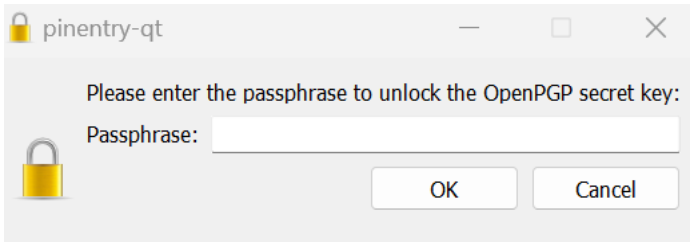
1. Click the **Notepad** icon.



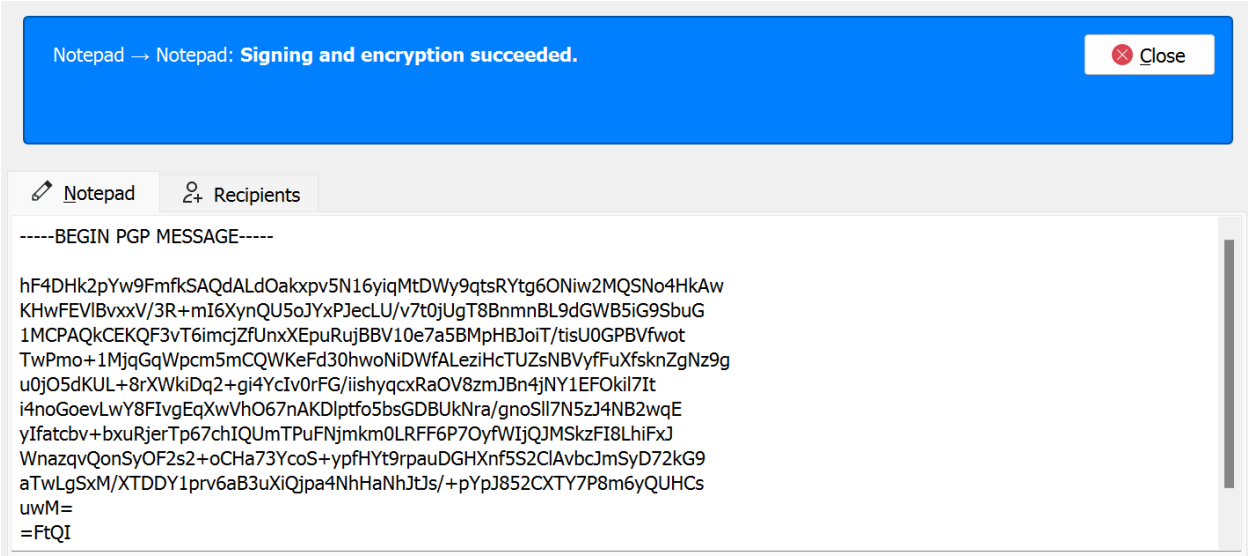
2. Type a simple message in the prompt box.



3. Click on **Sign / Encrypt Notepad**.



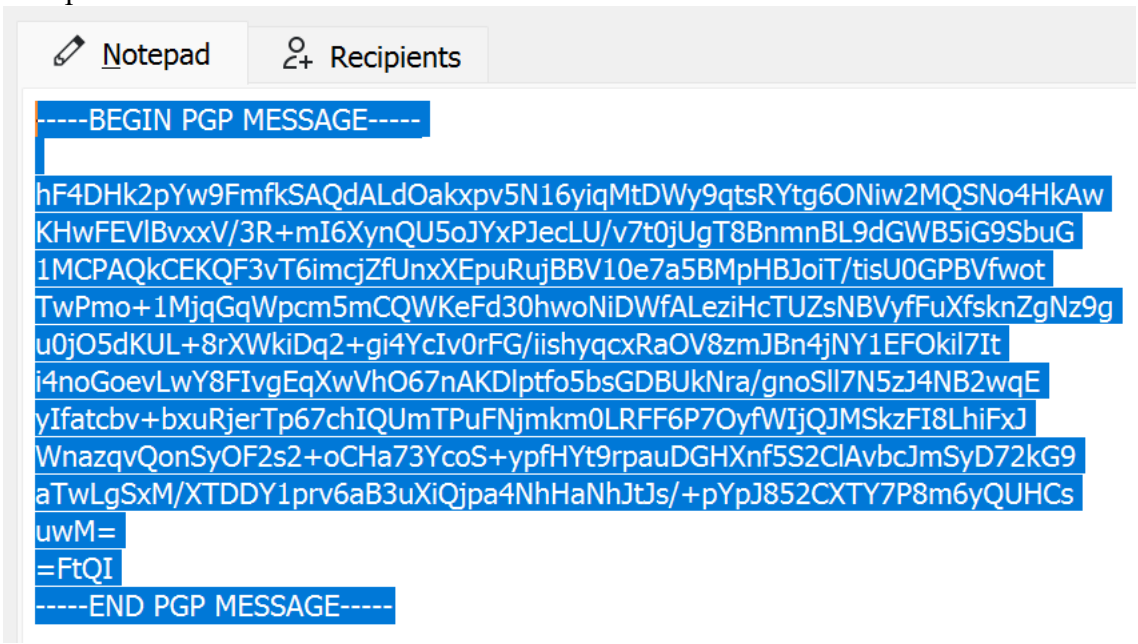
4. Key in your passphrase, then click **OK**. Kleopatra will now begin generating the digital signature.



5. Now you may select the whole text, paste them into your web-based email and send to your partner.

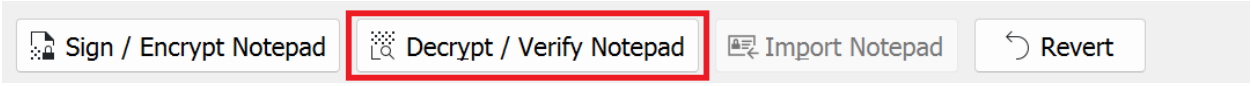
E. Verifying of Email Messages

1. When you receive the signed email message from your partner, select all text and copy to the Notepad.



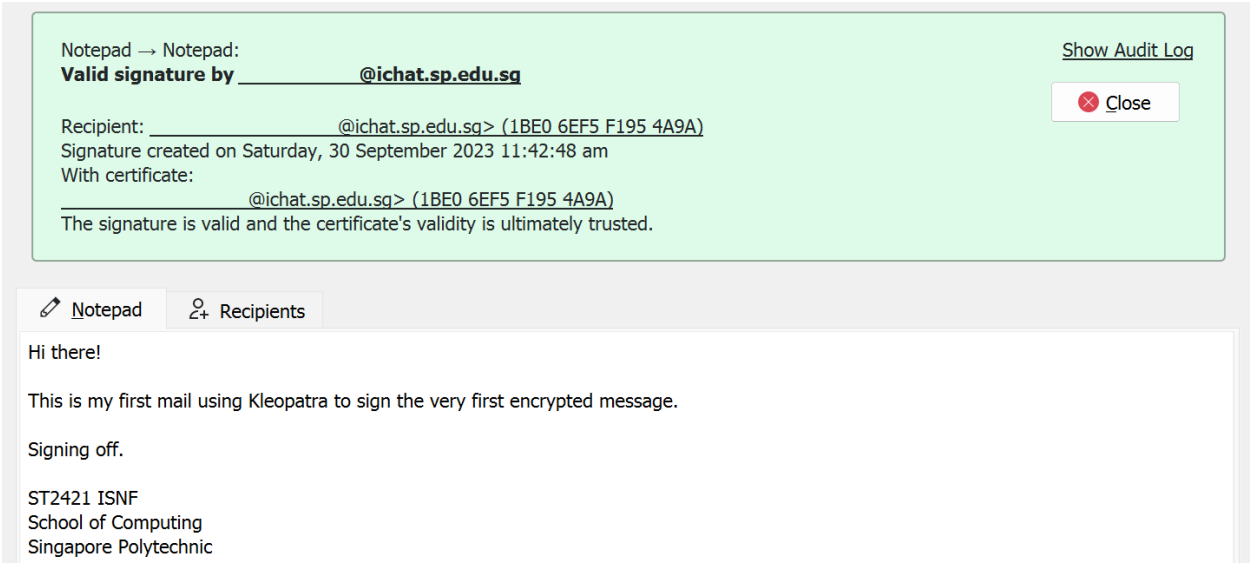
```
-----BEGIN PGP MESSAGE-----

hF4DHk2pYw9FmfkSAQdALdOakxpv5N16yiqMtDWy9qtsRYtg6ONiw2MQSNo4HkAw
KHwFEVlBvxxV/3R+mI6XynQU5oJYxPJecLU/v7t0jUgT8BnmnBL9dGWB5iG9SbuG
1MCPAQkCEKQF3vT6imcjZfUnxXEpuRujBBV10e7a5BMpHBJoiT/tisU0GPBVfwot
TwPmo+1MjqGqWpcm5mCQWKeFd30hwoNiDWfALeziHcTUZsNBVyfFuXfsknZgNz9g
u0jO5dKUL+8rXWkiDq2+gi4YcIv0rFG/iishyqcxRaOV8zmJBn4jNY1EFOkil7It
i4noGoevLwY8FIvgEqXwVhO67nAKDlptfo5bsGDBUkNra/gnoSll7N5zJ4NB2wqE
yIfatcbv+bxuRjerTp67chIQUmTPuFNjmkm0LRFF6P7OyfWIjQJMSkzFI8LhiFxJ
WnazqvQonSyOF2s2+oCHa73YcoS+ypfHYt9rpauDGHXnf5S2ClAvbcJmSyD72kG9
aTwLgSxM/XTDDY1prv6aB3uXiQjpa4NhHaNhJtJs/+pYpJ852CXTY7P8m6yQUHCs
uwM=
=FtQI
-----END PGP MESSAGE-----
```



2. Click on **Decrypt / Verify Notepad**.

3. The following dialog box appears.



4. This means that the email message is valid and is signed by the originator.

F. Optional Tasks

1. You can try encrypting a message using your friend's public key and send to him/her to decrypt the message.

2. You can also try to encrypt a file using your friend's public key and send to him/her to decrypt the file.

3. In addition, you can send your public key to a central managed directory of public keys to publicise your public key.

G. Submission task

Submit both your public.asc and secret.asc files onto the submission portal in PoliteMall.

--- End ---