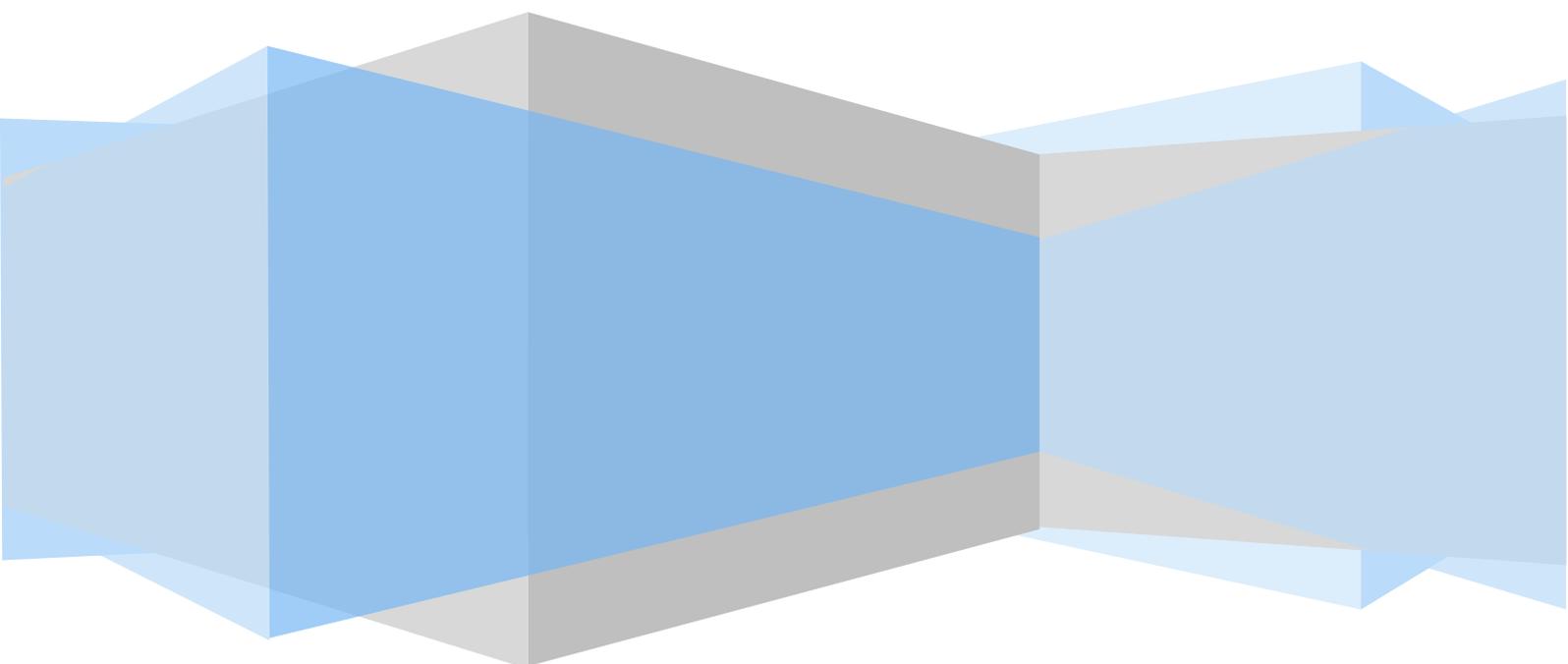# Anti-Money Laundering Council
Manila, Philippines

Transaction Security Protocol Manual

TRANSACTION SECURITY PROCESS

GUIDELINES

A. The File Transfer and Reporting Facility using the Hypertext Transfer Protocol over Secure Socket Layer (FTRF v 2.0) shall be used by the CPs in transmitting their respective reports.

B. Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a private, secure and graphical method of accessing web page information and/or sending information across a web. It is especially useful for encrypting forms-based information as it passes between clients and servers. HTTPS which is implemented under the File Transfer and Reporting Facility (FTRF v 2.0) will address the efficiency, integrity and security concerns of data collection from the Covered Persons.

C. File Transfer and Reporting Facility (FTRF) has the following features:

   a. Secure upload – provides data encryption, server authentication and message integrity;

   b. Self-signed Digital Identification & Certificate – allows encrypting and digital signing of messages; and

   c. Transactional Security Agreement – serves as a memorandum of agreement between AMLC and CP. It documents the details, terms and conditions and the use of the self-signed digital certificates.

D. The self-signed digital identification shall be implemented for all CPs. AMLC and the CPs shall use the Gnu Privacy Guard (GPG) software for their encryption and authentication and the GPG supported algorithm (MD5) for their signing. Installer of the said software shall be provided by AMLC upon registration.

E. The key of AMLC shall be used by the CPs in filling out/verifying the information stated in the Transaction Security Agreement.

F. The compliance officer of the CP shall likewise generate his private key as well as public key using GPG which shall be given to AMLC during the exchange of public keys.

G. The signed public key of the AMLC shall be used by the CPs to:

   a. Encrypt the electronic files (CTR/STR in csv format) to be submitted to AMLC; and
   b. Verify the signature of the files they will receive from AMLC.

H. The signed private key of the AMLC shall be used by AMLC to:
   a. Decrypt the encrypted files sent by the CPs which were encrypted using AMLC's signed public key; and
   b. Sign the electronic files they will send to the CPs.

I. The signed public key of the CP shall be used by the AMLC to:

a. Encrypt the validation messages that AMLC will send to the CP; and

b. Verify the signature of the files AMLC will receive from the CPs.

J. The signed private key of the CP shall be used by them to:

a. Decrypt the AMLC validation messages from AMLC; and

b. Sign the electronic files they will send to AMLC.

K. The CPs shall submit the duly accomplished notarized Transaction Security Agreement to Data Collection and Management Staff of the IMAG at the 6/F EDPC Building, BSP Complex, Malate Manila.

L. The form shall be enclosed in a sealed envelope with a signature on its flap.

M. After the exchange of keys, CPs are required to perform the back-up procedures of his public and private keys.

N. CPs are required to encrypt and sign the electronic CTR/STR files before transmitting them to AMLC via https (AMLC portal).

O. In cases wherein the public key is compromised, superseded or no longer in use, CPs should perform the recovery procedure, only if they have successfully performed the back-up procedure of their existing private and public keys, to be able to continue to encrypt file. Otherwise, a new pair of public and private keys shall be generated and newly accomplished Transaction Security Agreement shall be issued. CPs shall follow the same procedures discussed above.

TRANSACTION SECURITY PROTOCOL

1. Installing the GnuPG for Windows Software (Gpg4win 2.1.0)

- Download the gpg4win 2.1.0 from www.amlc.gov.ph, under Reporting Tools, then save this to your local drive.
- Double click **gpg4win-2.1.0.exe**. You will be asked if you want to allow the program to make changes in your computer.
- Click **Yes**. The Installer Language window will be displayed on the screen.
- Select *English*, then click **Ok**.

The Gpg4win Setup window will be displayed on the screen. Click **Next**.

The License Agreement window will be displayed on the screen. Click **Next**.
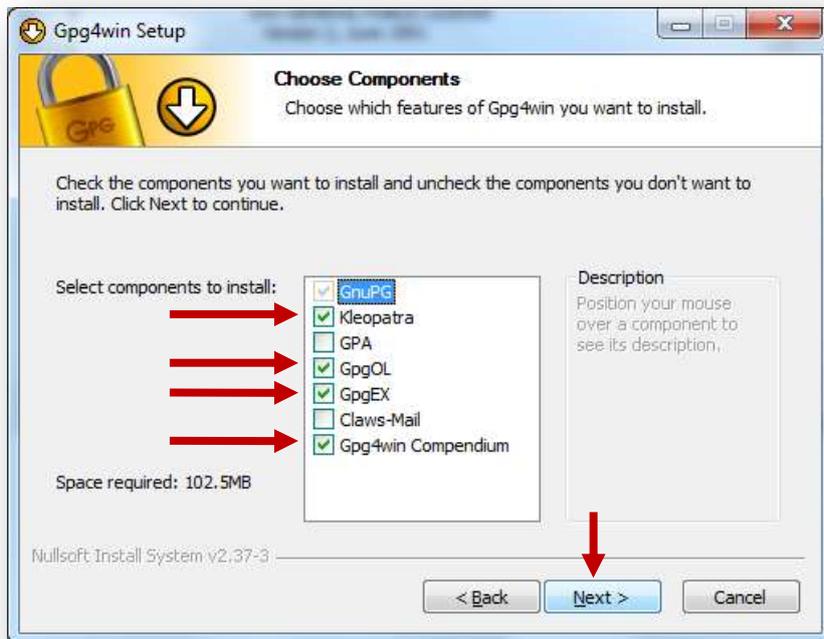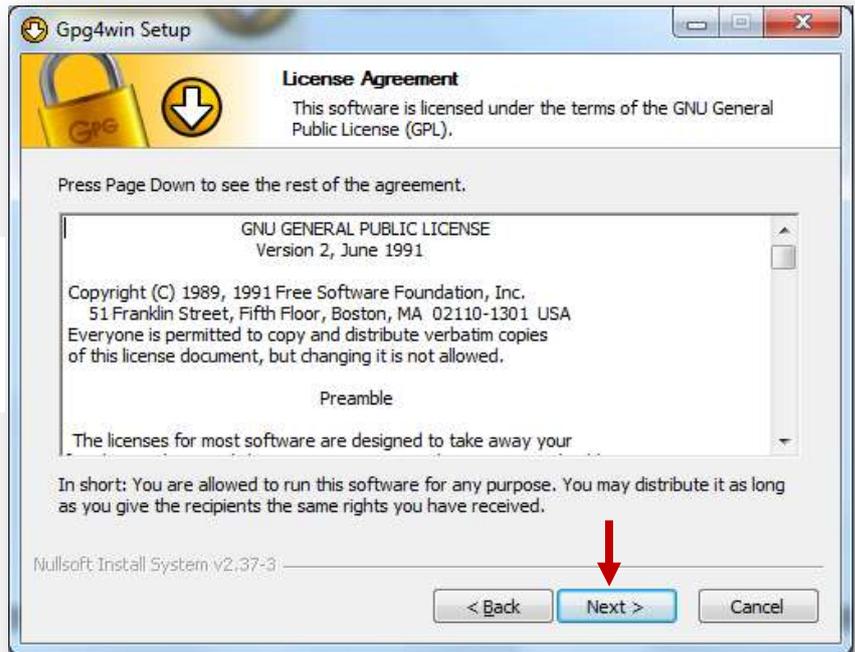
Select components to install. Check *Kleopatra*, *GpgEX*, and *Gpg4win Compendium*, then uncheck other components. Click **Next**.

Specify destination folder, then, click **Next**.

- **For 32 bit machine** the default directory is **C:\Program Files\GNU\GnuPG.**
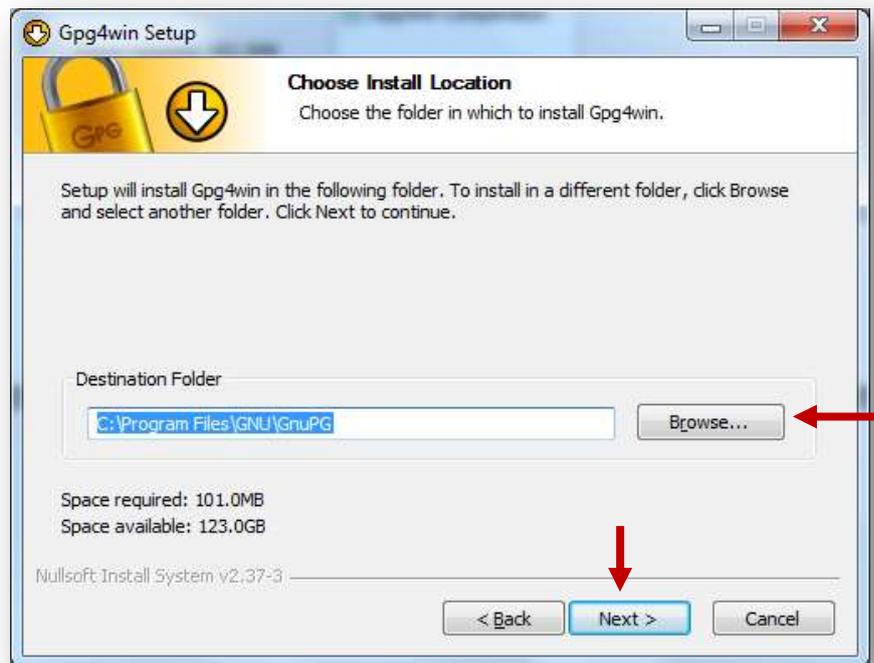
- **For 64 bit machine** the default directory is **C:\Program Files (x86)\GNU\GnuPG.**

Select where Gpg4win shall install links. Check **Start Menu** and **Desktop**, then click **Next**.
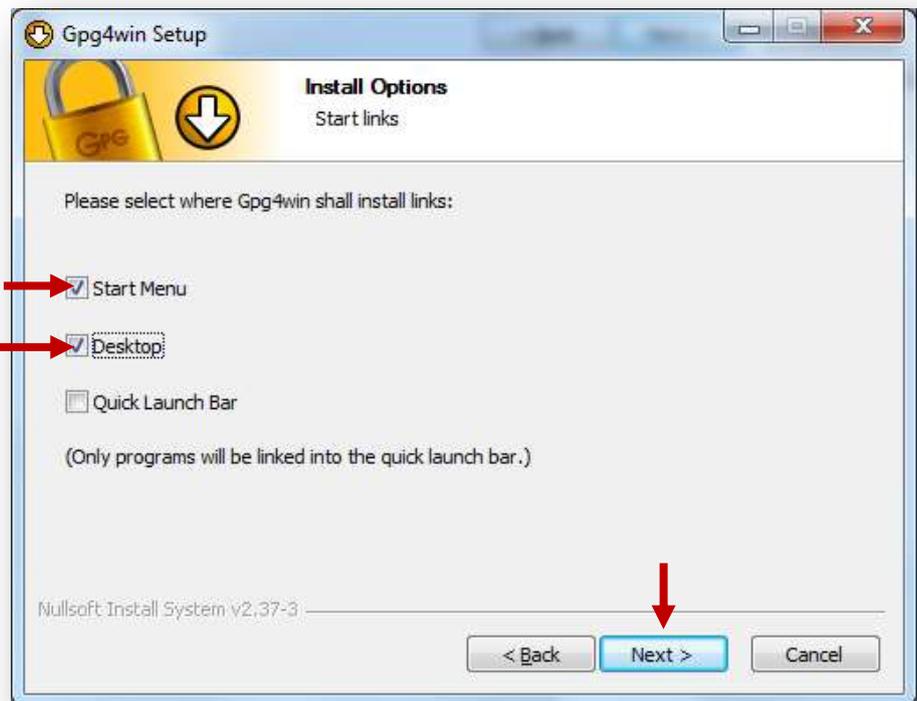
Choose Start Menu folder for the Gpg4win shortcuts. Enter **Gpg4win**, then click **Install**.

Please wait while Gpg4win is being installed.
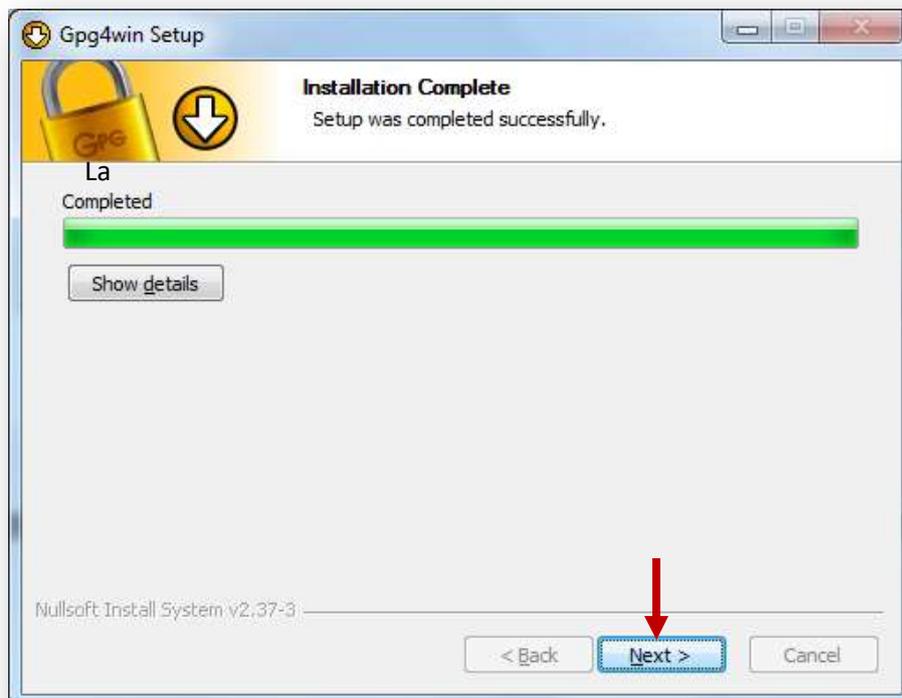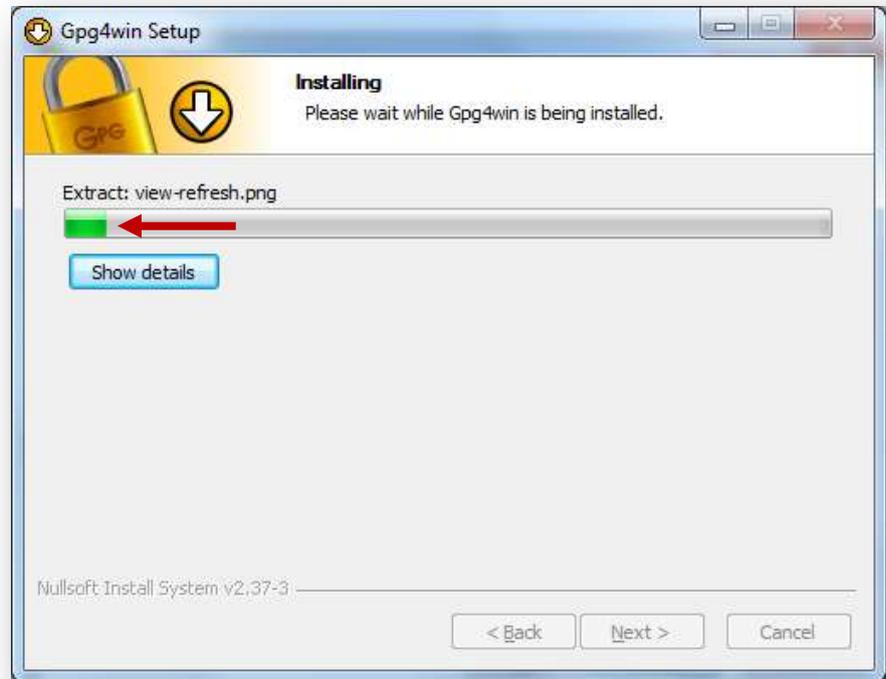
Once the setup is completed successfully, click **Next**.

Check Root certificate defined or skip configuration, then click **Next**.

Click **Finish**.

2. Generation of Key Pairs (One time Procedure)

From your desktop, double click **Kleopatra**. The Kleopatra main window will be displayed on the screen.
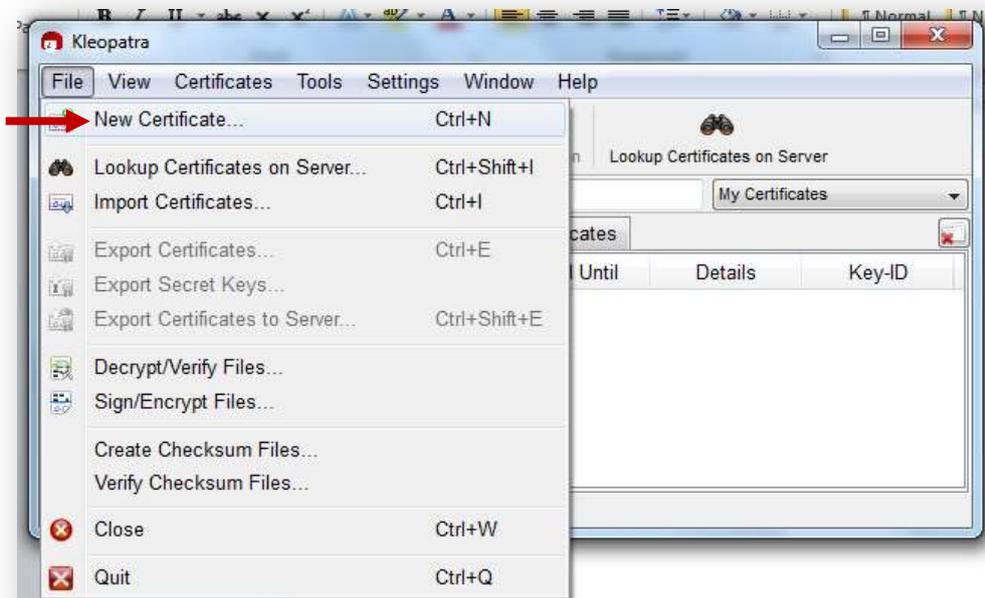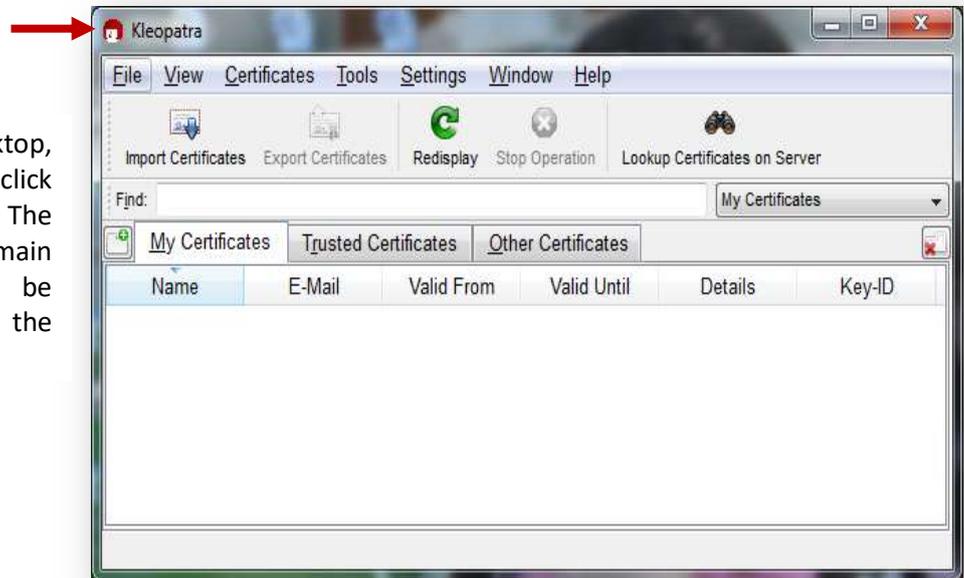
Click **File**, then select **New Certificate**.

Certificate Creation Wizard will be displayed on the screen. *Click Create a personal OpenPGP key pair*.
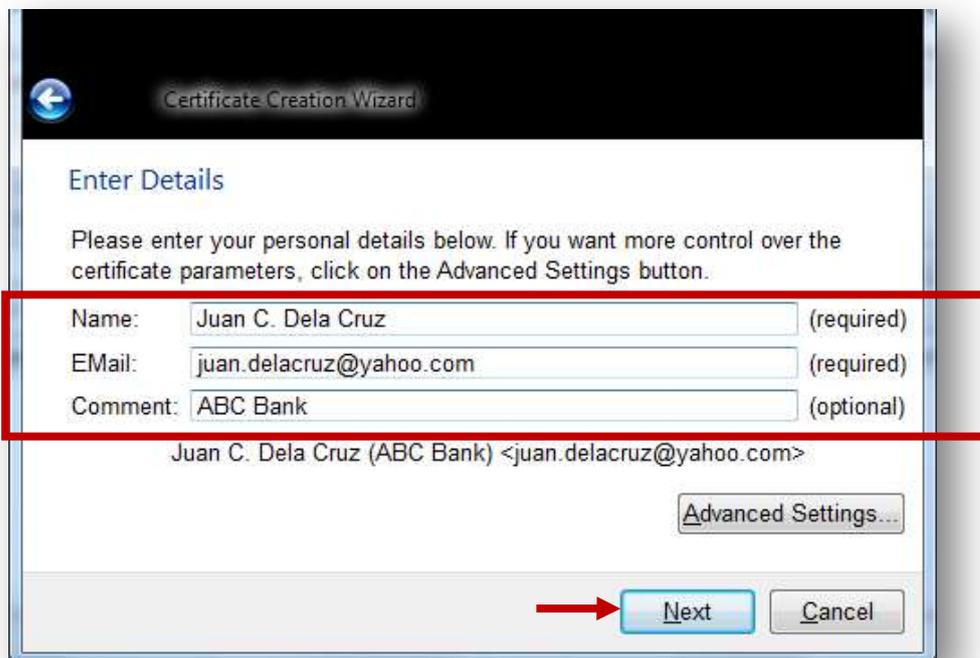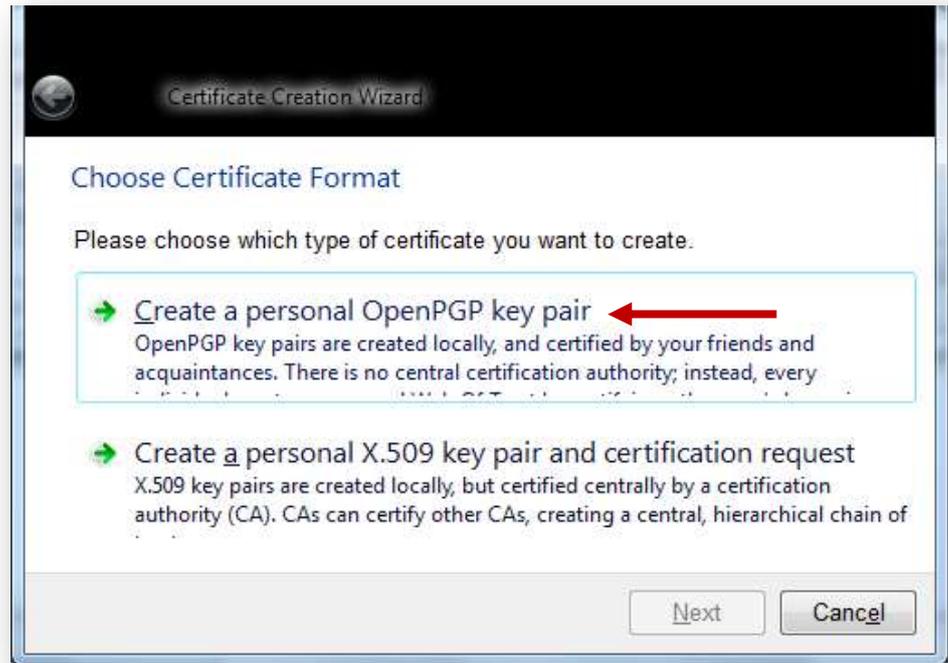
Enter Details, then click **Advance Settings**.

Note:
           Name – Name of Compliance Officer
           Email – Email address of Compliance Officer
           Comment – Name of the company

The **Technical Details** window will be displayed on the screen.

- From Key Material, select **DSA: 2,048 bits (default).**

- Check **+ Elgamal : 2,048 bits (default).**

- From Certificate Usage, check *Signing*, *Encryption* and *Certification*.

- Click **Ok**.
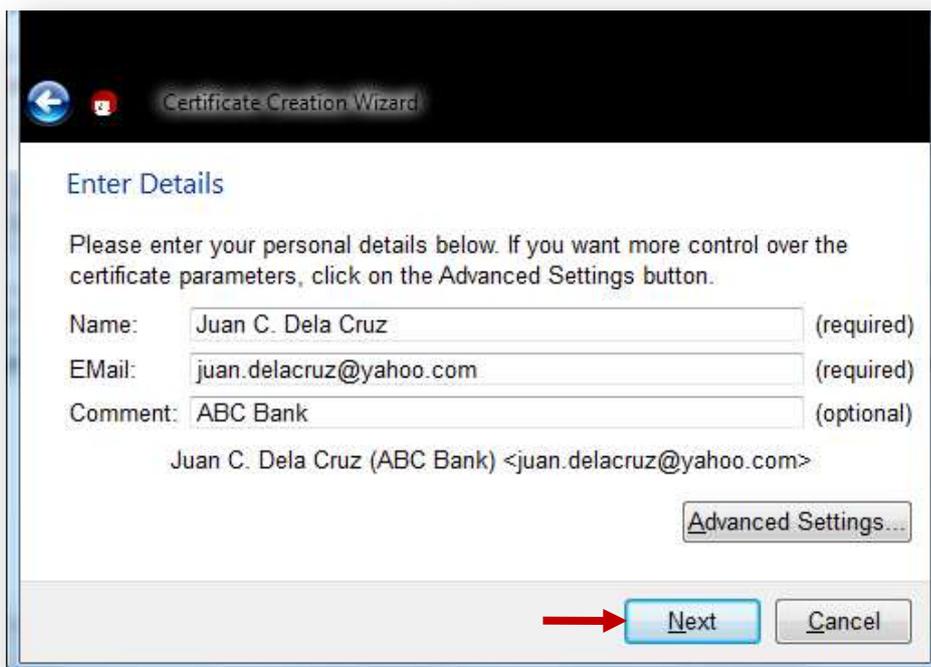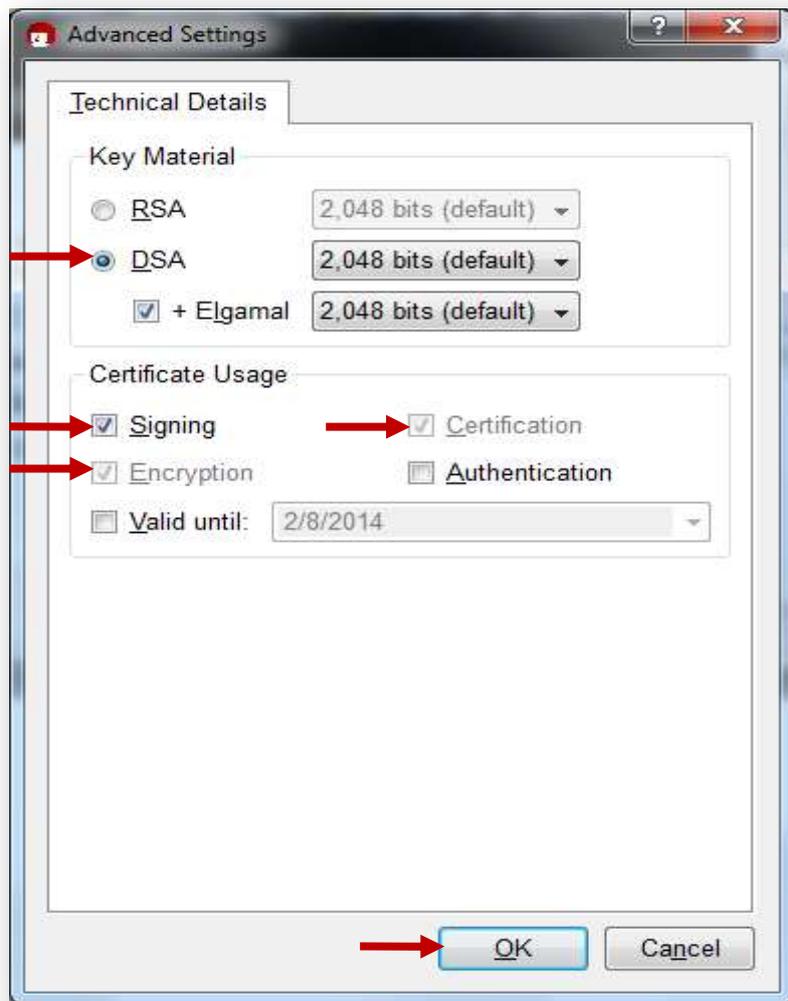
From the Certificate Creation Wizard window, click **Next**.

From Certificate Creation Wizard, check **Show all details**, review the certificate parameters, then click **Create Key**.
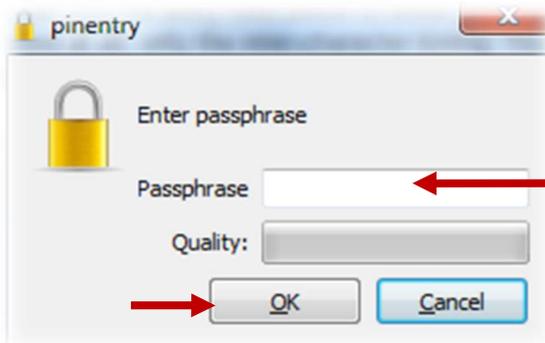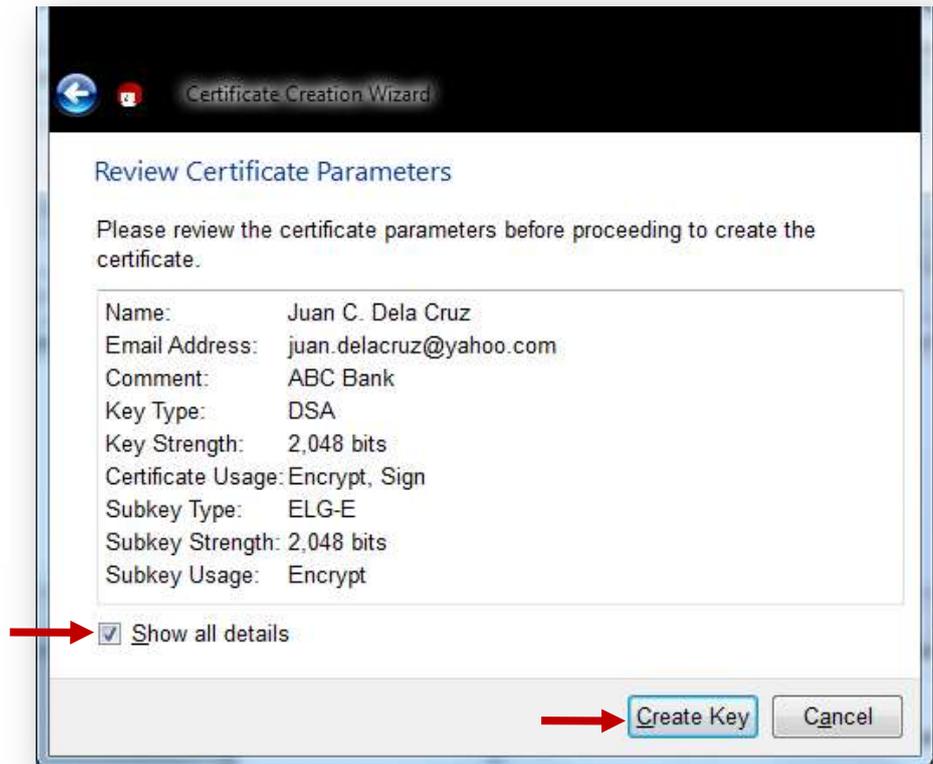
Pinentry window will be displayed on the screen. Enter Passphrase (gpg password of compliance officer), then click **Ok**.

Re-enter passphrase, then click **Ok**.
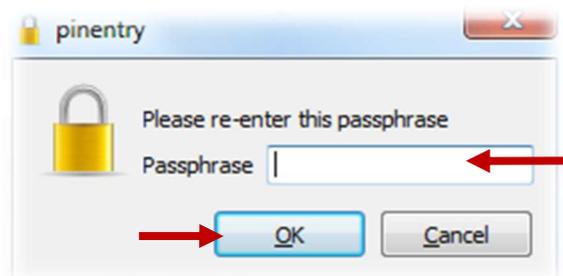
Please be reminded that once you forget your passphrase, you need to generate a new public key, since AMLC cannot retrieve the said passphrase.
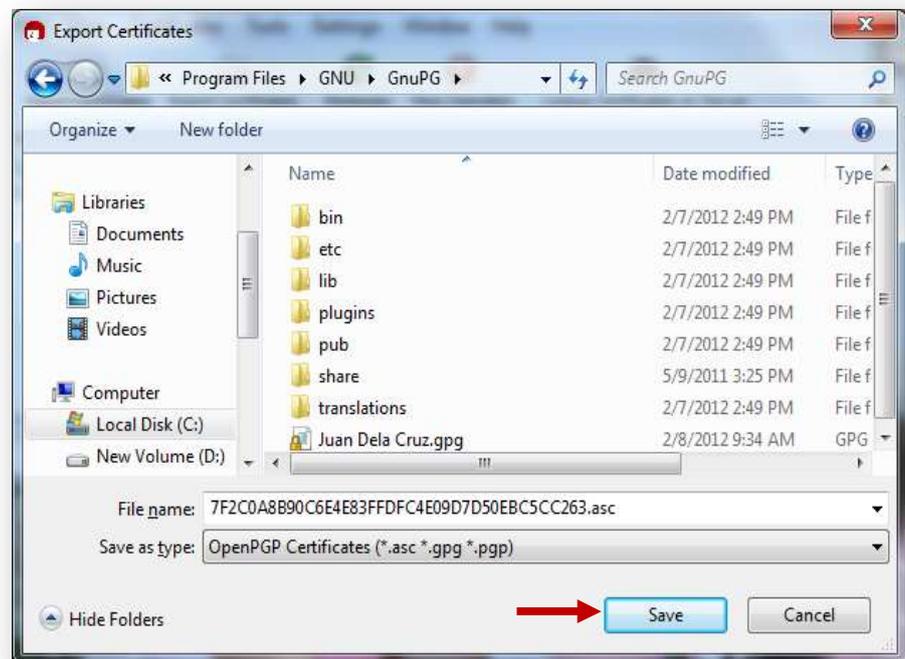
Wait until the key pair is successfully created.

Click **Finish**.

3. Exporting Public Key
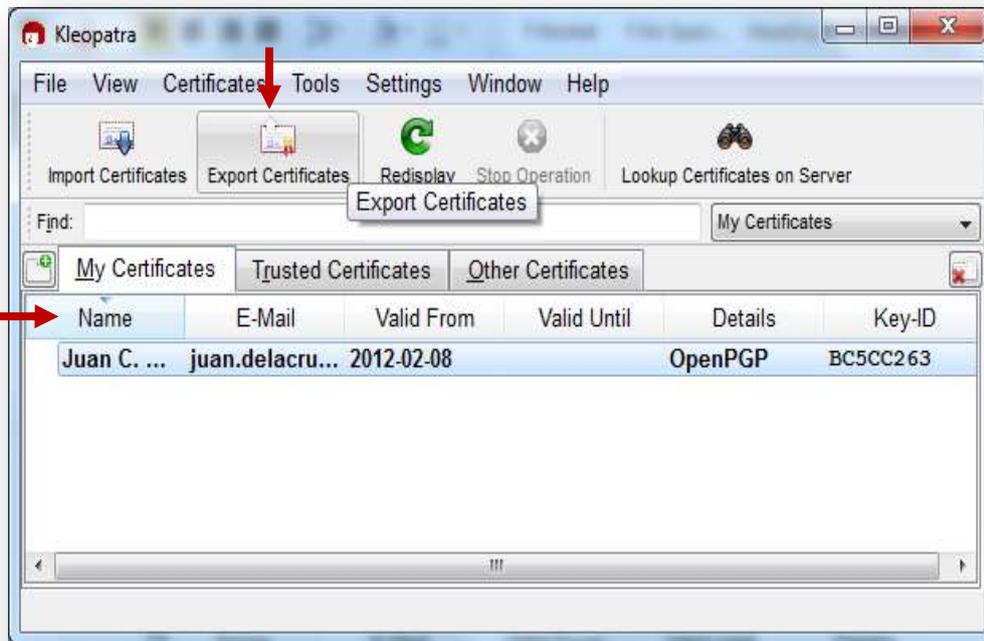
From your desktop, double click **Kleopatra**. The Kleopatra main window will be displayed on the screen.
Click the name of the compliance officer, then click **Export Certificates**.

Select the directory where the public key is to be saved, then click **Save**.

- **For 32 bit machine:** c:\Program Files\GNU\GnuPG\
- **For 64 bit machine:** c:\Program Files (x86)\GNU\GnuPG\

Note: The default filename of the public key is the key fingerprint.

Please be ready with the exported asc file as you will need this for ONLINE REGISTRATION

4. Saving AMLC public key

Get a copy of the AMLC public key (amlc.asc) from **www.amlc.gov.ph** under **Reporting Tools then save this to your local drive.**

- ▪ **For 32 bit machine:** c:\Program Files\GNU\GnuPG\
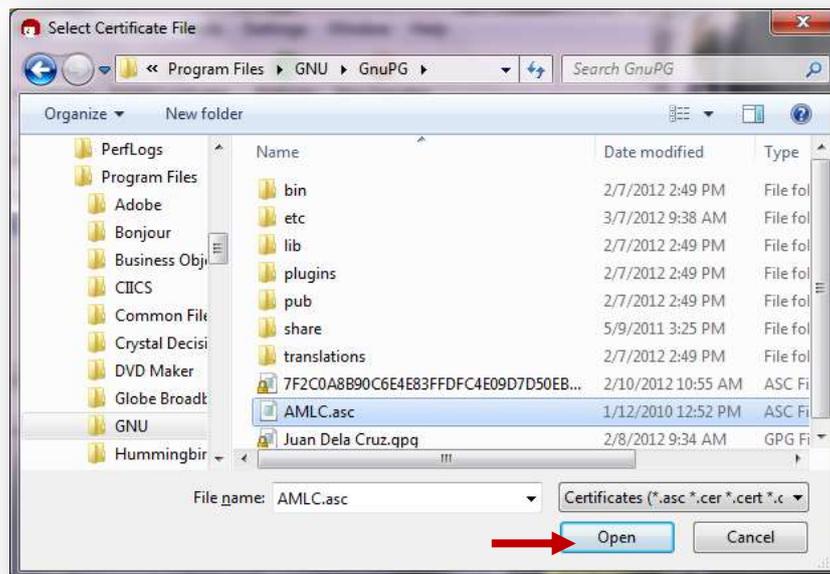- ▪ **For 64 bit machine:** c:\Program Files (x86)\GNU\GnuPG\
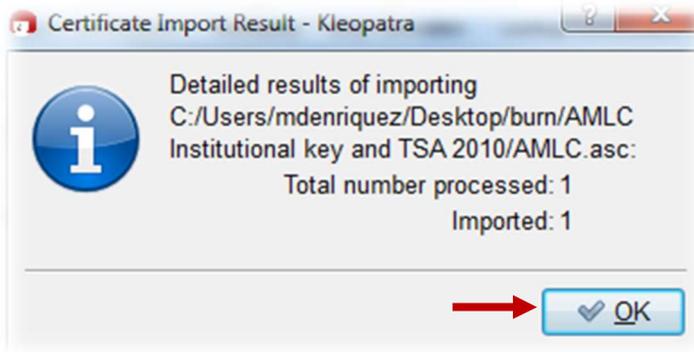
5. Importing of AMLC public key
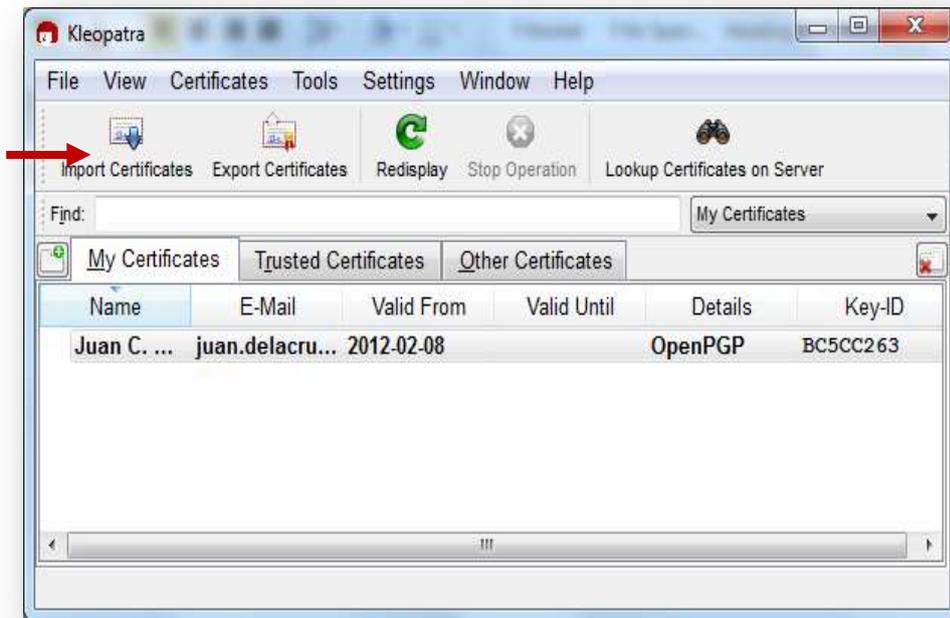
From your desktop, double click **Kleopatra**. The Kleopatra main window will be displayed on the screen.
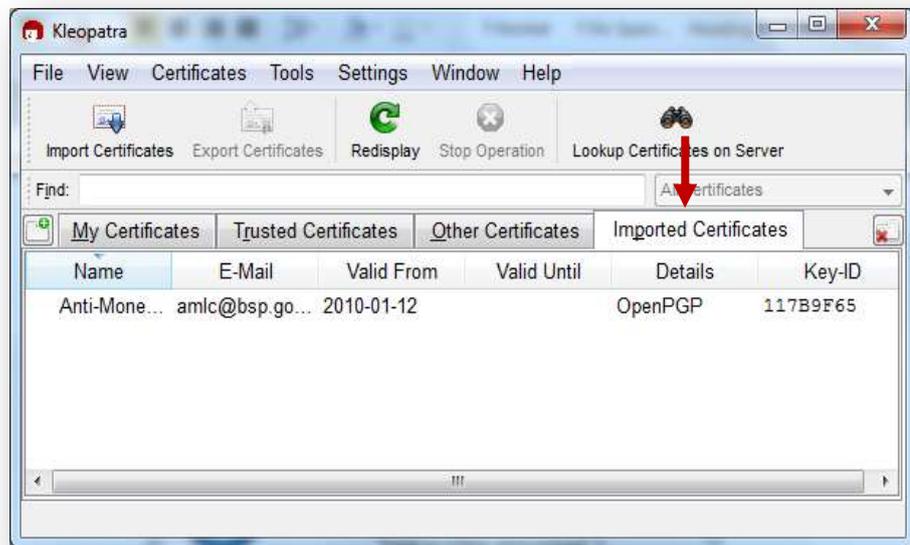
Click **Import Certificates**.

Select the directory where you have saved the **AMLC.asc**, then click **Open.**

The Certificate Import Result window will be displayed on the screen. Click **Ok**.

The imported public key will be displayed on Kleopatra – Imported Certificates tab.
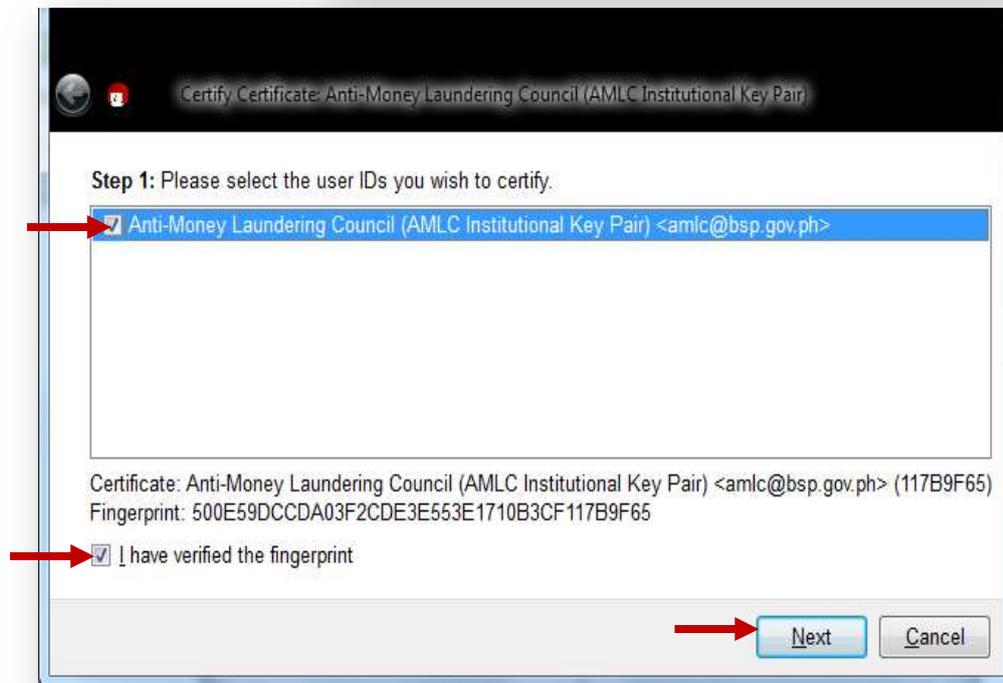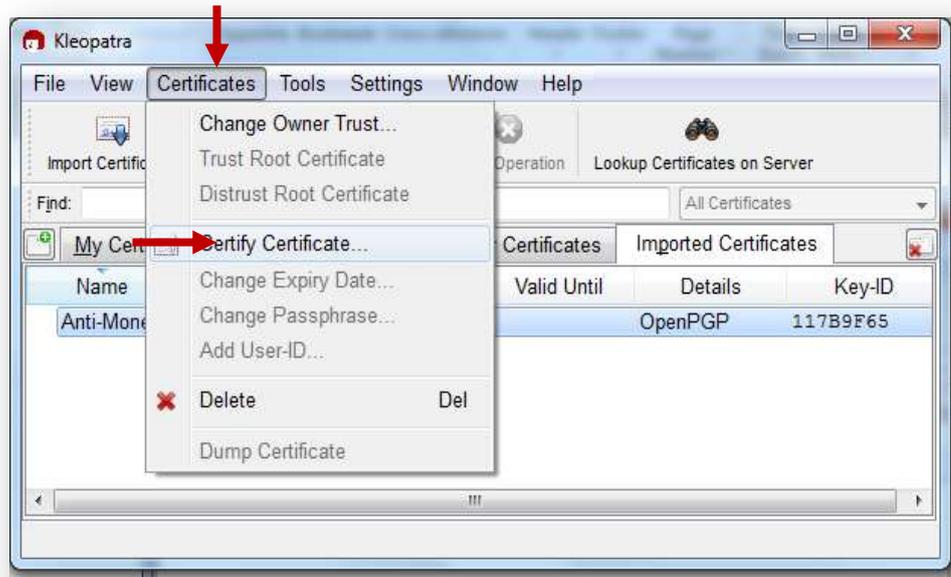
6. Certifying AMLC Key
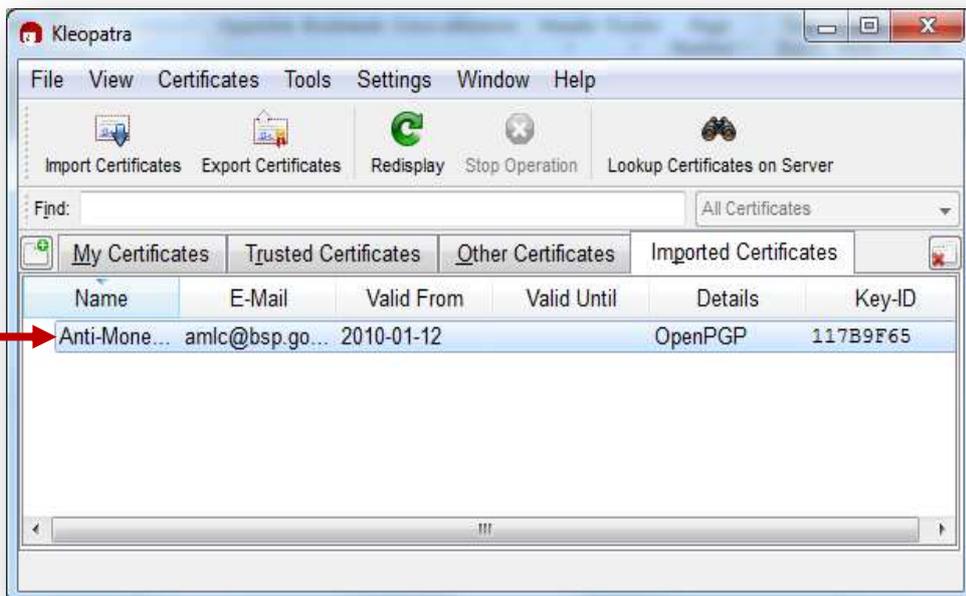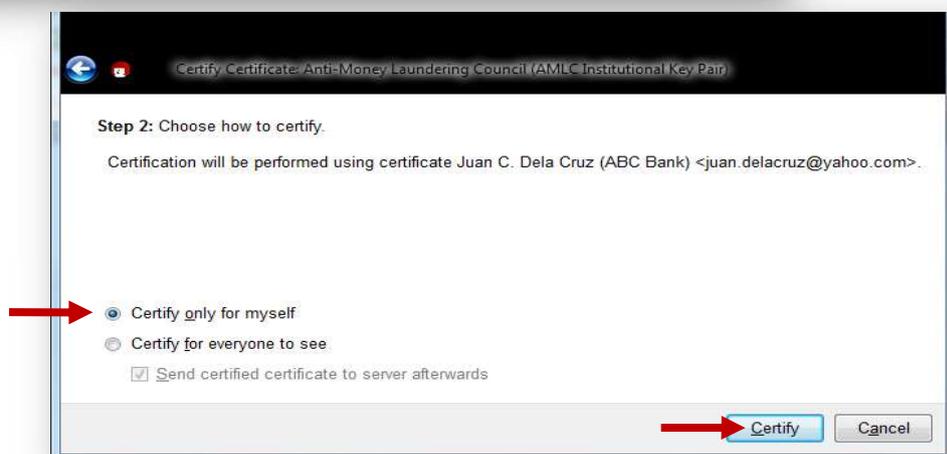

From your desktop, double click **Kleopatra**.

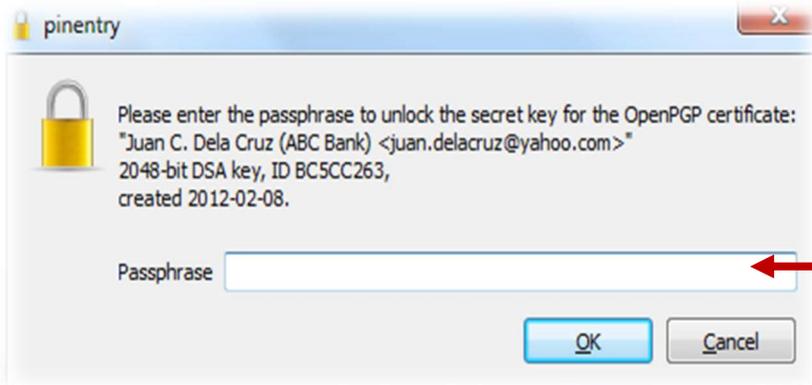From Kleopatra main window, click ***Anti-Money Laundering Council's public key***.

From the menu bar, click **Certificates**, then click **Certify Certificate**.

Check **Anti-Money Laundering Council**, then check **I have verified the fingerprint**. Click **Next**.
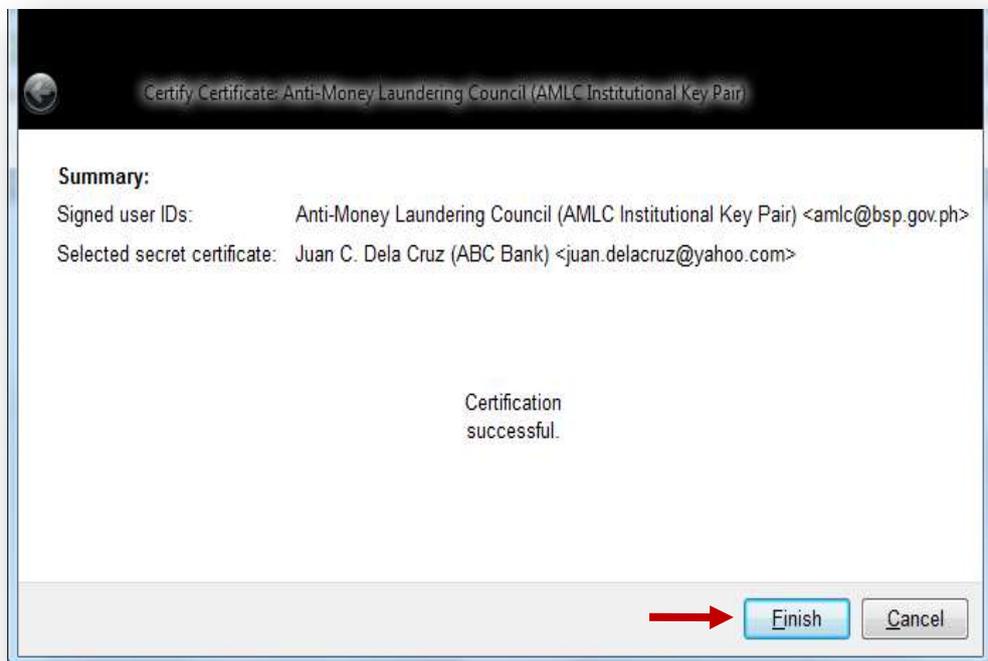
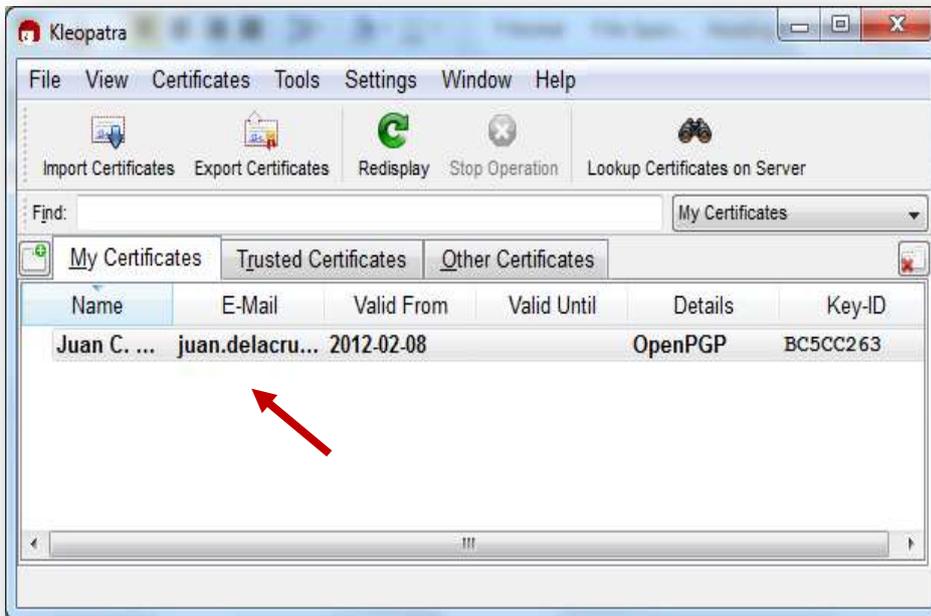Select **Certify only for myself**, then click **Certify**.

Enter passphrase of compliance officer, then click **Ok**.
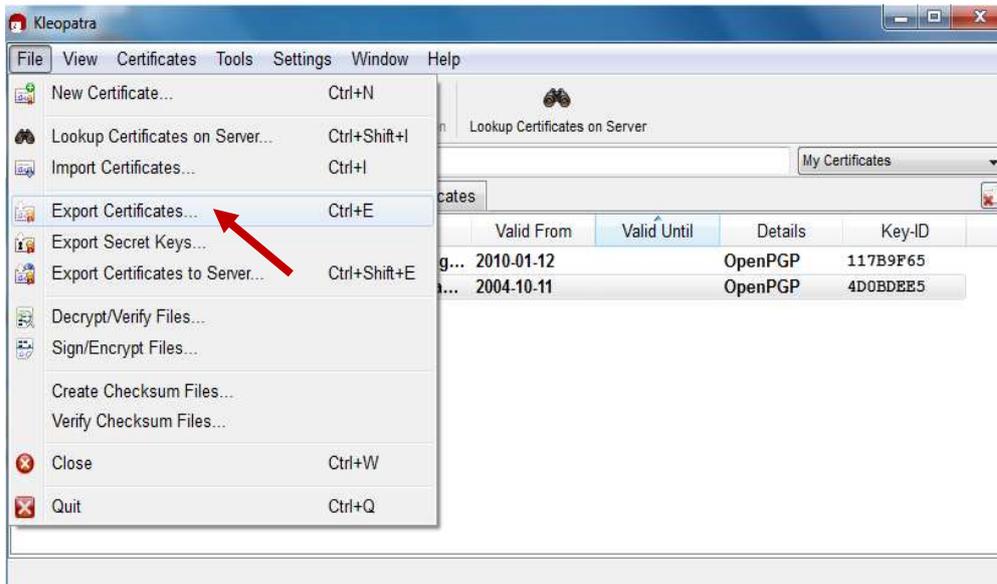
Click **Finish**.

7. Backup Procedure

Make sure to do this procedure to ensure that you will not perform all the steps enumerated above in the event that your public key has been corrupted.
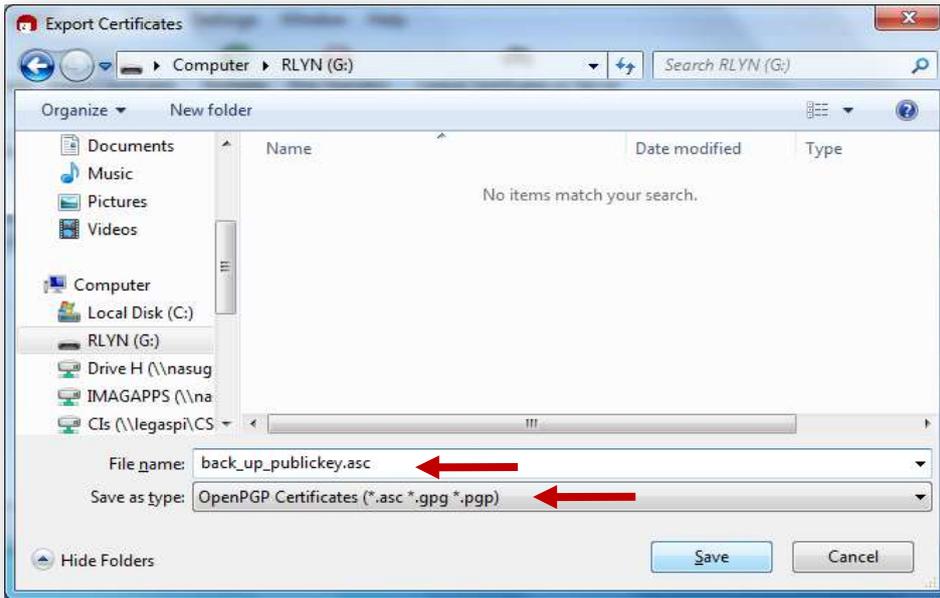

Open **Kleopatra.**

From My Certificates tab, click the name of the key owner (Compliance Officer).

From the menu bar, click **File** then select **Export Certificates.**

Select the directory where you want to save the backup of your public key (USB), by default filename is your fingerprint. (You have the option to change the filename) Click Save.
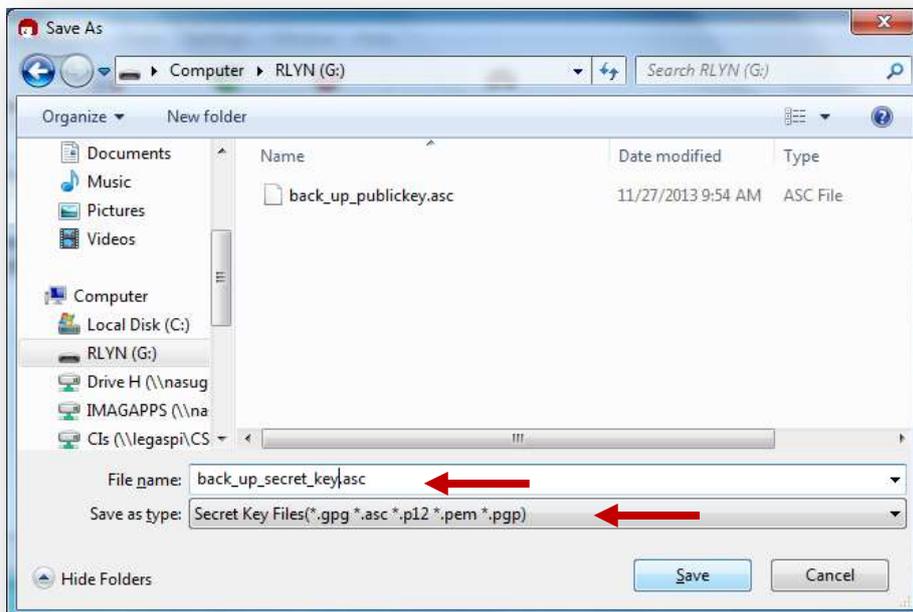
On My Certificates tab, click the name of the key owner (Compliance Officer).
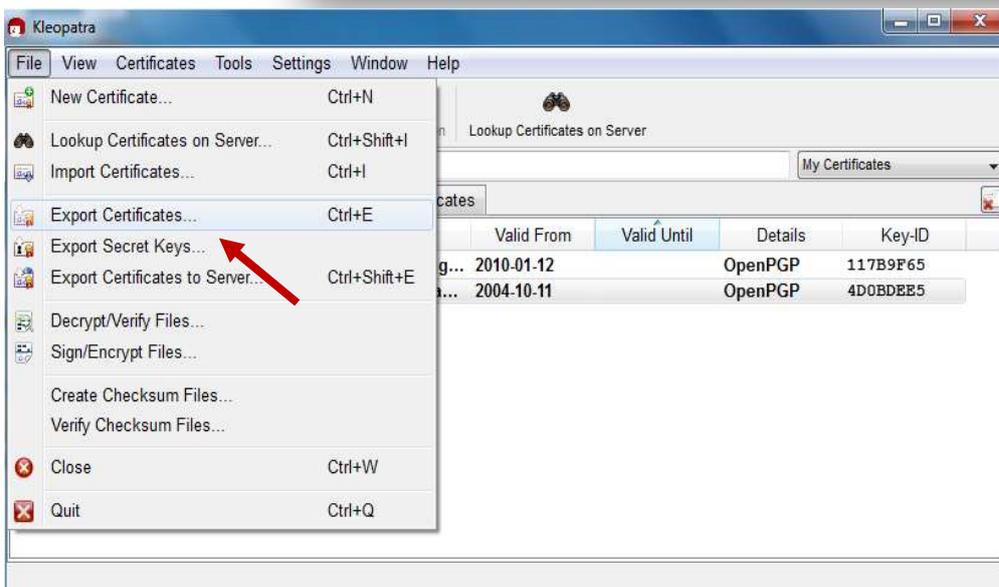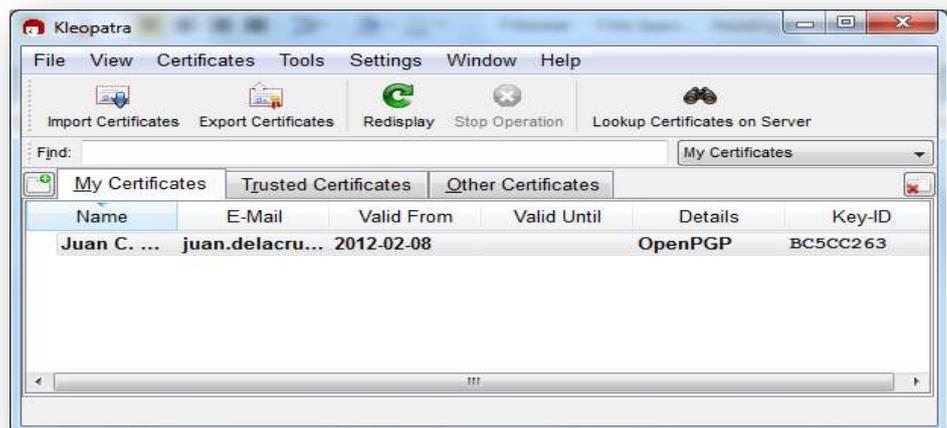
From the menu bar, click **File** then select **Export Secret Keys.**

Select the directory where you want to save the backup of your private key (USB) by clicking the diskette icon.

Create a filename for your secret key backup and select the directory where you want to save the backup of secret key (USB) then click Save.