Anti-Money Laundering Council

Manila, Philippines

Transaction Security Protocol Manual

Transaction Security Protocol

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

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 compliance officer of the CP shall generate his private key as well as public key using GPG which shall be uploaded during the Online Registration.

F. 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.

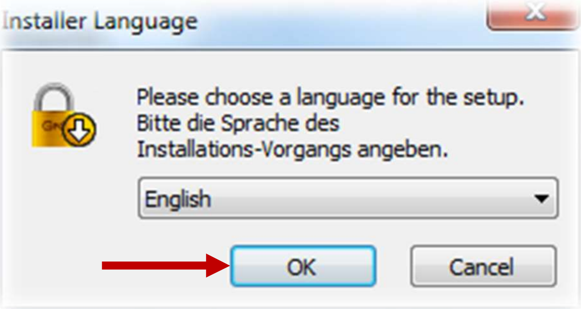
K. CPs are required to encrypt and sign the electronic CTR/STR files before transmitting them to AMLC via https (AMLC portal).

L. 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 to be uploaded via the Online Registration System.

PROCEDURES:

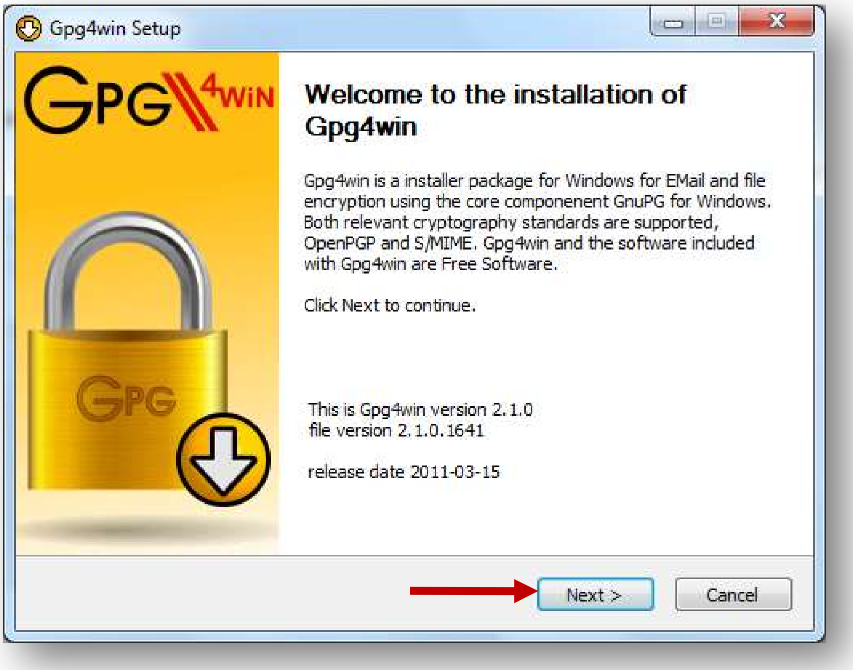
1. Installing the GnuPG for Windows Software (Gpg4win 2.1.0)

- 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**.



Installer Language

Please choose a language for the setup.
Bitte die Sprache des
Installations-Vorgangs angeben.



Gpg4win Setup

Welcome to the installation of Gpg4win

Gpg4win is a installer package for Windows for EMail and file encryption using the core componenent GnuPG for Windows. Both relevant cryptography standards are supported, OpenPGP and S/MIME. Gpg4win and the software included with Gpg4win are Free Software.

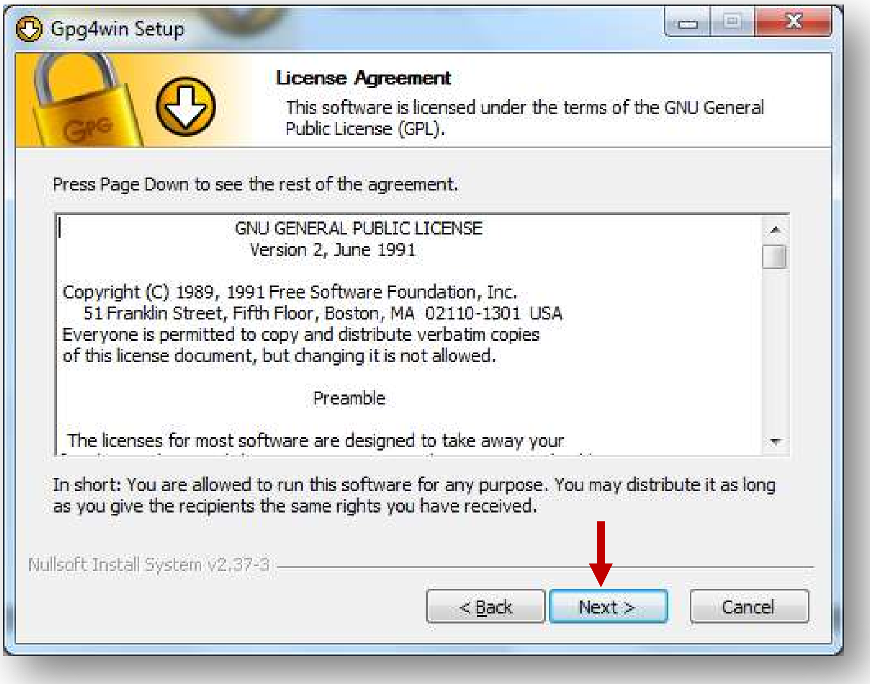
Click Next to continue.

This is Gpg4win version 2.1.0
file version 2.1.0.1641

release date 2011-03-15

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

The License Agreement window will be displayed on the screen. Click **Next**.



License Agreement

This software is licensed under the terms of the GNU General Public License (GPL).

Press Page Down to see the rest of the agreement.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

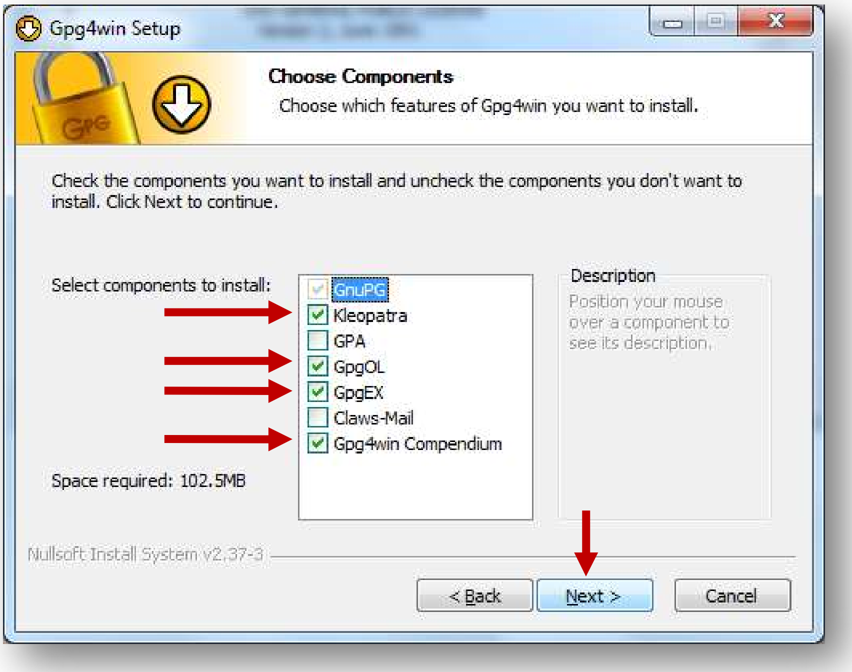
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your

In short: You are allowed to run this software for any purpose. You may distribute it as long as you give the recipients the same rights you have received.

Nullsoft Install System v2.37-3



Choose Components

Choose which features of Gpg4win you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ GnuPG
- ☑ Kleopatra
- □ GPA
- ☑ GpgOL
- ☑ GpgEX
- □ Claws-Mail
- ☑ Gpg4win Compendium

Description

Position your mouse over a component to see its description.

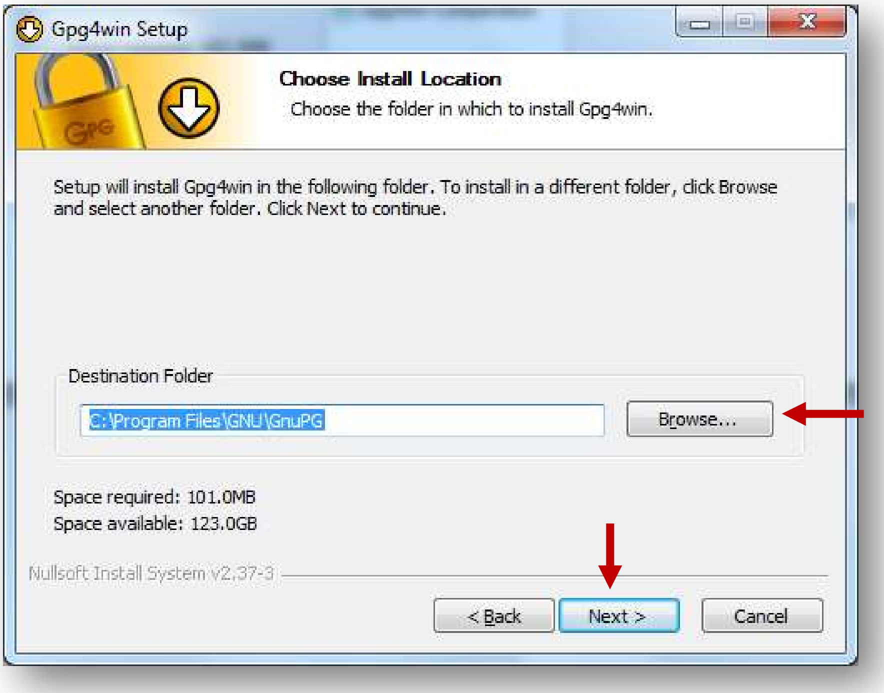
Space required: 102.5MB

Nullsoft Install System v2.37-3

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.**



Gpg4win Setup

Choose Install Location

Choose the folder in which to install Gpg4win.

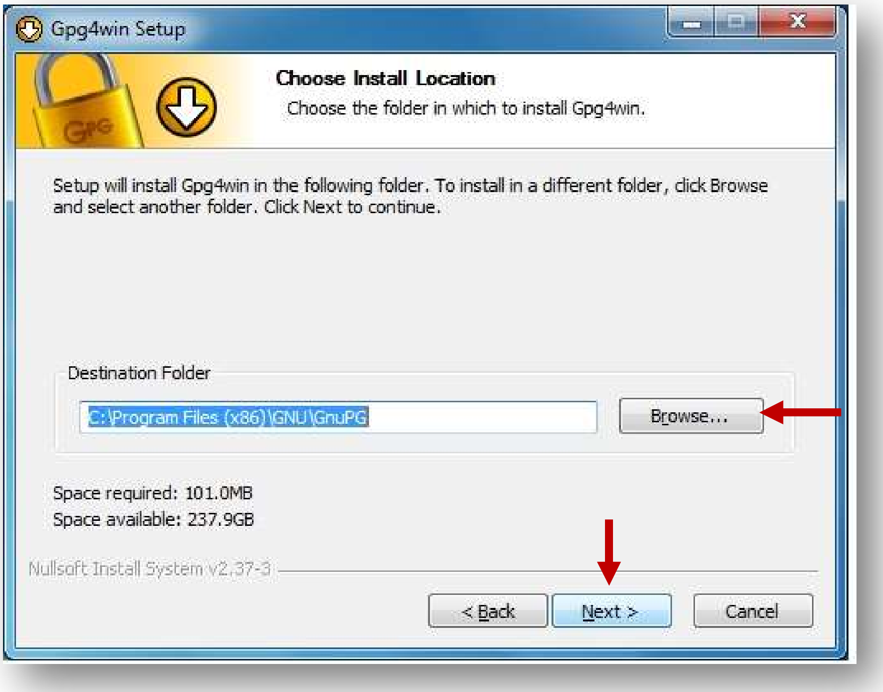
Setup will install Gpg4win in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder

C:\Program Files\GNU\GnuPG

Space required: 101.0MB
Space available: 123.0GB

Nullsoft Install System v2.37-3



Gpg4win Setup

Choose Install Location

Choose the folder in which to install Gpg4win.

Setup will install Gpg4win in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder

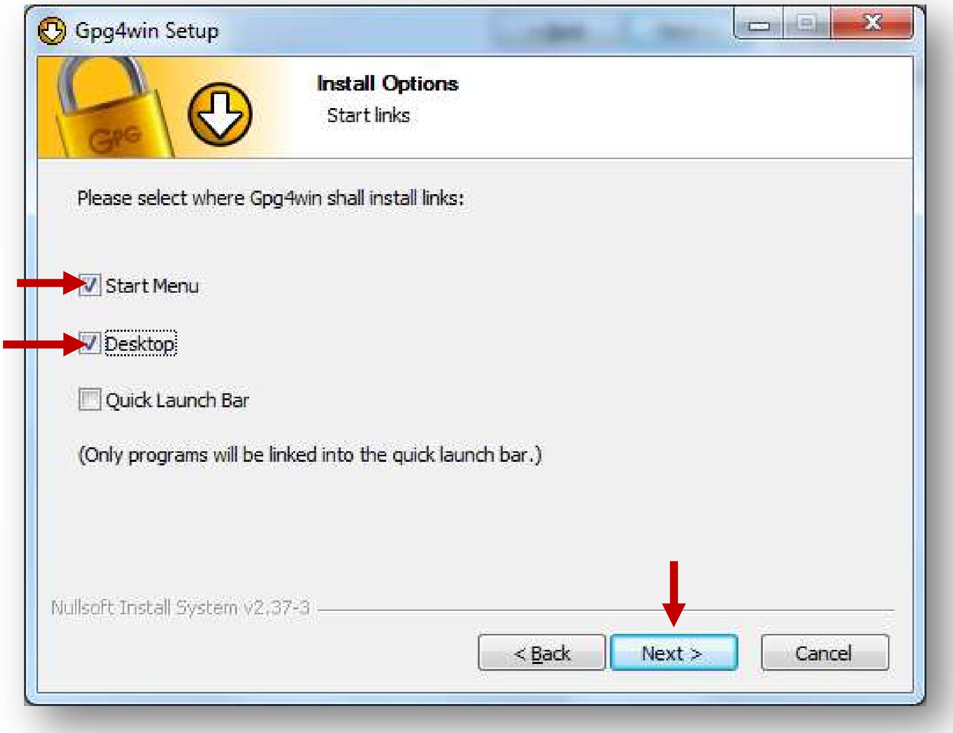
C:\Program Files (x86)\GNU\GnuPG

Space required: 101.0MB
Space available: 237.9GB

Nullsoft Install System v2.37-3

- **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**.



Install Options

Start links

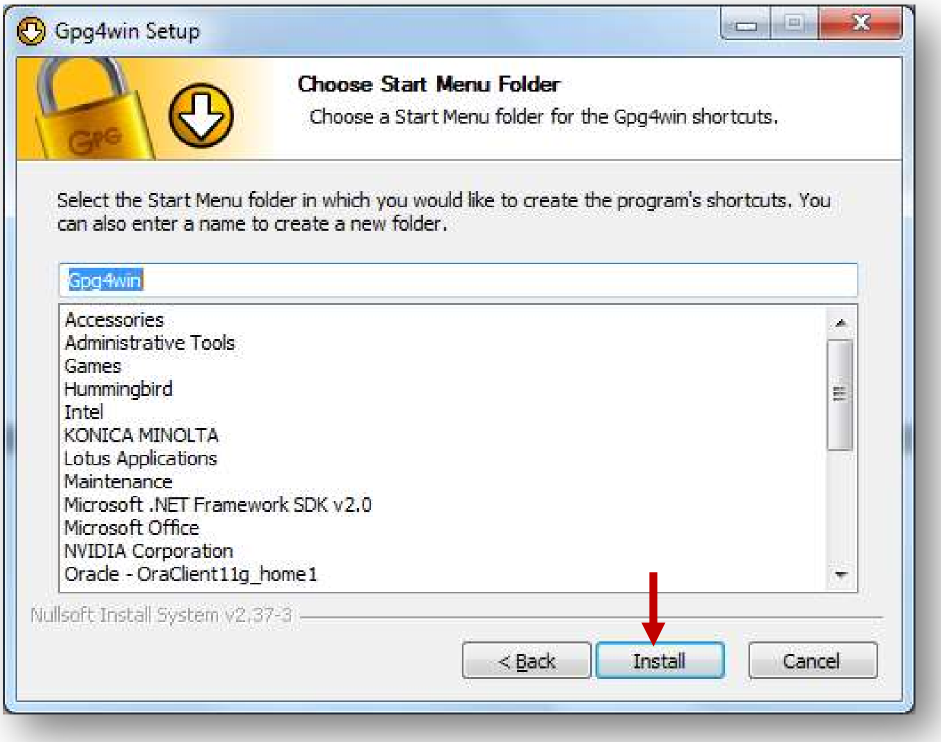
Please select where Gpg4win shall install links:

☑ Start Menu

☑ Desktop

□ Quick Launch Bar

(Only programs will be linked into the quick launch bar.)



Choose Start Menu Folder

Choose a Start Menu folder for the Gpg4win shortcuts.

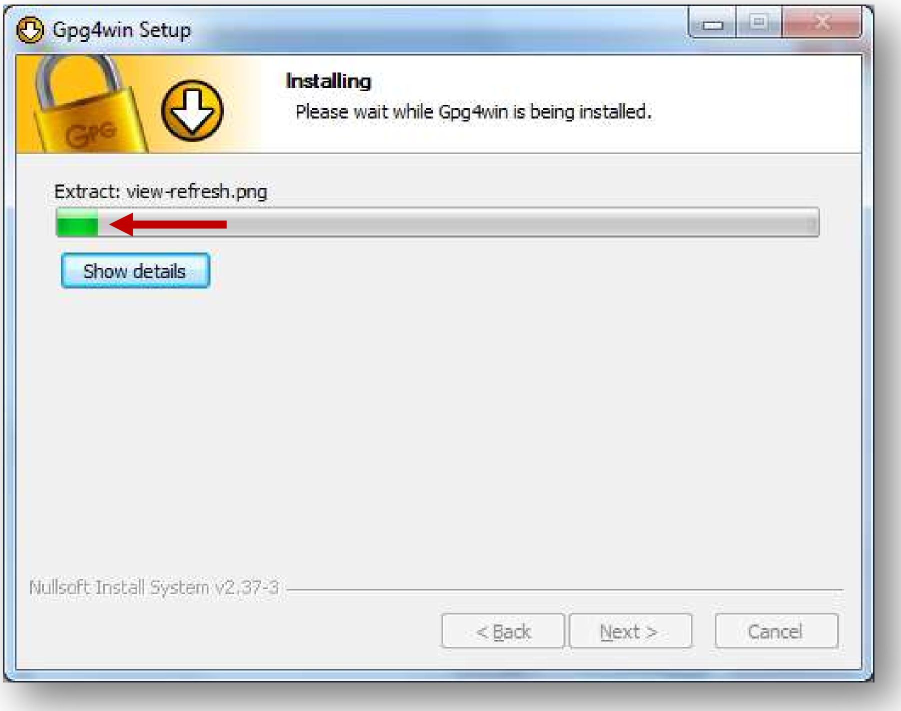
Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

Gpg4win

Accessories
Administrative Tools
Games
Hummingbird
Intel
KONICA MINOLTA
Lotus Applications
Maintenance
Microsoft .NET Framework SDK v2.0
Microsoft Office
NVIDIA Corporation
Oracle - OraClient11g_home1

Choose Start Menu folder for the Gpg4win shortcuts. Enter **Gpg4win**, then click **Install**.

Please wait while Gpg4win is being installed.

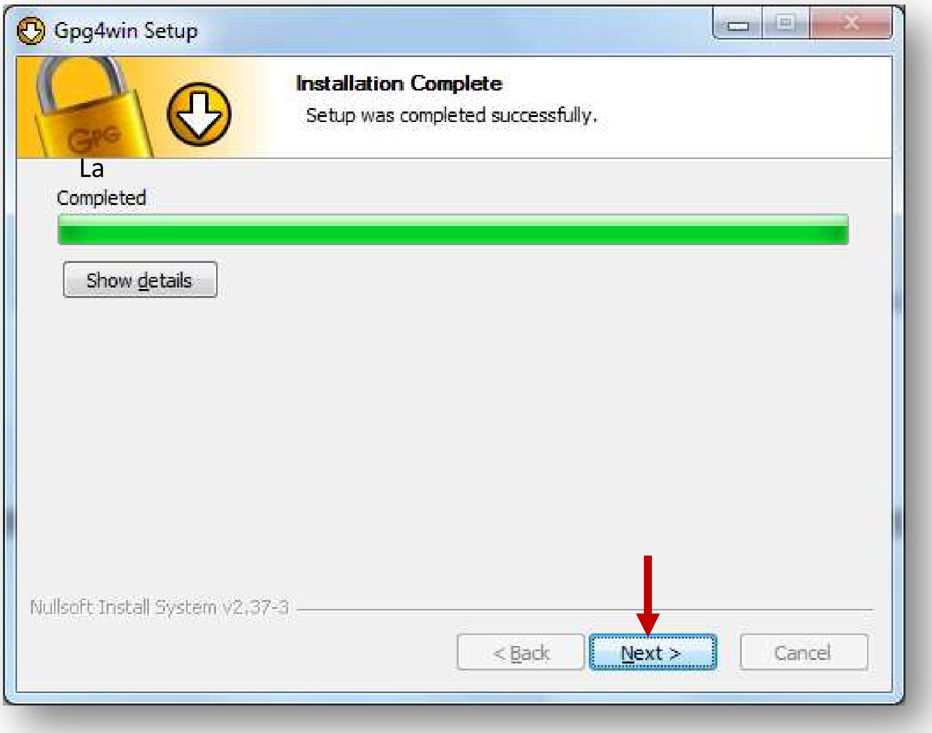


Gpg4win Setup

Installing

Please wait while Gpg4win is being installed.

Extract: view-refresh.png



Gpg4win Setup

Installation Complete

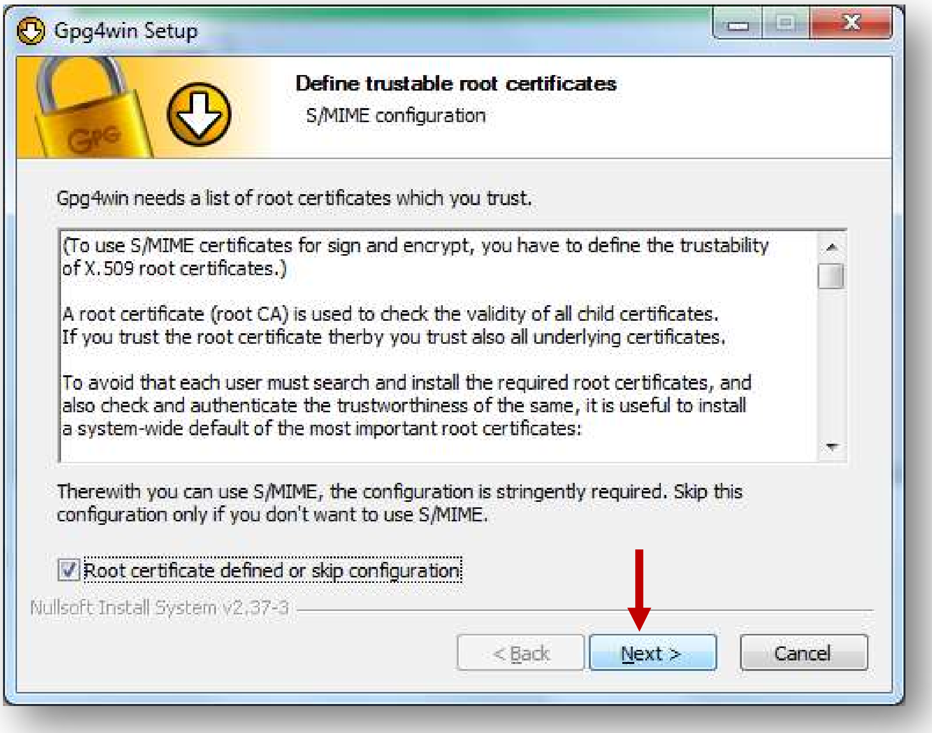
Setup was completed successfully.

La

Completed

Once the setup is completed successfully, click **Next**.

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



Gpg4win Setup

Define trustable root certificates

S/MIME configuration

Gpg4win needs a list of root certificates which you trust.

(To use S/MIME certificates for sign and encrypt, you have to define the trustability of X.509 root certificates.)

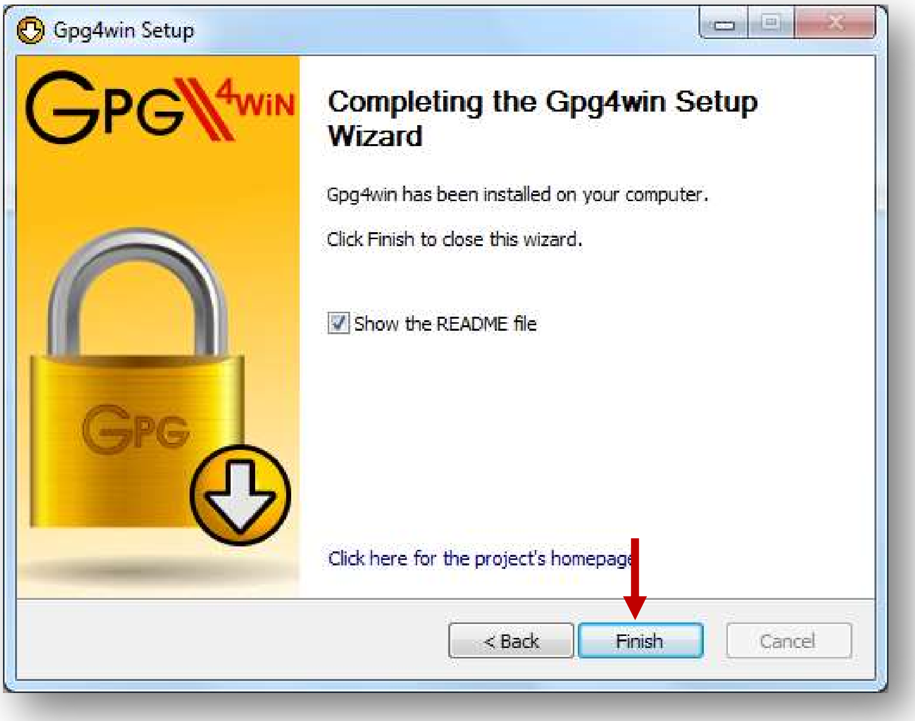
A root certificate (root CA) is used to check the validity of all child certificates. If you trust the root certificate therby you trust also all underlying certificates.

To avoid that each user must search and install the required root certificates, and also check and authenticate the trustworthiness of the same, it is useful to install a system-wide default of the most important root certificates:

Therewith you can use S/MIME, the configuration is stringently required. Skip this configuration only if you don't want to use S/MIME.

☑ Root certificate defined or skip configuration

Nullsoft Install System v2.37-3



Gpg4win Setup

Completing the Gpg4win Setup Wizard

Gpg4win has been installed on your computer.

Click Finish to close this wizard.

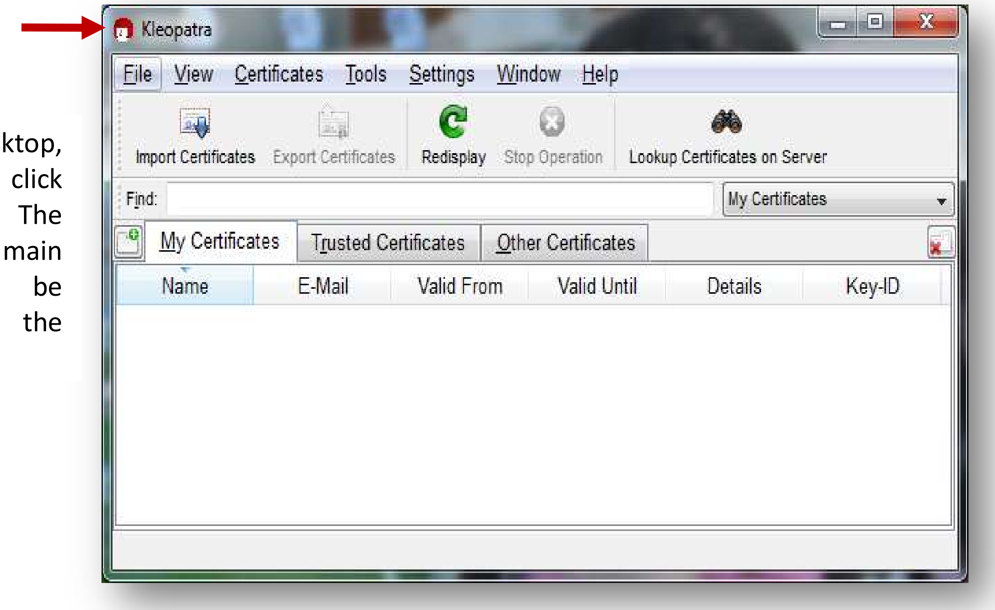
☑ Show the README file

Click here for the project's homepage

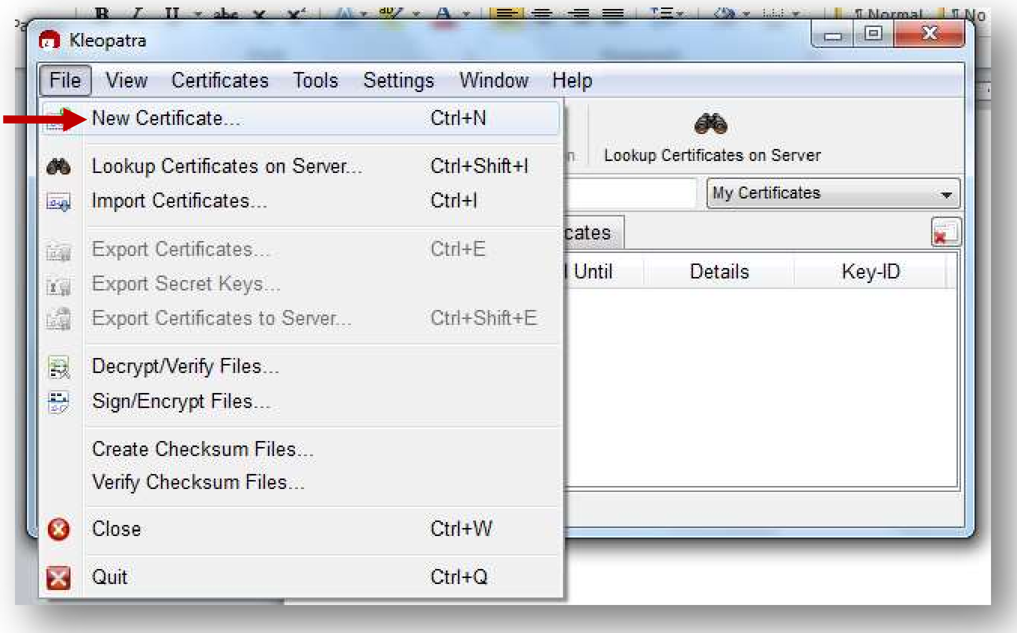
Click **Finish**.

2. Generation of Key Pairs (One time Procedure)

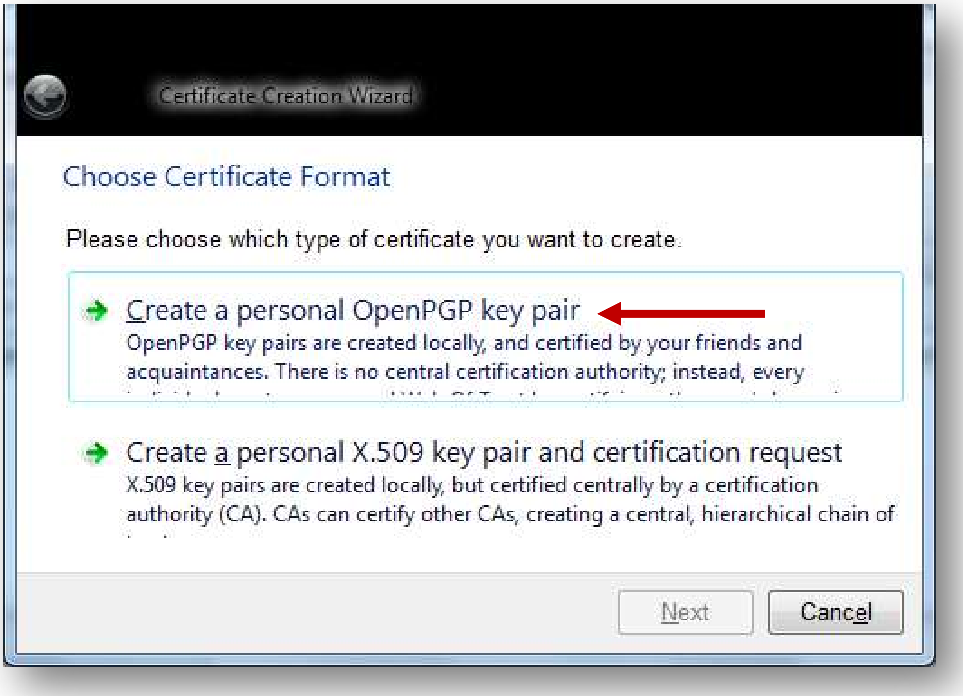
From your desktop, double click **Kleopatra**. The Kleopatra main window will be displayed on the screen.



Click **File**, then select **New Certificate**.


Kleopatra
File View Certificates Tools Settings Window Help
New Certificate... Ctrl+N
Lookup Certificates on Server... Ctrl+Shift+I
Import Certificates... Ctrl+I
Export Certificates... Ctrl+E
Export Secret Keys...
Export Certificates to Server... Ctrl+Shift+E
Decrypt/Verify Files...
Sign/Encrypt Files...
Create Checksum Files...
Verify Checksum Files...
Close Ctrl+W
Quit Ctrl+Q
Lookup Certificates on Server
My Certificates
cates
Until
Details
Key-ID

Certificate Creation Wizard will be displayed on the screen. ***Click Create a personal OpenPGP key pair***.

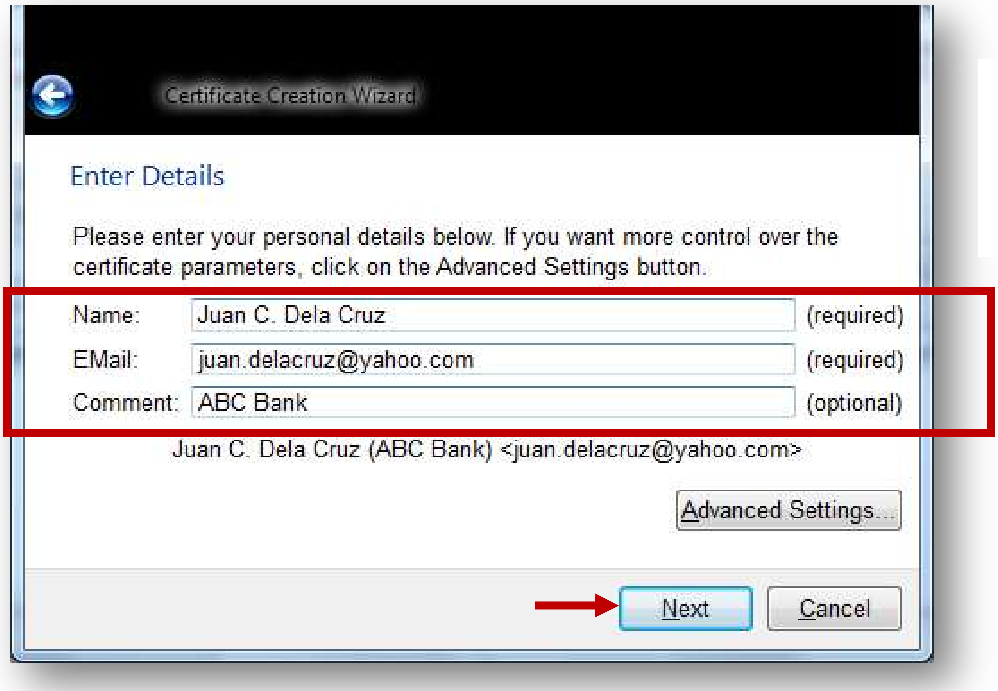


Choose Certificate Format

Please choose which type of certificate you want to create.

Create a personal OpenPGP key pair
OpenPGP key pairs are created locally, and certified by your friends and acquaintances. There is no central certification authority; instead, every

Create a personal X.509 key pair and certification request
X.509 key pairs are created locally, but certified centrally by a certification authority (CA). CAs can certify other CAs, creating a central, hierarchical chain of



Enter Details

Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button.

Name: Juan C. Dela Cruz (required)
EMail: juan.delacruz@yahoo.com (required)
Comment: ABC Bank (optional)

Juan C. Dela Cruz (ABC Bank) <juan.delacruz@yahoo.com>

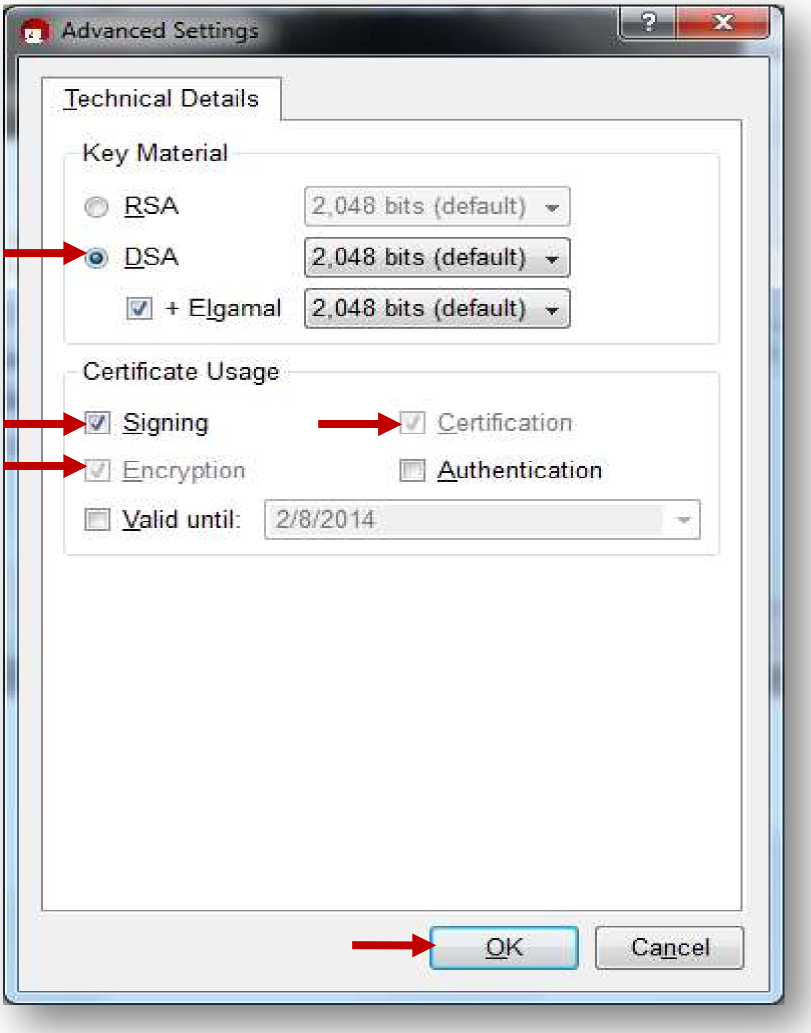
Enter Details, then click **Advance Settings**.

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**.



Advanced Settings

Technical Details

Key Material

○ RSA 2,048 bits (default)

● DSA 2,048 bits (default)

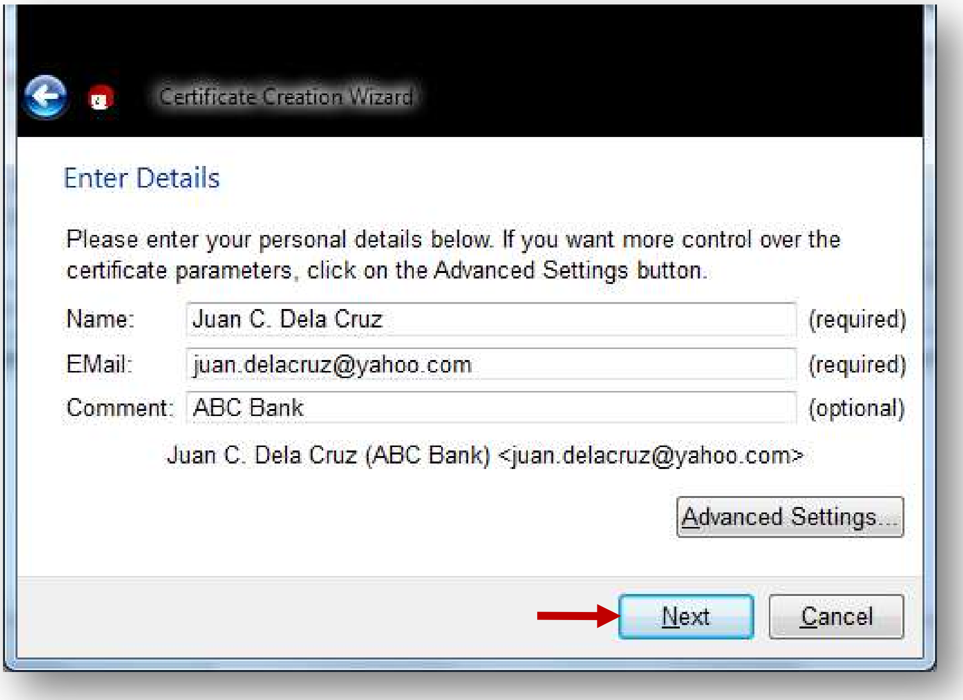
☑ + Elgamal 2,048 bits (default)

Certificate Usage

☑ Signing ☑ Certification

☑ Encryption □ Authentication

□ Valid until: 2/8/2014



Certificate Creation Wizard

Enter Details

Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button.

Name: Juan C. Dela Cruz (required)

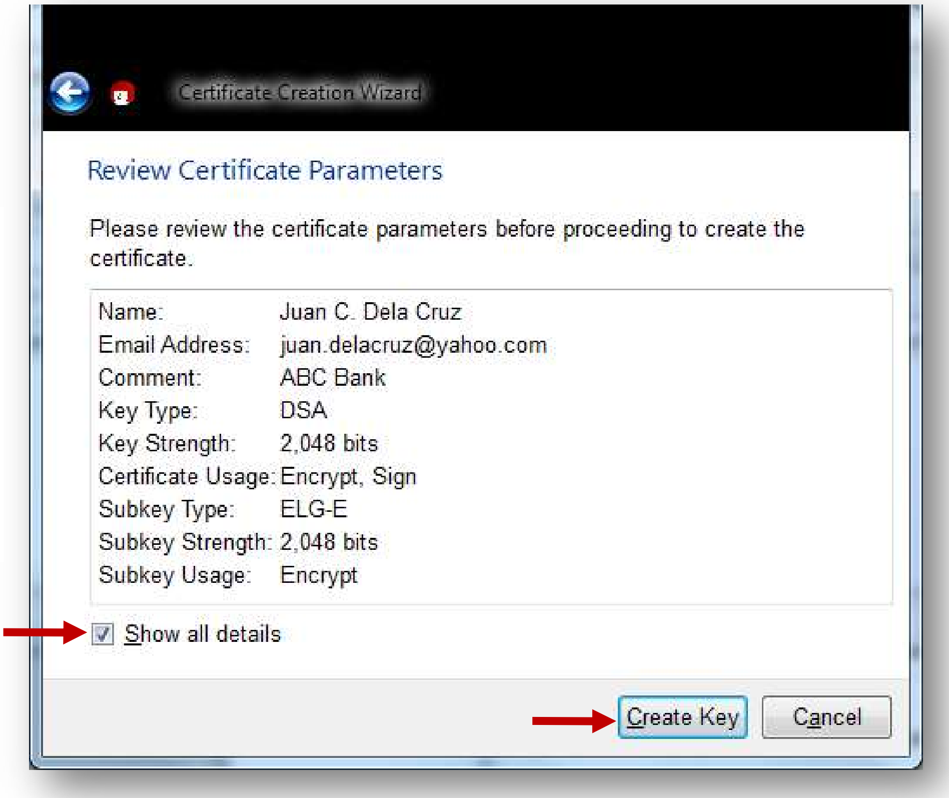
EMail: juan.delacruz@yahoo.com (required)

Comment: ABC Bank (optional)

Juan C. Dela Cruz (ABC Bank) <juan.delacruz@yahoo.com>

From the Certificate Creation Wizard window, click **Next**.

From Certificate Creation Wizard, check **Show all details**, review the certificate parameters, then click **Create Key**.

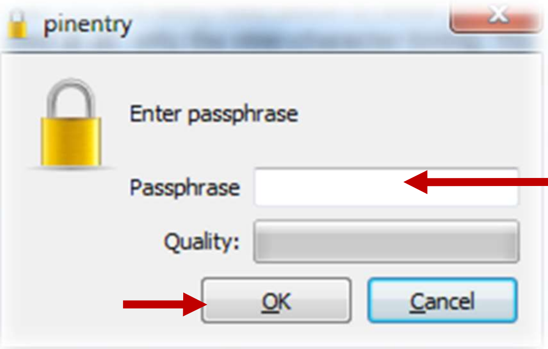


Review Certificate Parameters

Please review the certificate parameters before proceeding to create the certificate.

Name: Juan C. Dela Cruz
Email Address: juan.delacruz@yahoo.com
Comment: ABC Bank
Key Type: DSA
Key Strength: 2,048 bits
Certificate Usage: Encrypt, Sign
Subkey Type: ELG-E
Subkey Strength: 2,048 bits
Subkey Usage: Encrypt

☑ Show all details



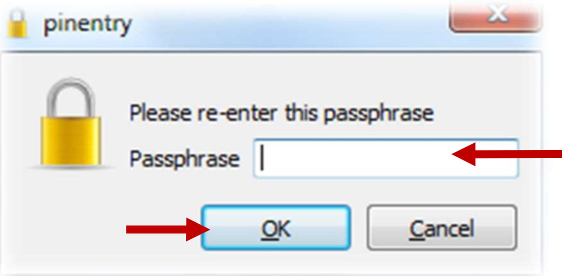
Enter passphrase

Passphrase

Quality:

Pin entry window will be displayed on the screen. Enter Passphrase (gpg password of compliance officer), then click **Ok**.

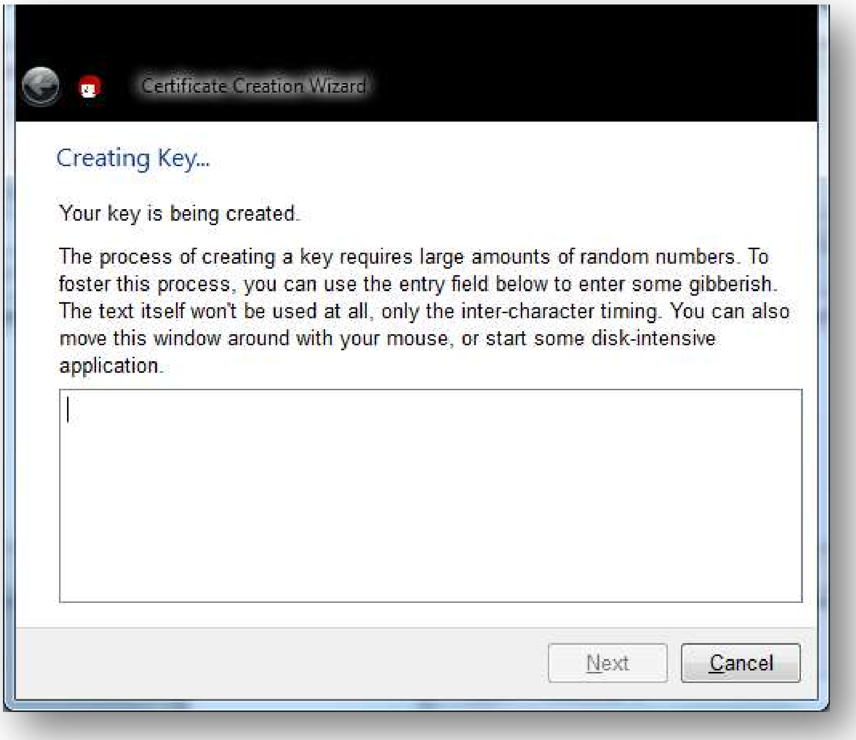
Re-enter passphrase, then click **Ok**.



Please re-enter this passphrase

Passphrase

Please be reminded that once you forget your passphrase, you need to generate a new public key, since AMLC cannot retrieve the said passphrase.

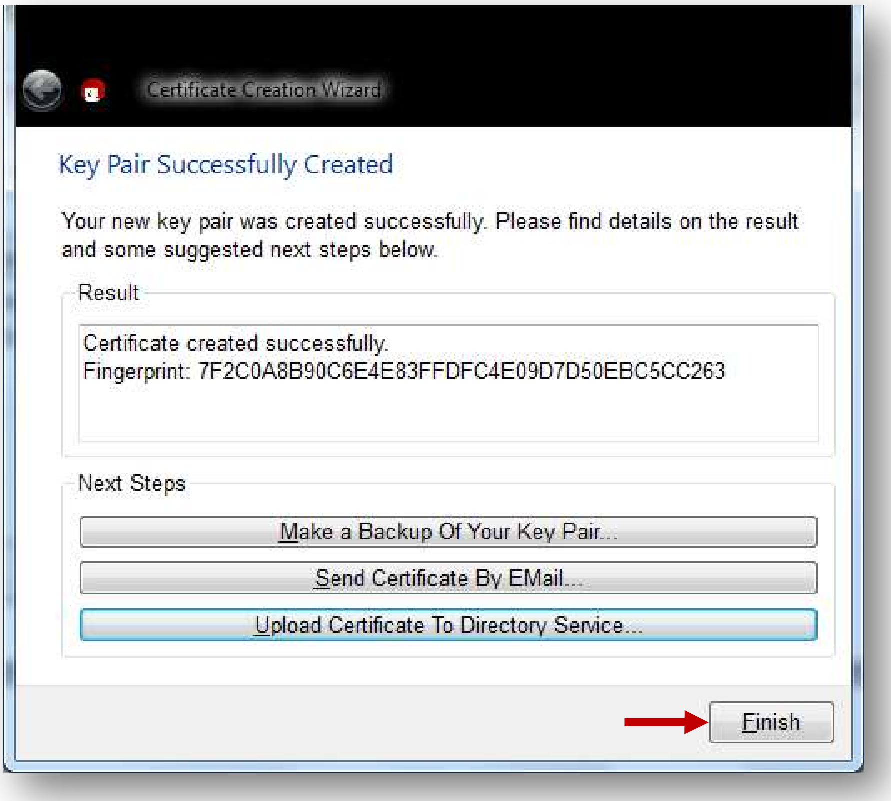


Creating Key...

Your key is being created.

The process of creating a key requires large amounts of random numbers. To foster this process, you can use the entry field below to enter some gibberish. The text itself won't be used at all, only the inter-character timing. You can also move this window around with your mouse, or start some disk-intensive application.

Wait until the key pair is successfully created.


Certificate Creation Wizard

Key Pair Successfully Created

Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

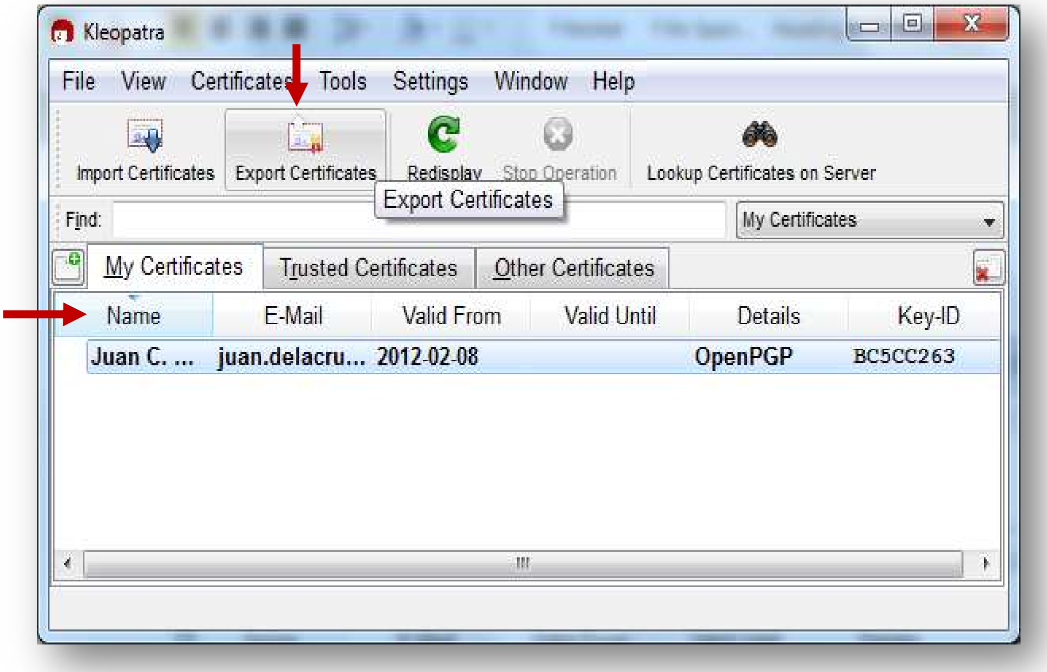
Result

Certificate created successfully.
Fingerprint: 7F2C0A8B90C6E4E83FFDFC4E09D7D50EBC5CC263

Next Steps
Make a Backup Of Your Key Pair...
Send Certificate By EMail...
Upload Certificate To Directory Service...
Finish

Click **Finish**.

3. Exporting Public Key



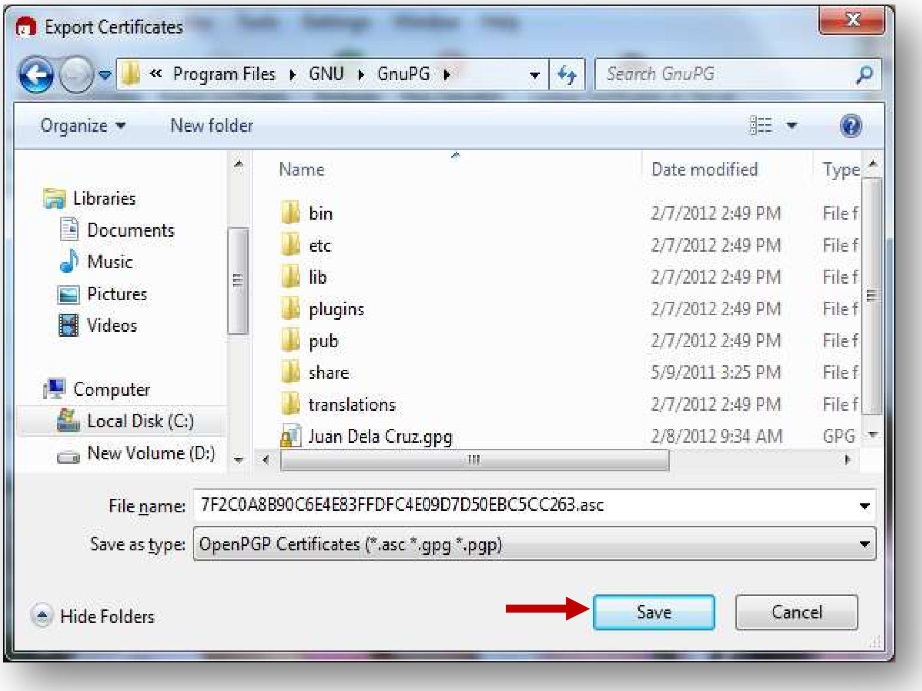
Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Juan C. ...	juan.delacru...	2012-02-08		OpenPGP	BC5CC263

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\



Name	Date modified	Type
bin	2/7/2012 2:49 PM	File f
etc	2/7/2012 2:49 PM	File f
lib	2/7/2012 2:49 PM	File f
plugins	2/7/2012 2:49 PM	File f
pub	2/7/2012 2:49 PM	File f
share	5/9/2011 3:25 PM	File f
translations	2/7/2012 2:49 PM	File f
Juan Dela Cruz.gpg	2/8/2012 9:34 AM	GPG

File name: 7F2C0A8B90C6E4E83FFDFC4E09D7D50EBC5CC263.asc

Save as type: OpenPGP Certificates (*.asc *.gpg *.pgp)

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

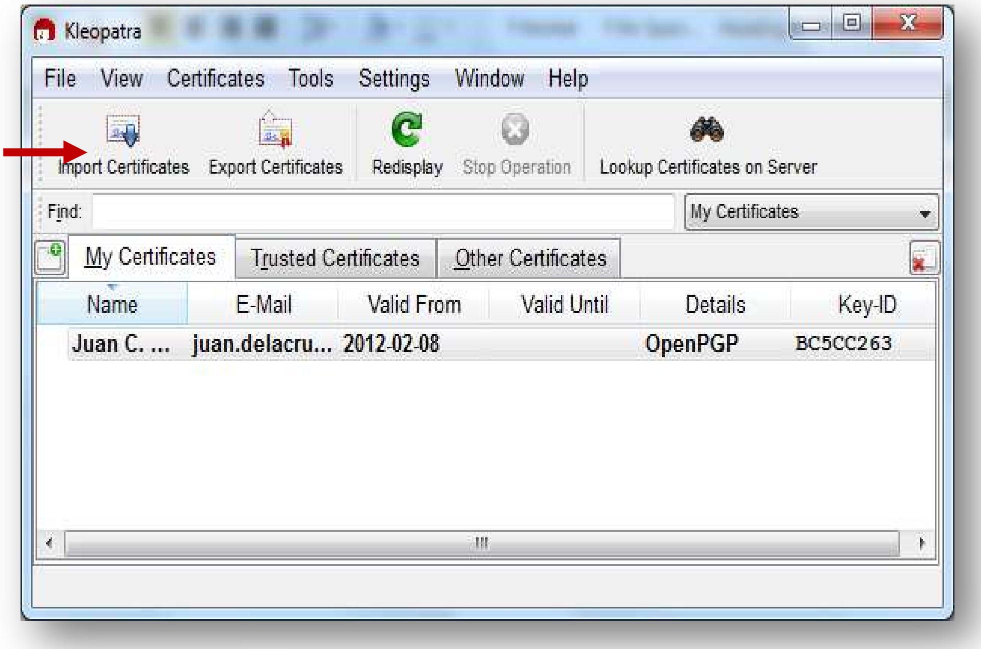
Please be ready with the exported asc file as you will need this for ONLINE REGISTRATION

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\

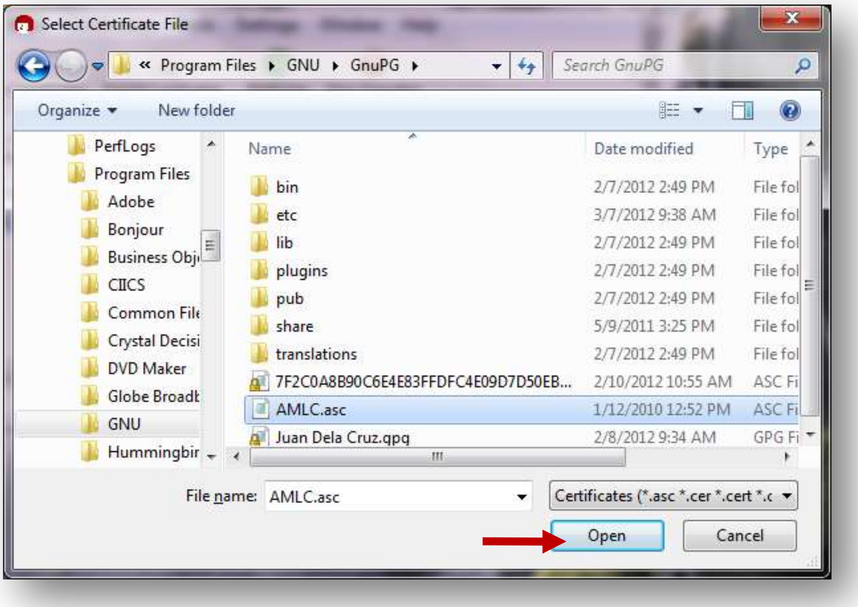
5. Importing of AMLC public key



Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Juan C. ...	juan.delacru...	2012-02-08		OpenPGP	BC5CC263

From your desktop, double click **Kleopatra**. The Kleopatra main window will be displayed on the screen.

Click **Import Certificates**.

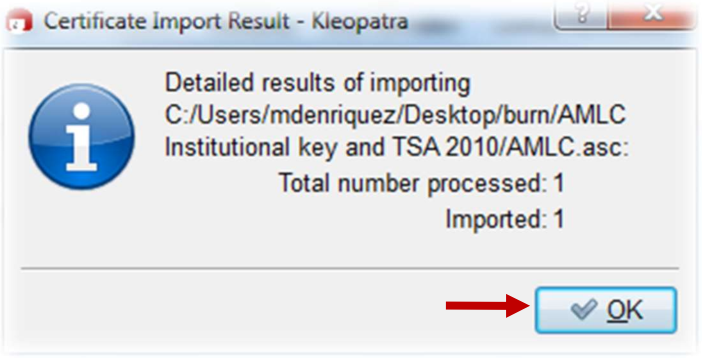


Name	Date modified	Type
bin	2/7/2012 2:49 PM	File fol
etc	3/7/2012 9:38 AM	File fol
lib	2/7/2012 2:49 PM	File fol
plugins	2/7/2012 2:49 PM	File fol
pub	2/7/2012 2:49 PM	File fol
share	5/9/2011 3:25 PM	File fol
translations	2/7/2012 2:49 PM	File fol
7F2C0A8B90C6E4E83FFDFC4E09D7D50EB...	2/10/2012 10:55 AM	ASC Fi
AMLC.asc	1/12/2010 12:52 PM	ASC Fi
Juan Dela Cruz.gpg	2/8/2012 9:34 AM	GPG Fi

File name: AMLC.asc

Certificates (*.asc *.cer *.cert *.c

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



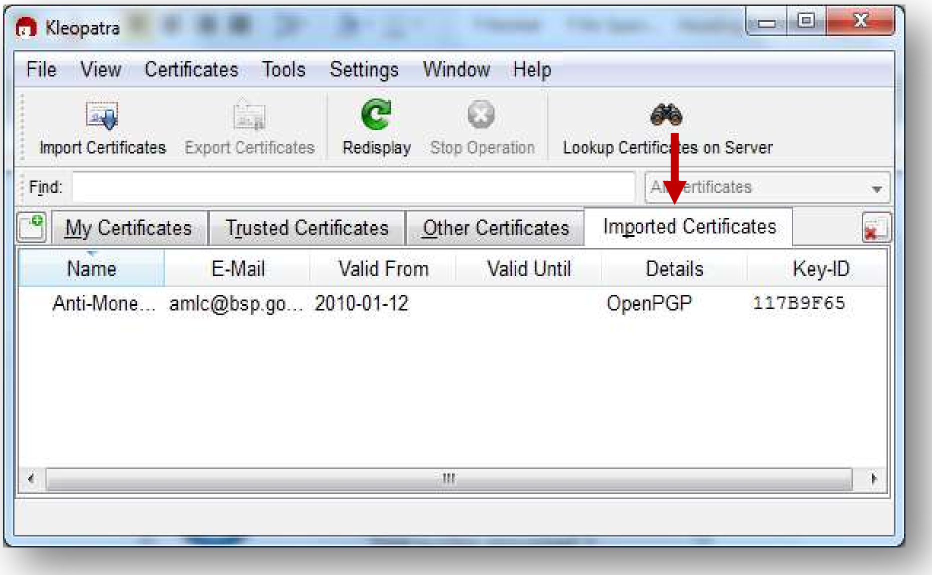
Detailed results of importing C:/Users/mdenriquez/Desktop/burn/AMLC Institutional key and TSA 2010/AMLC.asc:

Total number processed: 1

Imported: 1

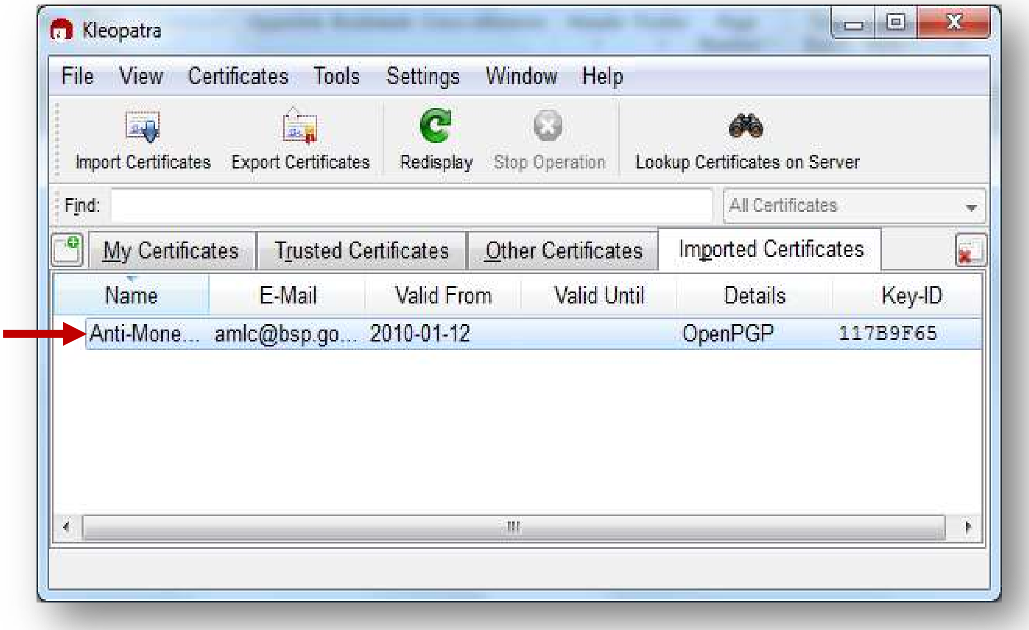
The Certificate Import Result window will be displayed on the screen. Click **Ok**.

The imported public key will be displayed on Kleopatra – Imported Certificates tab.



Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Anti-Mone...	amlc@bsp.go...	2010-01-12		OpenPGP	117B9F65

6. Certifying AMLC Key

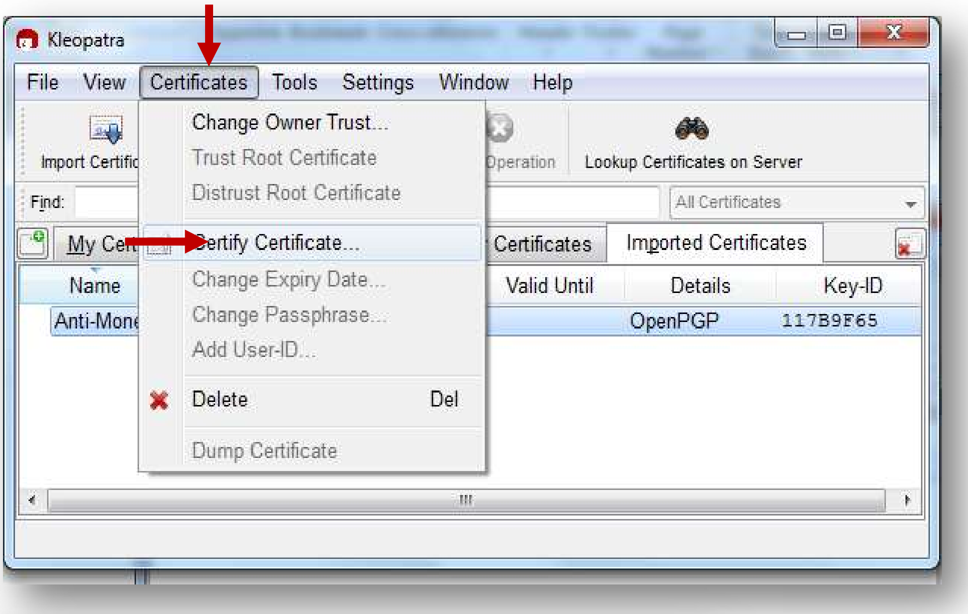


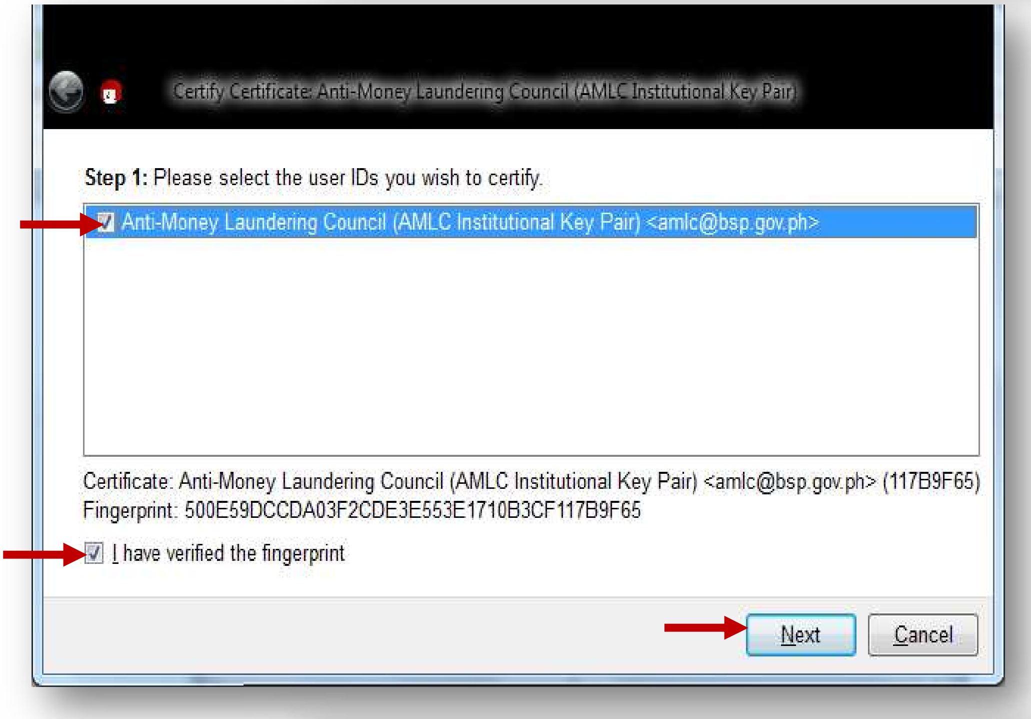
Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Anti-Mone...	amlc@bsp.go...	2010-01-12		OpenPGP	117B9F65

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**.




Certify Certificate: Anti-Money Laundering Council (AMLC Institutional Key Pair)

Step 1: Please select the user IDs you wish to certify.

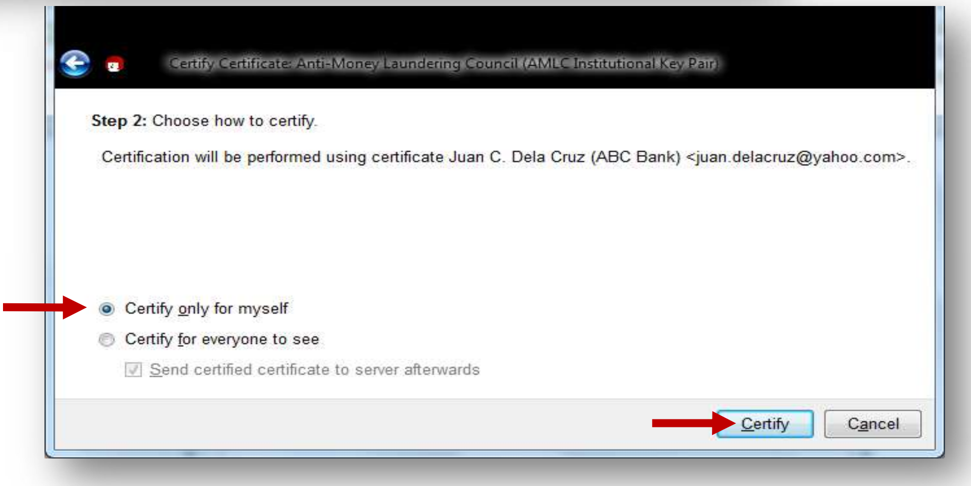
☑ Anti-Money Laundering Council (AMLC Institutional Key Pair) <amlc@bsp.gov.ph>

Certificate: Anti-Money Laundering Council (AMLC Institutional Key Pair) <amlc@bsp.gov.ph> (117B9F65)
Fingerprint: 500E59DCCDA03F2CDE3E553E1710B3CF117B9F65

☑ I have verified the fingerprint

Check ***Anti-Money Laundering Council***, then check ***I have verified the fingerprint***. Click **Next**.

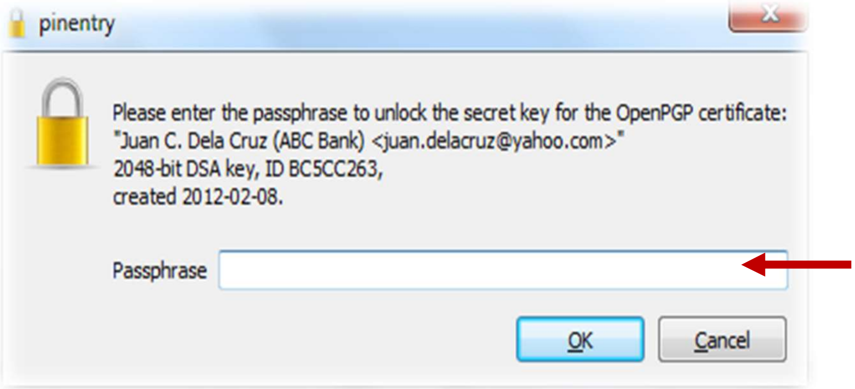
Select **Certify only for myself**, then click **Certify**.


Certify Certificate: Anti-Money Laundering Council (AMLC Institutional Key Pair)

Step 2: Choose how to certify.

Certification will be performed using certificate Juan C. Dela Cruz (ABC Bank) <juan.delacruz@yahoo.com>.

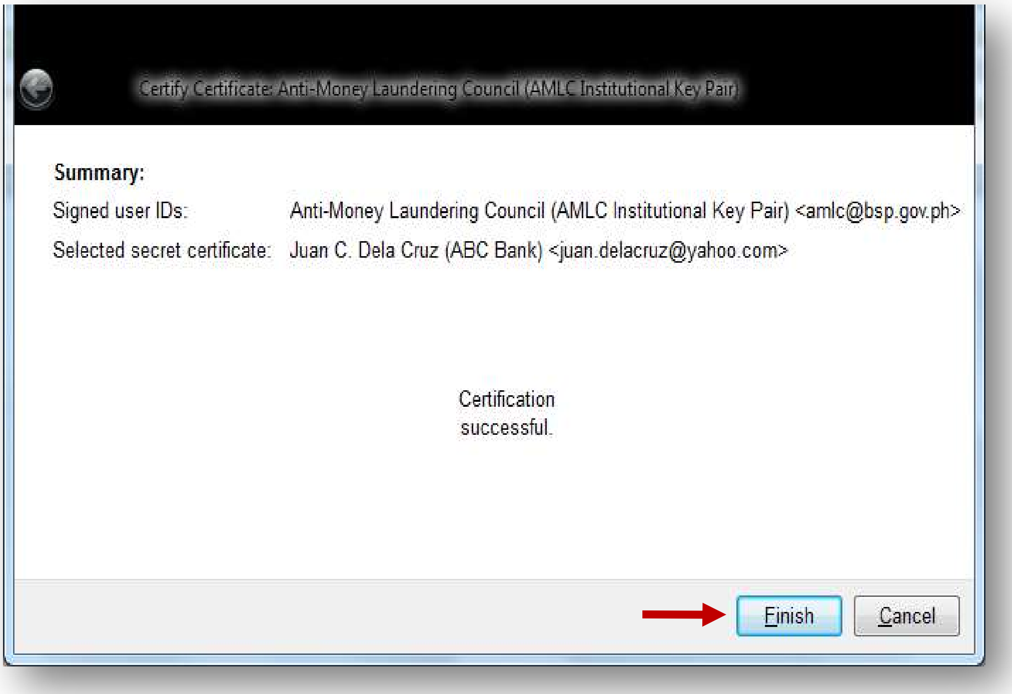
● Certify only for myself
○ Certify for everyone to see
☑ Send certified certificate to server afterwards



Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"Juan C. Dela Cruz (ABC Bank) <juan.delacruz@yahoo.com>"
2048-bit DSA key, ID BC5CC263,
created 2012-02-08.

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

Click **Finish**.



Certify Certificate: Anti-Money Laundering Council (AMLC Institutional Key Pair)

Summary:

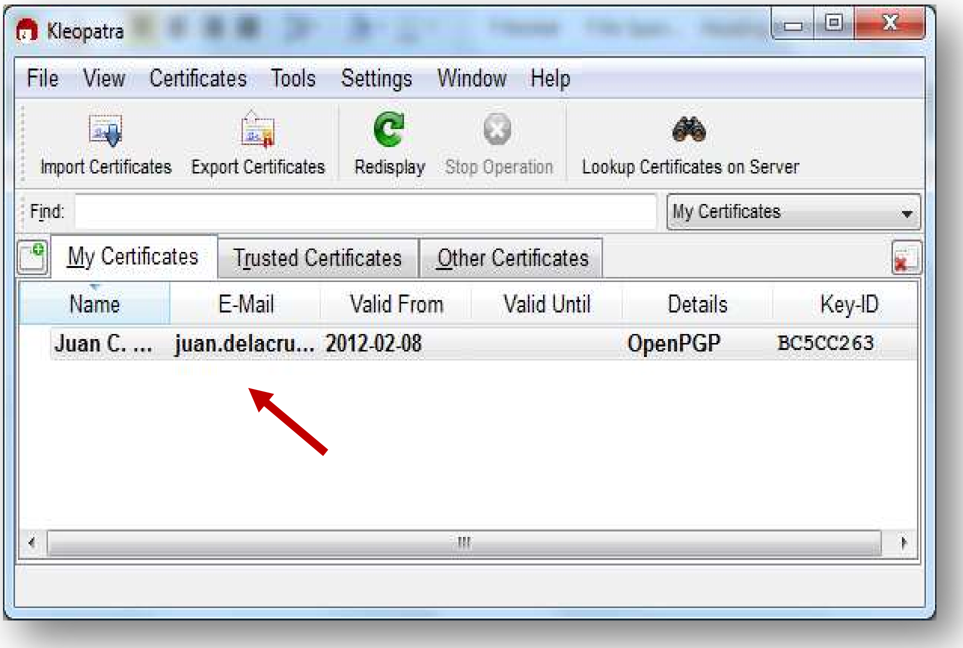
Signed user IDs: Anti-Money Laundering Council (AMLC Institutional Key Pair) <amlc@bsp.gov.ph>

Selected secret certificate: Juan C. Dela Cruz (ABC Bank) <juan.delacruz@yahoo.com>

Certification successful.

7. Backup Procedure

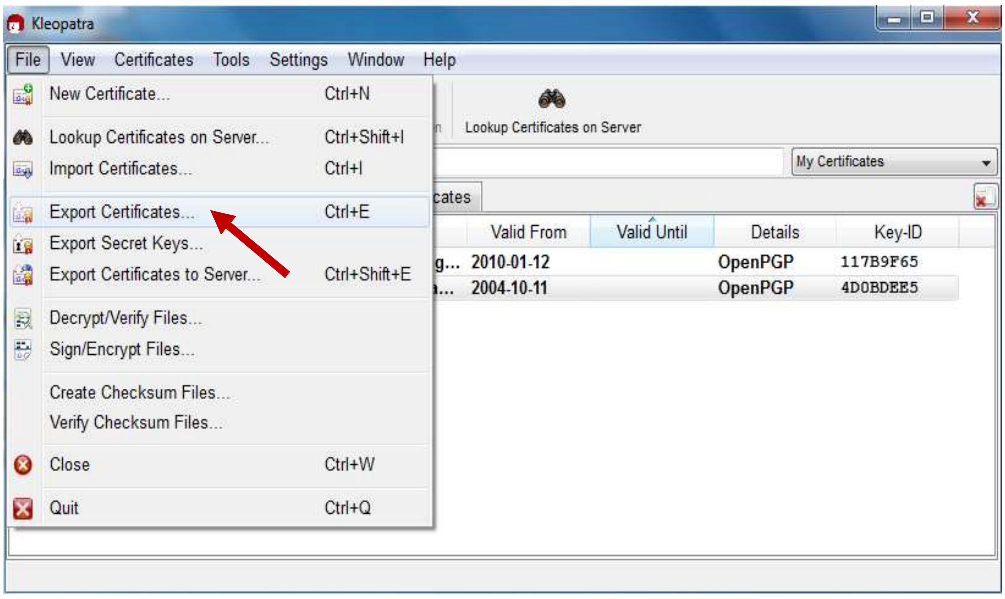
Make sure to do this procedure to ensure that you will not perform all the steps enumerated above in the event that your public key has been corrupted.



Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Juan C. ...	juan.delacru...	2012-02-08		OpenPGP	BC5CC263

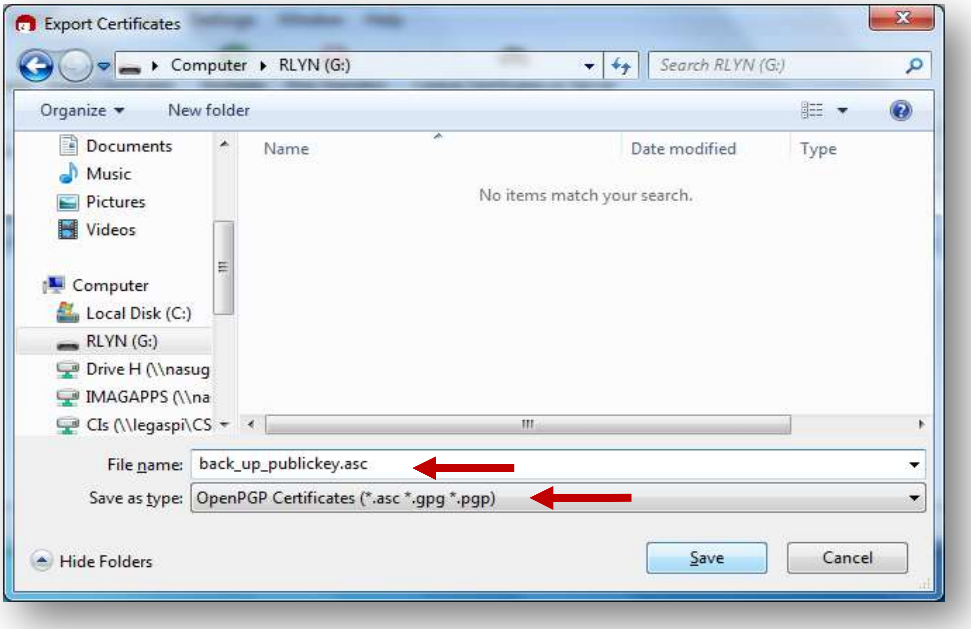
Open **Kleopatra.**

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


Kleopatra
File View Certificates Tools Settings Window Help
New Certificate... Ctrl+N
Lookup Certificates on Server... Ctrl+Shift+I
Import Certificates... Ctrl+I
Export Certificates... Ctrl+E
Export Secret Keys...
Export Certificates to Server... Ctrl+Shift+E
Decrypt/Verify Files...
Sign/Encrypt Files...
Create Checksum Files...
Verify Checksum Files...
Close Ctrl+W
Quit Ctrl+Q
Lookup Certificates on Server
My Certificates
cates

	Valid From	Valid Until	Details	Key-ID
g...	2010-01-12		OpenPGP	117B9F65
...	2004-10-11		OpenPGP	4D0BDEE5

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

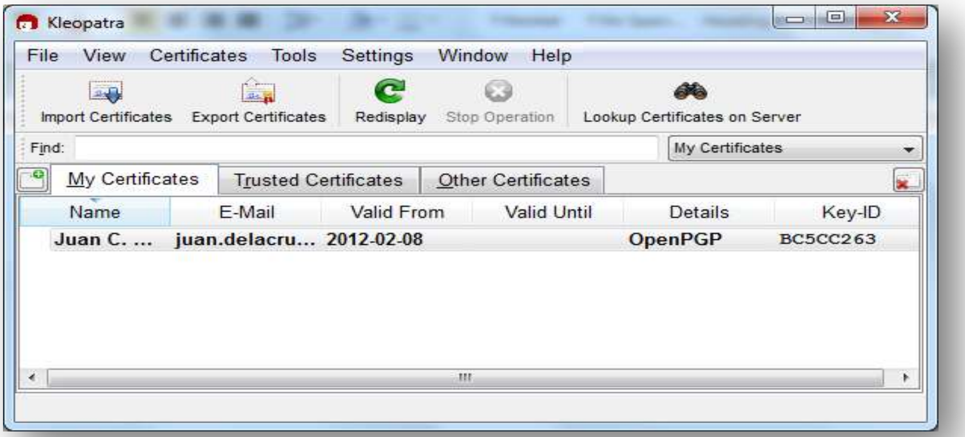


File name: back_up_publickey.asc

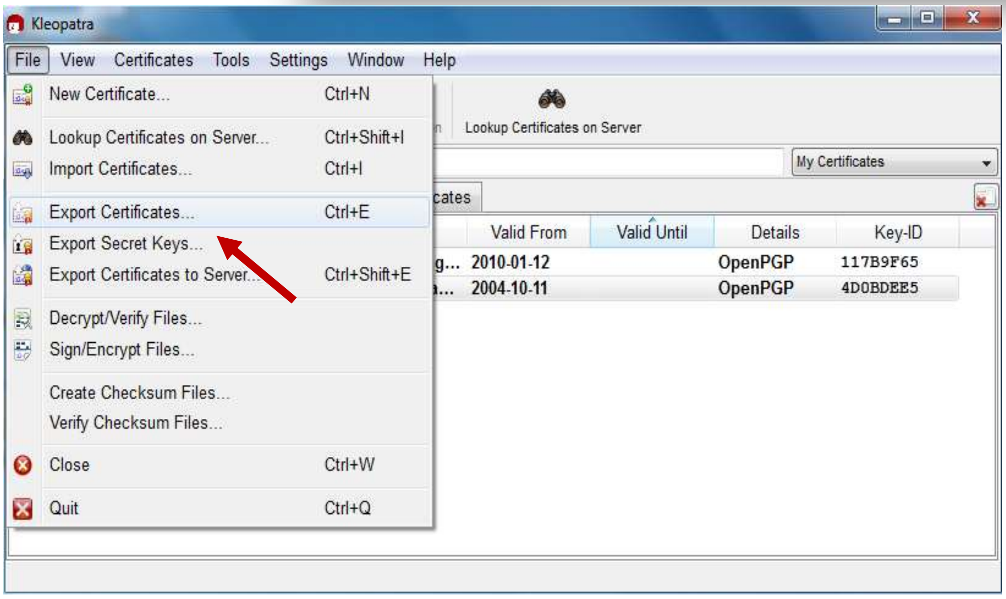
Save as type: OpenPGP Certificates (*.asc *.gpg *.pgp)

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).

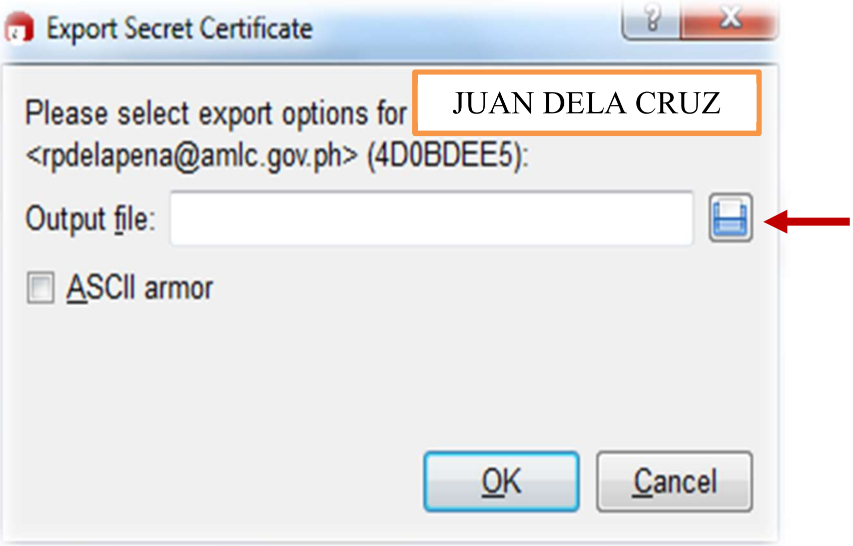


Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Juan C. ...	juan.delacru...	2012-02-08		OpenPGP	BC5CC263



	Valid From	Valid Until	Details	Key-ID
g...	2010-01-12		OpenPGP	117B9F65
a...	2004-10-11		OpenPGP	4D0BDEE5

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



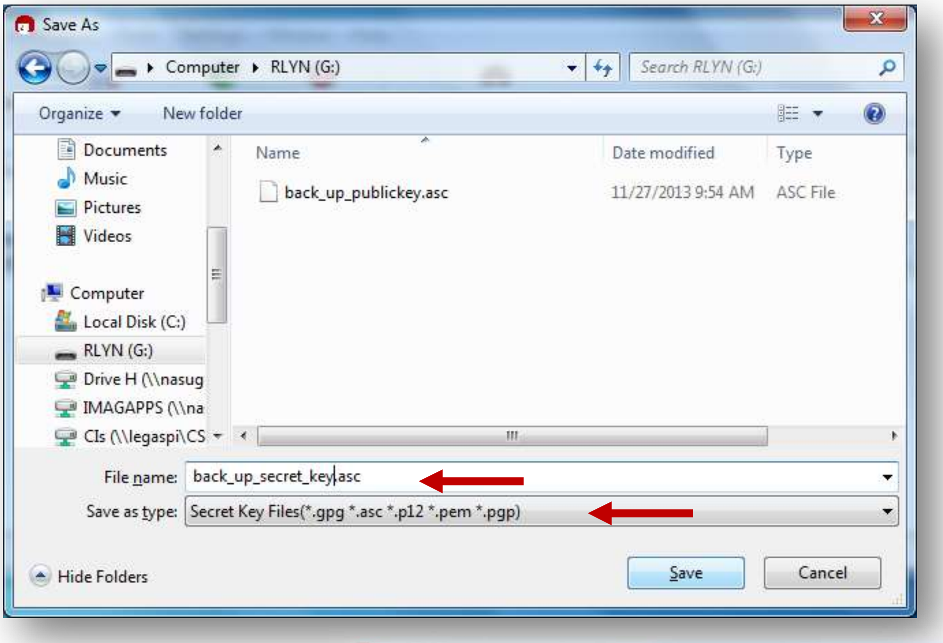
Export Secret Certificate

Please select export options for JUAN DELA CRUZ <rpdelapena@amlc.gov.ph> (4D0BDEE5):

Output file:

□ ASCII armor

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



Save As

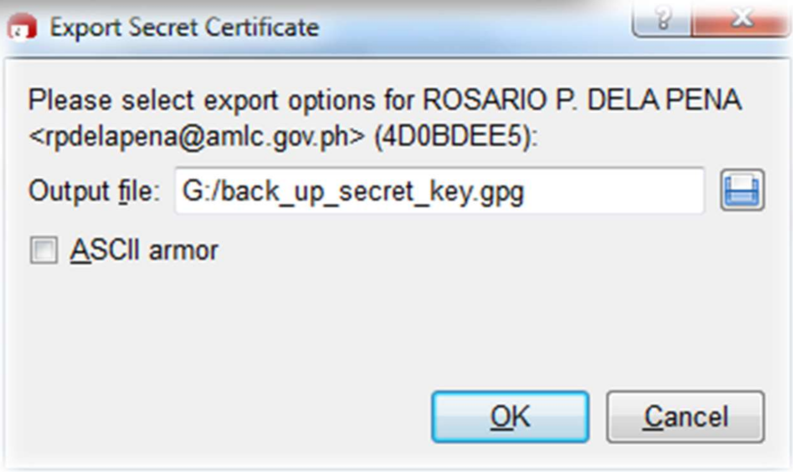
Computer ▸ RLYN (G:)

Name	Date modified	Type
back_up_publickey.asc	11/27/2013 9:54 AM	ASC File

File name: back_up_secret_key.asc

Save as type: Secret Key Files(*.gpg *.asc *.p12 *.pem *.pgp)

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.



Export Secret Certificate

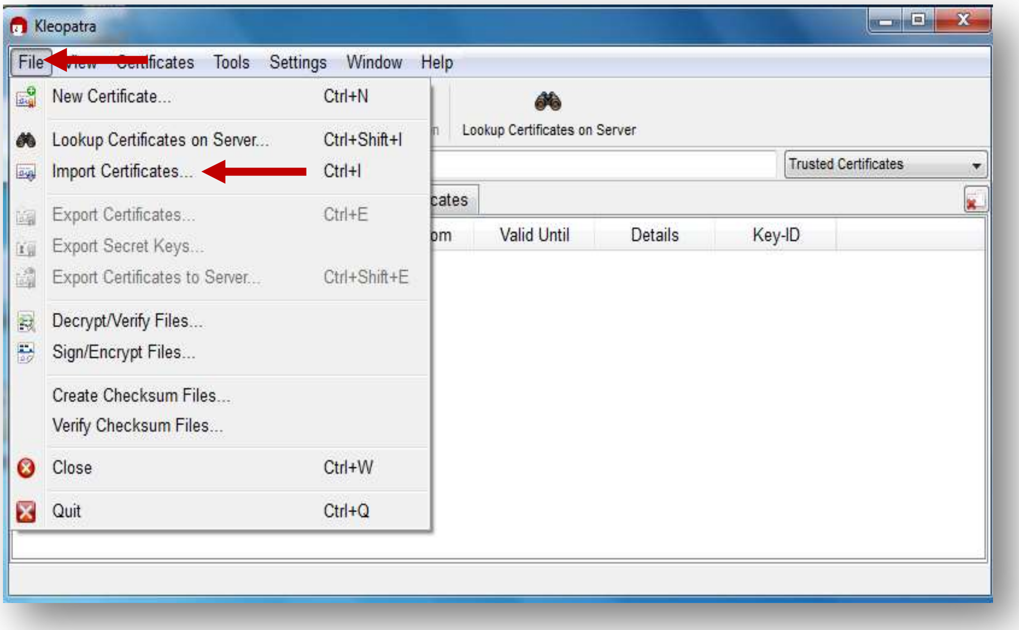
Please select export options for ROSARIO P. DELA PENA <rpdelapena@amlc.gov.ph> (4D0BDEE5):

Output file: G:/back_up_secret_key.gpg

□ ASCII armor

7. Recovery Procedure

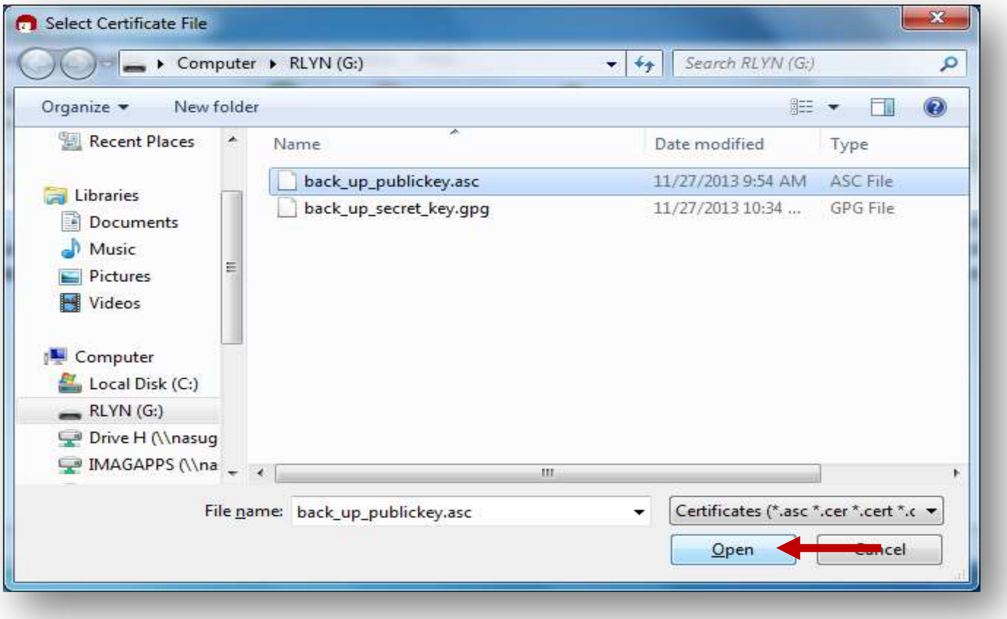
This is done if the public key is compromised, only if the CPs have performed the back-up procedure for their private and public keys.

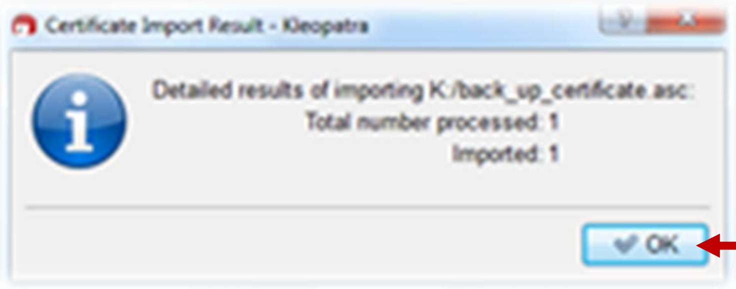

Kleopatra
File View Certificates Tools Settings Window Help
New Certificate... Ctrl+N
Lookup Certificates on Server... Ctrl+Shift+I
Import Certificates... Ctrl+I
Export Certificates... Ctrl+E
Export Secret Keys...
Export Certificates to Server... Ctrl+Shift+E
Decrypt/Verify Files...
Sign/Encrypt Files...
Create Checksum Files...
Verify Checksum Files...
Close Ctrl+W
Quit Ctrl+Q
Lookup Certificates on Server
Trusted Certificates
Valid Until
Details
Key-ID

Follow the procedure in installing the GPG Software.

Once installed, Open Kleopatra then click File then Select Import Certificate.

Select the directory where the backup of your public key (.asc) is saved then click Open.

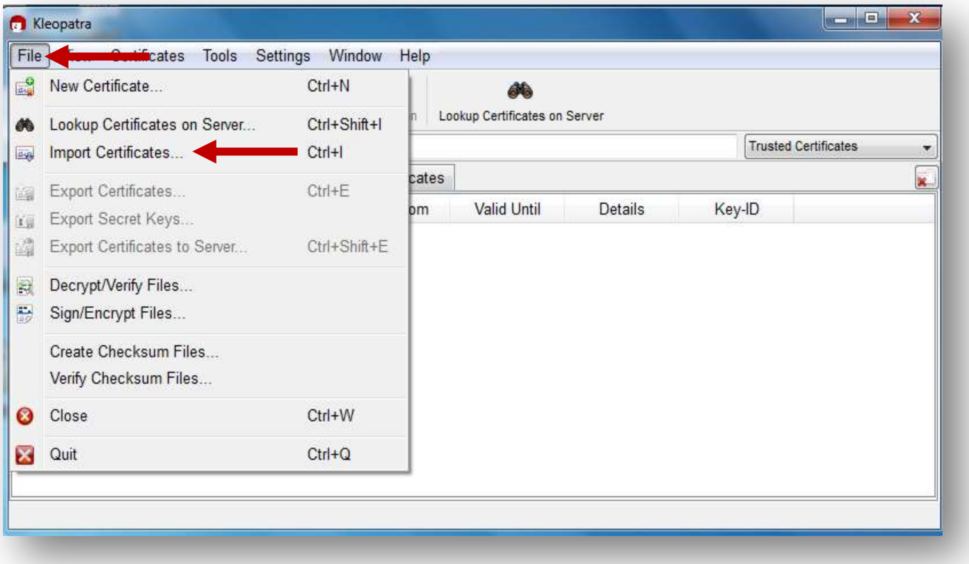


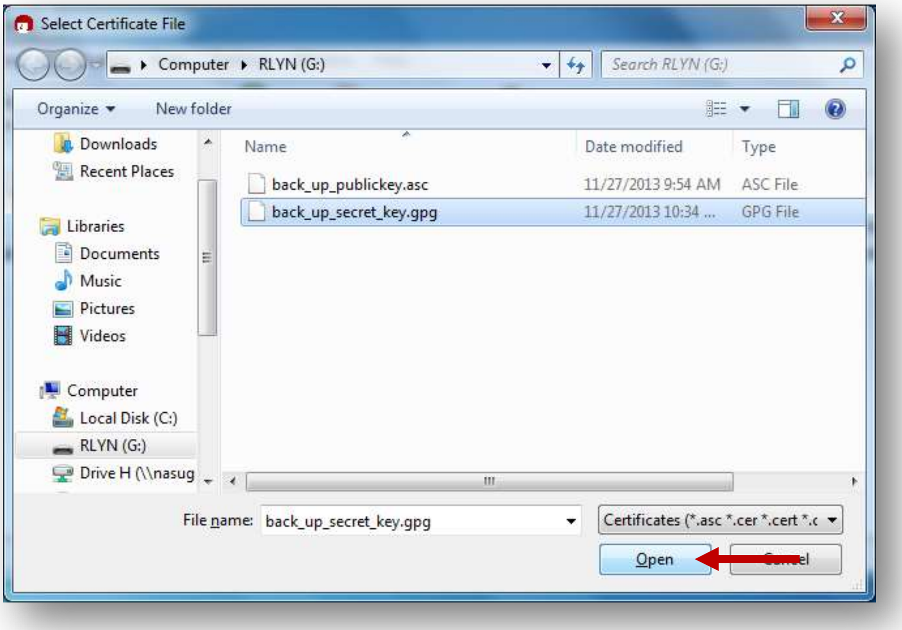


Detailed results of importing K:/back_up_certificate.asc:
Total number processed: 1
Imported: 1

Certificate Import Result window will appear then click Ok.

To import your secret key, click file then select Import Certificate.



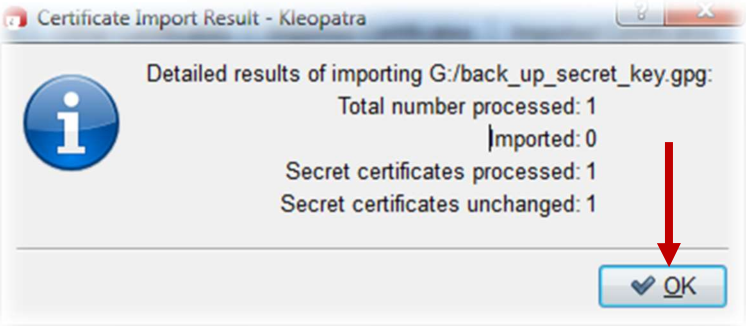


Name	Date modified	Type
back_up_publickey.asc	11/27/2013 9:54 AM	ASC File
back_up_secret_key.gpg	11/27/2013 10:34 ...	GPG File

File name: back_up_secret_key.gpg

Certificates (*.asc *.cer *.cert *.c

Select the directory where the backup of your private key (.gpg) is saved then click Open.



Detailed results of importing G:/back_up_secret_key.gpg:
Total number processed: 1
Imported: 0
Secret certificates processed: 1
Secret certificates unchanged: 1

Certificate Import Result window will appear then click Ok.

Repeat Procedures 4-6 of the Transaction Security Protocol.