University
of Houston
Clear Lake

Uploading encrypted forms from an OmniUpdate web site using Gpg4win

February 24, 2016

Table of Contents

I. Introduction

On occasion, University departments are required to provide their constituents with a facility to send scanned images of completed, physical forms to department personnel.

Note – the form documents to which we refer are not web forms where data is manually entered by the user field-by-field directly into a web page. Rather, we are referring to standard Microsoft Word or Adobe .pdf document files that are filled in by the user within the Word or Adobe environment, printed, signed, scanned and uploaded.

In a typical web-based, "document upload" implementation, a user clicks a button on the page to indicate that one or more documents are to be uploaded. After the button is clicked, the user is presented with a file selection window to pick the file(s) to be uploaded. Once the file or files have been selected, the user clicks a button to begin the document transfer. The documents often are transmitted via an e-mail to a predefined departmental e-mail box where departmental personnel can pick up the documents.

Unfortunately, when an uploaded documents contains information that is sensitive in nature, this method cannot be used, since e-mail is not a secure method of exchanging sensitive information, and the use of e-mail in this case would not be consistent with University policy.

To overcome the security issues associated with an e-mail-based approach, UCT has developed a mechanism for uploading sensitive documents from within a UHCL web page that combines the simplicity of an e-mail-based solution with the security of modern encryption techniques. The key to this solution is the implementation of software, called "Gpg4win", that allows users and applications to exchange data in a secure manner using encryption technology. With Gpg4win installed, files holding sensitive data can be encrypted and decrypted where necessary throughout the business process in the following ways:

- Transparently from within Microsoft Outlook, or
- Manually, using Gpg4win commands either entered through a command line interface or coded into an application program or web page.

Gpg4win also performs other encryption-based functions, such as the digital signing of documents, and the verification of those signatures that can be useful, but are not integral parts of the web-based, document upload process.

II. How Gpg4win is integrated into your department's web site

If you need to allow users to securely send scanned documents to your department, contact the OU Support team to review your form upload requirements and to help you integrate the encrypted upload function into your web content.

The team will set up your web page so that the web page content is downloaded to the browser of any of your users carries the Gpg4win software and your department's generated encryption key. When the user selects the documents to be transmitted and clicks the upload button, the document will be encrypted automatically before it is sent. Thanks to Gpg4win's integration with Microsoft Outlook, the departmental staff who receive encrypted document(s) can decrypt the uploaded document by clicking a button that Gpg4win installs in his or her e-mail client.

If the encrypted document will be delivered to department personnel, typically via e-mail, the individuals who will receive the forms will need to have Gpg4win installed on the workstations they may use to receive the forms. Instructions for installing Gpg4win can be found in the section entitled **IV. Installing Gpg4win**.

Once Gpg4win is installed, the receiving department will need to create a set of encryption keys for the department. The key generation process generates two keys, called a "key pair". One key, called the "public key" can be freely shared with anyone in the world who needs to send the key owner any encrypted data. The second key is called the "private key" that is only used by authorized recipients to decrypt the encrypted, incoming files. Whenever the private key is used, it must be "unlocked" by the user who must enter in the "passphrase" that the person who generates the key pair supplies when the key pair was generated. Instructions for creating a key pair or certificate, as it can also be called, can be found in the section entitled **V. Creating your public and private keys**.

Since, in most cases there will be more than one individual in a department who may receive the uploaded form, the same key pair can be used by all authorized department personnel who know the private key passphrase.

As mentioned earlier, anyone needing to upload a form to your department will need to obtain your public key to encrypt the file they wish to upload. Fortunately, the OmniUpdate implementation that we have developed simplifies this task. If you need your web page to contain a function to securely upload a document, OU Support will set up your web content so that, when the web page is downloaded to the browser of any of your users, the page will carry the Gpg4win software and your department's "public key" that was generated. When the user clicks the upload button, the document will be encrypted automatically before it is transmitted.

You will need to provide your generated public key to OU Support for the web page setup step. Instructions for exporting your public key certificate to OU Support or anyone who needs to send you encrypted files or messages can be found in the section entitled **VI. Exporting your public key to another GPG user**.

Once the software and keys have been installed, you can begin to receive and decrypt the messages uploaded via your web site. When you receive the encrypted form in your e-mail, all you need to do is to follow the procedure contained in the sections entitled **VII. Decrypting an encrypted e-mail message that has been sent to you** or **VIII. Decrypting an encrypted e-mail attachment** depending on the implementation design.

III. Other Gpg4win functions that enable users to securely exchange documents and files via e-mail

It is worth noting that Gpg4win provides additional functions that are not part of our document upload mechanism but that enable individual users to encrypt, decrypt, sign and verify the signature on e-mail messages and files exchanged with other Gpg4win users.

To use these functions, each user who will exchange encrypted and/or signed e-mail messages with others must set up his or her computer by performing the following steps:

- Install Gpg4win on his or her computer using the instructions that can be found in the section entitled **IV. Installing Gpg4win**. The installation process will add the following functions into your Microsoft Outlook client: Encrypt, Decrypt, Sign and Verify (signature).

- Create a personal key pair or certificate using the instructions that can be found in the section entitled **V. Creating your public and private keys**.

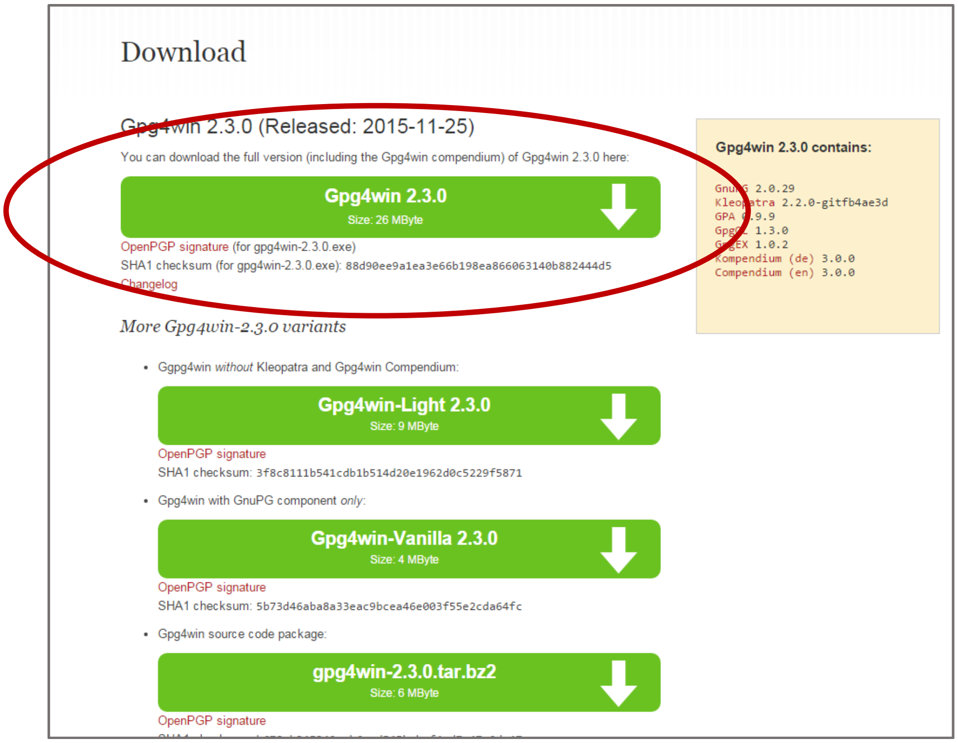
- Export his or her public key certificate to anyone who will send the user an encrypted document or file using the instructions that can be found in the section entitled **VI. Exporting your public key to another GPG user**.

- Import into his or her key file or "key ring" the public key certificates received from other users using the instructions that can be found in the section entitled **VII. Importing another user's public key into your GPG key file**

A description of the individual e-mail-based functions that Gpg4win provides can be found in sections VIII through XIII of this document.

IV. Installing Gpg4win

1. Visit www.gpg4win.org. Click on the "Gpg4win 2.3.0" button.



Download

Gpg4win 2.3.0 (Released: 2015-11-25)

You can download the full version (including the Gpg4win compendium) of Gpg4win 2.3.0 here:

OpenPGP signature (for gpg4win-2.3.0.exe)
SHA1 checksum (for gpg4win-2.3.0.exe): 88d90ee9a1ea3e66b198ea866063140b882444d5
Changelog

Gpg4win 2.3.0 contains:

```
GnuPG 2.0.29
Kleopatra 2.2.0-gitfb4ae3d
GPA 0.9.9
GpgOL 1.3.0
GpgEX 1.0.2
Kompendium (de) 3.0.0
Compendium (en) 3.0.0
```

More Gpg4win-2.3.0 variants

- Ggpg4win *without* Kleopatra and Gpg4win Compendium:

OpenPGP signature
SHA1 checksum: 3f8c8111b541cdb1b514d20e1962d0c5229f5871

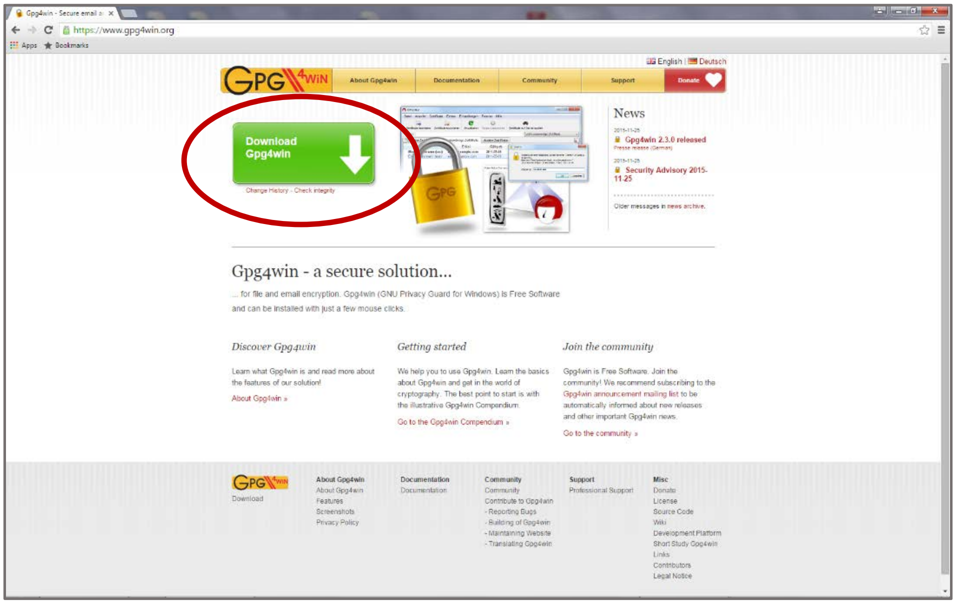
- Gpg4win with GnuPG component *only*:

OpenPGP signature
SHA1 checksum: 5b73d46aba8a33eac9bcea46e003f55e2cda64fc

- Gpg4win source code package:

OpenPGP signature

2. On the following screen, click the "Download Gpg4win" button.



News

2015-11-25
Gpg4win 2.3.0 released
Presse release (German)

2015-11-25
Security Advisory 2015-11-25

Older messages in news archive.

Gpg4win - a secure solution...

... for file and email encryption. Gpg4win (GNU Privacy Guard for Windows) is Free Software and can be installed with just a few mouse clicks.

Discover Gpg4win

Learn what Gpg4win is and read more about the features of our solution!

About Gpg4win »

Getting started

We help you to use Gpg4win. Learn the basics about Gpg4win and get in the world of cryptography. The best point to start is with the illustrative Gpg4win Compendium.

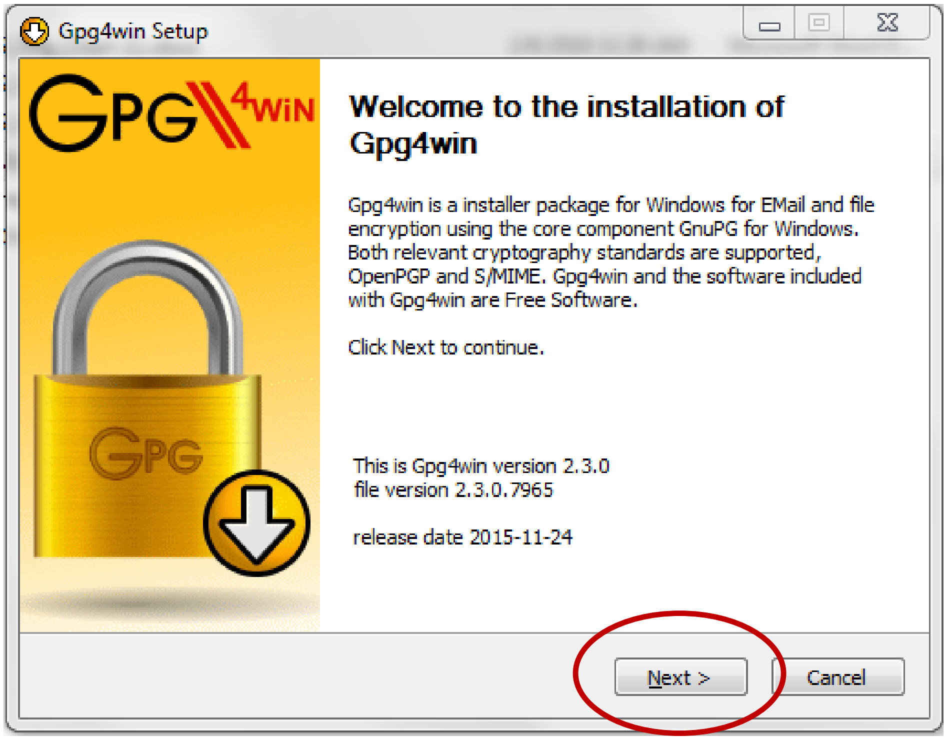
Go to the Gpg4win Compendium »

Join the community

Gpg4win is Free Software. Join the community! We recommend subscribing to the Gpg4win announcement mailing list to be automatically informed about new releases and other important Gpg4win news.

Go to the community »

3. When the "Welcome" screen is displayed, click the "Next" button.



Welcome to the installation of Gpg4win

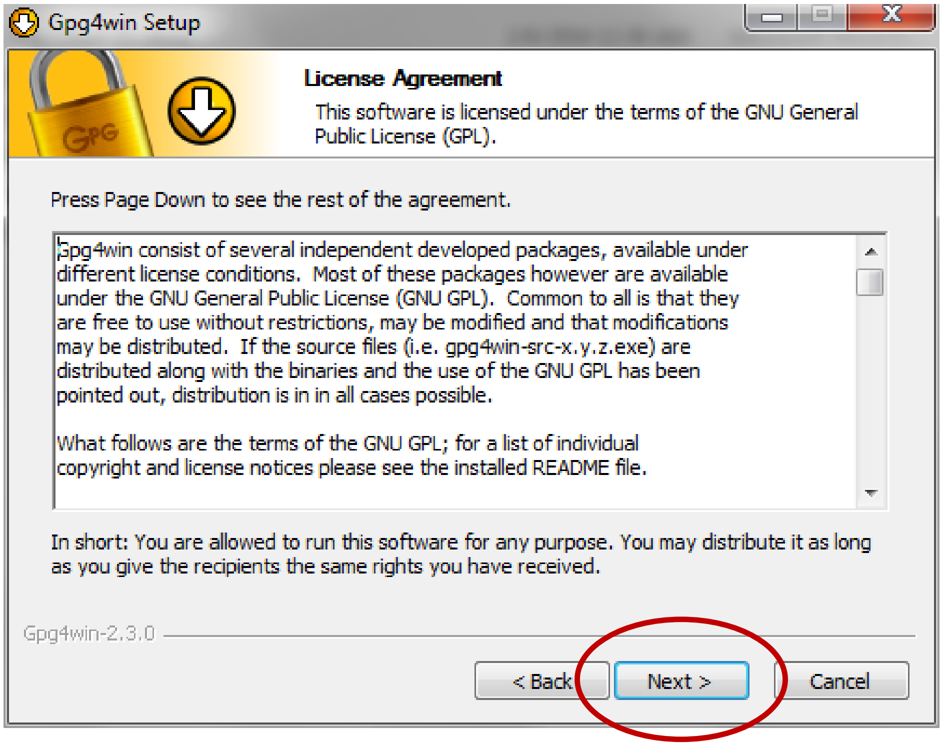
Gpg4win is a installer package for Windows for EMail and file encryption using the core component GnuPG for Windows. Both relevant cryptography standards are supported, OpenPGP and S/MIME. Gpg4win and the software included with Gpg4win are Free Software.

Click Next to continue.

This is Gpg4win version 2.3.0
file version 2.3.0.7965

release date 2015-11-24

4. When the "License Agreement" page is displayed, click the "Next" button.



License Agreement

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

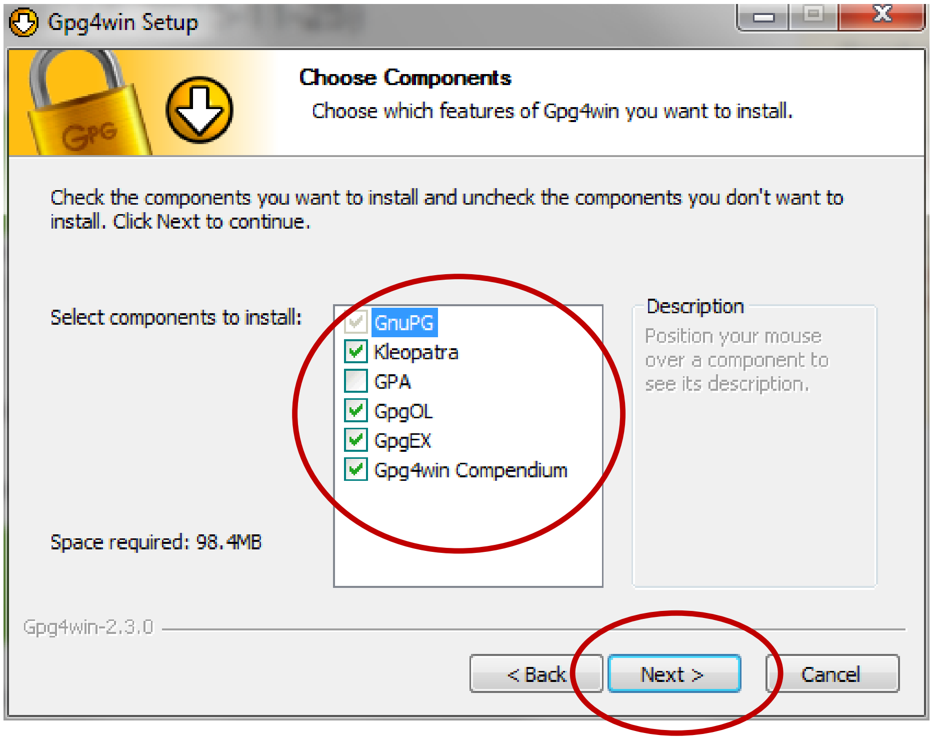
Press Page Down to see the rest of the agreement.

Gpg4win consist of several independent developed packages, available under different license conditions. Most of these packages however are available under the GNU General Public License (GNU GPL). Common to all is that they are free to use without restrictions, may be modified and that modifications may be distributed. If the source files (i.e. gpg4win-src-x.y.z.exe) are distributed along with the binaries and the use of the GNU GPL has been pointed out, distribution is in in all cases possible.

What follows are the terms of the GNU GPL; for a list of individual copyright and license notices please see the installed README file.

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.

5. Set the check box values as specified below, then click the "Next" button.


Gpg4win Setup

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
- ☑ Gpg4win Compendium

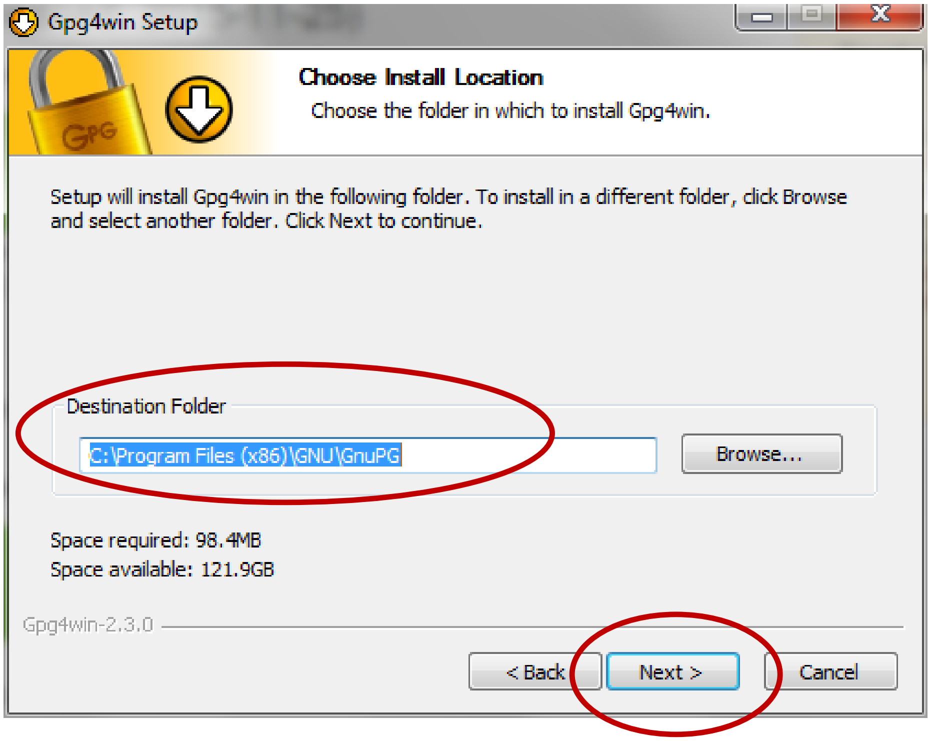
Description

Position your mouse over a component to see its description.

Space required: 98.4MB

Gpg4win-2.3.0

6. Set the location where you want the software to be installed. The default location is fine. Then, click the "Next" button.


Gpg4win Setup

Choose Install Location

Choose the folder in which to install Gpg4win.

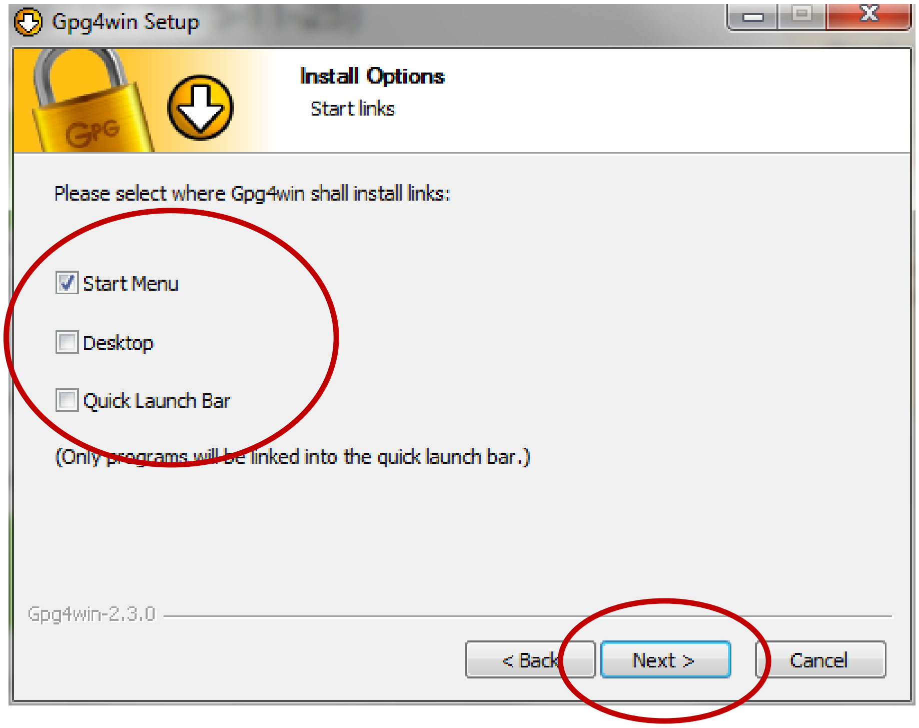
Setup will install Gpg4win in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

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

Space required: 98.4MB
Space available: 121.9GB

Gpg4win-2.3.0

7. Specify where you want shortcuts to the software placed, then click the "Next" button.


Gpg4win Setup

Install Options

Start links

Please select where Gpg4win shall install links:

☑ Start Menu

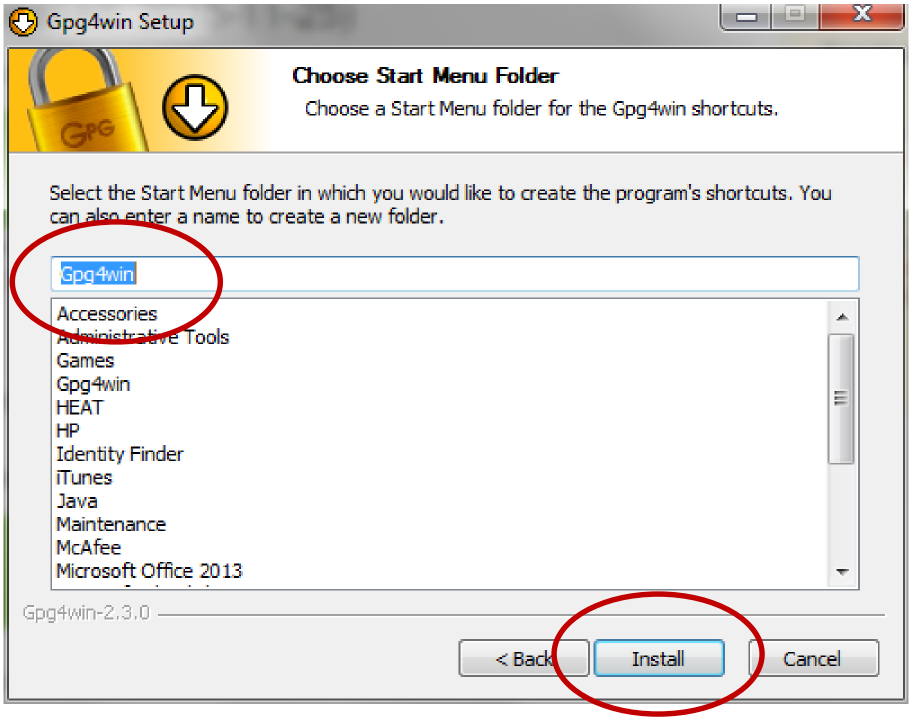
□ Desktop

□ Quick Launch Bar

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

Gpg4win-2.3.0

8. If you selected to have a GPG shortcut in your Start Menu, specify the folder in which it will be placed. The default "Gpg4win" is OK. Click the "Install" button to continue.


Gpg4win Setup

Choose Start Menu Folder

Choose a Start Menu folder for the Gpg4win shortcuts.

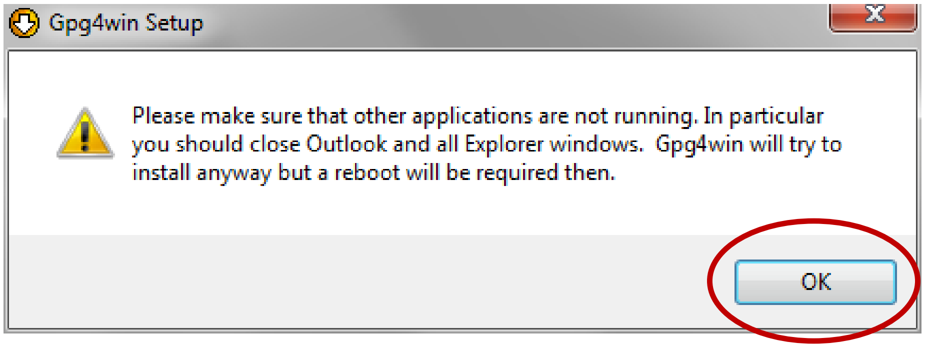
Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

Gpg4win

Accessories
Administrative Tools
Games
Gpg4win
HEAT
HP
Identity Finder
iTunes
Java
Maintenance
McAfee
Microsoft Office 2013

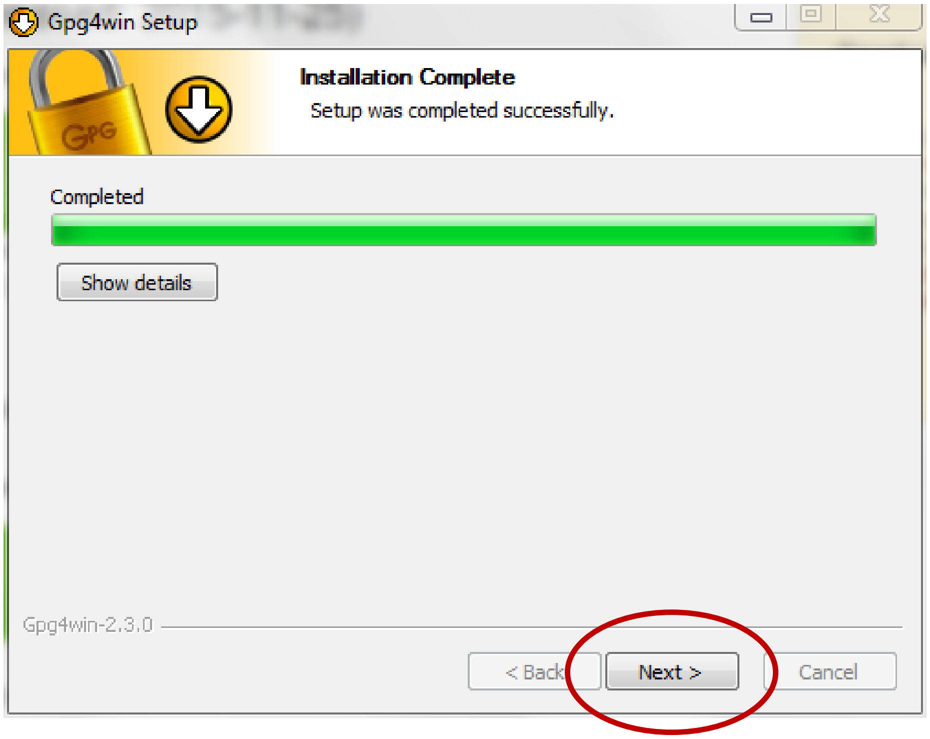
Gpg4win-2.3.0

9. A warning will be displayed if you have Outlook or Explorer opened. If this occurs, click the "OK" button.



Please make sure that other applications are not running. In particular you should close Outlook and all Explorer windows. Gpg4win will try to install anyway but a reboot will be required then.

10. The installation process will tell you when it is complete. Click the "Next" button.

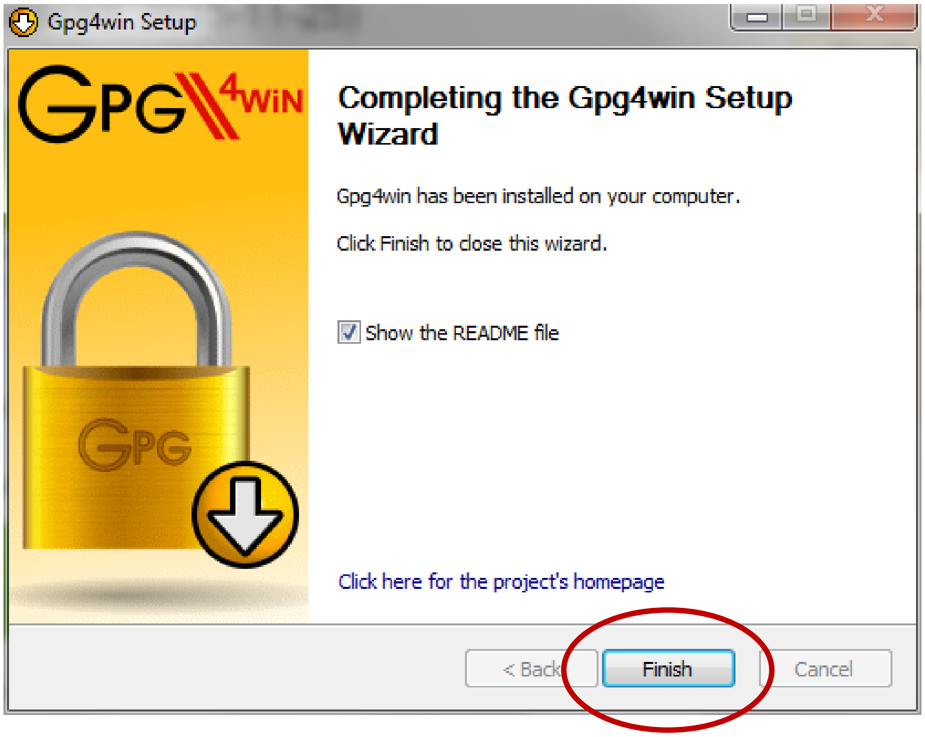


Installation Complete

Setup was completed successfully.

Completed

11. Once the Gpg4win setup wizard is complete, the following screen will be displayed. Click the “Finish” button.



Completing the Gpg4win Setup Wizard

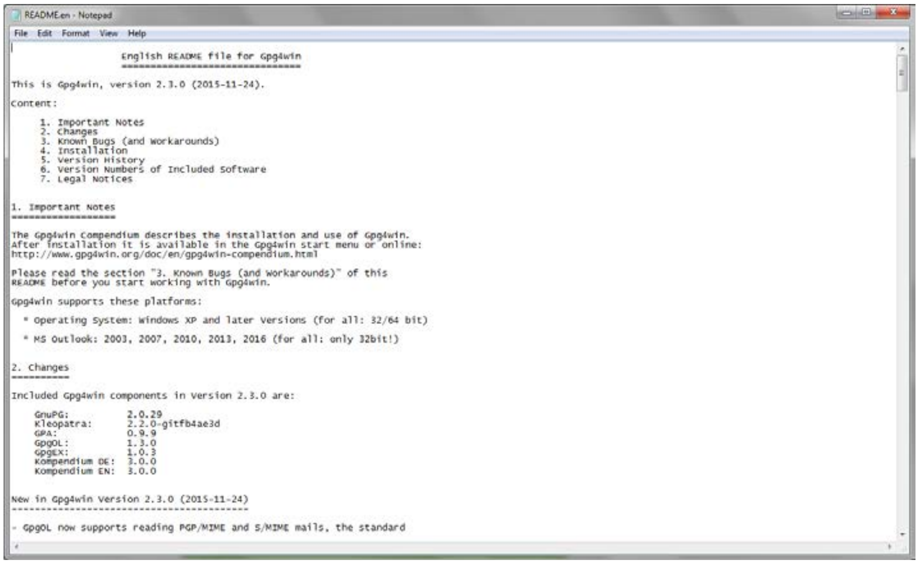
Gpg4win has been installed on your computer.

Click Finish to close this wizard.

☑ Show the README file

Click here for the project's homepage

12. If you do not uncheck the “Show the README file” check box, the README file will be displayed. The window can be closed after you’ve reviewed it.



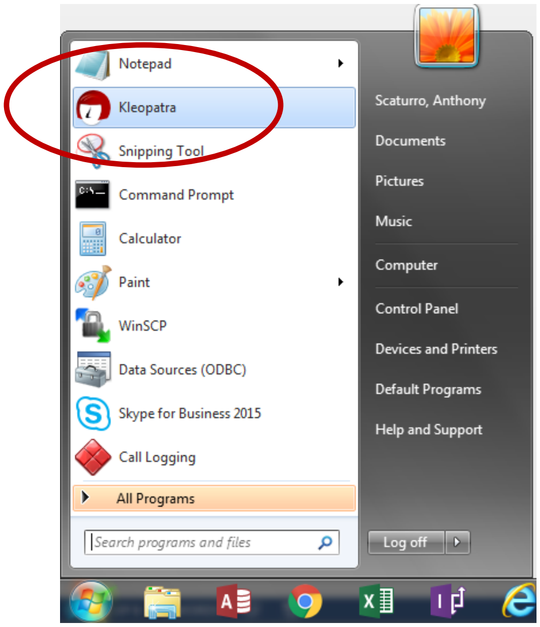
```
                      English README file for Gpg4win
                      ===============================

This is Gpg4win, version 2.3.0 (2015-11-24).

Content:

     1. Important Notes
     2. Changes
     3. Known Bugs (and workarounds)
     4. Installation
     5. Version History
     6. Version Numbers of Included Software
     7. Legal Notices

1. Important Notes
==================

The Gpg4win Compendium describes the installation and use of Gpg4win.
After installation it is available in the Gpg4win start menu or online:
http://www.gpg4win.org/doc/en/gpg4win-compendium.html

Please read the section "3. Known Bugs (and workarounds)" of this
README before you start working with Gpg4win.

Gpg4win supports these platforms:

  * Operating System: Windows XP and later Versions (for all: 32/64 bit)

  * MS Outlook: 2003, 2007, 2010, 2013, 2016 (for all: only 32bit!)

2. Changes
==========

Included Gpg4win components in Version 2.3.0 are:

    GnuPG:          2.0.29
    Kleopatra:      2.2.0-gitfb4ae3d
    GPA:            0.9.9
    GpgOL:          1.3.0
    GpgEX:          1.0.3
    Kompendium DE:  3.0.0
    Kompendium EN:  3.0.0

New in Gpg4win Version 2.3.0 (2015-11-24)
-----------------------------------------

- GpgOL now supports reading PGP/MIME and S/MIME mails, the standard
```

V. Creating your public and private keys

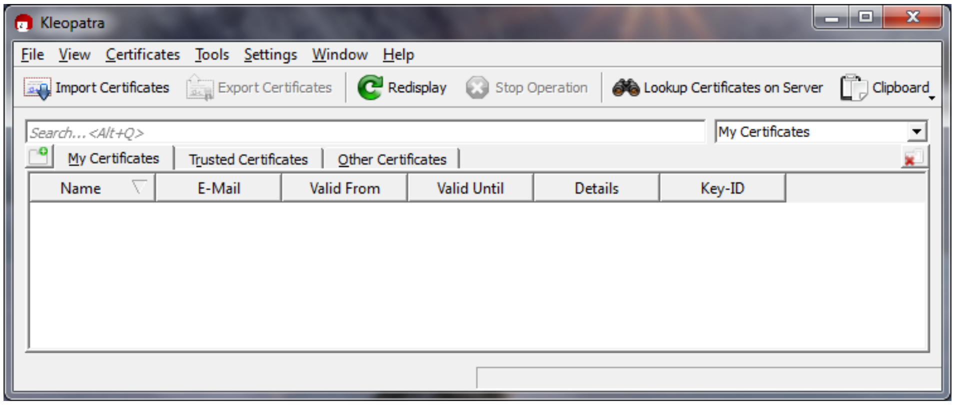
GPG encryption and decryption is based upon the keys of the person who will be receiving the encrypted file or message. Any individual who wants to send the person an encrypted file or message must possess the recipient's public key certificate to encrypt the message. The recipient must have the associated private key, which is different than the public key, to be able to decrypt the file.

The public and private key pair for an individual is usually generated by the individual on his or her computer using the installed GPG program, called "Kleopatra" and the following procedure:

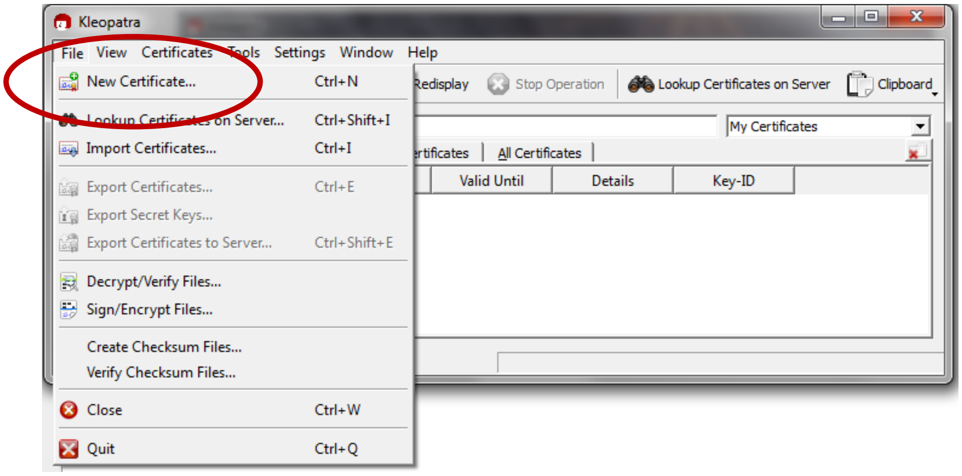
1. From your start bar, select the "Kleopatra" icon to start the Kleopatra certificate management software.



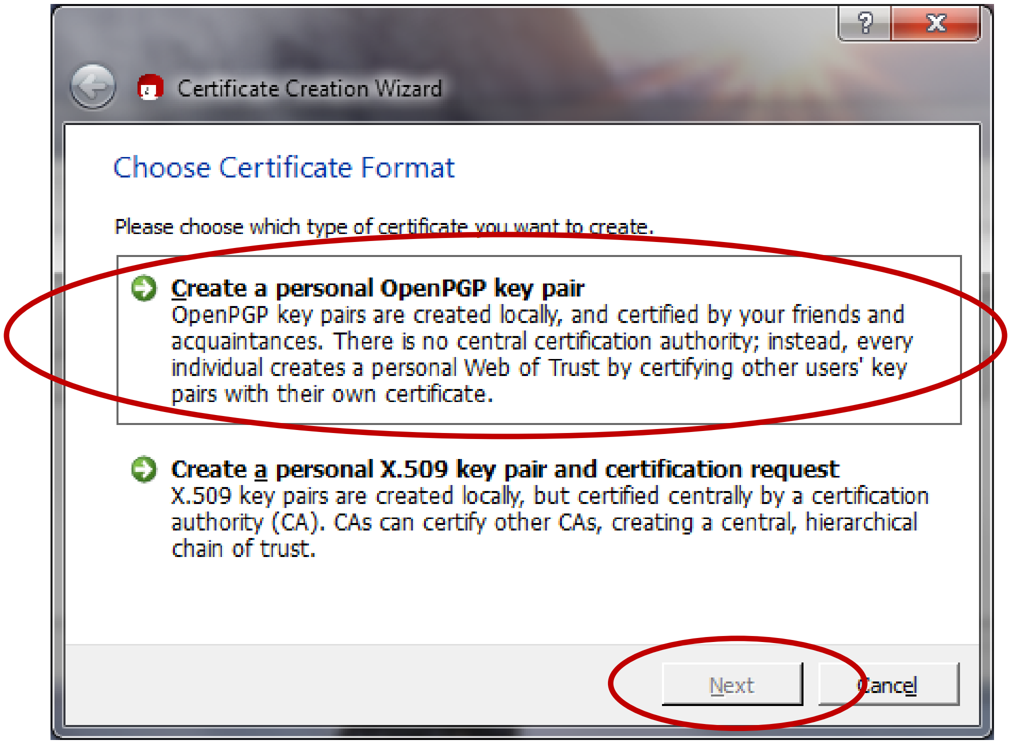
2. The following screen will be displayed



3. From the “File” dropdown, click on the “New Certificate” option.


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
Redisplay
Stop Operation
Lookup Certificates on Server
Clipboard
My Certificates
rtificates
All Certificates
Valid Until
Details
Key-ID

4. The following screen will be displayed. Click on “Create a personal OpenGPG key pair” and the “Next” button.



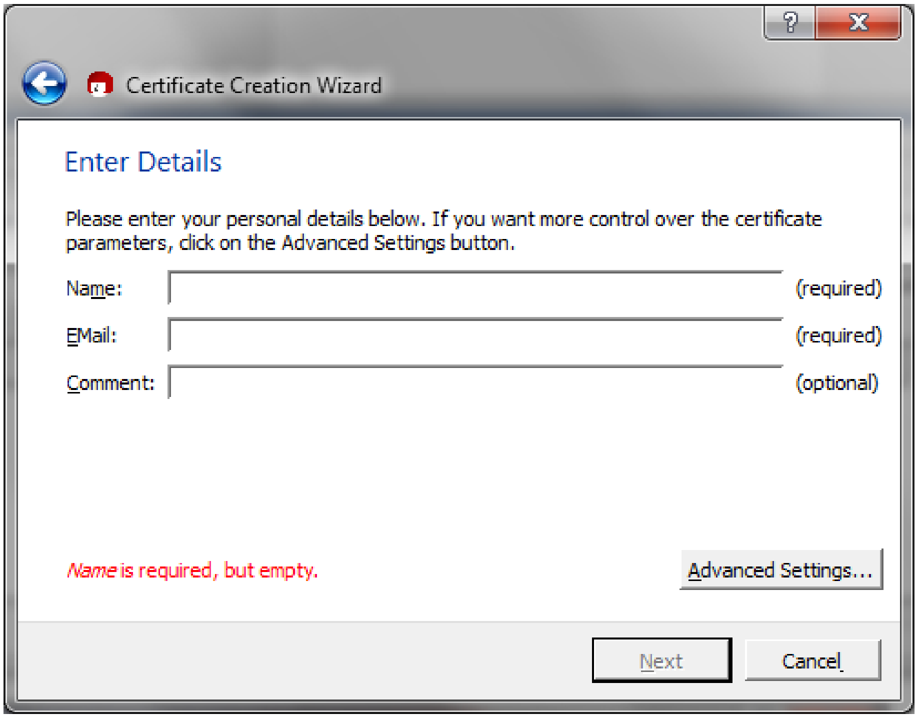
Choose Certificate Format

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 individual creates a personal Web of Trust by certifying other users' key pairs with their own certificate.

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 trust.

5. The Certificate Creation Wizard will start and display the following:



Enter Details

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

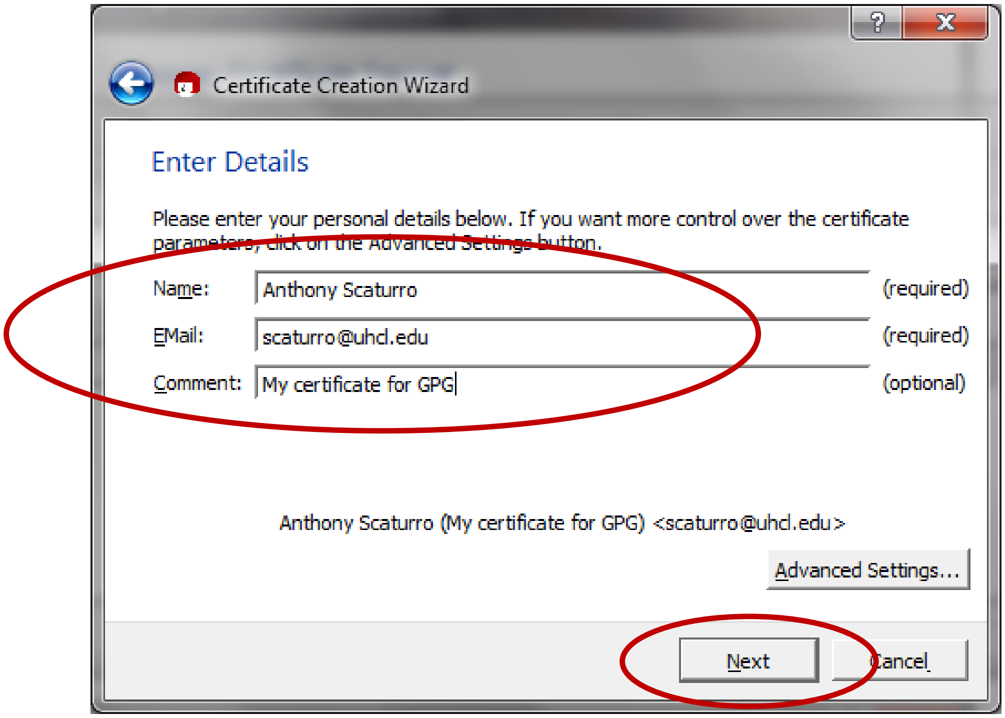
Name: (required)

EMail: (required)

Comment: (optional)

Name is required, but empty.

6. Enter your name and e-mail address. You may also enter an optional comment. Then, click the "Next" button



Enter Details

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

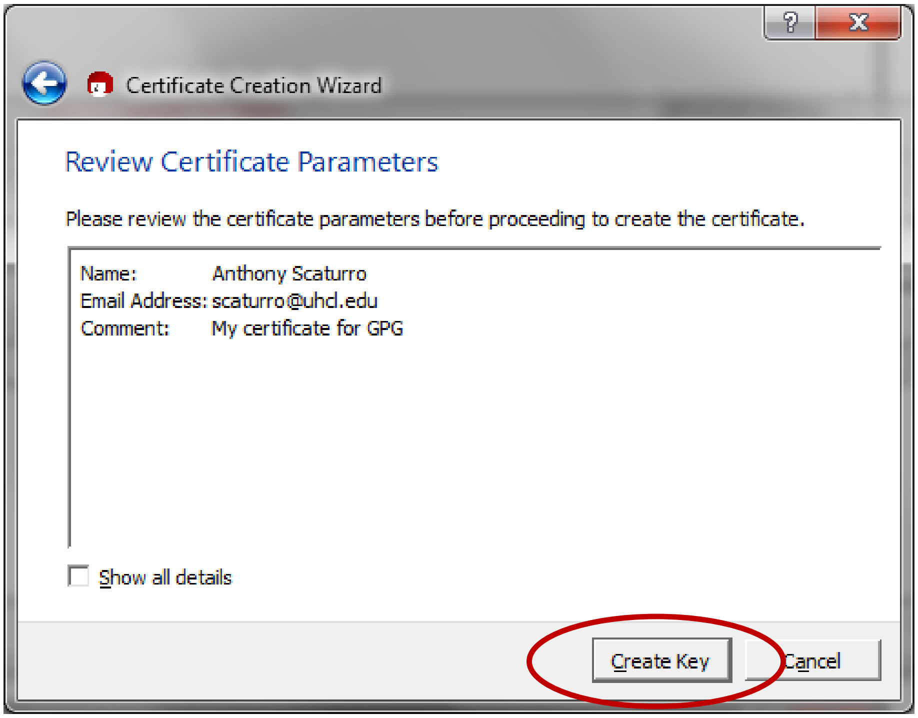
Name: Anthony Scaturro (required)

EMail: scaturro@uhcl.edu (required)

Comment: My certificate for GPG (optional)

Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu>

7. Review your entered values. If OK, click the "Create Key" button.



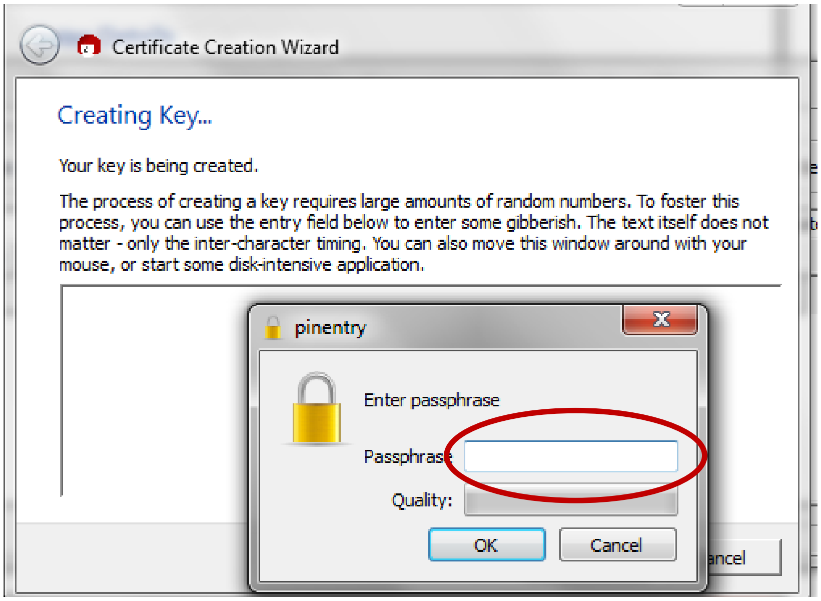
Review Certificate Parameters

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

Name: Anthony Scaturro
Email Address: scaturro@uhcl.edu
Comment: My certificate for GPG

□ Show all details

8. You will be asked to enter a passphrase.

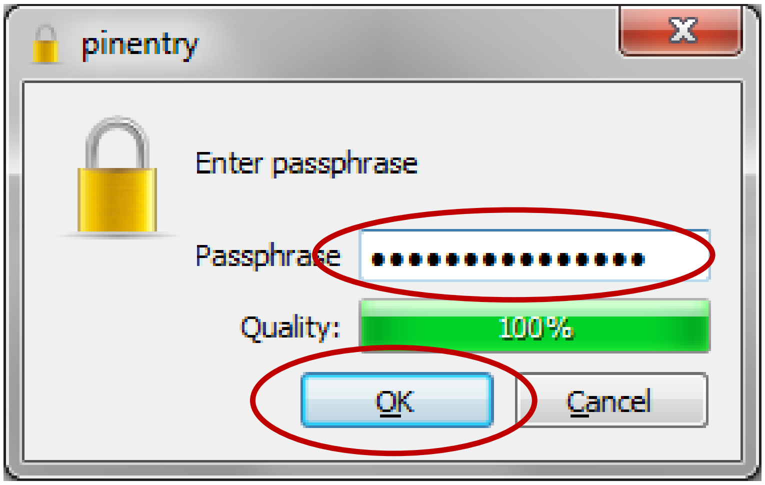


Creating Key...

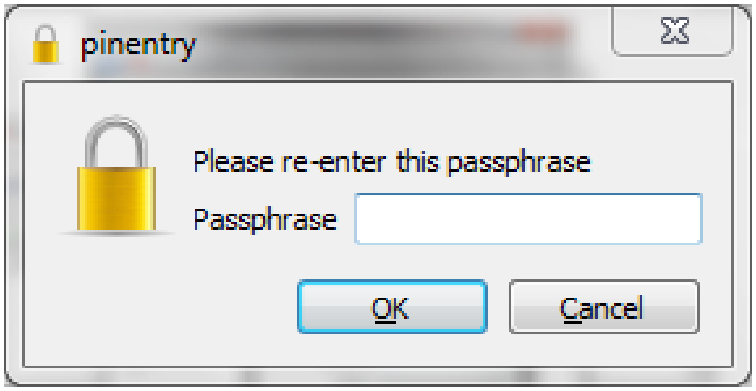
Your key is being created.

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 does not matter - only the inter-character timing. You can also move this window around with your mouse, or start some disk-intensive application.

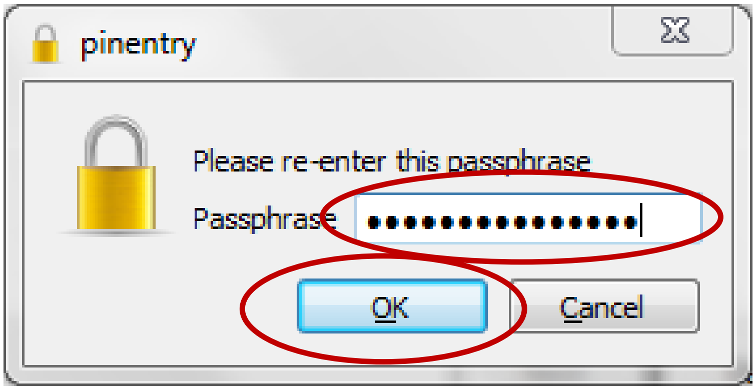
9. The passphrase should follow strong password standards. After you've entered your passphrase, click the "OK" button.



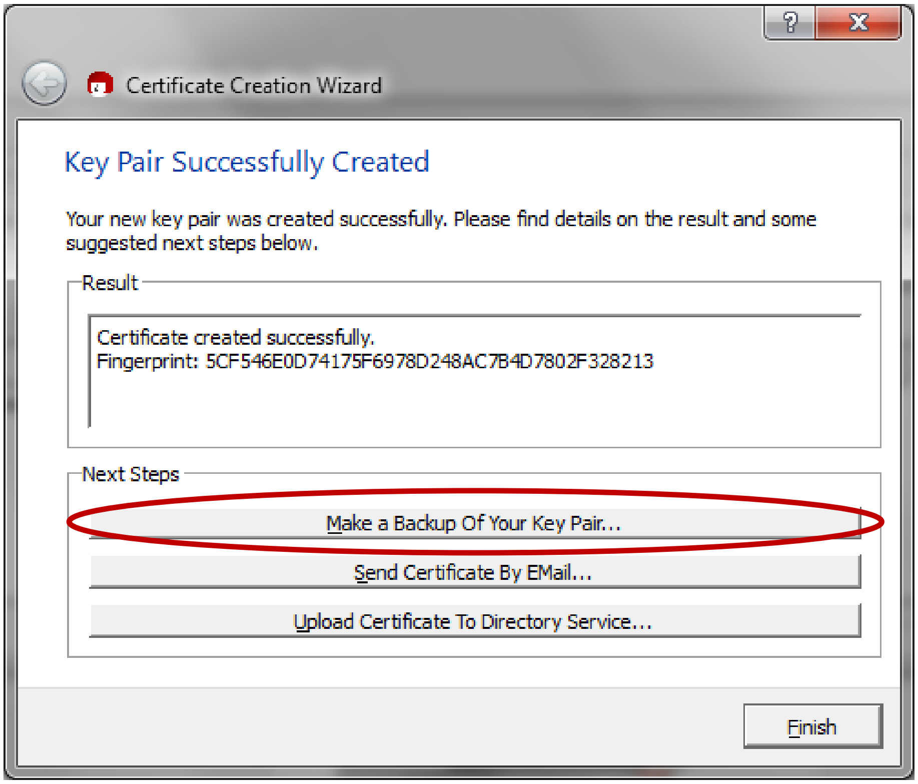
10. You will be asked to re-enter the passphrase



11. Re-enter the passphrase value. Then click the "OK" button. If the passphrases match, the certificate will be created.



12. Once the certificate is created, the following screen will be displayed. You can save a backup of your public and private keys by clicking the “Make a backup Of Your Key Pair” button. This backup can be used to copy certificates onto other authorized computers.


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.

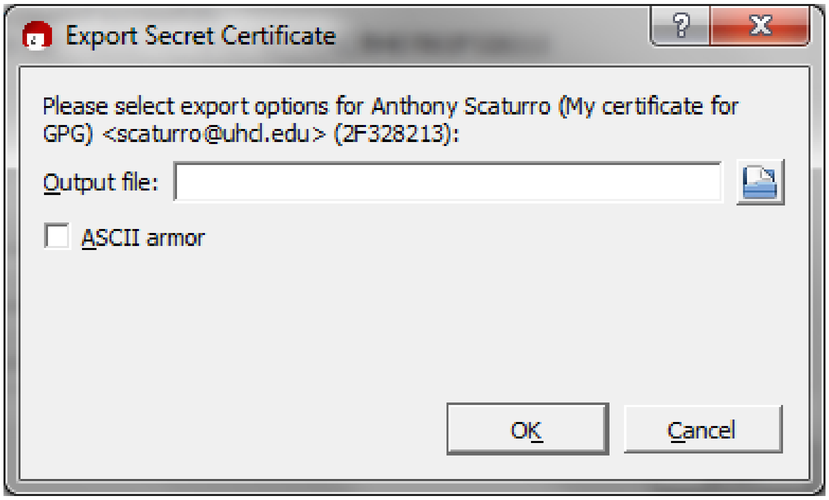
Result

Certificate created successfully.
Fingerprint: 5CF546E0D74175F6978D248AC7B4D7802F328213

Next Steps

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

13. If you choose to backup your key pair, you will be presented with the following screen:

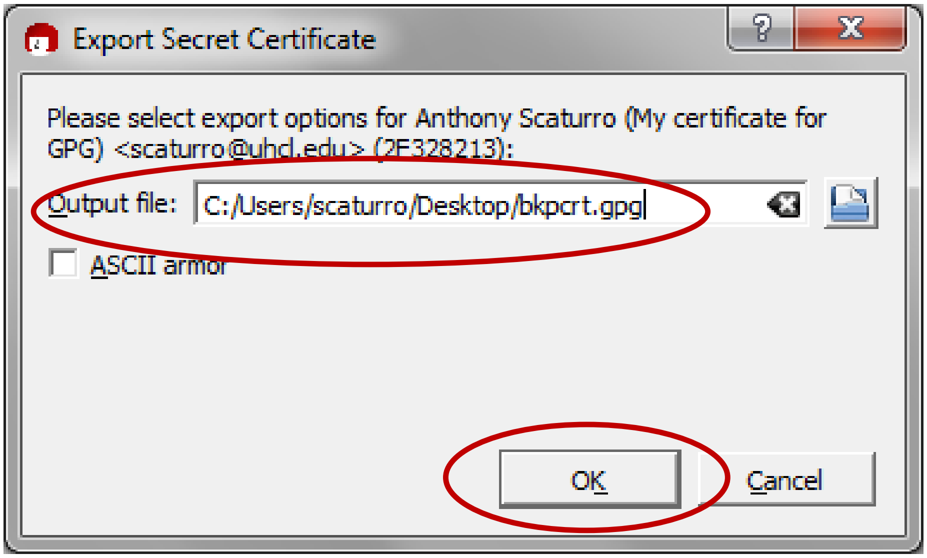


Please select export options for Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu> (2F328213):

Output file:

☐ ASCII armor

14. Specify the folder and name the file. Then click the "OK" button.



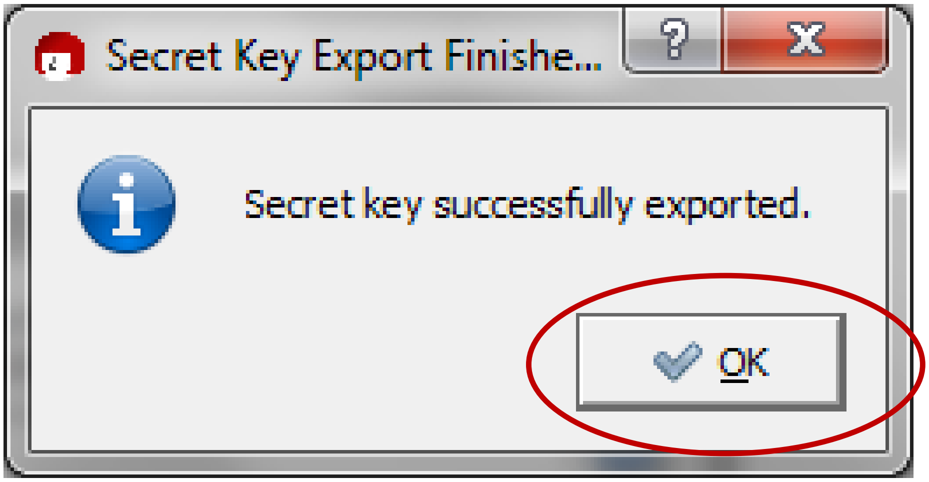
Export Secret Certificate

Please select export options for Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu> (2F328213):

Output file: C:/Users/scaturro/Desktop/bkpcrt.gpg

□ ASCII armor

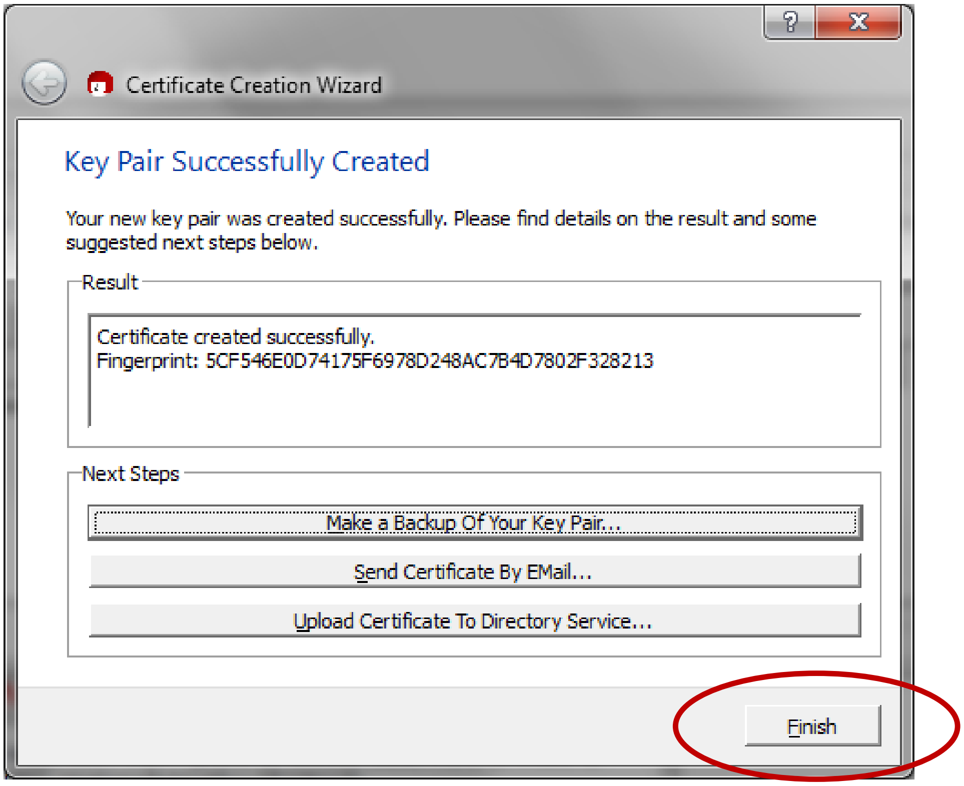
15. After the key is exported, the following will be displayed. Click the "OK" button.



Secret Key Export Finishe...

Secret key successfully exported.

16. You will be returned to the "Key Pair Successfully Created" screen. Click the "Finish" button.

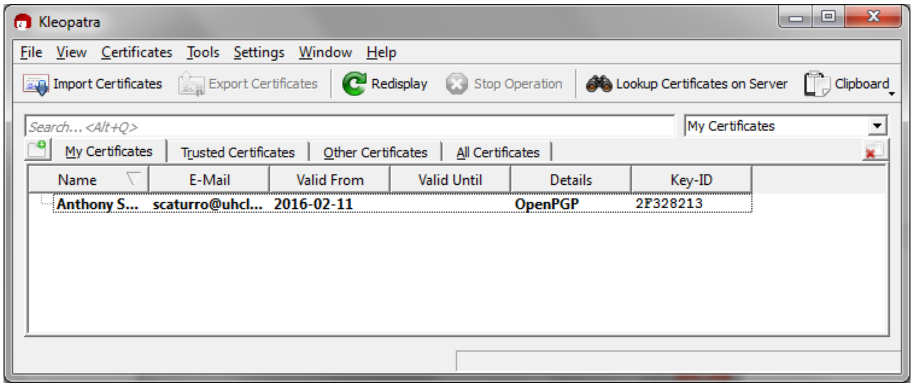

Certificate Creation Wizard
Result
Next Steps
Make a Backup Of Your Key Pair...
Send Certificate By EMail...
Upload Certificate To Directory Service...
Finish

Key Pair Successfully Created

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

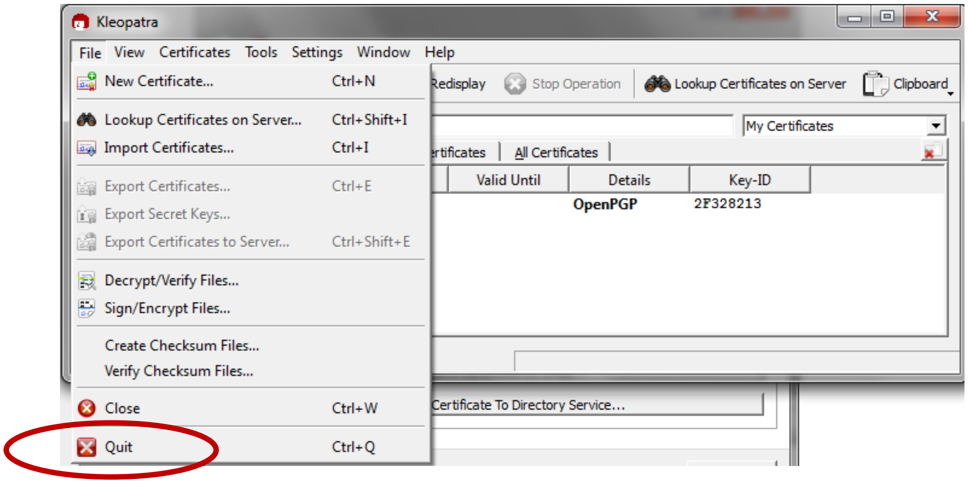
Certificate created successfully.
Fingerprint: 5CF546E0D74175F6978D248AC7B4D7802F328213

17. The wizard will end and you will be back to the Kleopatra main screen.

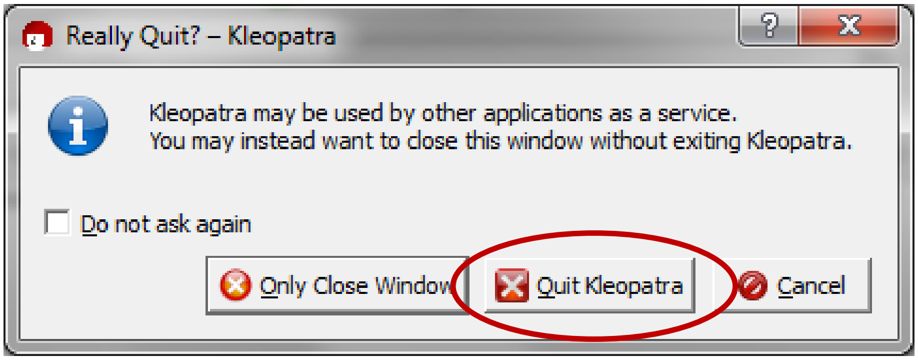


Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Anthony S...	scaturro@uhcl...	2016-02-11		OpenPGP	2F328213

18. To exit, click in the "Quit" entry in the "File" menu.


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
Redisplay
Stop Operation
Lookup Certificates on Server
Clipboard
My Certificates
rtificates
All Certificates
Valid Until
Details
Key-ID
OpenPGP
2F328213
Certificate To Directory Service...

19. Before the program closes, you will need to confirm that you want to close the program by clicking on the "Quit Kleopatra" button.


Really Quit? – Kleopatra

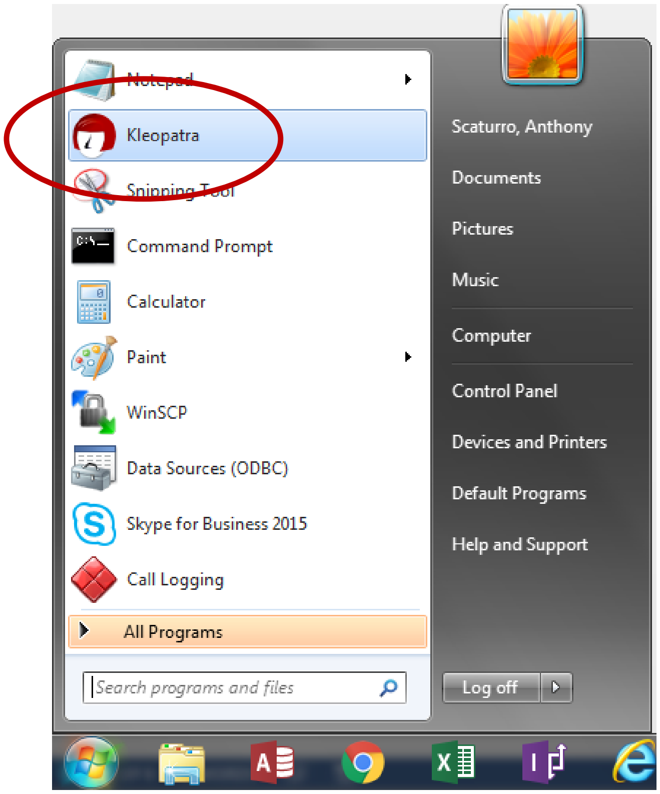
Kleopatra may be used by other applications as a service.
You may instead want to close this window without exiting Kleopatra.

☐ Do not ask again

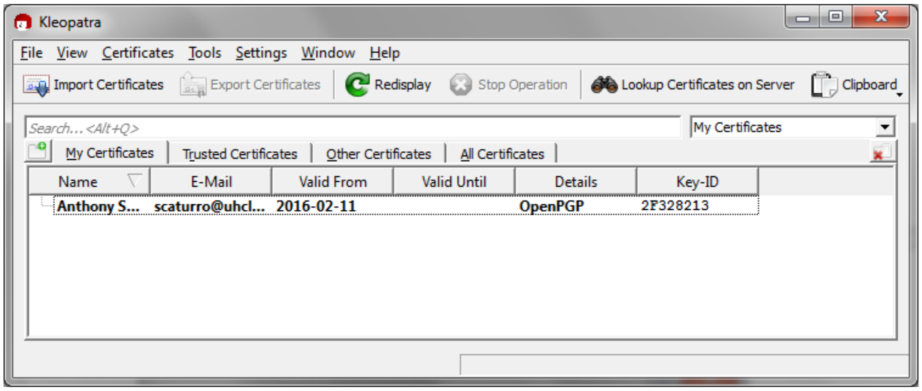
VI. Exporting your public key to another GPG user

To allow someone to send you encrypted files and messages, you must export your public key certificate that is stored in your GPG environment and send it to them using the following procedure. Any prospective sender to whom you send your public key certificate, must add your certificate into their key file or "key ring" following the procedure in the section entitled **VI. Importing another user's public key into your GPG key file**.

1. From your start bar, select the "Kleopatra" icon to start the Kleopatra certificate management software.

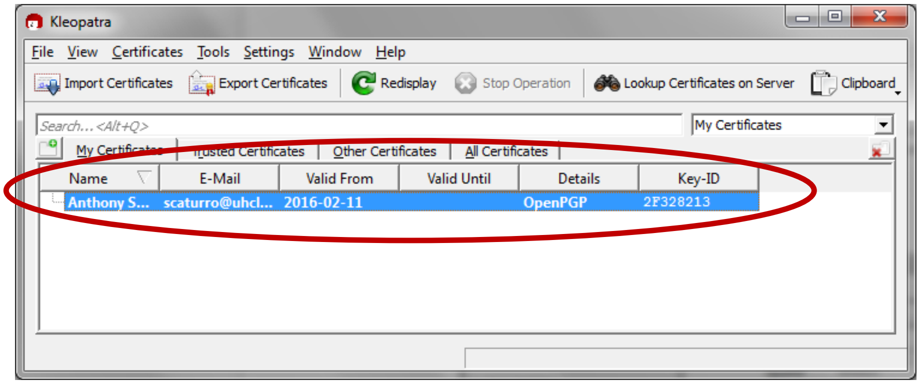


2. The following screen will be displayed with your key information.



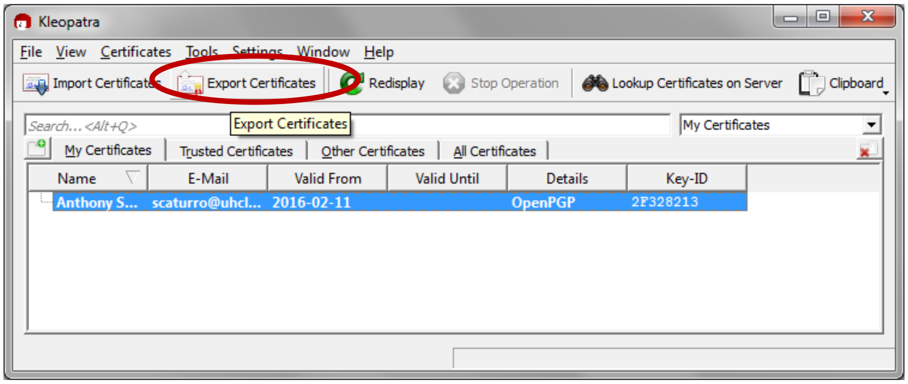
Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Anthony S...	scaturro@uhcl...	2016-02-11		OpenPGP	2F328213

3. Select the key that you wish to export.



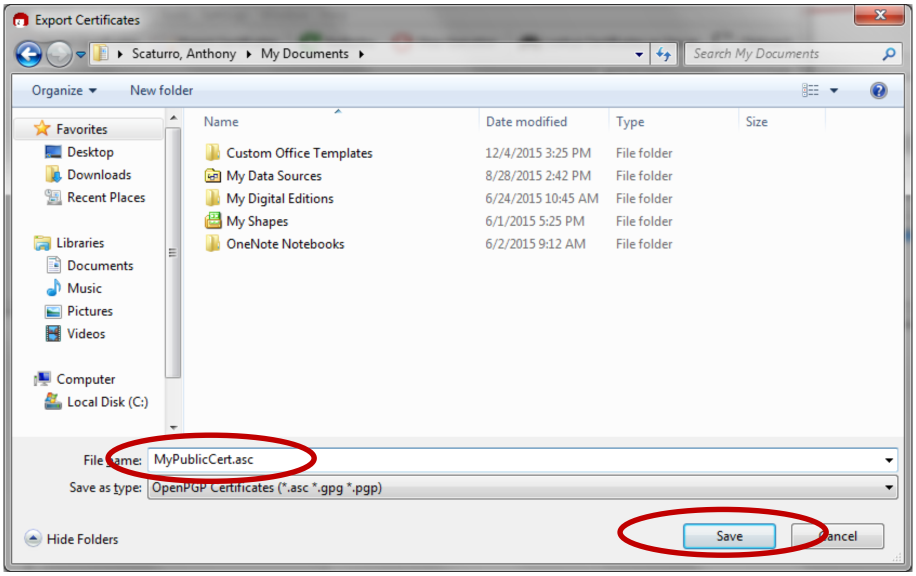
Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Anthony S...	scaturro@uhcl...	2016-02-11		OpenPGP	2F328213

4. Click the "Export Certificates" button.



Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Anthony S...	scaturro@uhcl...	2016-02-11		OpenPGP	2F328213

5. Browse to the folder into which the public key certificate will be exported, give the file a name, and click the "Save" button.

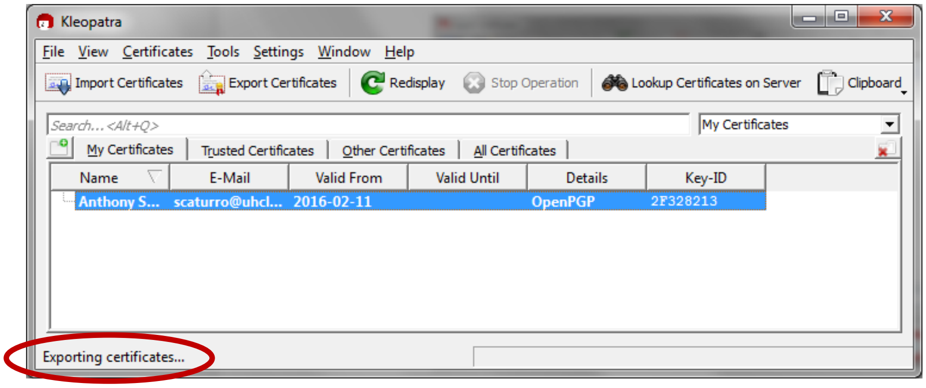


Name	Date modified	Type	Size
Custom Office Templates	12/4/2015 3:25 PM	File folder	
My Data Sources	8/28/2015 2:42 PM	File folder	
My Digital Editions	6/24/2015 10:45 AM	File folder	
My Shapes	6/1/2015 5:25 PM	File folder	
OneNote Notebooks	6/2/2015 9:12 AM	File folder	

File name: MyPublicCert.asc

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

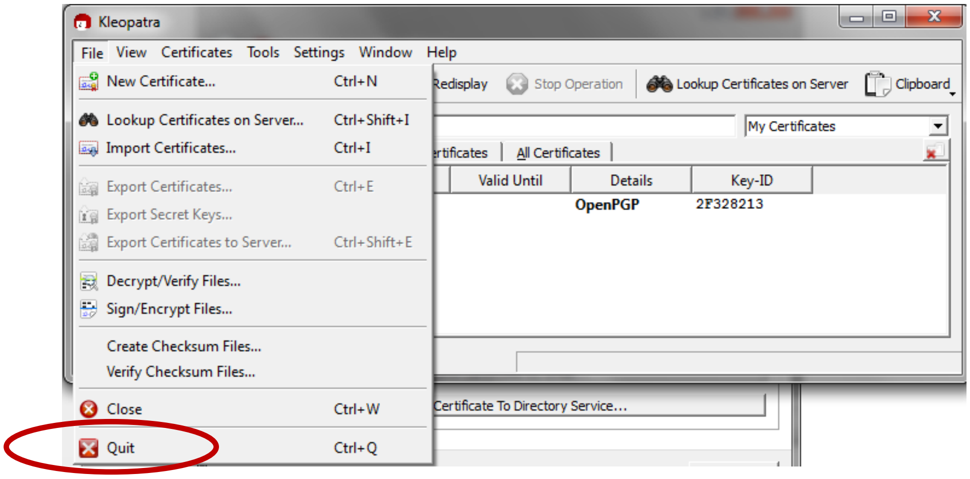
6. The status line on the bottom left of the window will display the status.



Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Anthony S...	scaturro@uhcl...	2016-02-11		OpenPGP	2F328213

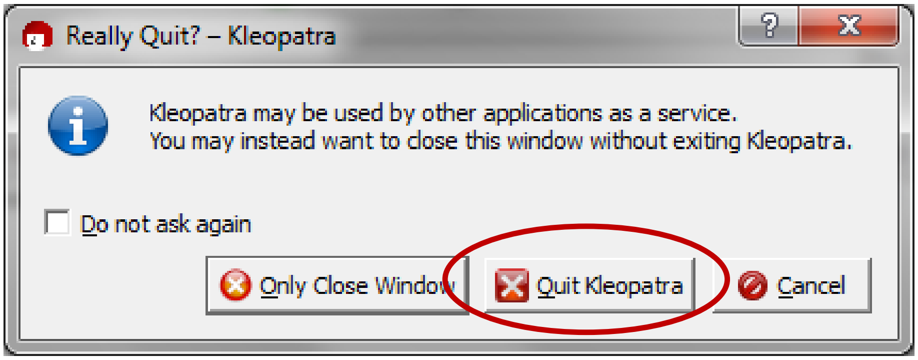
Exporting certificates...

7. To exit, click in the “Quit” entry in the “File” menu.


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
Redisplay
Stop Operation
Lookup Certificates on Server
Clipboard
My Certificates
rtificates
All Certificates
Certificate To Directory Service...

Valid Until	Details	Key-ID
	OpenPGP	2F328213

8. Before the program closes, you will need to confirm that you want to close the program by clicking on the “Quit Kleopatra” button.



Kleopatra may be used by other applications as a service.
You may instead want to close this window without exiting Kleopatra.

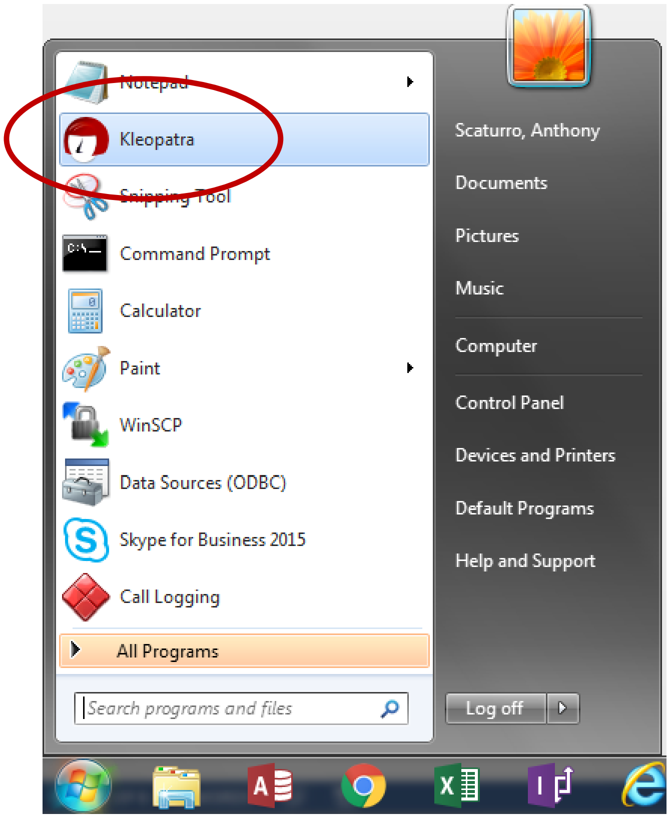
□ Do not ask again

9. The exported certificate may be sent via e-mail or can be copied onto a USB key and passed to whomever needs to send you encrypted files. In the case of the sender being a UHCL web site, the exported certificate should be sent to Kurt Lund at lund@uhcl.edu.

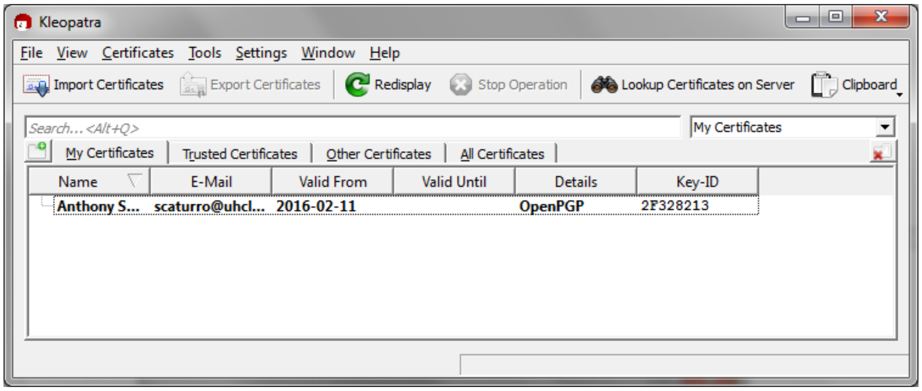
VII. Importing another user's public key into your GPG key file

If someone sends you their public key so that you can send that person an encrypted file or message, you must import their public key certificate into your GPG key file or "key ring". To import the certificate into your GPG environment, perform the following steps:

1. From your start bar, select the "Kleopatra" icon to start the Kleopatra certificate management software.

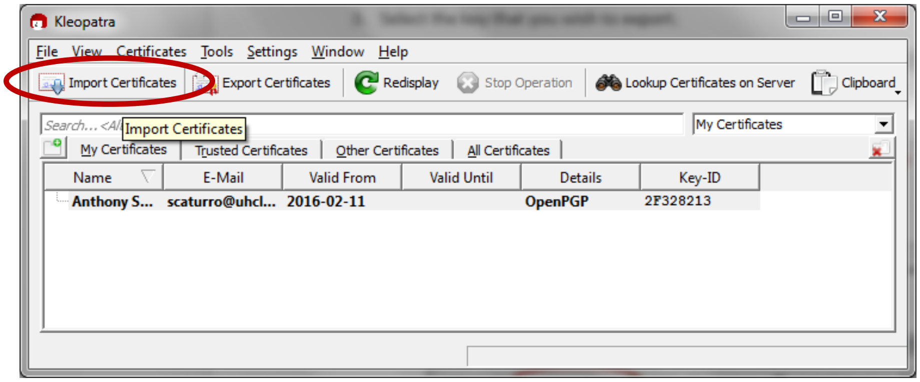


2. The following screen will be displayed with your key information.



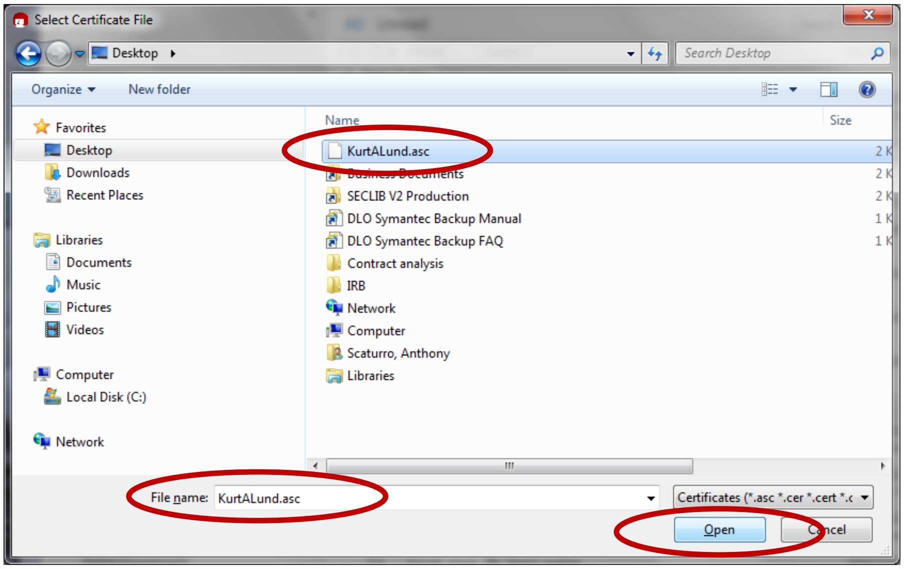
Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Anthony S...	scaturro@uhcl...	2016-02-11		OpenPGP	2F328213

3. Click the “Import Certificates” button.



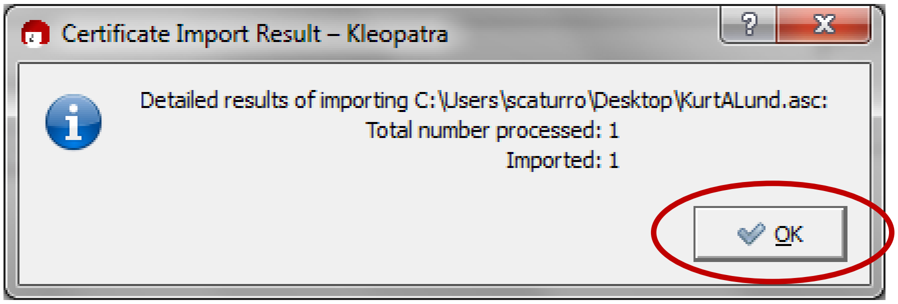
Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Anthony S...	scaturro@uhcl...	2016-02-11		OpenPGP	2F328213

4. Browse to the folder from where the public key certificate will be imported and click the “Open” button.



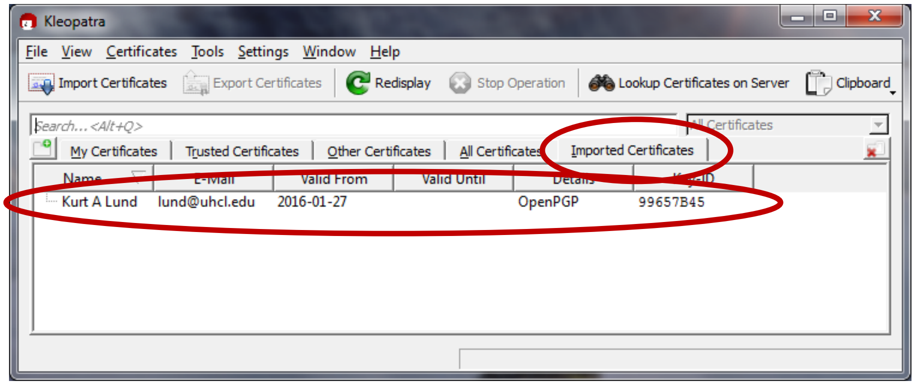
File name: KurtALund.asc

5. The following status window will be displayed indicating the certificate was imported.



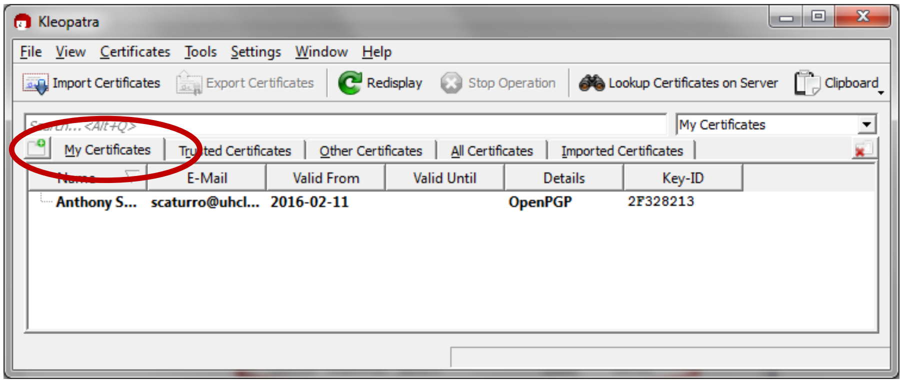
Detailed results of importing C:\Users\scaturro\Desktop\KurtALund.asc:
Total number processed: 1
Imported: 1

6. Click the "OK" button and the Kleopatra window will switch to the "Imported Certificates" tab, showing the newly imported certificate.



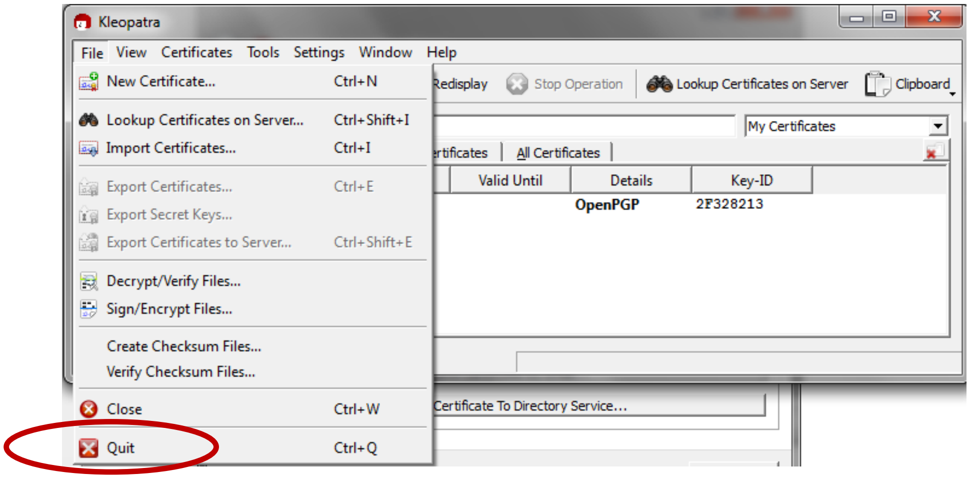
Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Kurt A Lund	lund@uhcl.edu	2016-01-27		OpenPGP	99657B45

7. Clicking the "My Certificates" tab will bring you back to the original tab.



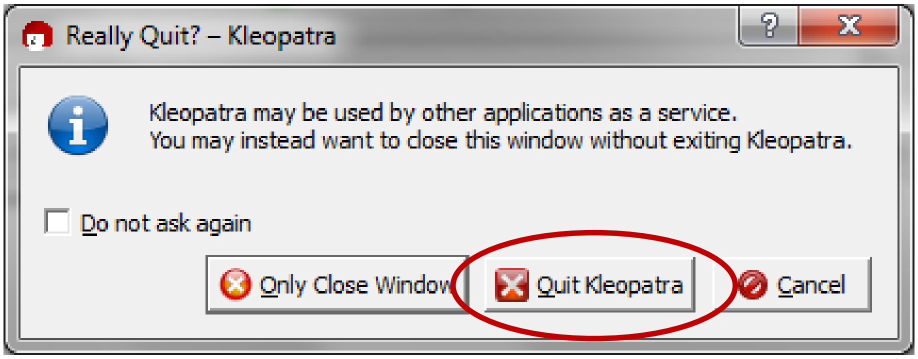
Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Anthony S...	scaturro@uhcl...	2016-02-11		OpenPGP	2F328213

8. To exit, click in the "Quit" entry in the "File" menu.


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
Redisplay
Stop Operation
Lookup Certificates on Server
Clipboard
My Certificates
rtificates
All Certificates
Certificate To Directory Service...

Valid Until	Details	Key-ID
	OpenPGP	2F328213

9. Before the program closes, you will need to confirm that you want to close the program by clicking on the "Quit Kleopatra" button.



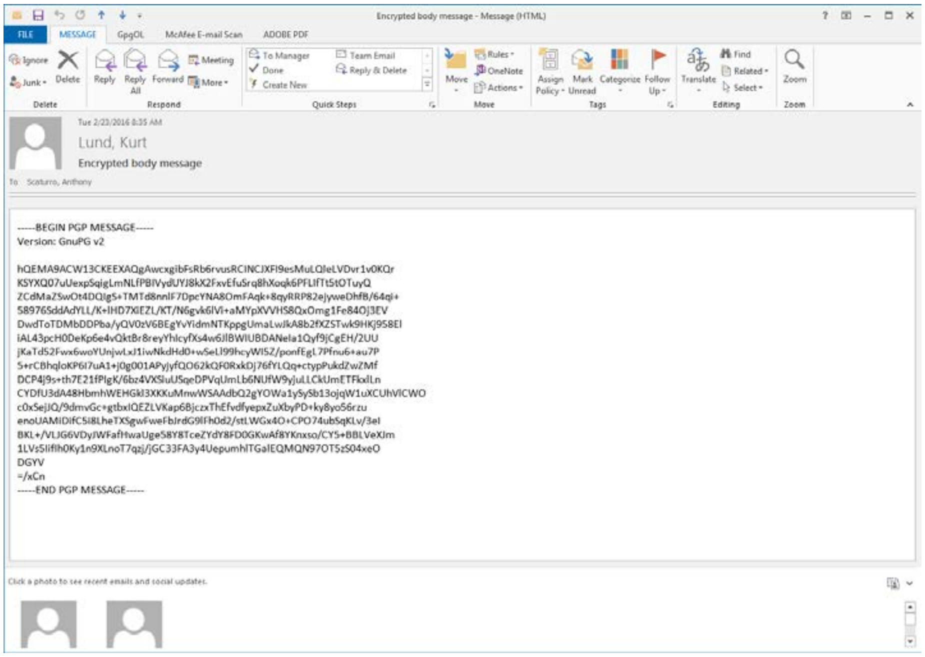
Really Quit? – Kleopatra

Kleopatra may be used by other applications as a service.
You may instead want to close this window without exiting Kleopatra.

□ Do not ask again

VIII. Decrypting an encrypted e-mail that has been sent to you

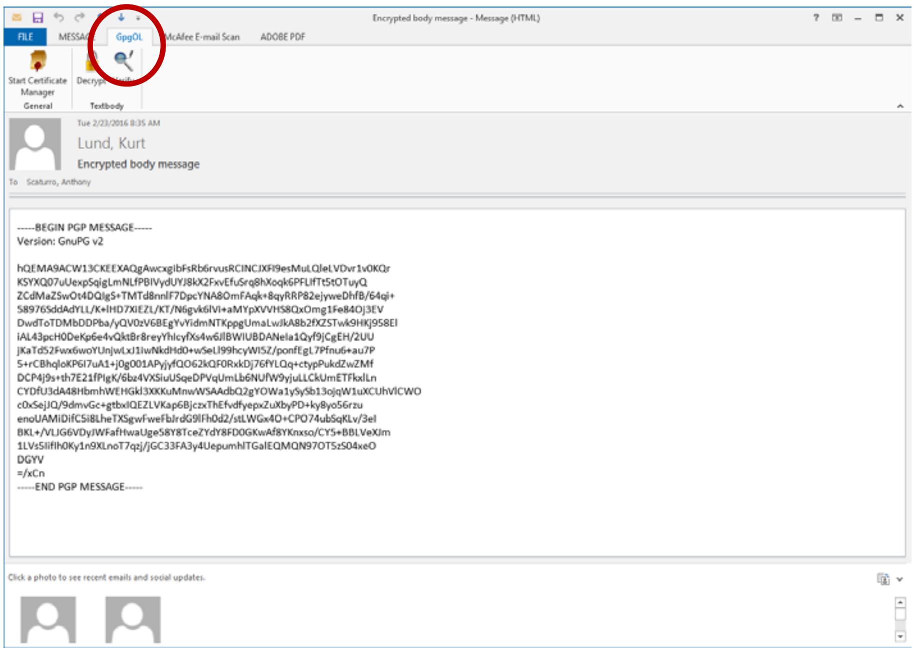
1. Open the e-mail message.



Tue 2/23/2016 8:35 AM
Lund, Kurt
Encrypted body message
To Scaturro, Anthony

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQEMA9ACW13CKEEXAQgAwcxgibFsRb6rvusRCINCJXFI9esMuLQleLVDvr1v0KQr
KSYXQ07uUexpSqigLmNLfPBIVydUYJ8kX2FxvEfuSrq8hXoqk6PFLIfTt5tOTuyQ
ZCdMaZSwOt4DQIg5+TMTd8nnlF7DpcYNA8OmFAqk+8qyRRP82ejyweDhfB/64qi+
58976SddAdYLL/K+lHD7XIEZL/KT/N6gvk6lVi+aMYpXVVHS8QxOmg1Fe84OJ3EV
DwdToTDMbDDPba/yQV0zV6BEgYvYidmNTKppgUmaLwJkA8b2fXZSTwk9HKj958El
iAL43pcH0DeKp6e4vQktBr8reyYhIcyfXs4w6JlBWIUBDANela1Qyf9jCgEH/2UU
jKaTd52Fwx6woYUnjwLxJ1iwNkdHd0+wSeLl99hcyWI5Z/ponfEgL7Pfnu6+au7P
5+rCBhqloKP6I7uA1+j0g001APyjyfQO62kQF0RxkDj76fYLQq+ctypPukdZwZMf
DCP4j9s+th7E21fPlgK/6bz4VXSluUSqeDPVqUmLb6NUfW9yjuLLCkUmETFkxlLn
CYDfU3dA48HbmhWEHGkl3XKKuMnwWSAAdbQ2gYOWa1ySySb13ojqW1uXCUhVlCWO
c0xSejJQ/9dmvGc+gtbxIQEZLVKap6BjczxThEfvdfyepxZuXbyPD+ky8yo56rzu
enoUAMiDIfC5i8LheTXSgwFweFbJrdG9lFh0d2/stLWGx4O+CPO74ubSqKLv/3eI
BKL+/VLJG6VDyJWFafHwaUge58Y8TceZYdY8FD0GKwAf8YKnxso/CY5+BBLVeXIm
1LVs5IiflhOKy1n9XLnoT7qzj/jGC33FA3y4UepumhlTGaIEQMQN97OT5zS04xeO
DGYV
=/xCn
-----END PGP MESSAGE-----
```

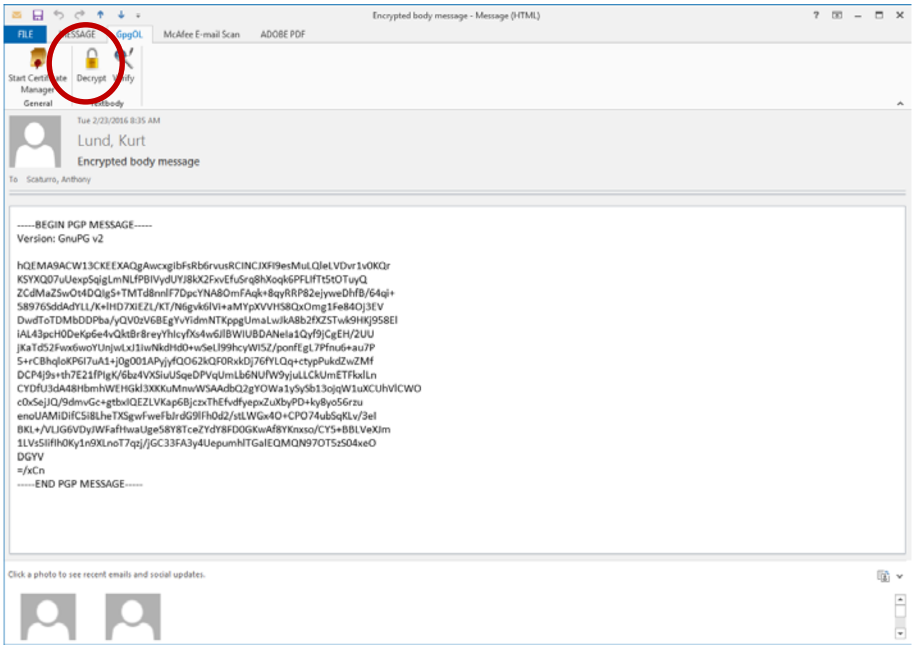
2. Select the GpgOL tab.


Encrypted body message - Message (HTML)
FILE
MESSAGE
GpgOL
McAfee E-mail Scan
ADOBE PDF
Start Certificate Manager
General
Decrypt
Textbody
Click a photo to see recent emails and social updates.

Tue 2/23/2016 8:35 AM
Lund, Kurt
Encrypted body message
To Scaturro, Anthony

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQEMA9ACW13CKEEXAQgAwcxgibFsRb6rvusRCINCJXFI9esMuLQleLVDvr1v0KQr
KSYXQ07uUexpSqigLmNLfPBIVydUYJ8kX2FxvEfuSrq8hXoqk6PFLIfTt5tOTuyQ
ZCdMaZSwOt4DQIg5+TMTd8nnlF7DpcYNA8OmFAqk+8qyRRP82ejyweDhfB/64qi+
58976SddAdYLL/K+lHD7XIEZL/KT/N6gvk6lVi+aMYpXVVHS8QxOmg1Fe84OJ3EV
DwdToTDMbDDPba/yQV0zV6BEgYvYidmNTKppgUmaLwJkA8b2fXZSTwk9HKj958El
iAL43pcH0DeKp6e4vQktBr8reyYhIcyfXs4w6JlBWIUBDANela1Qyf9jCgEH/2UU
jKaTd52Fwx6woYUnjwLxJ1iwNkdHd0+wSeLl99hcyWI5Z/ponfEgL7Pfnu6+au7P
5+rCBhqloKP6I7uA1+j0g001APyjyfQO62kQF0RxkDj76fYLQq+ctypPukdZwZMf
DCP4j9s+th7E21fPlgK/6bz4VXSluUSqeDPVqUmLb6NUfW9yjuLLCkUmETFkxlLn
CYDfU3dA48HbmhWEHGkl3XKKuMnwWSAAdbQ2gYOWa1ySySb13ojqW1uXCUhVlCWO
c0xSejJQ/9dmvGc+gtbxIQEZLVKap6BjczxThEfvdfyepxZuXbyPD+ky8yo56rzu
enoUAMiDIfC5i8LheTXSgwFweFbJrdG9lFh0d2/stLWGx4O+CPO74ubSqKLv/3eI
BKL+/VLJG6VDyJWFafHwaUge58Y8TceZYdY8FD0GKwAf8YKnxso/CY5+BBLVeXIm
1LVs5IiflhOKy1n9XLnoT7qzj/jGC33FA3y4UepumhlTGaIEQMQN97OT5zS04xeO
DGYV
=/xCn
-----END PGP MESSAGE-----
```

3. Click the "Decrypt" button.


FILE
MESSAGE
GpgOL
McAfee E-mail Scan
ADOBE PDF
Start Certificate Manager
General
Decrypt
Verify
Textbody
Click a photo to see recent emails and social updates.

Encrypted body message - Message (HTML)

Tue 2/23/2016 8:35 AM

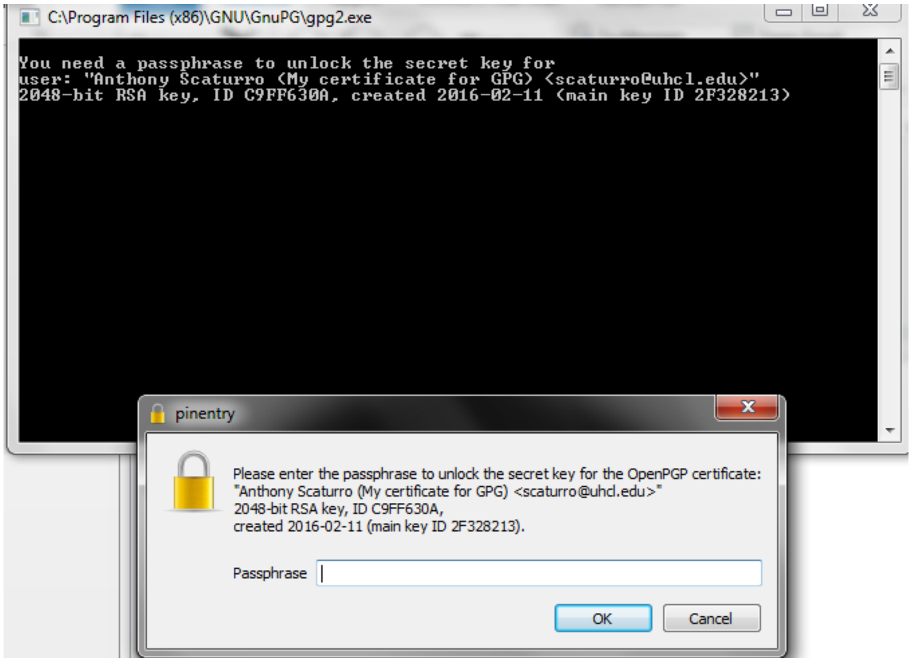
Lund, Kurt

Encrypted body message

To Scaturro, Anthony

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQEMA9ACW13CKEEXAQgAwcxglbFsRb6rvusRCINCJXFl9esMuLQleLVDvr1v0KQr
KSYXQ07uUexpSqigLmNLfPBIVydUYJ8kX2FxvEfuSrq8hXoqk6PFLIfTt5tOTuyQ
ZCdMaZ5wOt4DQIgS+TMTd8nnlF7DpcYNA8OmFAqk+8qyRRP82ejyweDhfB/64qi+
58976SddAdYLL/K+lHD7XIEZL/KT/N6gvk6lVi+aMYpXVVHS8QxOmg1Fe84Oj3EV
DwdToTDMbDDPba/yQV0zV6BEgYvYidmNTKppgUmaLwJkA8b2fXZ5Twk9HKj958EI
iAL43pcH0DeKp6e4vQktBr8reyYhlcyfXs4w6JlBWIUBDANela1Qyf9jCgEH/2UU
jKaTd52Fwx6woYUnjwLxJ1iwNkdHd0+wSeLl99hcyWI5Z/ponfEgL7Pfnu6+au7P
5+rCBhqloKP6I7uA1+j0g001APyjyfQO62kQF0RxkDj76fYLQq+ctypPukdZwZMf
DCP4j9s+th7E21fPlgK/6bz4VXSiuUSqeDPVqUmLb6NUfW9yjuLLCkUmETFkxlLn
CYDfU3dA48HbmhWEHGkl3XKKuMnwWSAAdbQ2gYOWa1ySySb13ojqW1uXCUhVlCWO
c0xSejJQ/9dmvGc+gtbxIQEZLVKap6BjczxThEfvdfyepxZuXbyPD+ky8yo56rzu
enoUAMiDifC5i8LheTXSgwFweFbJrdG9lFh0d2/stLWGx4O+CPO74ubSqKLv/3eI
BKL+/VLJG6VDyJWFafHwaUge58Y8TceZYdY8FD0GKwAf8YKnxso/CY5+BBLVeXJm
1LVs5IiflhOKy1n9XLnoT7qzj/jGC33FA3y4UepumhlTGaIEQMQN97OT5zS04xeO
DGYV
=/xCn
-----END PGP MESSAGE-----
```

4. A command window will open along with a window that asks for the Passphrase to your private key that will be used to decrypt the incoming message.



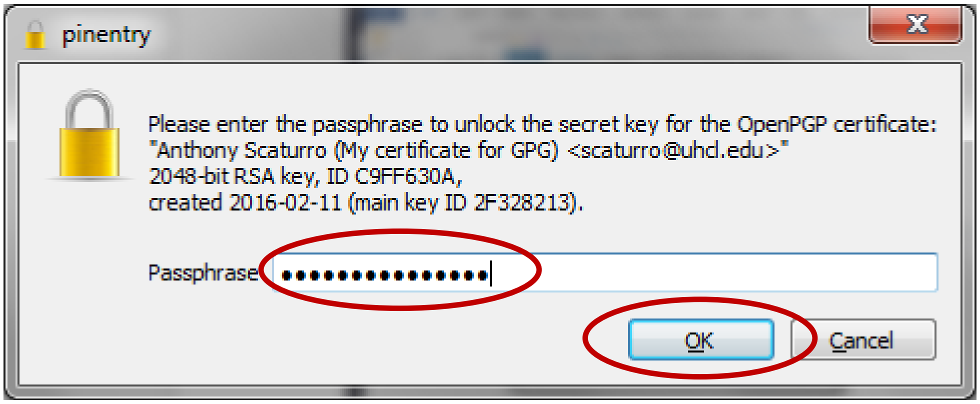
C:\Program Files (x86)\GNU\GnuPG\gpg2.exe

```
You need a passphrase to unlock the secret key for
user: "Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu>"
2048-bit RSA key, ID C9FF630A, created 2016-02-11 (main key ID 2F328213)
```

Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu>"
2048-bit RSA key, ID C9FF630A,
created 2016-02-11 (main key ID 2F328213).

Passphrase

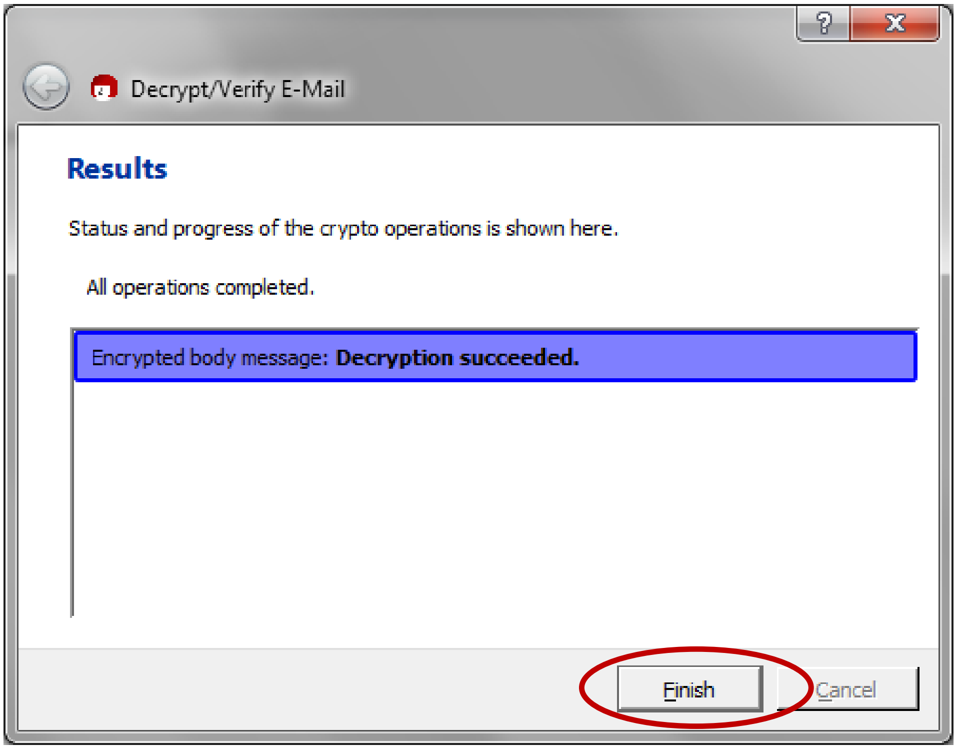
5. Enter your passphrase and click the "OK" button.



Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu>"
2048-bit RSA key, ID C9FF630A,
created 2016-02-11 (main key ID 2F328213).

Passphrase ●●●●●●●●●●●●●●●

6. The results window will tell you if the decryption succeeded. Click the "Finish" button top close the window.



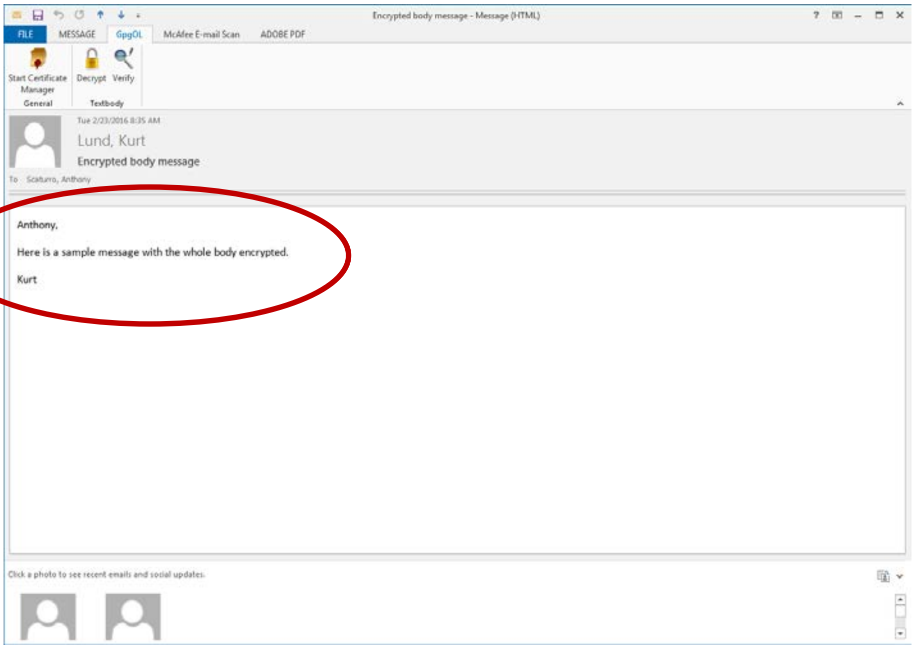
Results

Status and progress of the crypto operations is shown here.

All operations completed.

Encrypted body message: **Decryption succeeded.**

7. Your unencrypted e-mail message body will be displayed.



Tue 2/23/2016 8:35 AM

Lund, Kurt

Encrypted body message

To Scaturro, Anthony

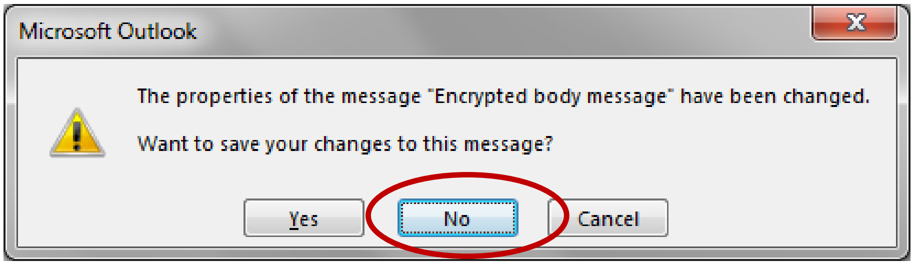
Anthony,

Here is a sample message with the whole body encrypted.

Kurt

Click a photo to see recent emails and social updates.

8. When you close the e-mail you will be asked if you want to save the e-mail message in its unencrypted form. For maximum security, click the "No" button. This will keep the message encrypted within the e-mail system and will require you to enter your passphrase each time you reopen the e-mail message.

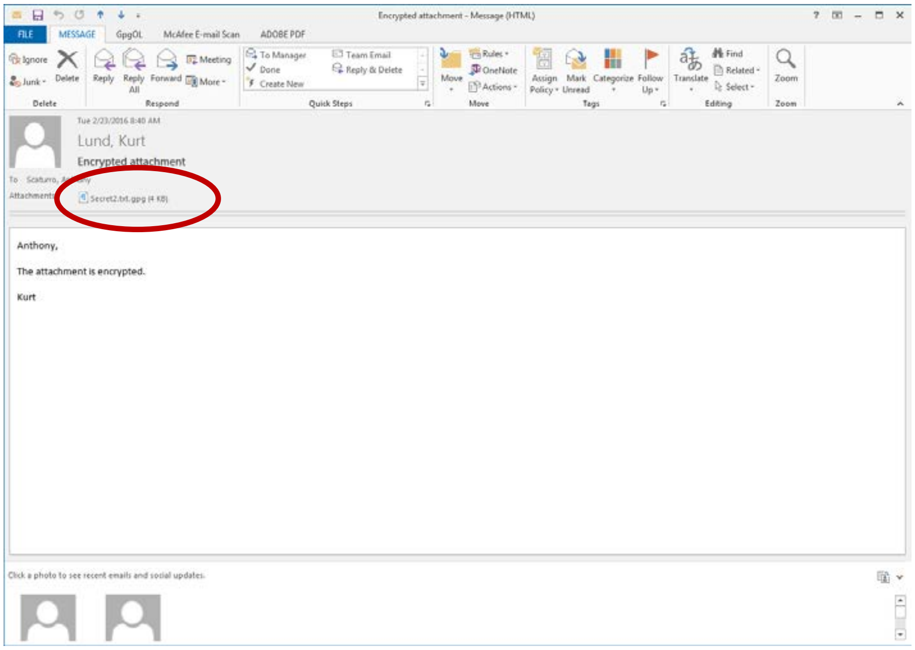


The properties of the message "Encrypted body message" have been changed.

Want to save your changes to this message?

IX. Decrypting an encrypted e-mail attachment

1. Open the e-mail message and double click the attachment.



Tue 2/23/2016 8:40 AM
Lund, Kurt
Encrypted attachment
To Scaturro, Anthony
Attachments Secret2.txt.gpg (4 KB)

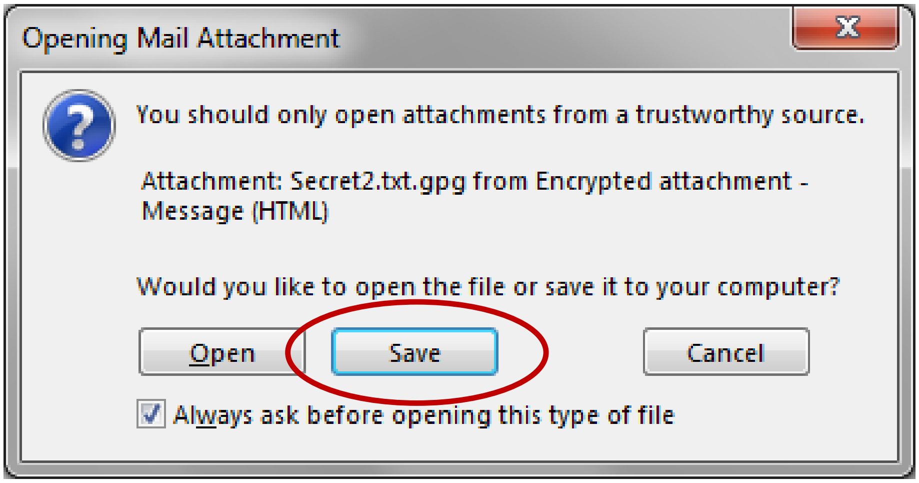
Anthony,

The attachment is encrypted.

Kurt

Click a photo to see recent emails and social updates.

2. You will be asked whether you want to open or save the attachment. Click the "Save" button to store the encrypted file.



Opening Mail Attachment

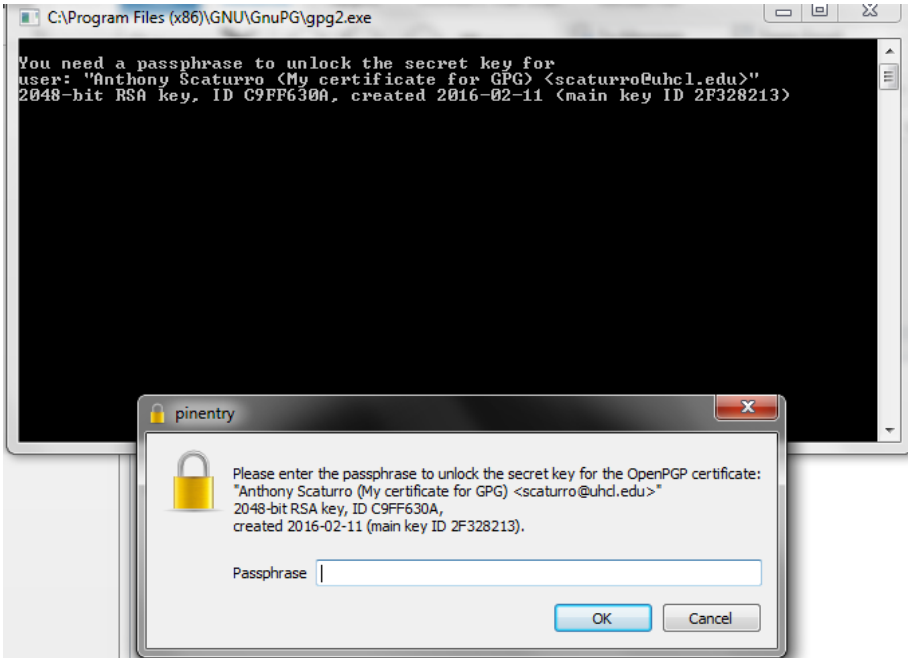
You should only open attachments from a trustworthy source.

Attachment: Secret2.txt.gpg from Encrypted attachment - Message (HTML)

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

3. A command window will open along with a window prompting you for your passphrase.

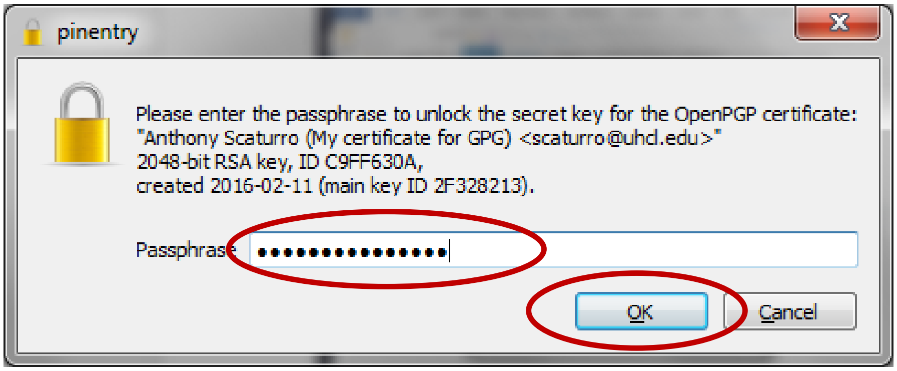


```
You need a passphrase to unlock the secret key for
user: "Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu>"
2048-bit RSA key, ID C9FF630A, created 2016-02-11 (main key ID 2F328213)
```

Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu>"
2048-bit RSA key, ID C9FF630A,
created 2016-02-11 (main key ID 2F328213).

Passphrase

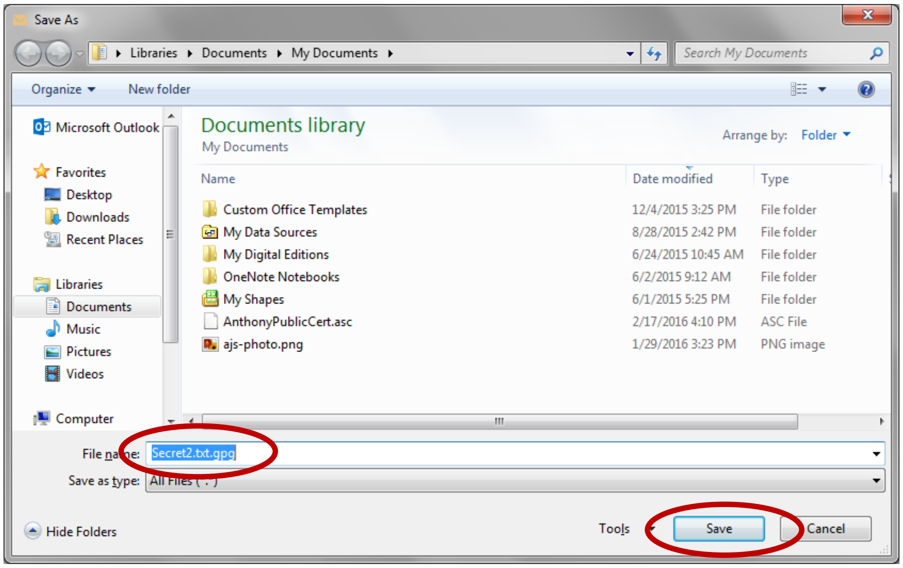
4. Enter your passphrase and click the “OK” button.



Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu>"
2048-bit RSA key, ID C9FF630A,
created 2016-02-11 (main key ID 2F328213).

Passphrase ●●●●●●●●●●●●●●●

5. Select the appropriate folder and enter the name that you want the file stored as. Then, click the "Save" button.

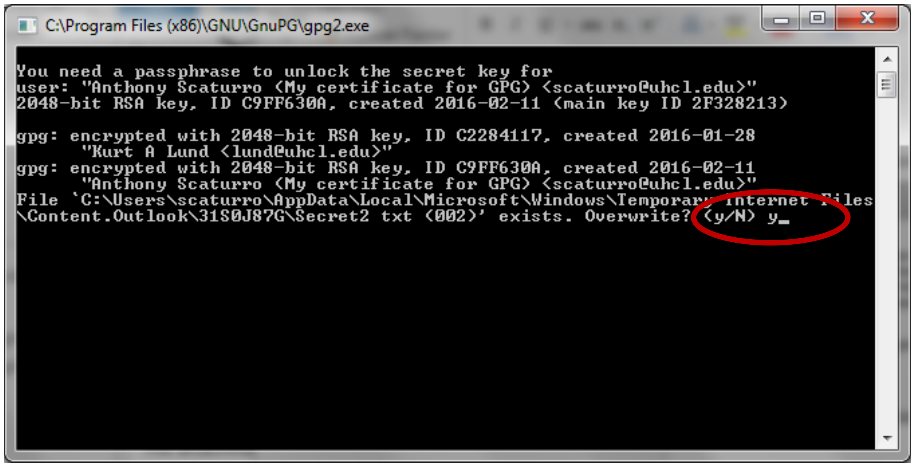


Name	Date modified	Type
Custom Office Templates	12/4/2015 3:25 PM	File folder
My Data Sources	8/28/2015 2:42 PM	File folder
My Digital Editions	6/24/2015 10:45 AM	File folder
OneNote Notebooks	6/2/2015 9:12 AM	File folder
My Shapes	6/1/2015 5:25 PM	File folder
AnthonyPublicCert.asc	2/17/2016 4:10 PM	ASC File
ajs-photo.png	1/29/2016 3:23 PM	PNG image

File name: Secret2.txt.gpg

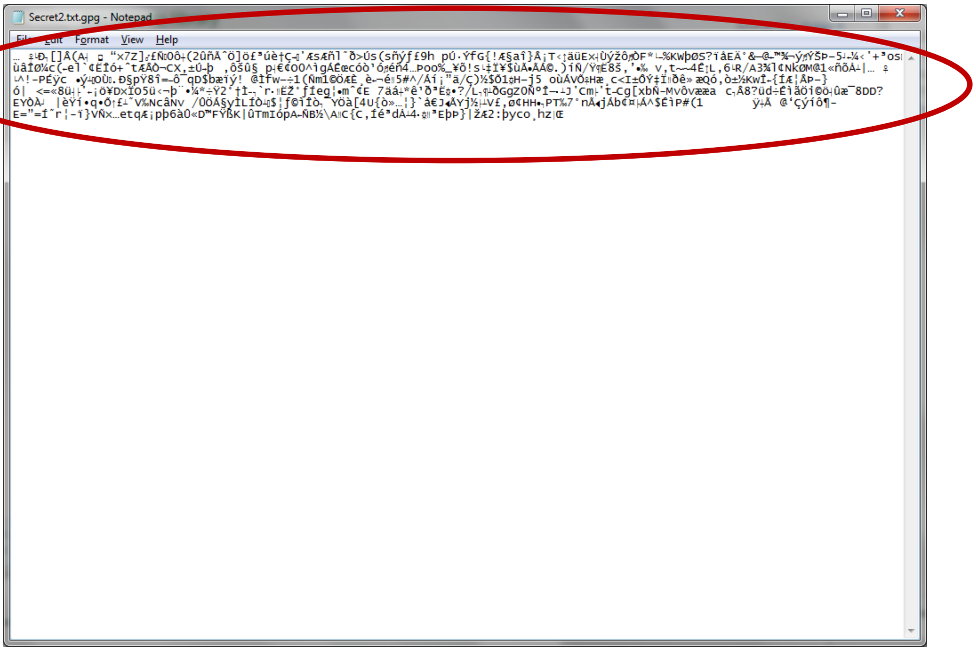
Save as type: All Files (*.*)

6. If the file name already exists in the folder you have selected, enter a "y" into the command window to replace the old file.



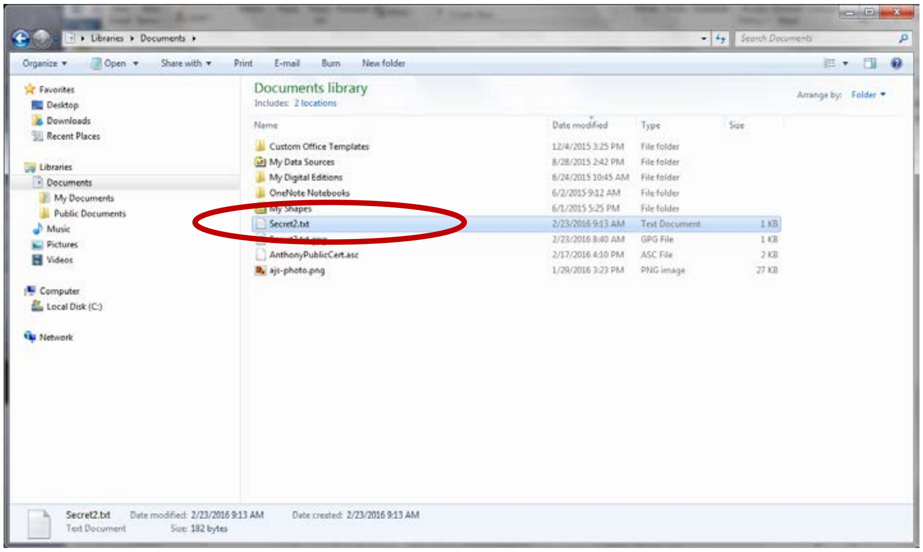
```
You need a passphrase to unlock the secret key for
user: "Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu>"
2048-bit RSA key, ID C9FF630A, created 2016-02-11 (main key ID 2F328213)

gpg: encrypted with 2048-bit RSA key, ID C2284117, created 2016-01-28
      "Kurt A Lund <lund@uhcl.edu>"
gpg: encrypted with 2048-bit RSA key, ID C9FF630A, created 2016-02-11
      "Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu>"
File `C:\Users\scaturro\AppData\Local\Microsoft\Windows\Temporary Internet Files
\Content.Outlook\31S0J87G\Secret2 txt (002)' exists. Overwrite? (y/N) y_
```

7. The file should be unreadable.



```
… ♀└Ð┐[]Å(A┤ ◘ “x7Z]╒£Ñ▯0ô┼(2ûñÄˆö]öf³úè†Ç┤▯'ÆsÆñl˜ð>Ús(sñýƒ£9h pÚ·ÝfG{!Æ§aî}Å¡T‹↨äüEx┤ÙýžôÐF*└–%KWþØS?ïåEÄ˚&—@┘™¾¬ý╔ÝŠÞ–5┘┘¼‹'+³os
ùâÎØ¼c(←el`¢ËÎó+ˆtÆÅÒ¬CX,±Ú┘þ ,ôšû§ p┤€¢oO^ìgÁÊœcóò'ó╔éñ4…Þoo%_¥õ!s└‡Ï¥$ùÅ•ÅÁ©.)íÑ/Ÿ¶Ë8š,'•‰ v,t~~4Ê↨L,6└R/A3¾l¢NkØM@1«ñÕÅ┘|… ♀
└^!–PÉÿc •ý┘▯OÙ▯.Ð§pŸ8î=–ô¯qD$bæïý! @Îfw–÷1(Ñm1©ÖÆÈ¸è←¬é‼5#^/Áí¡"ä/Ç)½$Õ1☼H–j5 oùÁVÕ♀Hæ¸c<I±ÔÝ‡Ï‼ðê» æQó,ò±½KwÎ←{ÍÆ¦ÂÞ–}
ó|  <=«8ü┤├'←¡ö¥DxÏO5ü‹¬þ¨•¼*÷Ÿ2˚†Î–┐`r·‼ËŽ˚ƒÍeg¦•mˆ¢E 7äá┼*ê'ð³Ë☼•?/L┐¶┘ðGgZ0Ñ°Î–→┘J'Cm├'t–Cg[xbÑ–Mvôvææa c┐Å8?üd÷Êìãöï©ö┤ûæ¯8DD?
EYÒÀ┘ |èŸí•q•Õ↑£┴˜V‰NcâNv /ÛÖÁ§yÌLÍÒ┘▯$¦ƒ©ìÎò┐¯YÖà[4U{ò»…¦}`â€J◄ÅYj½┤┴V£,ø¢HH•┐PT%7˚nÅ◄jÁb¢¤┤Á^$ÊìP#(1       ÿ┼Ä @'Çýíô¶–
E="=Í˜r¦–ï}VÑx…etqÆ¡pþ6à0«D™FŸßK|ûTmIópA←ÑB½\A‼C{C,Íé³dÅ┴4·☼‼³EþP}|žÆ2:þyco¸hz‼Œ
```

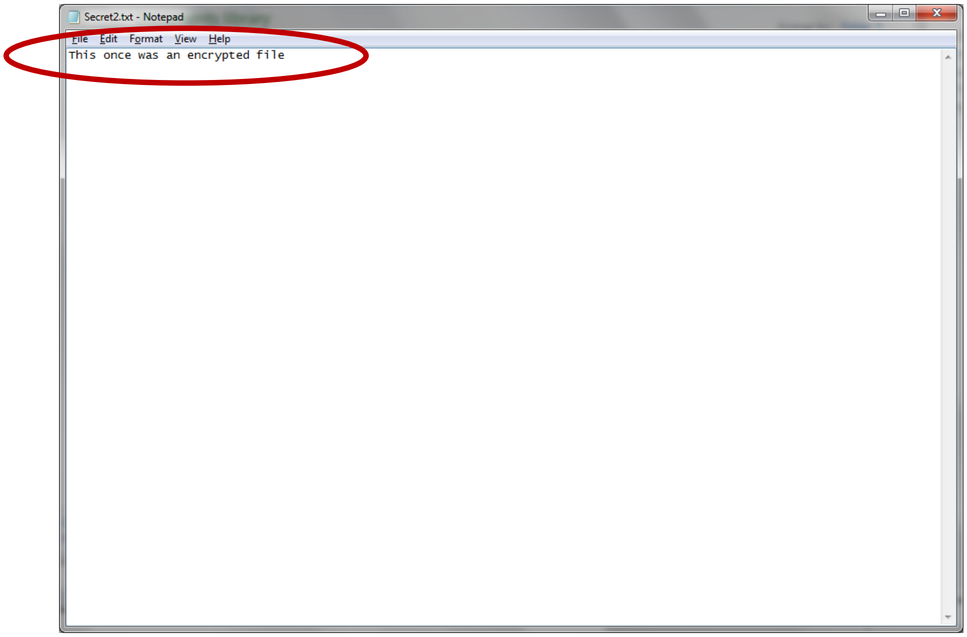
8. Open Windows Explorer and click the decrypted file to open it.



Name	Date modified	Type	Size
Custom Office Templates	12/4/2015 3:25 PM	File folder	
My Data Sources	8/28/2015 2:42 PM	File folder	
My Digital Editions	6/24/2015 10:45 AM	File folder	
OneNote Notebooks	6/2/2015 9:12 AM	File folder	
My Shapes	6/1/2015 5:25 PM	File folder	
Secret2.txt	2/23/2016 9:13 AM	Text Document	1 KB
Secret2.txt.gpg	2/23/2016 8:40 AM	GPG File	1 KB
AnthonyPublicCert.asc	2/17/2016 4:10 PM	ASC File	2 KB
ajs-photo.png	1/29/2016 3:23 PM	PNG image	27 KB

Secret2.txt Date modified: 2/23/2016 9:13 AM Date created: 2/23/2016 9:13 AM
Text Document Size: 182 bytes

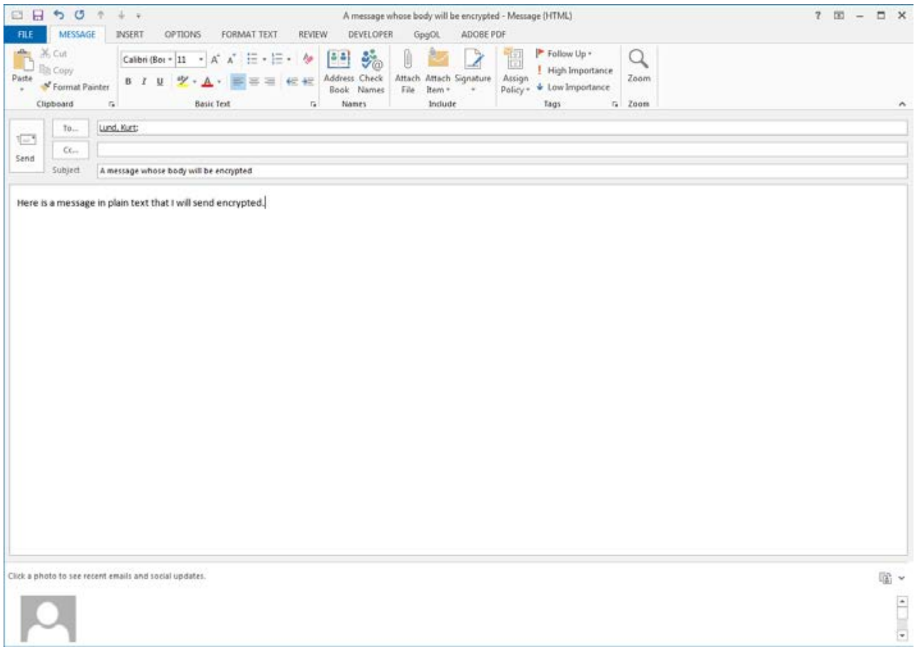
9. The file should be readable.



This once was an encrypted file

X. Sending an e-mail message with an encrypted body

1. Type the message body as you usually do.



A message whose body will be encrypted - Message (HTML)

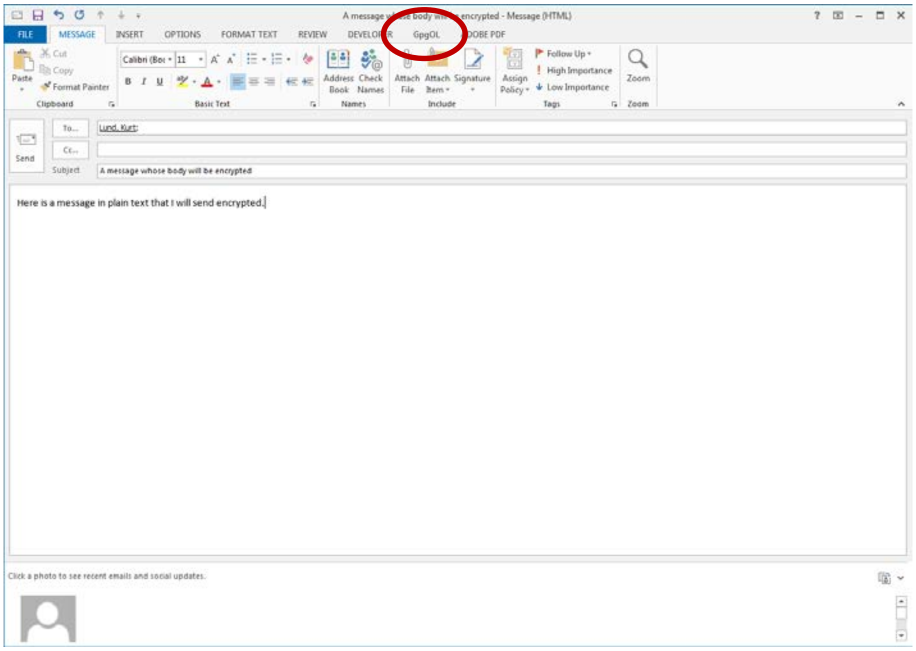
To... Lund, Kurt;

Subject: A message whose body will be encrypted

Here is a message in plain text that I will send encrypted.

Click a photo to see recent emails and social updates.

2. Select the GpgOL tab.



A message whose body will be encrypted - Message (HTML)

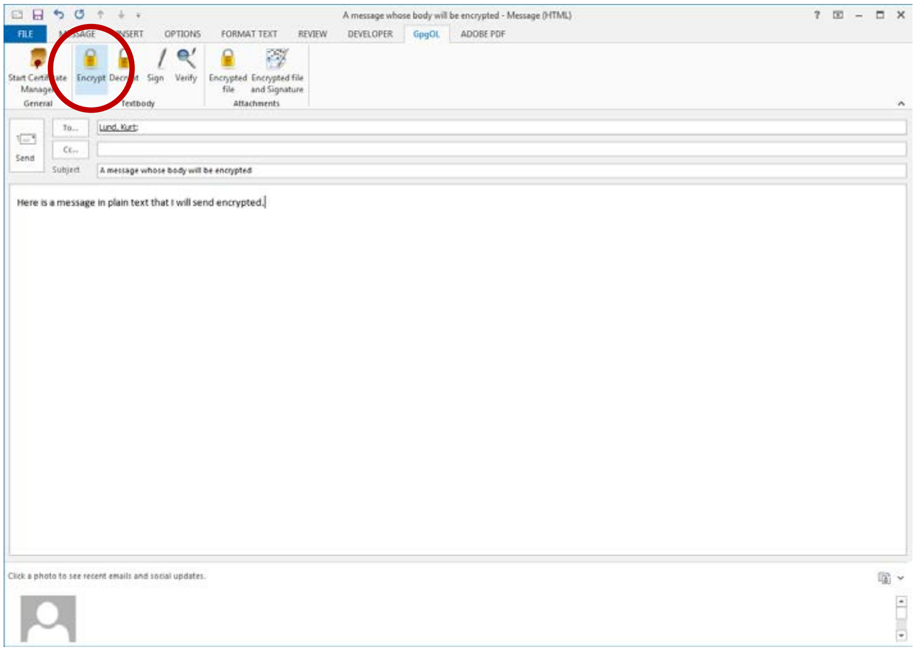
To... Lund, Kurt;

Subject: A message whose body will be encrypted

Here is a message in plain text that I will send encrypted.

Click a photo to see recent emails and social updates.

3. Click the “Encrypt” button.

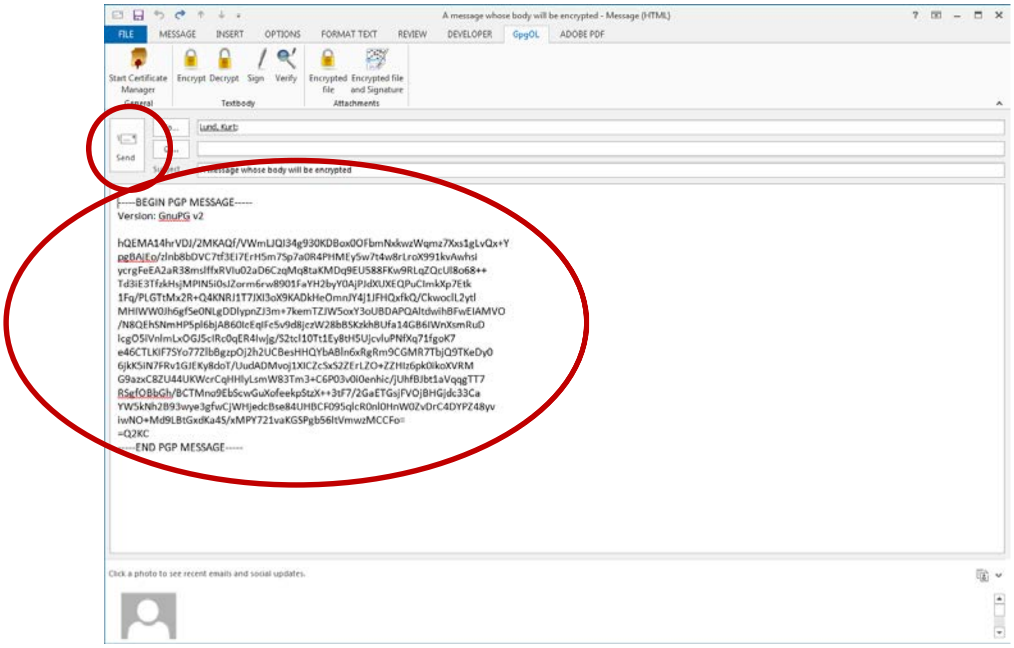

A message whose body will be encrypted - Message (HTML)
FILE
MESSAGE
INSERT
OPTIONS
FORMAT TEXT
REVIEW
DEVELOPER
GpgOL
ADOBE PDF
Start Certificate Manager
General
Encrypt
Decrypt
Sign
Verify
Textbody
Encrypted file
Encrypted file and Signature
Attachments
Send
To...
Cc...
Subject
Click a photo to see recent emails and social updates.

To... Lund, Kurt;

Subject: A message whose body will be encrypted

Here is a message in plain text that I will send encrypted.

4. The message text will be encrypted and become unreadable. Click the normal "Send" button to send the message to the intended recipients.


A message whose body will be encrypted - Message (HTML)
FILE
MESSAGE
INSERT
OPTIONS
FORMAT TEXT
REVIEW
DEVELOPER
GpgOL
ADOBE PDF
Start Certificate Manager
General
Encrypt
Decrypt
Sign
Verify
Textbody
Encrypted file
Encrypted file and Signature
Attachments
Send
Click a photo to see recent emails and social updates.

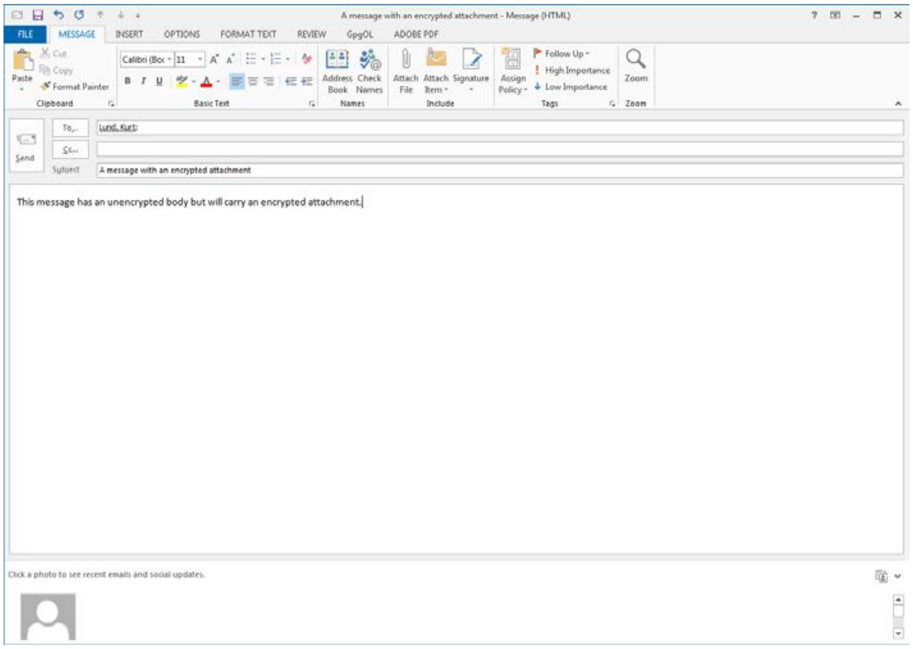
To... Lund, Kurt;

Subject: A message whose body will be encrypted

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQEMA14hrVDJ/2MKAQf/VWmLJQI34g930KDBox0OFbmNxkwzWqmz7Xxs1gLvQx+Y
pgBAjEo/zlnb8bDVC7tf3Ei7ErH5m7Sp7a0R4PHMEy5w7t4w8rLroX991kvAwhsl
ycrgFeEA2aR38mslffxRVlu02aD6CzqMq8taKMDq9EU588FKw9RLqZQcUl8o68++
Td3iE3TfzkHsjMPIN5i0sJZorm6rw8901FaYH2byY0AjPJdXUXEQPuClmkXp7Etk
1Fq/PLGTtMx2R+Q4KNRJ1T7JXl3oX9KADkHeOmnJY4J1JFHQxfkQ/CkwoclL2ytl
MHIWW0Jh6gf5e0NLgDDlypnZJ3m+7kemTZJW5oxY3oUBDAPQAltdwihBFwEIAMVO
/N8QEh5NmHP5pl6bJAB60lcEqlFc5v9d8jczW28bBSKzkhBUfa14GB6IWnXsmRuD
lcgO5lVnlmLxOGJ5clRc0qER4lwjg/S2tcl10Tt1Ey8tH5UjcvluPNfXq71fgoK7
e46CTLKlF7SYo77Zlb8gzpOj2h2UCBesHHQYbABln6xRgRm9CGMR7TbjQ9TKeDy0
6jkK5iN7FRv1GJEKy8doT/UudADMvoj1XICZc5x52ZErLZO+ZZHlz6pk0ikoXVRM
G9azxC8ZU44UKWcrCqHHlyLsmW83Tm3+C6P03v0i0enhic/jUhfBJbt1aVqqgTT7
RSgfOBbGh/BCTMno9EbScwGuXofeekpStzX++3tF7/2GaETGsjFVOjBHGjdc33Ca
YW5kNh2B93wye3gfwCJWHjedcBse84UHBCF095qlcR0nl0HnW0ZvDrC4DYPZ48yv
iwNO+Md9LBtGxdKa4S/xMPY721vaKGSPgb56ltVmwzMCCFo=
=Q2KC
-----END PGP MESSAGE-----
```

XI. Sending an e-mail message with an encrypted attachment

1. Type the message body as you usually do but do not add the attachment yet.



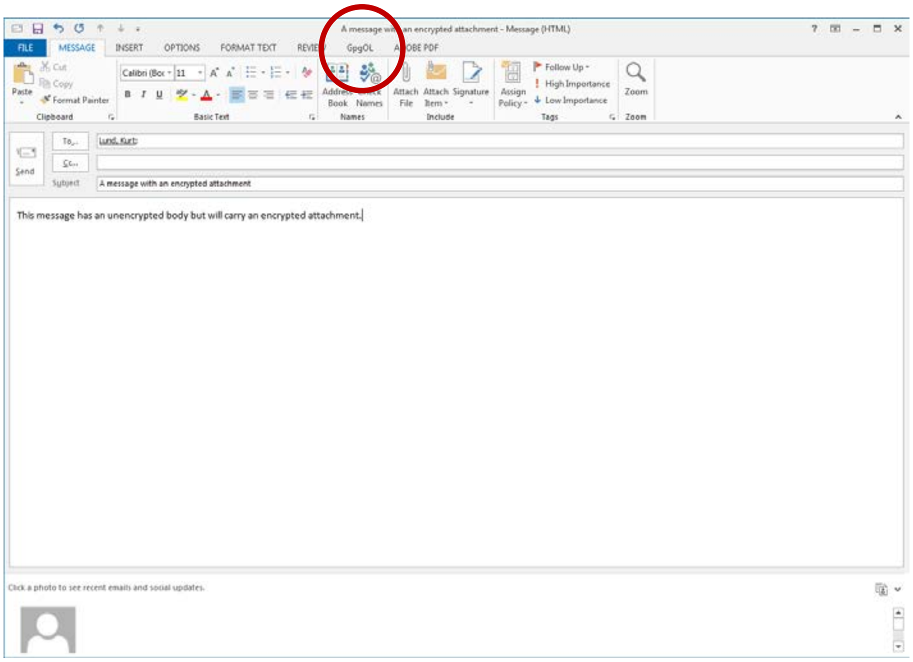
A message with an encrypted attachment - Message (HTML)

To... Lund, Kurt;

Subject: A message with an encrypted attachment

This message has an unencrypted body but will carry an encrypted attachment.

2. Select the GpgOL tab.



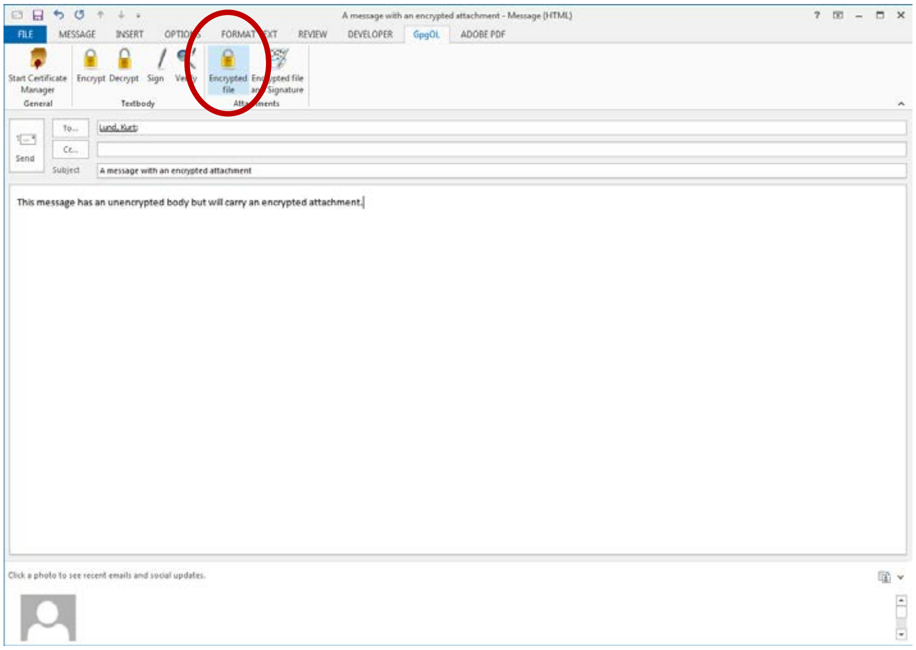
A message with an encrypted attachment - Message (HTML)

To... Lund, Kurt;

Subject: A message with an encrypted attachment

This message has an unencrypted body but will carry an encrypted attachment.

3. Click the “Encrypted File” button.

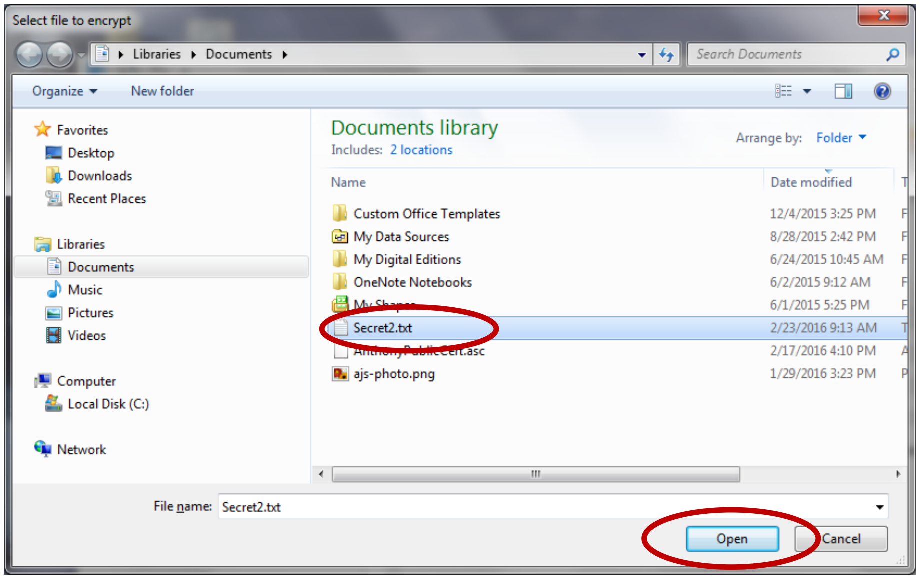

A message with an encrypted attachment - Message (HTML)
FILE
MESSAGE
INSERT
OPTIONS
FORMAT TEXT
REVIEW
DEVELOPER
GpgOL
ADOBE PDF
Start Certificate Manager
General
Encrypt
Decrypt
Sign
Verify
Textbody
Encrypted file
Encrypted file and Signature
Attachments
Send
To...
Cc...
Click a photo to see recent emails and social updates.

To...: Lund, Kurt;

Subject: A message with an encrypted attachment

This message has an unencrypted body but will carry an encrypted attachment.

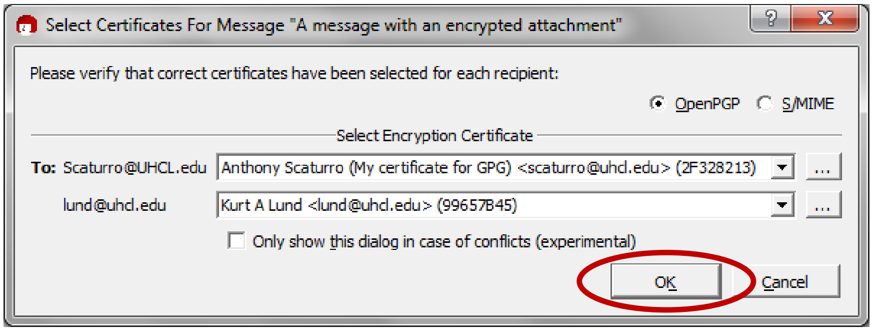
4. A file selection box will be presented. Navigate to and select the file to be encrypted.



Name	Date modified
Custom Office Templates	12/4/2015 3:25 PM
My Data Sources	8/28/2015 2:42 PM
My Digital Editions	6/24/2015 10:45 AM
OneNote Notebooks	6/2/2015 9:12 AM
My Shapes	6/1/2015 5:25 PM
Secret2.txt	2/23/2016 9:13 AM
AnthonyPublicCert.asc	2/17/2016 4:10 PM
ajs-photo.png	1/29/2016 3:23 PM

File name: Secret2.txt

5. A window will pop up asking you to verify the certificates that will be used. Click the "OK" button to confirm.



Select Certificates For Message "A message with an encrypted attachment"

Please verify that correct certificates have been selected for each recipient:

● OpenPGP ○ S/MIME

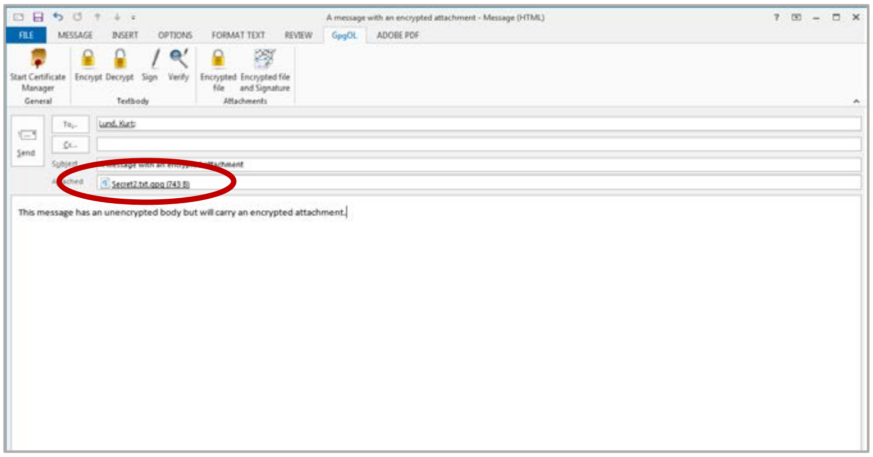
Select Encryption Certificate

To: Scaturro@UHCL.edu — Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu> (2F328213)

lund@uhcl.edu — Kurt A Lund <lund@uhcl.edu> (99657B45)

□ Only show this dialog in case of conflicts (experimental)

6. The file with an extra extension of .gpg will be added to the e-mail message.



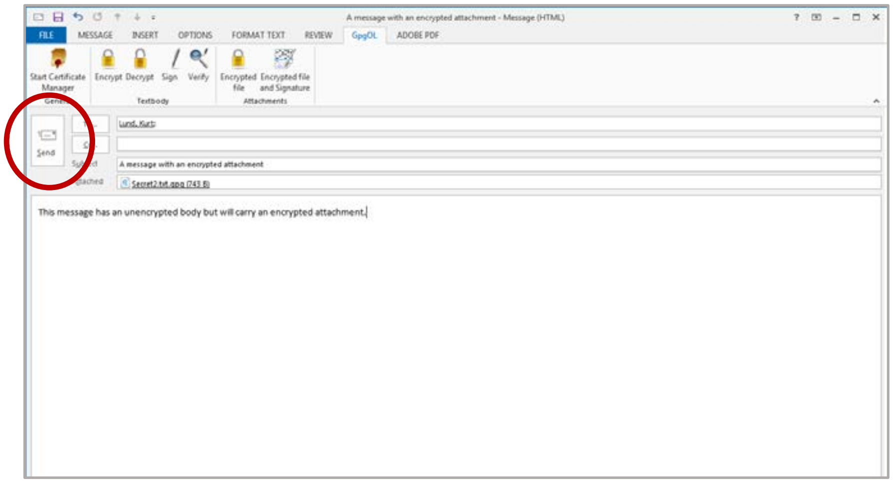
A message with an encrypted attachment - Message (HTML)

To... Lund, Kurt;

Attached: Secret2.txt.gpg (743 B)

This message has an unencrypted body but will carry an encrypted attachment.

7. Click the "Send" button to send the message.



A message with an encrypted attachment - Message (HTML)

To... Lund, Kurt;

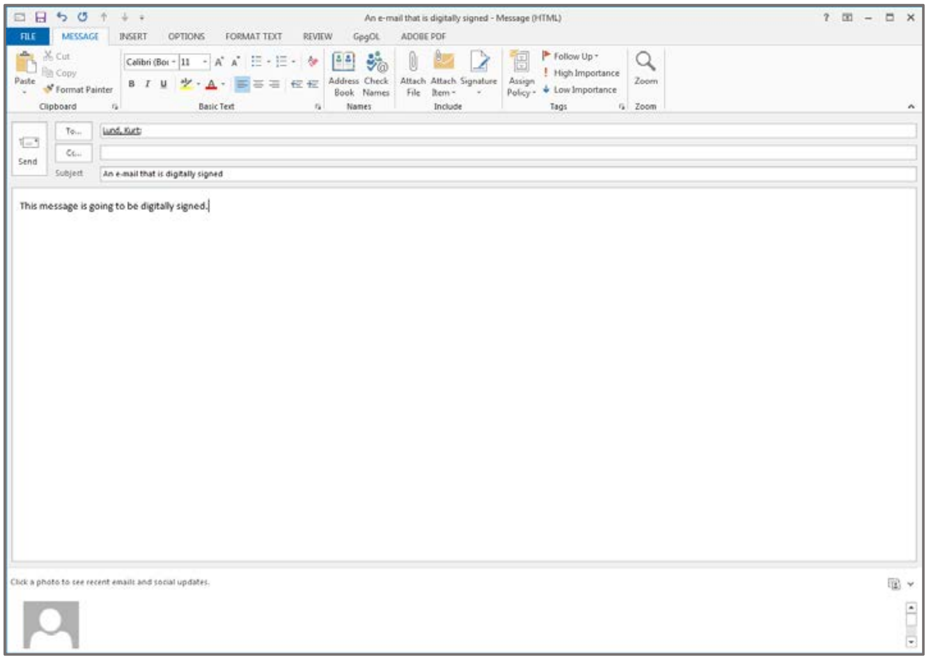
Subject: A message with an encrypted attachment

Attached: Secret2.txt.gpg (743 B)

This message has an unencrypted body but will carry an encrypted attachment.

XII. Digitally signing an e-mail message

1. Open a "Compose" window in Outlook and type in your message content as you usually do.



An e-mail that is digitally signed - Message (HTML)

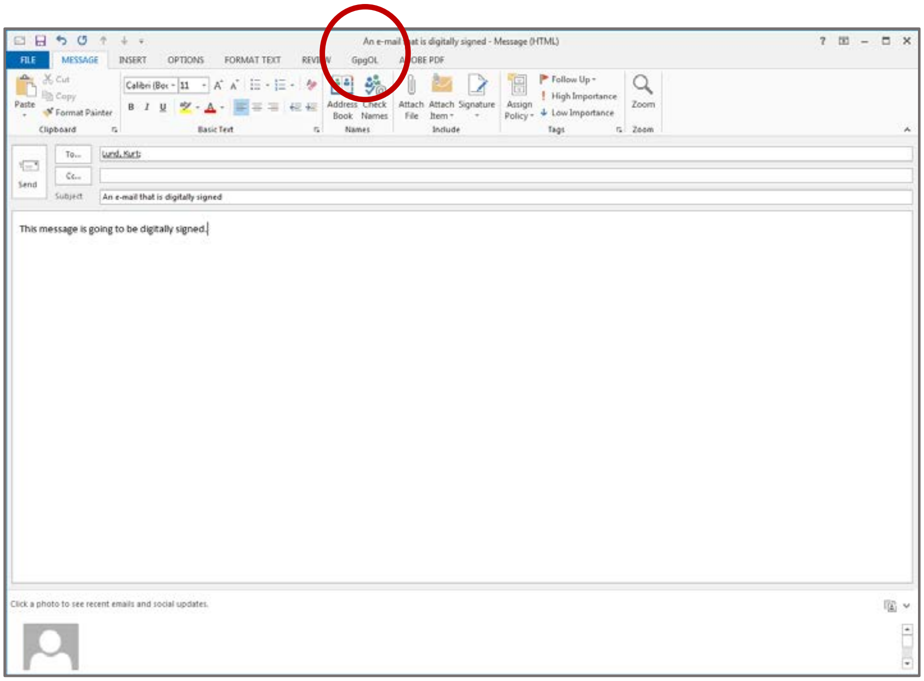
To... Lund, Kurt

Cc...

Subject: An e-mail that is digitally signed

This message is going to be digitally signed.

2. Select the "GpgOL" tab.



An e-mail that is digitally signed - Message (HTML)

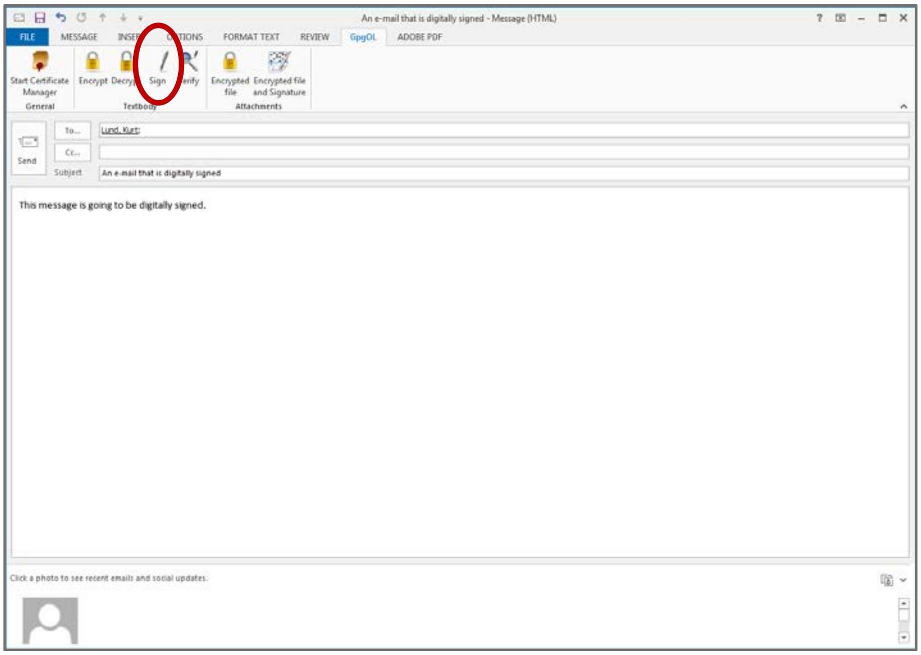
To... Lund, Kurt

Cc...

Subject: An e-mail that is digitally signed

This message is going to be digitally signed.

3. Click the “Sign” button.

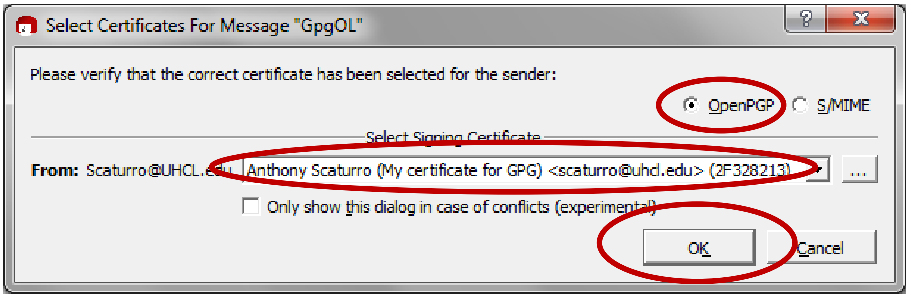

An e-mail that is digitally signed - Message (HTML)
FILE
MESSAGE
INSERT
OPTIONS
FORMAT TEXT
REVIEW
GpgOL
ADOBE PDF
Start Certificate Manager
General
Encrypt
Decrypt
Sign
Verify
Textbody
Encrypted file
Encrypted file and Signature
Attachments
Send
To...
Cc...
Subject
Click a photo to see recent emails and social updates.

To... Lund, Kurt;

Subject: An e-mail that is digitally signed

This message is going to be digitally signed.

4. You will be asked to verify that the correct private key certificate is being used. Check that the certificate is the one expected and the OpenPGP radio button is selected. Click the “OK” button to confirm.


Select Certificates For Message "GpgOL"

Please verify that the correct certificate has been selected for the sender:

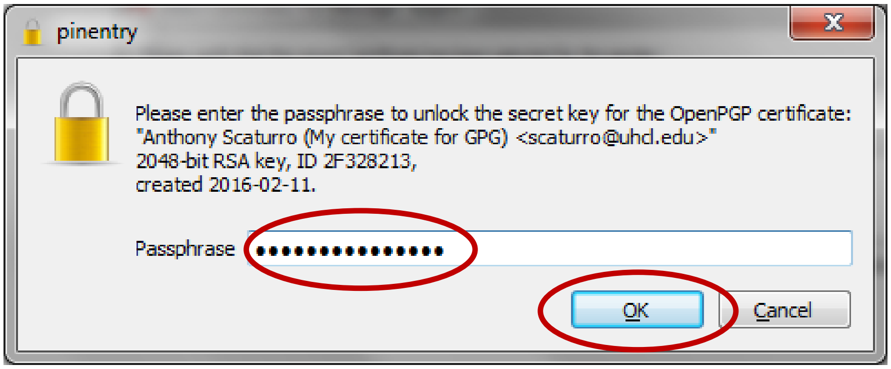
● OpenPGP ○ S/MIME

Select Signing Certificate

From: Scaturro@UHCL.edu Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu> (2F328213)

□ Only show this dialog in case of conflicts (experimental)

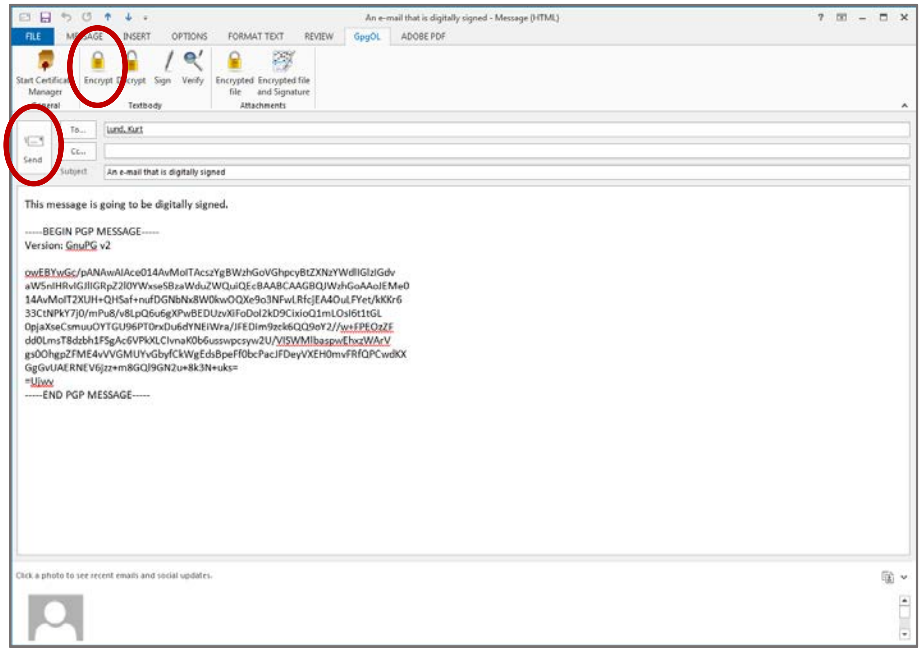
5. You will be prompted to enter your passphrase to unlock your private key. Enter your passphrase and click the “OK” button.


pinentry

Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu>"
2048-bit RSA key, ID 2F328213,
created 2016-02-11.

Passphrase ●●●●●●●●●●●●●●●

6. The digital signature will be added to the end of your message. If you do not wish to encrypt the message, click the "Send" button to send the e-mail and to end the process. Otherwise click the "Encrypt" button and continue to step 7.

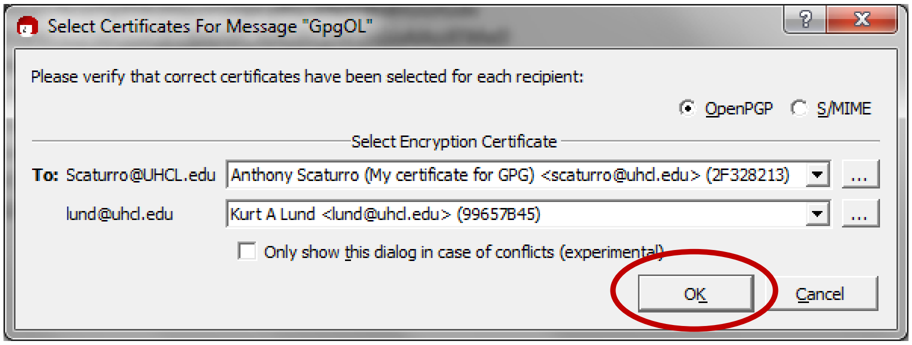

An e-mail that is digitally signed - Message (HTML)
FILE
MESSAGE
INSERT
OPTIONS
FORMAT TEXT
REVIEW
GpgOL
ADOBE PDF
Start Certificate Manager
General
Encrypt
Decrypt
Sign
Verify
Textbody
Encrypted file
Encrypted file and Signature
Attachments
Send
To...
Cc...
Subject
Click a photo to see recent emails and social updates.

To: lund, Kurt

Subject: An e-mail that is digitally signed

```
This message is going to be digitally signed.

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

owEBYwGc/pANAwAIAce014AvMolTAcszYgBWzhGoVGhpcyBtZXNzYWdlIGlzIGdv
aW5nIHRvIGJlIGRpZ2l0YWxseSBzaWduZWQuiQEcBAABCAAGBQJWzhGoAAoJEMe0
14AvMolT2XUH+QHSaf+nufDGNbNx8W0kwOQXe9o3NFwLRfcjEA4OuLFYet/kKKr6
33CtNPkY7j0/mPu8/v8LpQ6u6gXPwBEDUzvXiFoDol2kD9CixioQ1mLOsl6t1tGL
OpjaXseCsmuuOYTGU96PT0rxDu6dYNEiWra/JFEDim9zck6QQ9oY2//w+FPEOzZF
dd0LmsT8dzbh1FSgAc6VPkXLClvnaK0b6usswpcsyw2U/VlSWMlbaspwEhxzWArV
gs0OhgpZFME4vVVGMUYvGbyfCkWgEdsBpeFf0bcPacJFDeyVXEH0mvFRfQPCwdKX
GgGvUAERNEV6jzz+m8GQJ9GN2u+8k3N+uks=
=Ujwy
-----END PGP MESSAGE-----
```

7. If you choose to encrypt, you must verify that the correct recipient public keys are selected. Click the "OK" button if the correct certificates are chosen.



Please verify that correct certificates have been selected for each recipient:

● OpenPGP ○ S/MIME

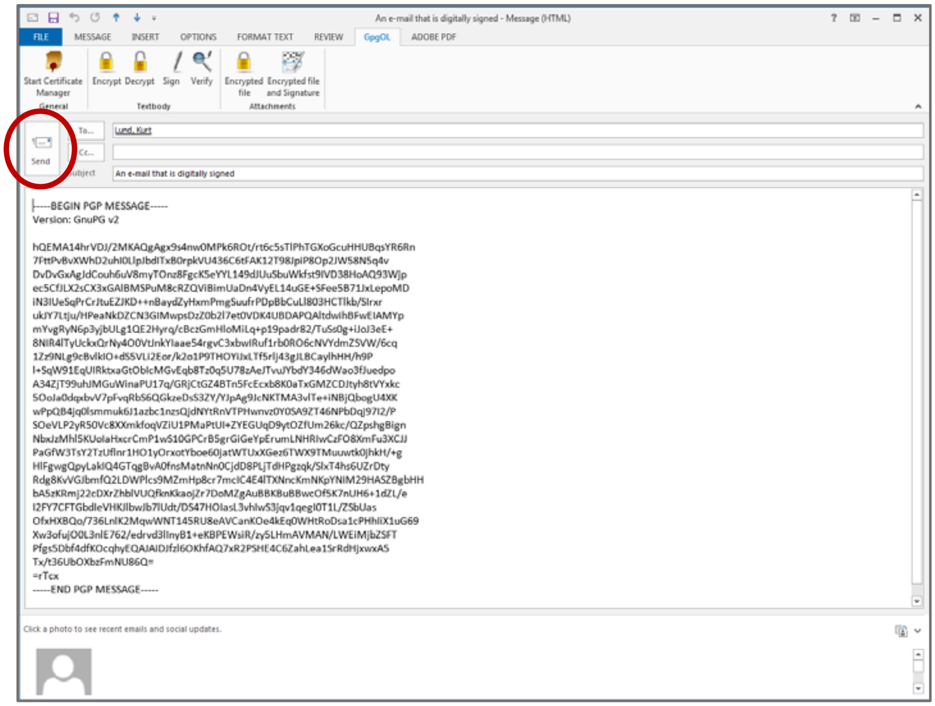
Select Encryption Certificate

To: Scaturro@UHCL.edu — Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu> (2F328213)

lund@uhcl.edu — Kurt A Lund <lund@uhcl.edu> (99657B45)

□ Only show this dialog in case of conflicts (experimental)

8. The entire message will be encrypted. Click the “Send” button to complete the process.


An e-mail that is digitally signed - Message (HTML)
FILE
MESSAGE
INSERT
OPTIONS
FORMAT TEXT
REVIEW
GpgOL
ADOBE PDF
Start Certificate Manager
General
Encrypt
Decrypt
Sign
Verify
Textbody
Encrypted file
Encrypted file and Signature
Attachments
Send
To...
Cc...
Subject
Click a photo to see recent emails and social updates.

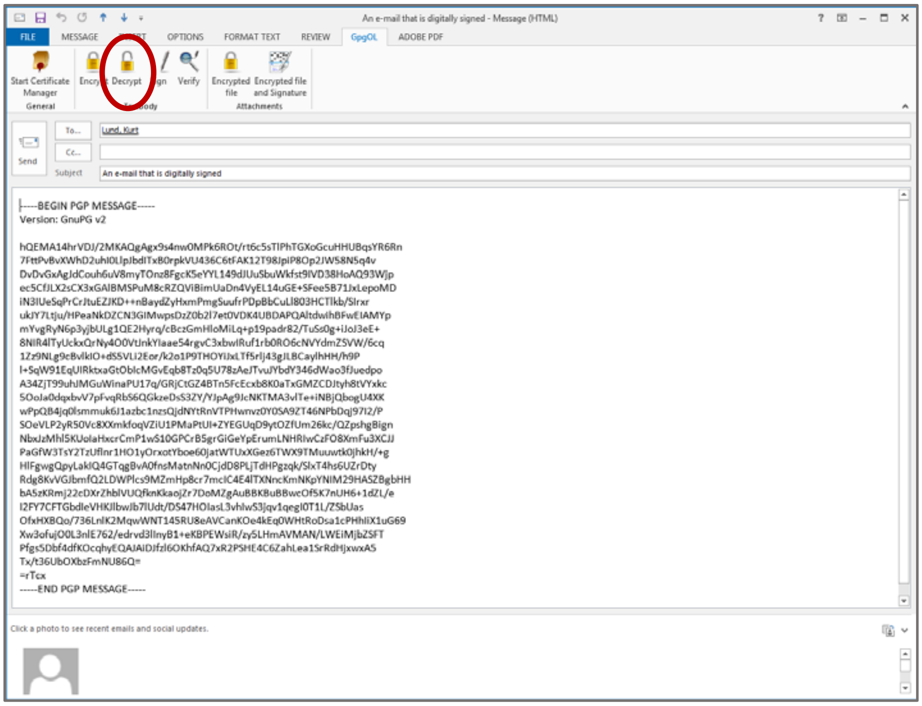
To...: Lund, Kurt

Subject: An e-mail that is digitally signed

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQEMA14hrVDJ/2MKAQgAgx9s4nw0MPk6ROt/rt6c5sTlPhTGXoGcuHHUBqsYR6Rn
7FttPvBvXWhD2uhI0LlpJbdITxB0rpkVU436C6tFAK12T98JpiP8Op2JW58N5q4v
DvDvGxAgJdCouh6uV8myTOnz8FgcK5eYYL149dJUuSbuWkfst9IVD38HoAQ93Wjp
ec5CfJLX2sCX3xGAlBMSPuM8cRZQViBimUaDn4VyEL14uGE+SFee5B71JxLepoMD
iN3IUeSqPrCrJtuEZJKD++nBaydZyHxmPmgSuufrPDpBbCuLl803HCTlkb/SIrxr
ukJY7Ltju/HPeaNkDZCN3GIMwpsDzZ0b2l7et0VDK4UBDAPQAltdwihBFwEIAMYp
mYvgRyN6p3yjbULg1QE2Hyrq/cBczGmHloMiLq+p19padr82/TuSs0g+iJoJ3eE+
8NIR4lTyUckxQrNy4O0VtJnkYlaae54rgvC3xbwIRuf1rb0RO6cNVYdmZSVW/6cq
1Zz9NLg9cBvlkIO+dS5VLi2Eor/k2o1P9THOYiJxLTf5rlj43gJLBCaylhHH/h9P
l+SqW91EqUIRktxaGtOblcMGvEqb8Tz0q5U78zAeJTvuJYbdY346dWao3fJuedpo
A34ZjT99uhJMGuWinaPU17q/GRjCtGZ4BTn5FcEcxb8K0aTxGMZCDJtyh8tVYxkc
5OoJa0dqxbvV7pFvqRb56QGkzeDsS3ZY/YJpAg9JcNKTMA3vlTe+iNBjQbogU4XK
wPpQB4jq0lsmmuk6J1azbc1nzsQjdNYtRnVTPHwnvz0Y0SA9ZT46NPbDqj97I2/P
SOeVLP2yR50Vc8XXmkfoqVZiU1PMaPtUI+ZYEGUqD9ytOZfUm26kc/QZpshgBign
NbxJzMhl5KUolaHxcrCmP1wS10GPCrB5grGiGeYpErumLNHRlwCzFO8XmFu3XCJJ
PaGfW3TsY2TzUflnr1HO1yOrxotYboe60jatWTUxXGez6TWX9TMuuwtk0jhkH/+g
HlFgwgQpyLakIQ4GTqgBvA0fnsMatnNn0CjdD8PLjTdHPgzqk/SlxT4hs6UZrDty
Rdg8KvVGJbmfQ2LDWPlcs9MZmHp8cr7mcIC4E4lTXNncKmNKpYNIM29HASZBgbHH
bA5zKRmj22cDXrZhblVUQfknKkaojZr7DoMZgAuBBKBuBBwcOf5K7nUH6+1dZL/e
l2FY7CFTGbdleVHKJlbwJb7lUdt/D547HOlasL3vhlw53jqv1qegI0T1L/Z5bUas
OfxHXBQo/736LnIK2MqwWNT145RU8eAVCanKOe4kEq0WHtRoDsa1cPHhliX1uG69
Xw3ofujO0L3nlE762/edrvd3lInyB1+eKBPEWsiR/zy5LHmAVMAN/LWEiMjbZSFT
Pfgs5Dbf4dfKOcqhyEQAJAiDJfzl6OKhfAQ7xR2PSHE4C6ZahLea1SrRdHjxwxA5
Tx/t36UbOXbzFmNU86Q=
=rTcx
-----END PGP MESSAGE-----
```

XIII. Verifying the digital signature on a signed e-mail

1. Open the signed e-mail message that you received and select the “GpgOL” tab. If the message is not encrypted, proceed to step 3. If it is, click the “Decrypt” button to decrypt the message.



To: Lund, Kurt

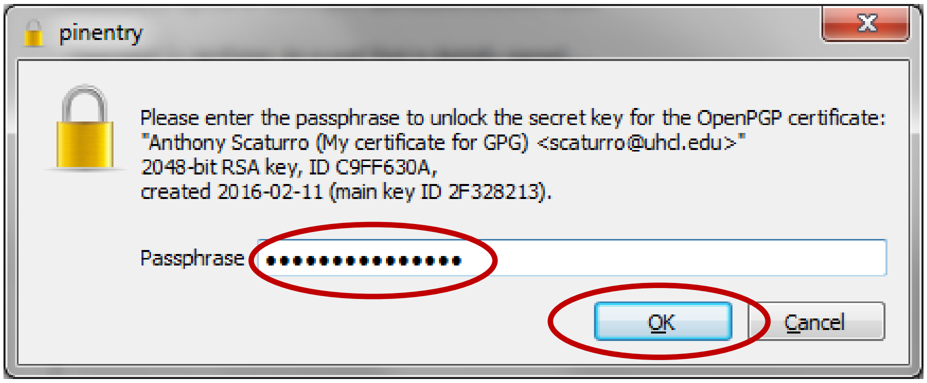
Subject: An e-mail that is digitally signed

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQEMA14hrVDJ/2MKAQgAgx9s4nw0MPk6ROt/rt6c5sTlPhTGXoGcuHHUBqsYR6Rn
7FttPvBvXWhD2uhI0LlpJbdITxB0rpkVU436C6tFAK12T98JpiP8Op2JW58N5q4v
DvDvGxAgJdCouh6uV8myTOnz8FgcK5eYYL149dJUuSbuWkfst9IVD38HoAQ93Wjp
ec5CfJLX2sCX3xGAlBMSPuM8cRZQViBimUaDn4VyEL14uGE+SFee5B71JxLepoMD
iN3IUeSqPrCrJtuEZJKD++nBaydZyHxmPmgSuufrPDpBbCuLl803HCTlkb/SIrxr
ukJY7Ltju/HPeaNkDZCN3GIMwpsDzZ0b2l7et0VDK4UBDAPQAltdwihBFwEIAMYp
mYvgRyN6p3yjbULg1QE2Hyrq/cBczGmHloMiLq+p19padr82/TuSs0g+iJoJ3eE+
8NIR4lTyUckxQrNy4O0VtUnkYlaae54rgvC3xbwIRuf1rb0RO6cNVYdmZSVW/6cq
1Zz9NLg9cBvlkIO+dS5VLi2Eor/k2o1P9THOYiJxLTf5rlj43gJLBCaylhHH/h9P
l+SqW91EqUIRktxaGtOblcMGvEqb8Tz0q5U78zAeJTvuJYbdY346dWao3fJuedpo
A34ZjT99uhJMGuWinaPU17q/GRjCtGZ4BTn5FcEcxb8K0aTxGMZCDJtyh8tVYxkc
5OoJa0dqxbvV7pFvqRbS6QGkzeDsS3ZY/YJpAg9JcNKTMA3vlTe+iNBjQbogU4XK
wPpQB4jq0lsmmuk6J1azbc1nzsQjdNYtRnVTPHwnvz0Y0SA9ZT46NPbDqj97I2/P
SOeVLP2yR50Vc8XXmkfoqVZiU1PMaPtUI+ZYEGUqD9ytOZfUm26kc/QZpshgBign
NbxJzMhl5KUolaHxcrCmP1w510GPCrB5grGiGeYpErumLNHRIwCzFO8XmFu3XCJJ
PaGfW3TsY2TzUflnr1HO1yOrxotYboe60jatWTUxXGez6TWX9TMuuwtk0jhkH/+g
HlFgwgQpyLakIQ4GTqgBvA0fnsMatnNn0CjdD8PLjTdHPgzqk/SlxT4hs6UZrDty
Rdg8KvVGJbmfQ2LDWPlcs9MZmHp8cr7mcIC4E4lTXNncKmNKpYNIM29HASZBgbHH
bA5zKRmj22cDXrZhblVUQfknKkaojZr7DoMZgAuBBKBuBBwcOf5K7nUH6+1dZL/e
I2FY7CFTGbdleVHKJlbwJb7lUdt/DS47HOlasL3vhlw53jqv1qegI0T1L/Z5bUas
OfxHXBQo/736LnIK2MqwWNT145RU8eAVCanKOe4kEq0WHtRoDsa1cPHhliX1uG69
Xw3ofujO0L3nlE762/edrvd3lInyB1+eKBPEWsiR/zy5LHmAVMAN/LWEiMjbZSFT
Pfgs5Dbf4dfKOcqhyEQAJAiDJfzl6OKhfAQ7xR2PSHE4C6ZahLea1SrRdHjxwxA5
Tx/t36UbOXbzFmNU86Q=
=rTcx
-----END PGP MESSAGE-----

Click a photo to see recent emails and social updates.

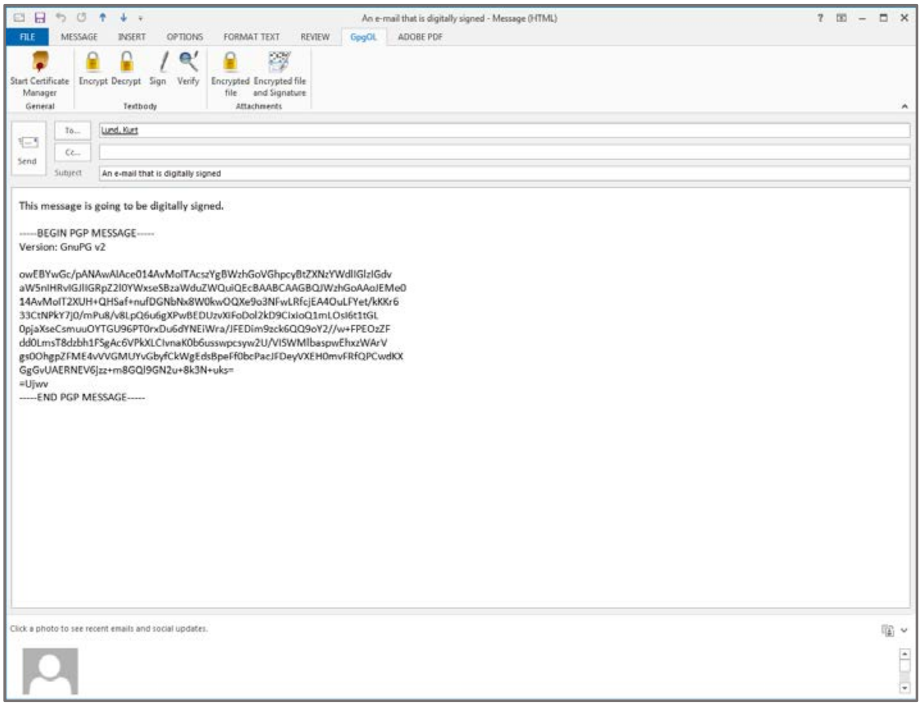
2. A window will be displayed asking for your passphrase. Enter your passphrase to unlock your private key, and click the “OK” button.



Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"Anthony Scaturro (My certificate for GPG) <scaturro@uhcl.edu>"
2048-bit RSA key, ID C9FF630A,
created 2016-02-11 (main key ID 2F328213).

Passphrase ●●●●●●●●●●●●●●●

3. The encryption block will be at the end of the message should be the digital signature of the sender. Click the “Verify” button to ensure that the digital signature is valid.


An e-mail that is digitally signed - Message (HTML)
FILE
MESSAGE
INSERT
OPTIONS
FORMAT TEXT
REVIEW
GpgOL
ADOBE PDF
Start Certificate Manager
Encrypt
Decrypt
Sign
Verify
Encrypted file
Encrypted file and Signature
General
Textbody
Attachments
Send
To...
Cc...
Subject
Click a photo to see recent emails and social updates.

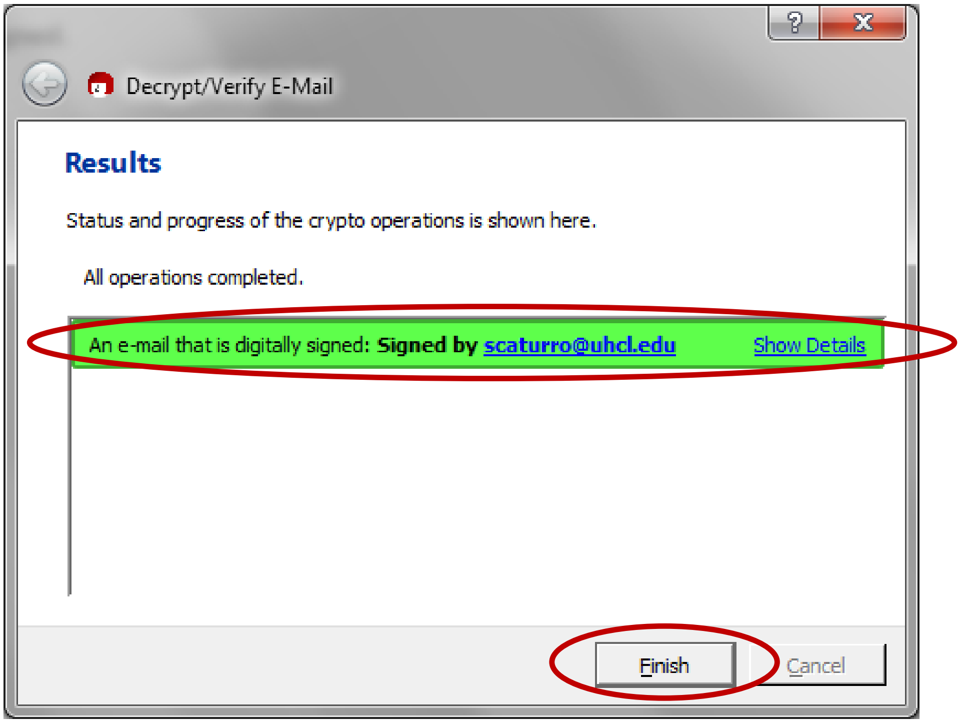
To... Lund, Kurt

Subject: An e-mail that is digitally signed

This message is going to be digitally signed.

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

owEBYwGc/pANAwAlAce014AvMolTAcszYgBWzhGoVGhpcyBtZXNzYWdlIGlzIGdv
aW5nIHRvIGJlIGRpZ2l0YWxseSBzaWduZWQuiQEcBAABCAAGBQJWzhGoAAoJEMe0
14AvMolT2XUH+QHSaf+nufDGNbNx8W0kwOQXe9o3NFwLRfcjEA4OuLFYet/kKKr6
33CtNPkY7j0/mPu8/v8LpQ6u6gXPwBEDUzvXIFoDol2kD9CixioQ1mLOsl6t1tGL
0pjaXseCsmuuOYTGU96PT0rxDu6dYNEiWra/JFEDim9zck6QQ9oY2//w+FPEOzZF
dd0LmsT8dzbh1FSgAc6VPkXLClvnaK0b6usswpcsyw2U/VISWMlbaspwEhxzWArV
gsOOhgpZFME4vVVGMUYvGbyfCkWgEdsBpeFf0bcPacJFDeyVXEH0mvFRfQPCwdKX
GgGvUAERNEV6Jzz+m8GQI9GN2u+8k3N+uks=
=Ujwv
-----END PGP MESSAGE-----
```

4. A popup widow will be displayed indicating whether or not the digital signature is valid. If the signature is invalid, do not trust the message. Click the “Finish” button to close the popup window.



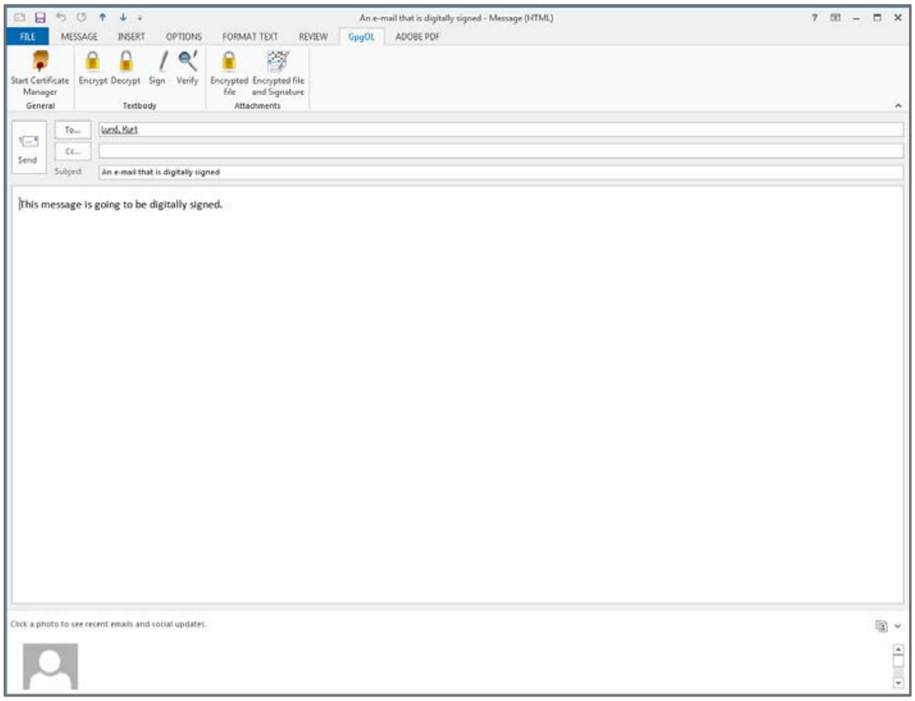
Results

Status and progress of the crypto operations is shown here.

All operations completed.

An e-mail that is digitally signed: **Signed by scaturro@uhcl.edu**

5. The “Verify” process removes the digital signature from the message.


An e-mail that is digitally signed - Message (HTML)
FILE
MESSAGE
INSERT
OPTIONS
FORMAT TEXT
REVIEW
GpgOL
ADOBE PDF
Start Certificate Manager
General
Encrypt
Decrypt
Sign
Verify
Textbody
Encrypted file
Encrypted file and Signature
Attachments
Send
To...
Cc...
Subject
Click a photo to see recent emails and social updates.

To... Lund, Kurt

Cc...

Subject An e-mail that is digitally signed

This message is going to be digitally signed.