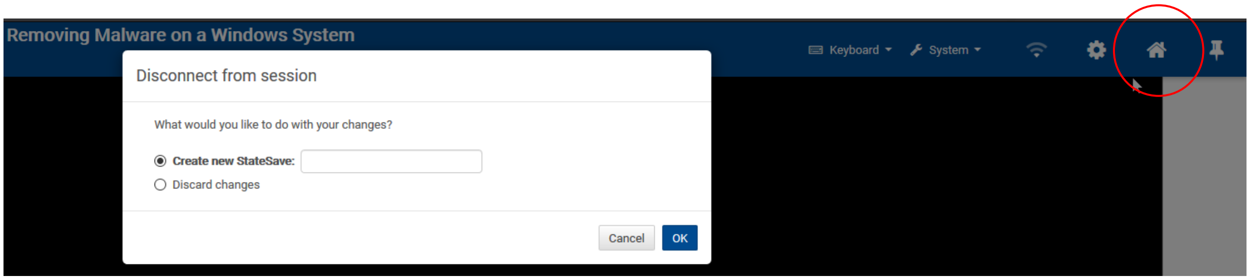
# Lab #2 (Required): Using Encryption to Enhance Confidentiality and Integrity*

### Introduction to Information Security (IST623)
### School of Information Studies
### Syracuse University

**Disclaimer:** The contents of this document are solely for educational purpose. Misused knowledge of this lab may result in damage of data, security breach, privacy violation, or other undesirable situations. Therefore, using knowledge of this lab other than for the original purpose is prohibited.

**** Save Your Lab Status!**** You may need to save your lab from time to time as each session allows you to be logged in only for two hours at a time. To save your current status in the lab environment, **click** the **Home** icon button (🏠) in the top right corner and choose **Create new StateSave** if it's your first time saving or **Overwrite existing StateSave** if you have saved it before.



Disconnect from session

What would you like to do with your changes?

● Create new StateSave:

○ Discard changes

## Learning Objectives

In this lab, you will learn how cryptography tools can be used to ensure message and file transfer integrity and how encryption can be used to maximize confidentiality. You will use Kleopatra, the certificate management component of GPG4Win, to generate both a public and private key as both a sender and a receiver. You will use the sender's keys to encrypt a file, send it to the receiver, and decrypt it with the receiver's copy of the keys.

Upon completing this lab, you will be able to:

- Apply the concepts of common cryptographic and encryption techniques to ensure confidentiality.
- Understand public and private key pairs and basic asymmetric cryptography.
- Generate a public and private key pair.

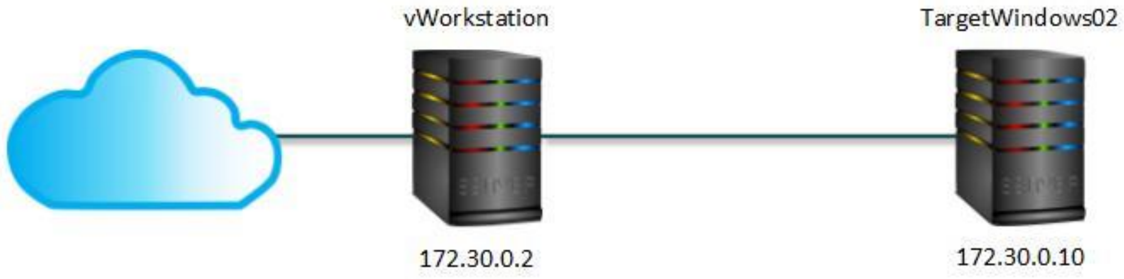
* Customized lab manual by Dr. Joon S. Park at the School of Information Studies for the virtual online labs provided by Jones & Bartlett Learning.

- Upload a certificate to Directory Services server on the Internet.
- Encrypt a data message using a public and private key pair.
- Decrypt a data message using a public and private key pair.

## Lab Structure

This lab has the following parts which should be completed in the following order:

1. In the first part of the lab, you will create a public and private key pair for the senders account on the LandingVM desktop.
2. In the second part of the lab, you create a public and private key pair for the receiver's account on the remote desktop, TargetWindows02.
3. In the third part of the lab, you will transfer and import the public key from the receiver, TargetWindows02.
4. In the fourth part of the lab, you will encrypt a file on the LandingVM desktop using the receiver's public key and digitally sign it using the sender's private key, send it to the remote machine, and then decrypt the file.
5. In the fifth part of this lab, you will answer a challenge question which will help you understand the difference between two well-known certificate types.



## Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- GPG4Win (Kleopatra)

## Lab Deliverables

- Upload completion of this lab, you are required to provide the following deliverables.
    - **One PDF file** that includes:
        - Screenshot from Part 1: Steps #11 and #17
        - Screenshot from Part 4: Step #22
        - Your analysis on the Challenge Question from Part 5 (in 200 words)
    - **The secret-message.txt.gpg file**, that you created in Part 4 (Step #9)

- Lab Report Submission
  - Please submit your deliverables through the LMS submission space.
  - The screenshots should be readable.
  - Make sure you include all the items required in your report.

## Part 1: Create a Public and Private Key Pair for the Sender

> **Note:** In the next steps, you will use Kleopatra to create a set of keys (private and public) that will enable you to encrypt and decrypt a file later in this lab. Keys are also referred to as certificates. Your public key can be used by others to decrypt files that you have encrypted with your private key. You only need to provide your public key, never your private key.

1. **Double-click** the **Kleopatra icon** on the desktop and open the Kleopatra component of the GPG4Win application. (Try resetting the lab if Kleopatra does not work properly).

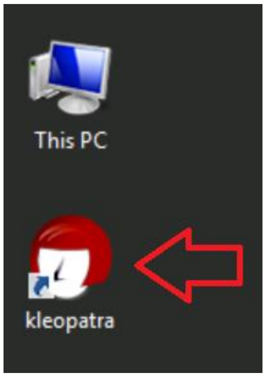


Figure 1 Kleopatra Icon

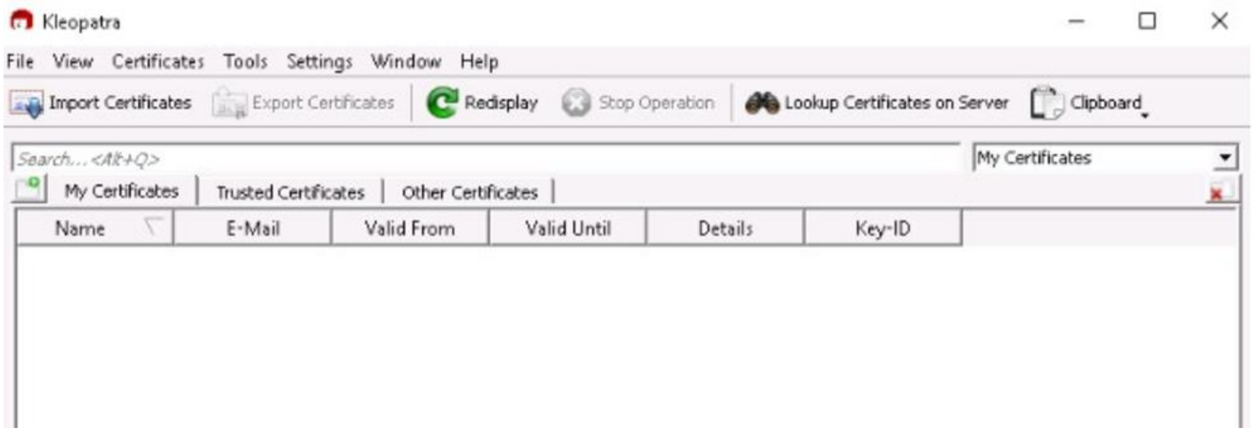


Figure 2 Kleopatra Application

2. **Click Settings** and **select Configure Kleopatra** from the menu.

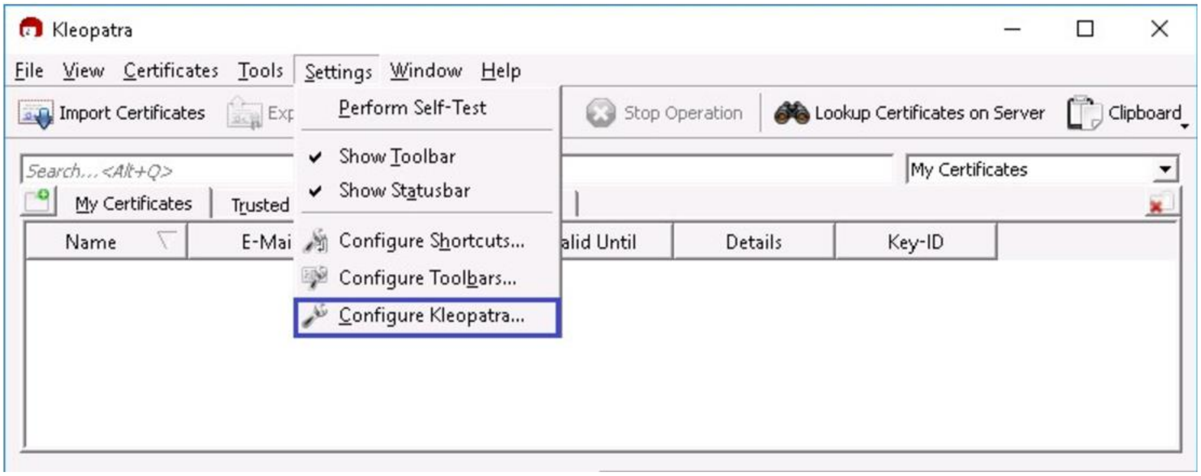
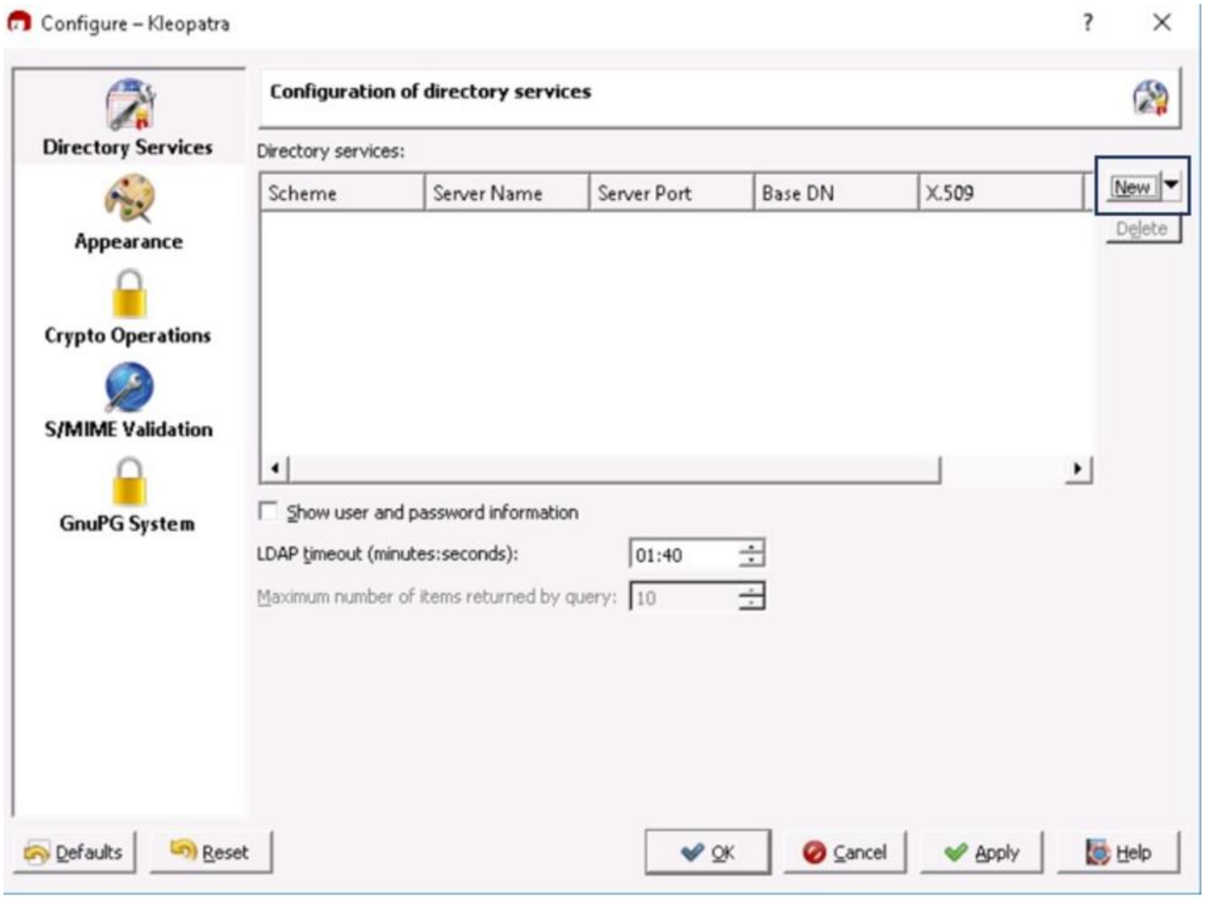


Figure 3 Configure Kleopatra

3. **Click** the **New button** in the top right corner to add a new directory services server.



☐ Show user and password information

LDAP timeout (minutes:seconds): 01:40

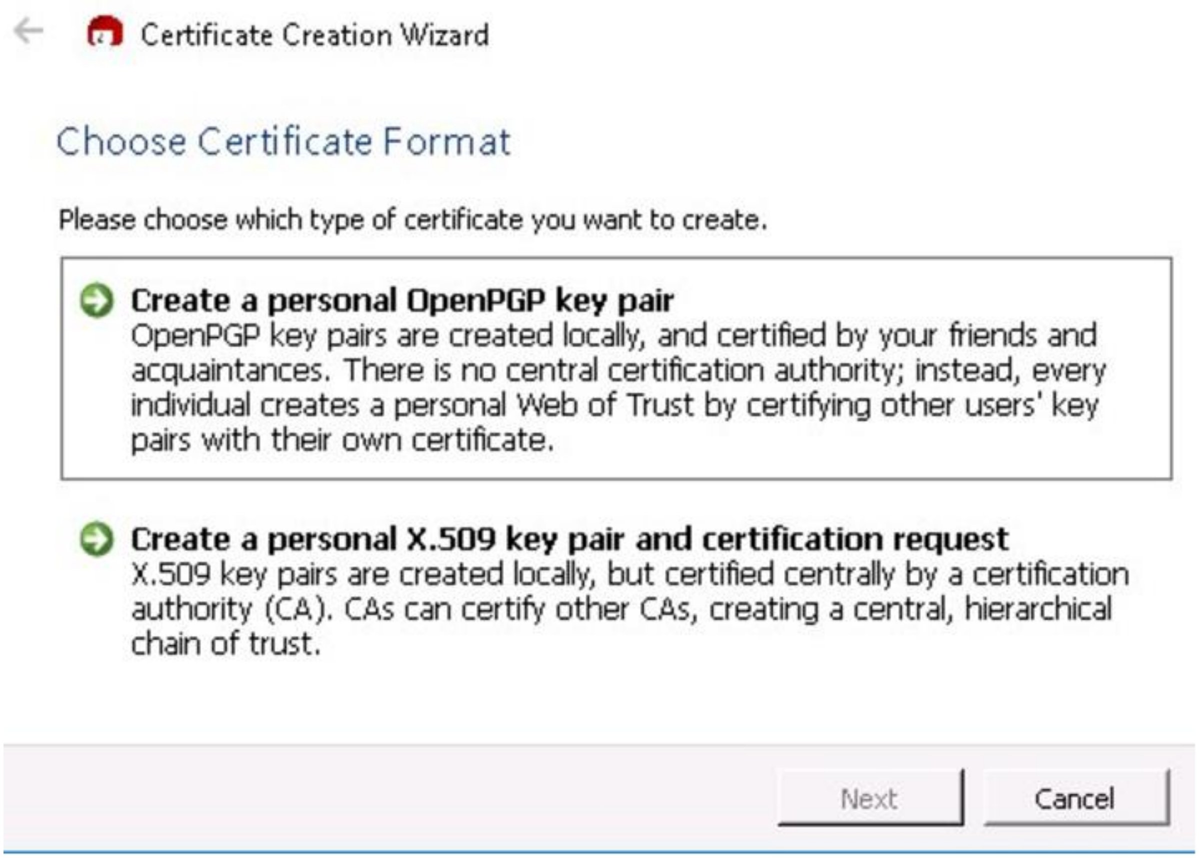
Maximum number of items returned by query: 10

Figure 4 Add directory services

4. **Click OK** to accept the default server name, keys.gnupg.net, and close the dialog box.

5. **Click File** and **select New Certificate** from the Kleopatra menu to open the Certificate Creation Wizard.

6. **Click** the **Create a personal OpenPGP key pair** option.



Certificate Creation Wizard

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.

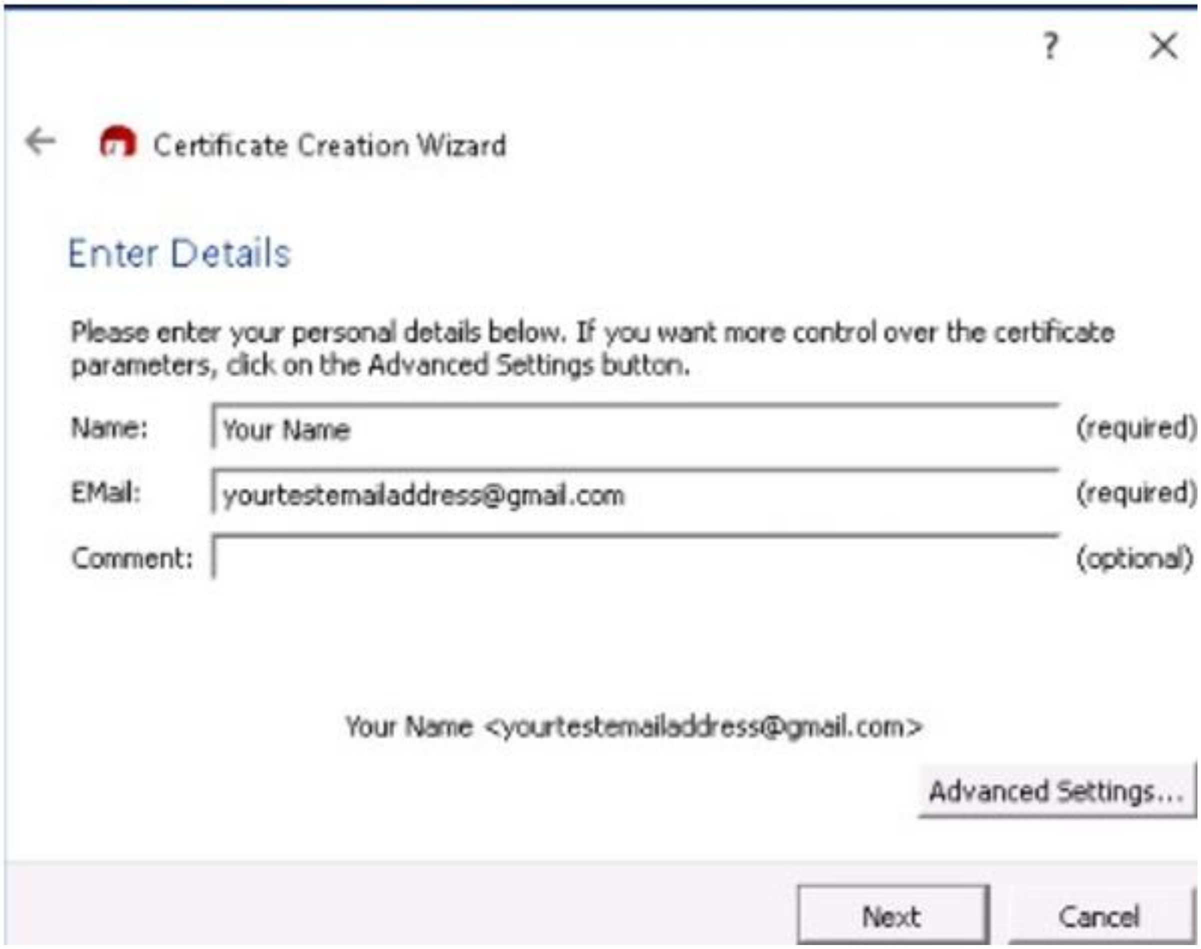
Figure 5 Create a new certificate using Kleopatra

7. In the Enter Details screen, **type** the following information, replacing the placeholder text for your own unique details, and **click Next** to continue.

- Name: ***Your own name***
- Email: ***Your own test email address***

**Note:** A valid email address is required for testing purposes. Your instructor should advise you to use your school email address, or to create a new one using a free email service (i.e., Gmail, Yahoo, Hotmail, etc.) for use during this course. You will give your instructor the email address you used in this lab, so s/he may verify it as part of your homework.

The Comment box can remain empty. While not required to create a key pair, it can be useful if you are creating a certificate for a specific purpose, such as testing or for a specific client. If you do add a comment, it becomes part of your login name, and will be visible to the receiver.



Enter Details

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

Name: Your Name (required)

EMail: yourtestemailaddress@gmail.com (required)

Comment: (optional)

Your Name <yourtestemailaddress@gmail.com>

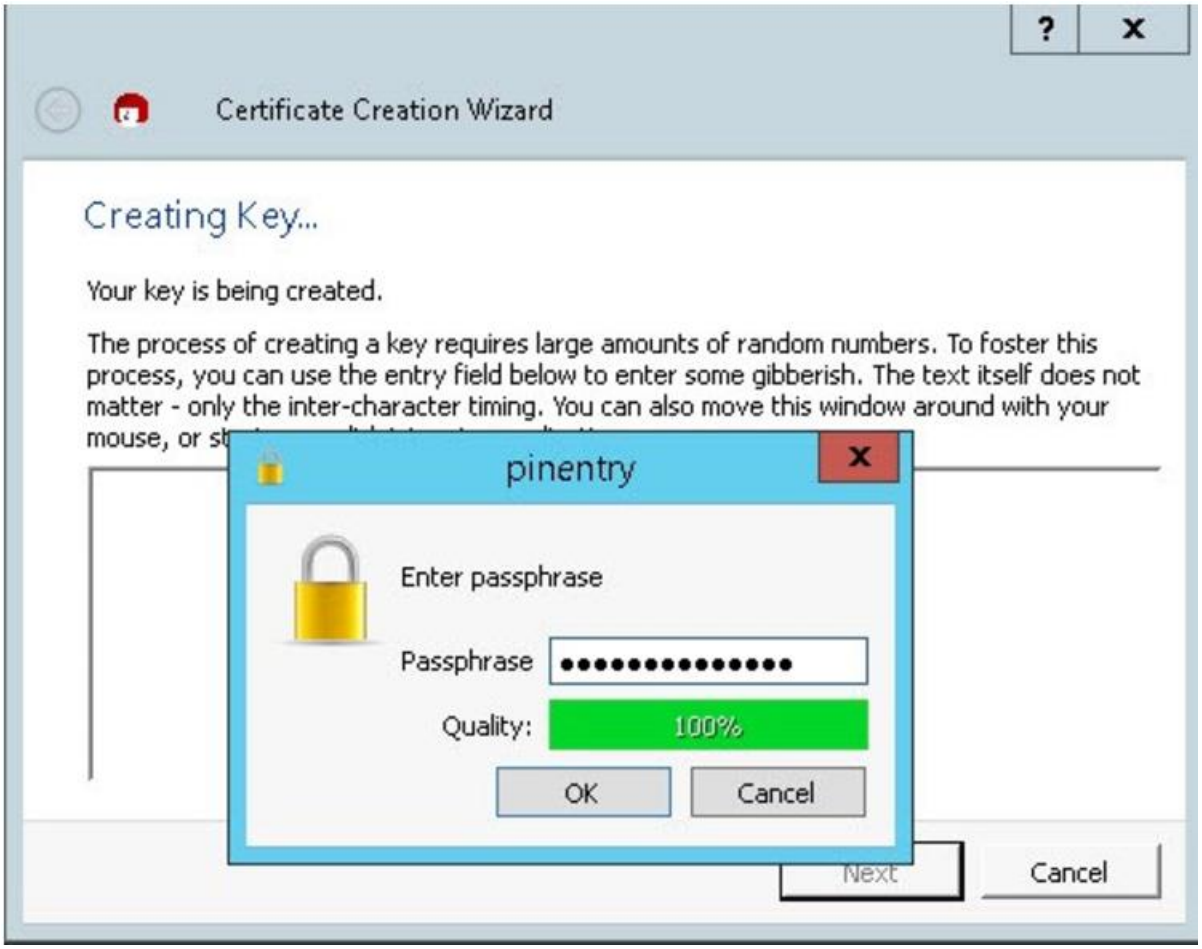
Figure 6 Enter certificate details

8. **Click** the **Next button and then click the Create Key button** on the Review Certificate Parameters page.

   A pinentry (pin entry) dialog box will pop up to complete the creation of a key. You need to enter a passphrase, or password.

9. In the pin entry dialog box, **type 1Tsecurity!** and **click OK**.

   As you type, notice that the Quality meter below the passphrase changes to indicate the degree of security offered by the passphrase. A password that includes upper- and lowercase letters as well as numbers is more secure than one that uses only numbers, such as a birthdate, or a recognizable word, such as *password*.



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 st

Enter passphrase

Passphrase ●●●●●●●●●●●●●●

Quality: 100%

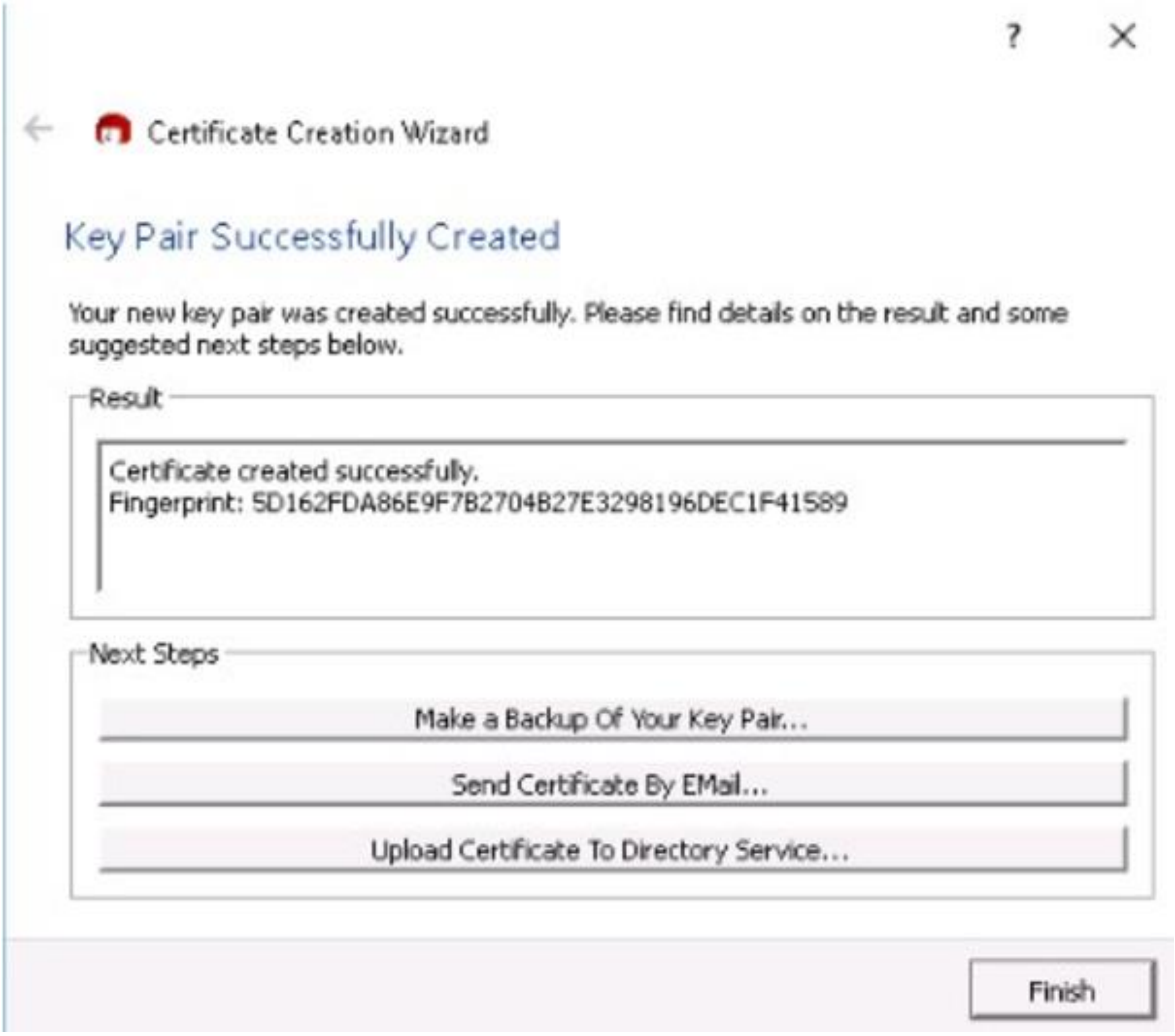
OK Cancel

Figure 7 Create a passphrase for the new certificate

10. You will be prompted to enter the passphrase again; **type 1Tsecurity!** again and **click OK** to generate the key.

    When the key is successfully created, a unique 40-character fingerprint will appear in the Result area of the dialog box. With the key created, you have several options for handling it:

    - **Make a Backup of Your Key Pair.** This option sends a copy of your private key to your computer where you can store it anywhere you'd like.
    - **Send Certificate By E-Mail.** This option will create a new e-mail and automatically attach your public key certificate.
    - **Upload Certificate to Directory Service.** You can store your certificate on a public Internet server.



?
×
←
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

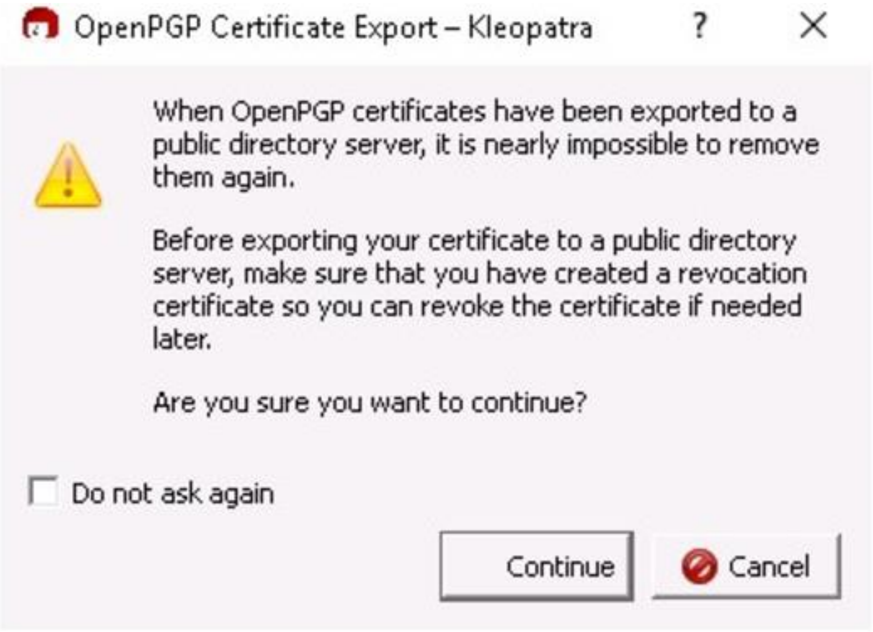
```
Certificate created successfully.
Fingerprint: 5D162FDA86E9F7B2704B27E3298196DEC1F41589
```

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

Figure 8 Successful key pair fingerprint

11. **Make a screen capture** showing the **fingerprint generated by the key creation process** and **paste** it into your Lab Report file.

12. **Click** the **Upload Certificate to Directory Service button** and then **click Continue** to ignore the warning message.



When OpenPGP certificates have been exported to a public directory server, it is nearly impossible to remove them again.

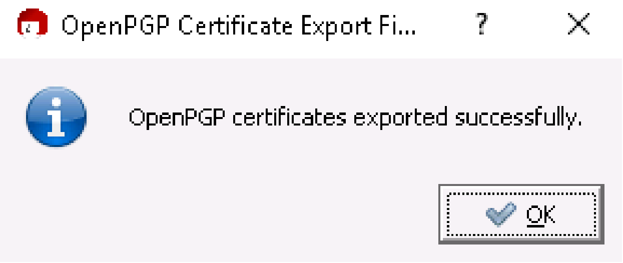
Before exporting your certificate to a public directory server, make sure that you have created a revocation certificate so you can revoke the certificate if needed later.

Are you sure you want to continue?

□ Do not ask again

Figure 9 Kleopatra warning message

13. **Click OK** when the export process is completed.



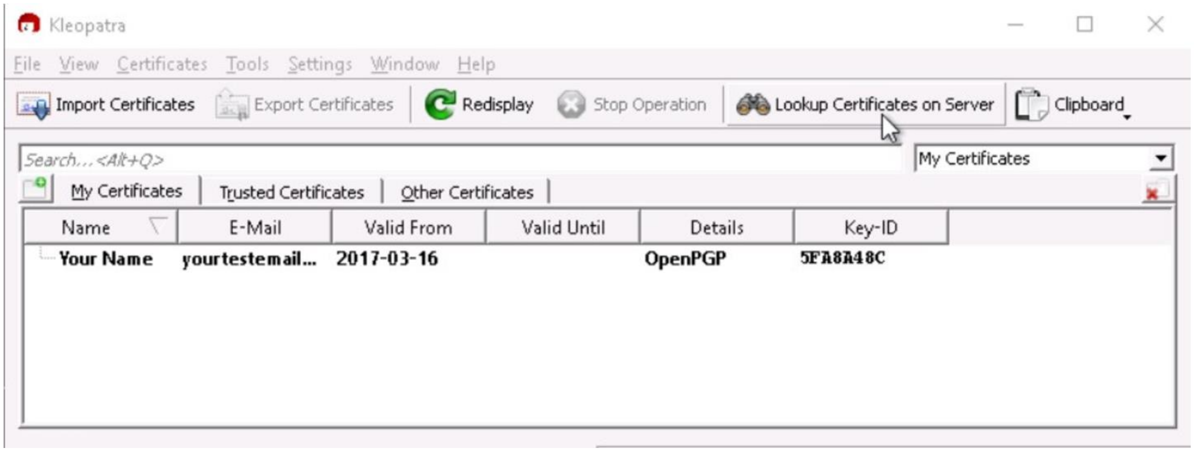
OpenPGP certificates exported successfully.

Figure 10 Successful export of certificate message

14. **Click Finish** to close the Certificate Creation Wizard.

    The new certificate appears in the My Certificates tab of the Kleopatra application. The Key-ID is the same as the last 8 digits of the fingerprint associated with this certificate. Each new certificate is created with no expiration (valid until) date, but you can set an expiration date in the Certificate Details screen. A key pair that has expired can be re-enabled with the private key and the passphrase. To revoke a key (render it unusable), you can create a special revocation signature file. Revocation keys cannot be created in the Kleopatra application.

15. **Click** the **Lookup Certificate on Server button** to verify the certificate.



Search...<Alt+Q>

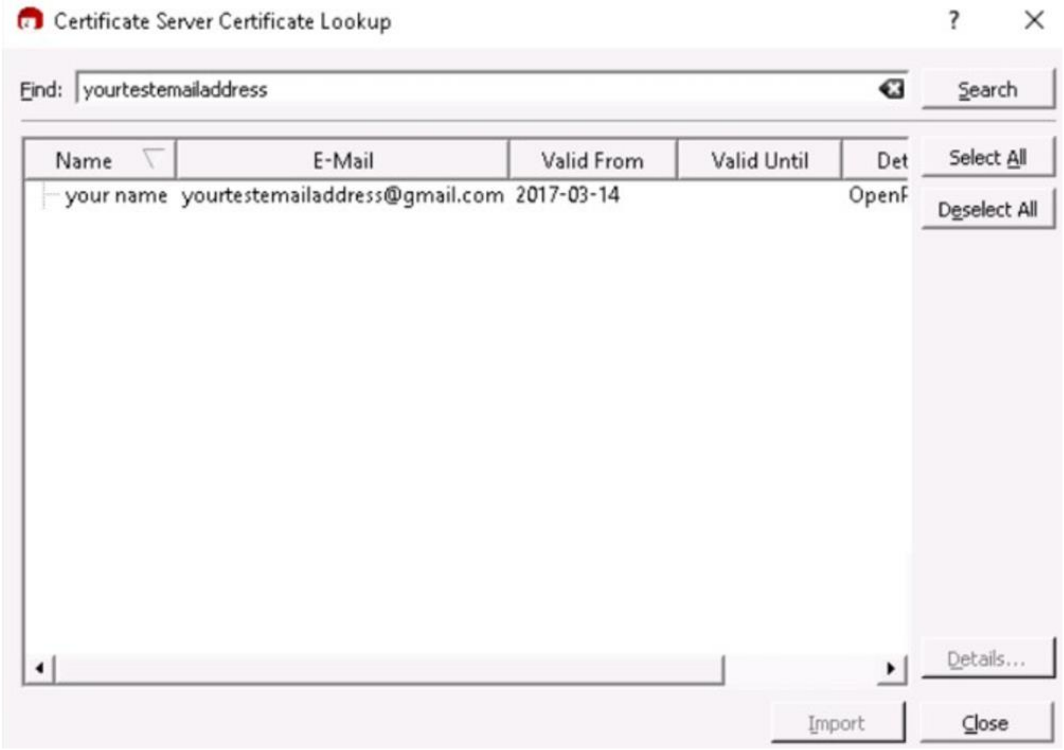
My Certificates

| Name | E-Mail | Valid From | Valid Until | Details | Key-ID |
|---|---|---|---|---|---|
| Your Name | yourtestemail... | 2017-03-16 |  | OpenPGP | 5FA8A48C |

Figure 11 Verify certificate

16. In the Find box, **type** the ***test email address*** you used to create the certificate, and **click Search** to confirm the certificate was uploaded to the Public Directory server.

    This process may take several minutes; you may click the Search button repeatedly to refresh the results of this screen. When your test email address appears in the search results section, adjust the column widths so that your name and email address are visible in their entirety.



Find: yourtestemailaddress

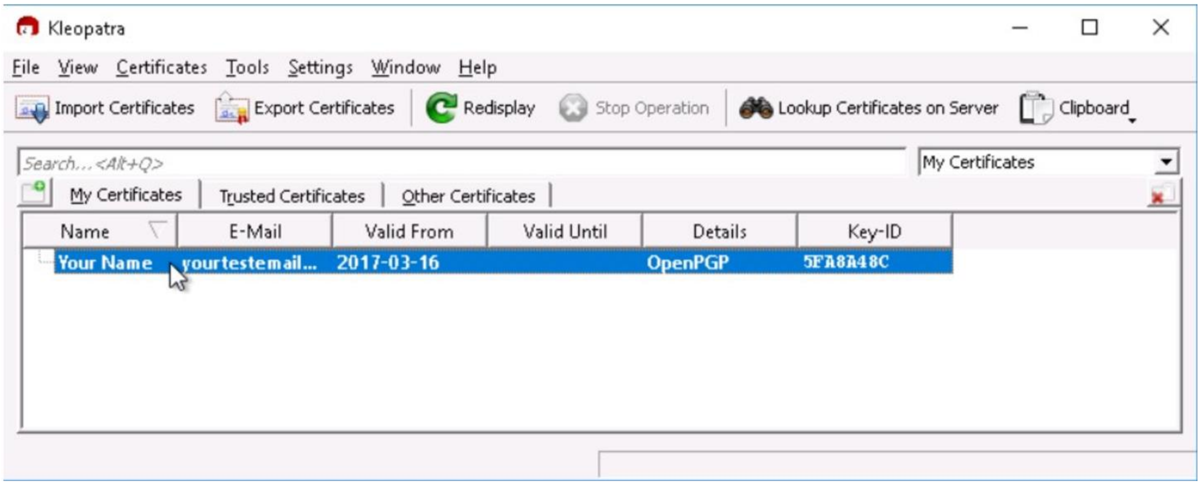
| Name | E-Mail | Valid From | Valid Until | Det |
|---|---|---|---|---|
| your name | yourtestemailaddress@gmail.com | 2017-03-14 |  | OpenP |

Figure 12 Certificate search

17. **Make a screen capture** showing ***your own test email address*** in the Certificate Server Certificate Lookup window and **paste** it into your Lab Report file.

18. **Click Close** to close the window.

19. **Click your newly created certificate** to select it.



| Name | E-Mail | Valid From | Valid Until | Details | Key-ID |
|---|---|---|---|---|---|
| Your Name | yourtestemail... | 2017-03-16 | | OpenPGP | 5FA8A48C |

Figure 13 Certificate preview

20. With the certificate selected, **click File** and **select Export Secret Keys** to save your private (secret) key.

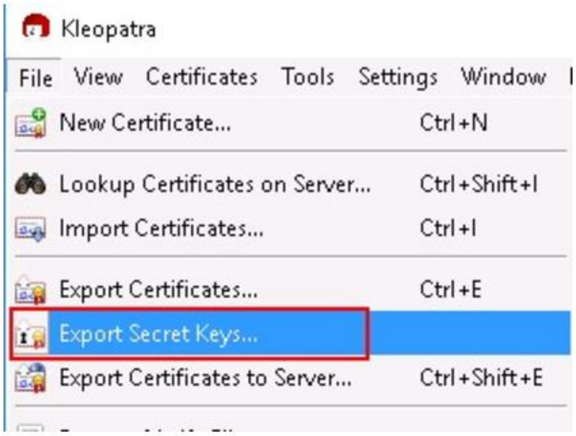
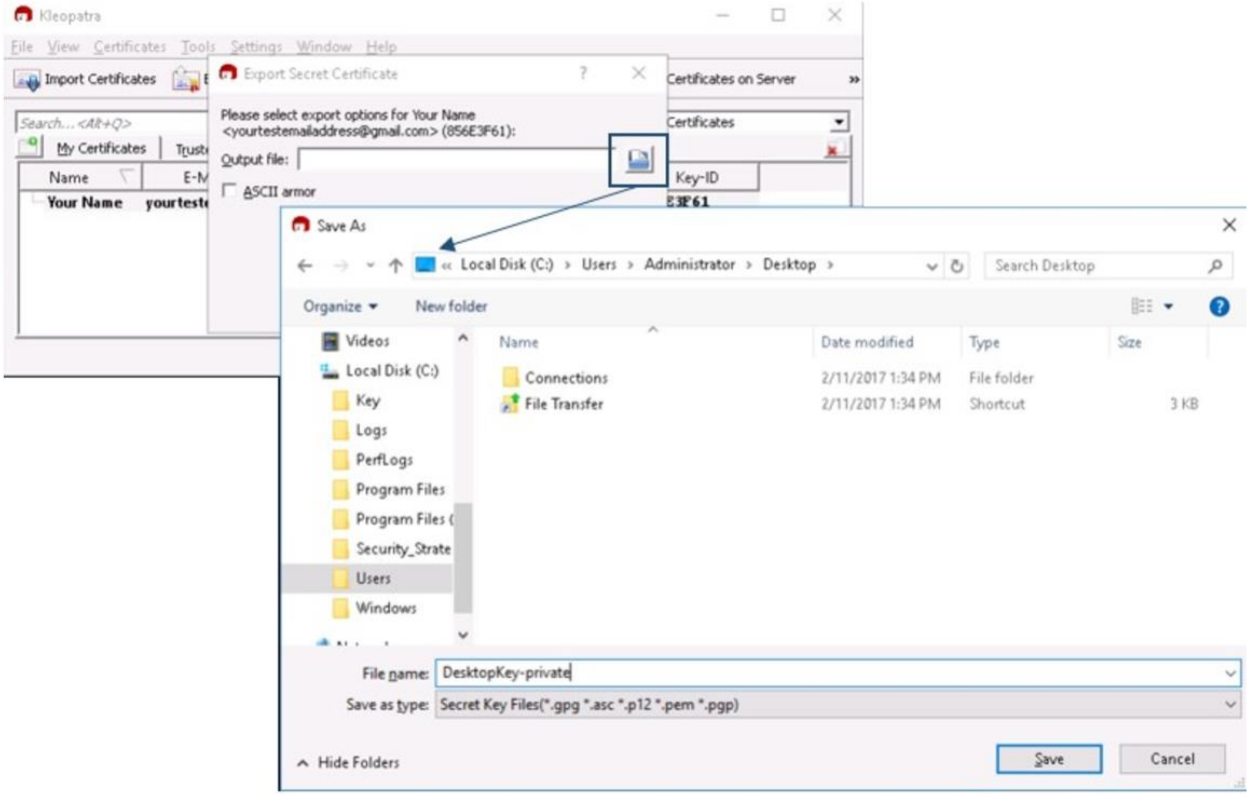

Kleopatra
File View Certificates Tools Settings Window
New Certificate... Ctrl+N
Lookup Certificates on Server... Ctrl+Shift+I
Import Certificates... Ctrl+I
Export Certificates... Ctrl+E
Export Secret Keys...
Export Certificates to Server... Ctrl+Shift+E

Figure 14 Export certificate

21. In the Output file box of the Export Secret Certificate dialog box, **click** the **Browse button** to open a Save As dialog box and then **navigate** to the vWorkstation desktop (**This PC > Local Disk (C:)** > **Users** > **Administrator** > **Desktop**), **type DesktopKey-private** in the File Name box, and **click Save** to return to the Export dialog box.


Please select export options for Your Name <yourtestemailaddress@gmail.com> (856E3F61):

Output file:

□ ASCII armor

Save As: Local Disk (C:) › Users › Administrator › Desktop ›

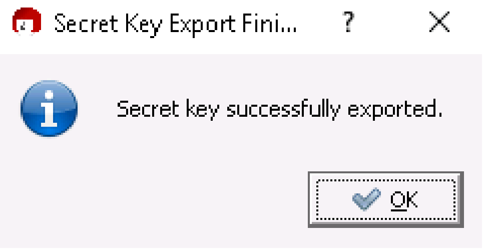
| Name | Date modified | Type | Size |
|---|---|---|---|
| Connections | 2/11/2017 1:34 PM | File folder | |
| File Transfer | 2/11/2017 1:34 PM | Shortcut | 3 KB |

File name: DesktopKey-private

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

Figure 15 Export Secret Certificate

22. **Click OK** to save a copy of your private key and close the Export Secret Certificate dialog box.


Secret Key Export Fini...

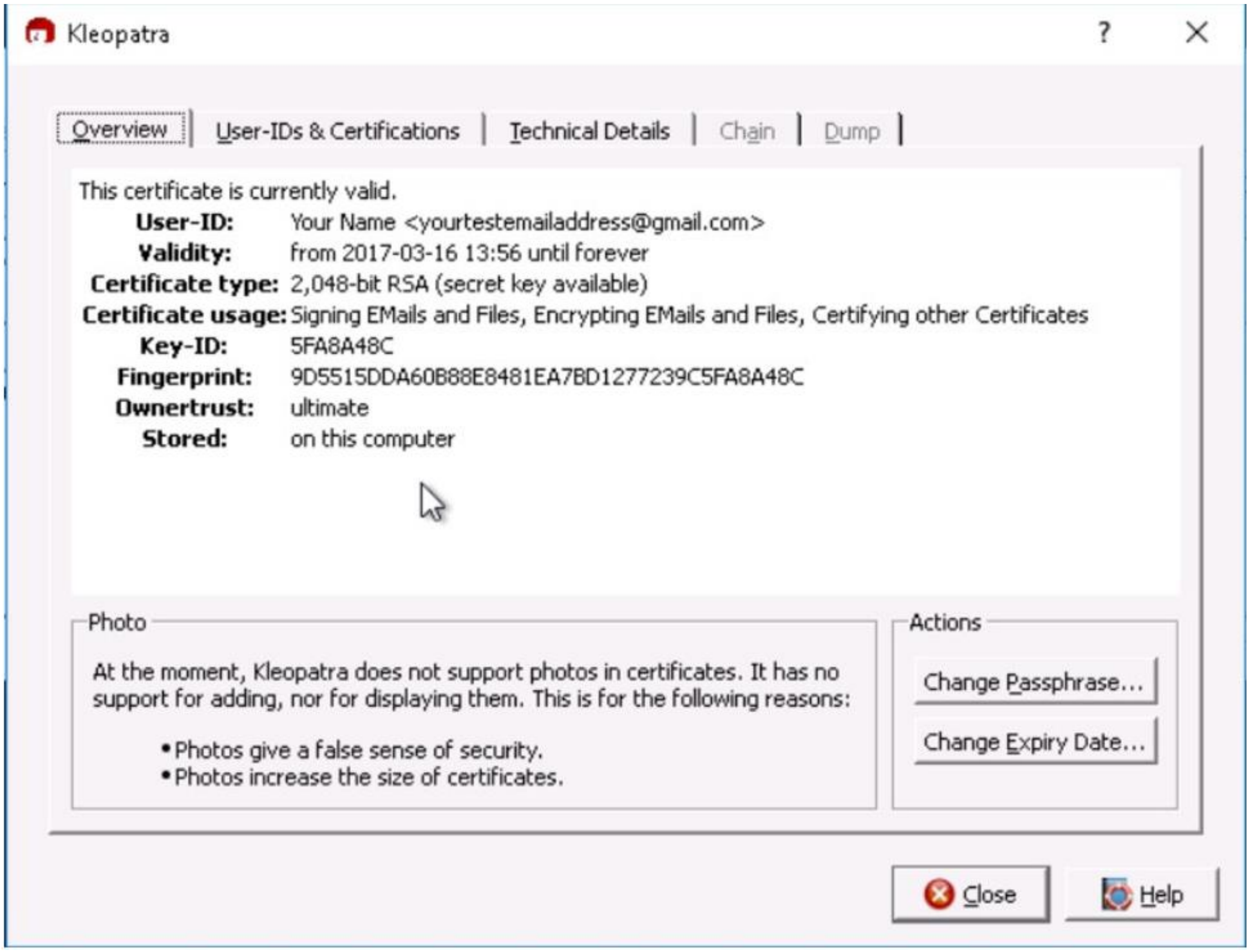
Secret key successfully exported.

Figure 16 Successful secret certificate export message

23. When prompted, **click OK** to acknowledge the export process is completed.

24. In the Kleopatra window, **double-click** the **certificate** you created to view all details related to the certificate:

    Note that the key/certificate type is RSA. Kleopatra uses both RSA (Rivest, Shamir, and Adelman encryption algorithm) and DSA (Digital Signature Algorithm) for encryption. Kleopatra uses RSA as the default encryption algorithm, but you could select DSA while you create a new certificate by clicking the Advanced Settings button on the Enter Details.



This certificate is currently valid.

**User-ID:** Your Name <yourtestemailaddress@gmail.com>
**Validity:** from 2017-03-16 13:56 until forever
**Certificate type:** 2,048-bit RSA (secret key available)
**Certificate usage:** Signing EMails and Files, Encrypting EMails and Files, Certifying other Certificates
**Key-ID:** 5FA8A48C
**Fingerprint:** 9D5515DDA60B88E8481EA7BD1277239C5FA8A48C
**Ownertrust:** ultimate
**Stored:** on this computer

At the moment, Kleopatra does not support photos in certificates. It has no support for adding, nor for displaying them. This is for the following reasons:

- Photos give a false sense of security.
- Photos increase the size of certificates.

Figure 17 Certificate details

25. **Click Close** to close the dialog box.

26. With your certificate highlighted in the Kleopatra window, **click** the **Export Certificates button** in the application’s toolbar to save a copy of your public key.

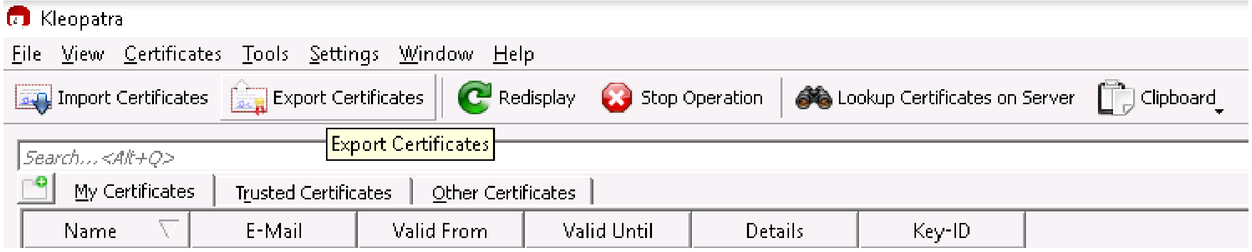
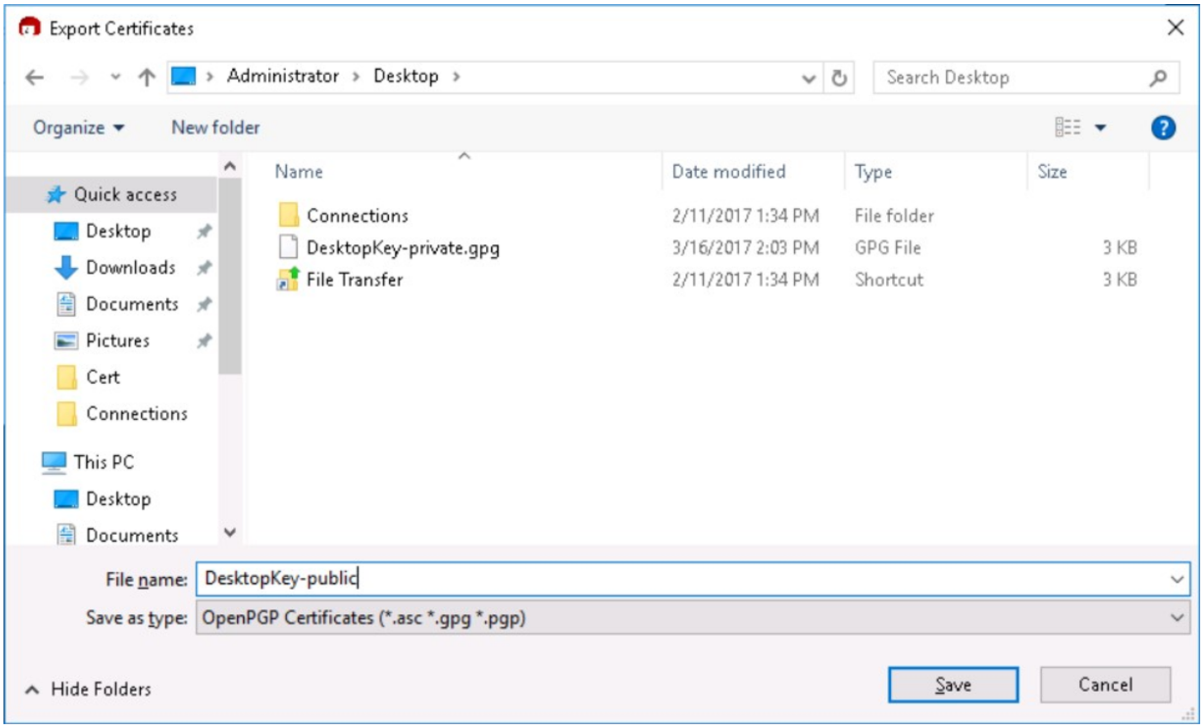


Figure 18 Export Certificates button in the application’s toolbar

27. In the Export Certificates dialog box, **navigate** to the vWorkstation desktop (**This PC > Local Disk (C:) > Users > Administrator > Desktop**), **type DesktopKey-public** in the File Name box, and **click Save** to save the public key file to the Desktop.



| Name | Date modified | Type | Size |
|---|---|---|---|
| Connections | 2/11/2017 1:34 PM | File folder | |
| DesktopKey-private.gpg | 3/16/2017 2:03 PM | GPG File | 3 KB |
| File Transfer | 2/11/2017 1:34 PM | Shortcut | 3 KB |

File name: DesktopKey-public

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

Figure 19 Export the public key

28. **Minimize** the **Kleopatra window**.

## Part 2: Create a Public and Private Key Pair for the Receiver

> **Note:** In the next steps, you will use Kleopatra to create a pair of keys on the remote TargetWindows01 desktop. You will use this key later in this lab to encrypt a file.

1. **Double-click** the **Connections folder** on the desktop.

2. **Open a remote connection** to the **TargetWindows02** machine.

   If prompted, **type** the following credentials and **click OK** to open the remote connection.

   - Username: **Administrator**
   - Password: **P@ssw0rd!**

3. On the TargetWindows02 desktop, **double-click** the **Kleopatra icon** to open the Kleopatra component of the GPG4Win application.

4. **Repeat Part 1, Steps 5-10** to create a personal OpenPGP key pair using the following information:

   - Name: **TargetWindows02**
   - Email: **TargetWindows02@vlabsolutions.com**
   - Pinentry Passphrase: **1Tsecurity!**

5. **Click Finish** to close the Certificate Creation Wizard.

6. **Repeat Part 1, Steps 19-23** to export the private key for this machine and save it to the TargetWindows02 desktop.

   Output file: **C:/Users/Administrator/Desktop/TargetWindows02-private.gpg**

7. **Repeat Part 1, Steps 26-27** to export a copy of the public key and save to the TargetWindows02 desktop.

   - File name: **TargetWindows02-public.asc**

8. **Close** the **Kleopatra window**.

## Part 3: Transfer and Import a Public Key from the Receiver

> **Note:** In the next steps, you will transfer the TargetWindows02 public key to the vWorkstation desktop and import it into Kleopatra.

1. **Click** the **Restore Down/ Minimize button** on the TargetWindows02 title bar to reduce the Connections window and display both vWorkstation and TargetWindows02 desktops.

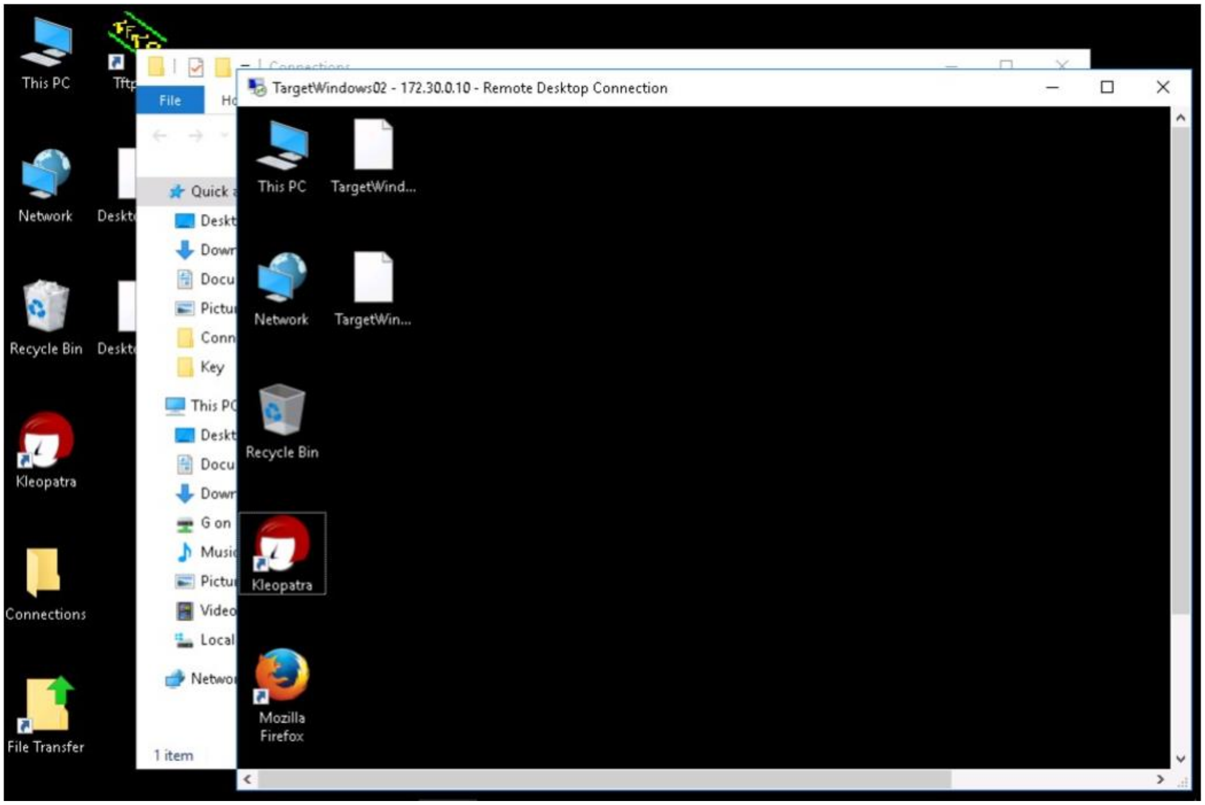


Figure 20 Display both virtual machines

2. On the vWorkstation, **close** the **Connections folder**.

   If necessary, **reposition** the **windows** so that the public and private keys for both machines are visible.

3. **Right-click** the **TargetWindows02-public.asc file** on the TargetWindows02 desktop and **copy** it to the Windows clipboard.

4. **Paste** the copied file to the vWorkstation desktop.

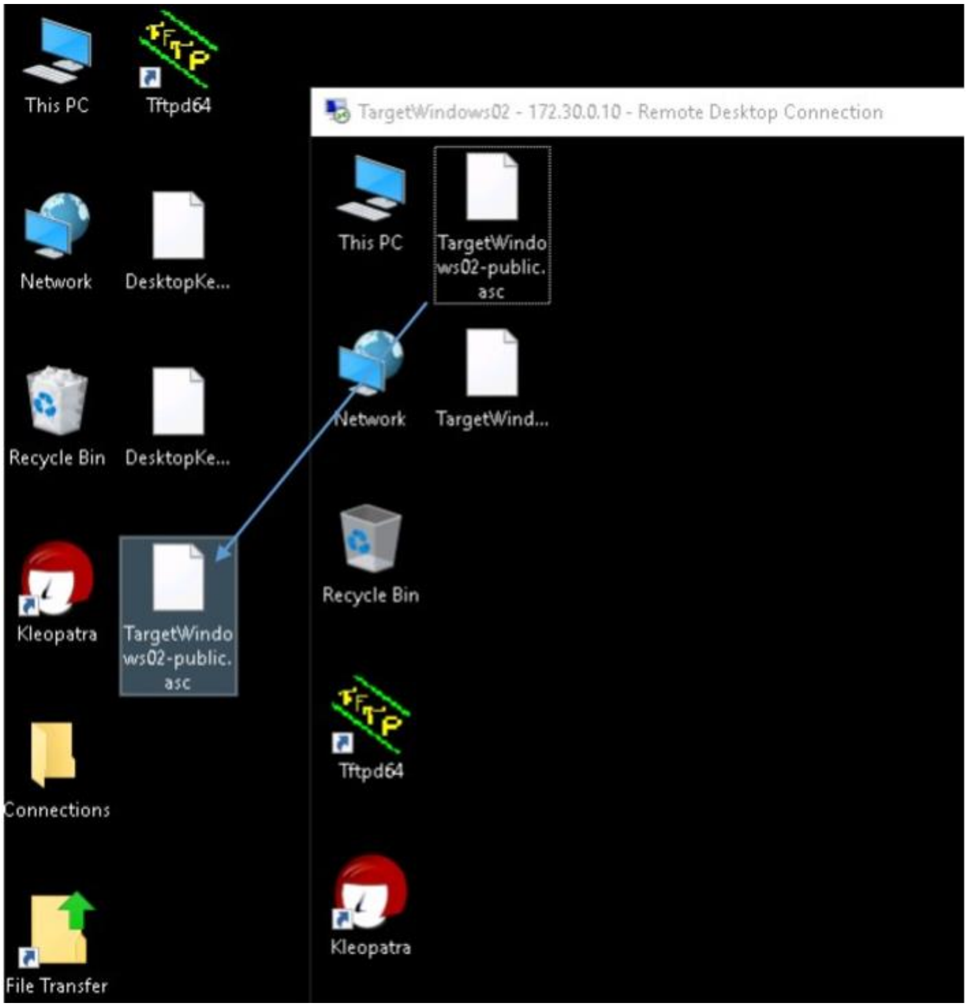


Figure 21 Transfer the public key

5. **Minimize** the **TargetWindows02 window**.

6. From the taskbar on the vWorkstation desktop, **click** the **Kleopatra icon** to re-open the application.

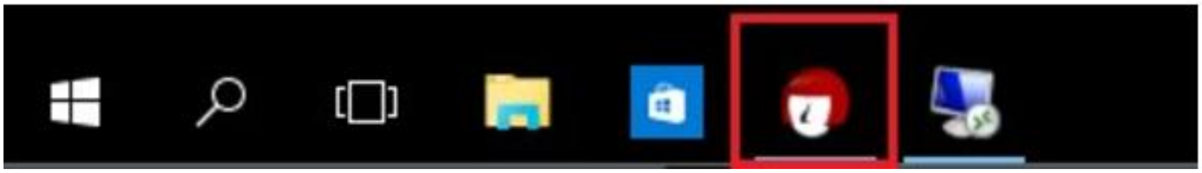
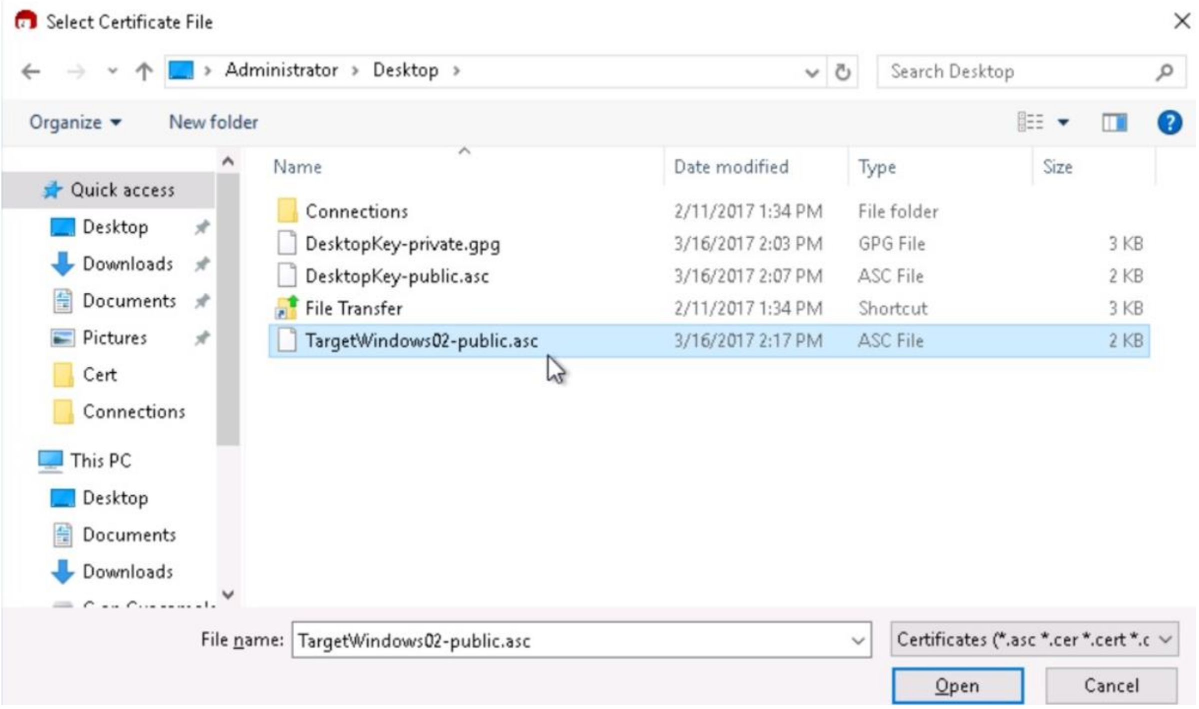


Figure 22 Kleopatra icon

7. From the Kleopatra toolbar, **click** the **Import Certificates button**.

8. In the Select Certificate File dialog box, **navigate** to the Desktop **This PC > Local Disk (C:) > Users > Administrator > Desktop**), **select** the **TargetWindows02-public.asc file**, and **click Open** to import the file.



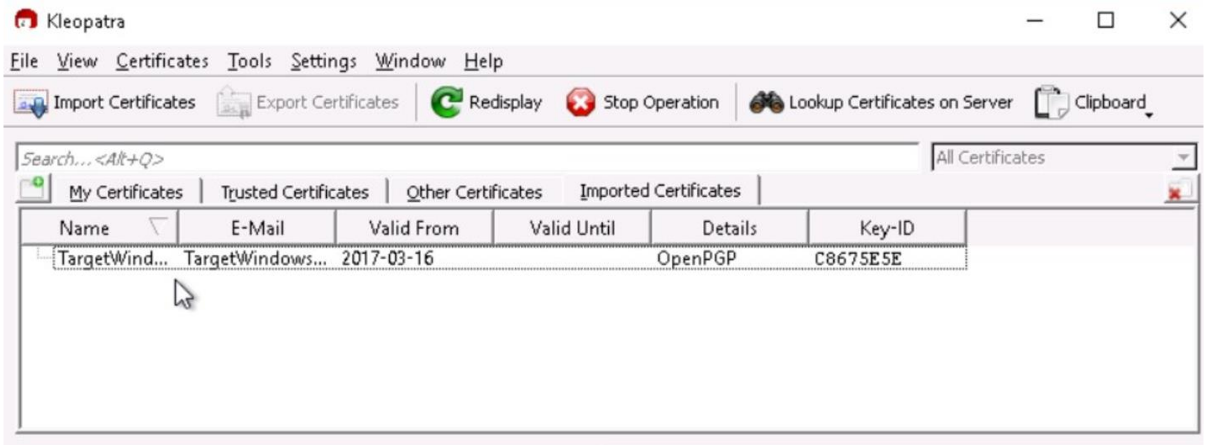
| Name | Date modified | Type | Size |
|---|---|---|---|
| Connections | 2/11/2017 1:34 PM | File folder | |
| DesktopKey-private.gpg | 3/16/2017 2:03 PM | GPG File | 3 KB |
| DesktopKey-public.asc | 3/16/2017 2:07 PM | ASC File | 2 KB |
| File Transfer | 2/11/2017 1:34 PM | Shortcut | 3 KB |
| TargetWindows02-public.asc | 3/16/2017 2:17 PM | ASC File | 2 KB |

File name: TargetWindows02-public.asc

Figure 23 Import the receiver’s public file

9. When prompted, **click OK** to close the dialog box.

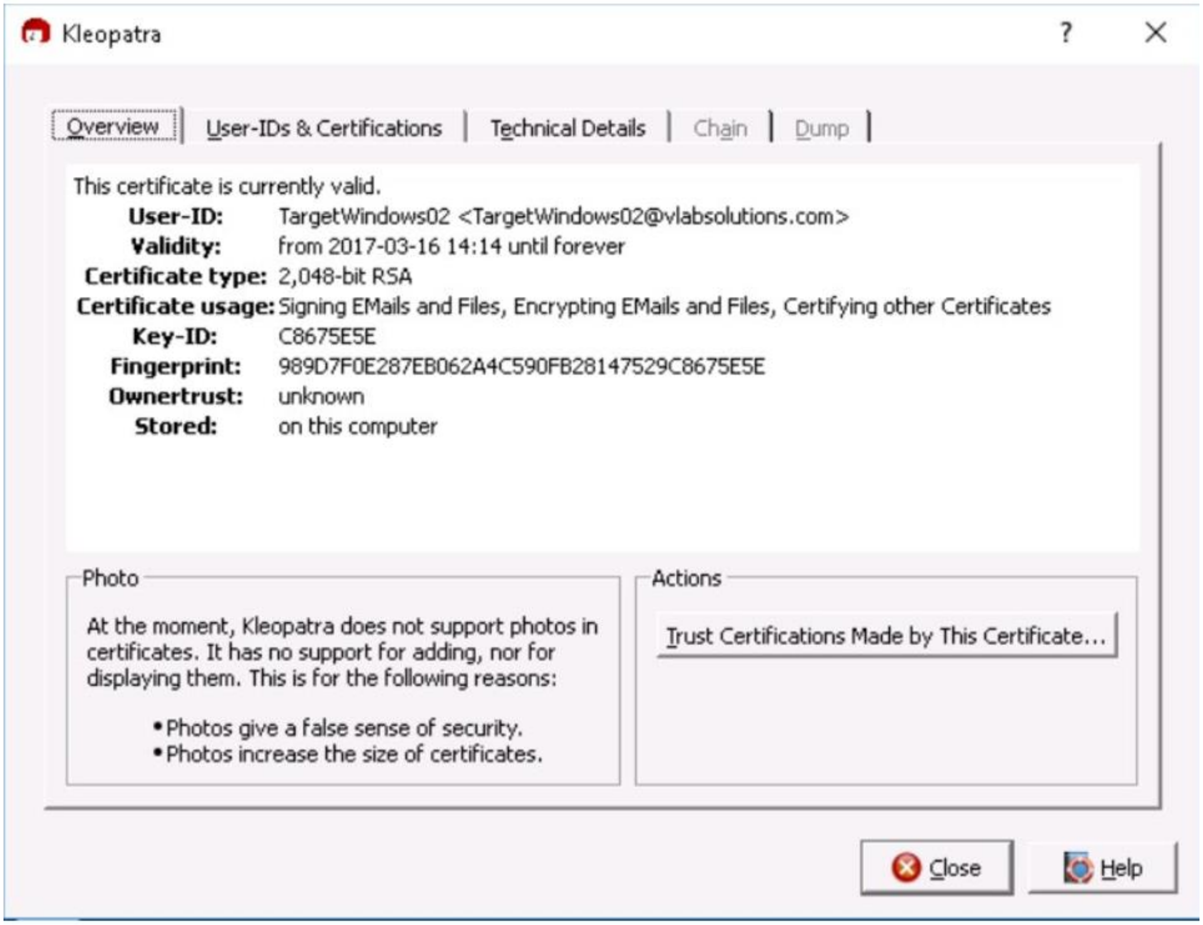
   The TargetWindows02-public.asc file is now listed as a new line item on the Imported Certificates tab of the Kleopatra application.



| Name | E-Mail | Valid From | Valid Until | Details | Key-ID |
|---|---|---|---|---|---|
| TargetWind... | TargetWindows... | 2017-03-16 | | OpenPGP | C8675E5E |

Figure 24 Imported Certificates tab

10. **Double-click** the **TargetWindows02 certificate** in Kleopatra to open the Certificate Details dialog box.


Kleopatra
Overview
User-IDs & Certifications
Technical Details
Chain
Dump
Photo
Actions
Trust Certifications Made by This Certificate...
Close
Help

This certificate is currently valid.

**User-ID:** TargetWindows02 <TargetWindows02@vlabsolutions.com>
**Validity:** from 2017-03-16 14:14 until forever
**Certificate type:** 2,048-bit RSA
**Certificate usage:** Signing EMails and Files, Encrypting EMails and Files, Certifying other Certificates
**Key-ID:** C8675E5E
**Fingerprint:** 989D7F0E287EB062A4C590FB28147529C8675E5E
**Ownertrust:** unknown
**Stored:** on this computer

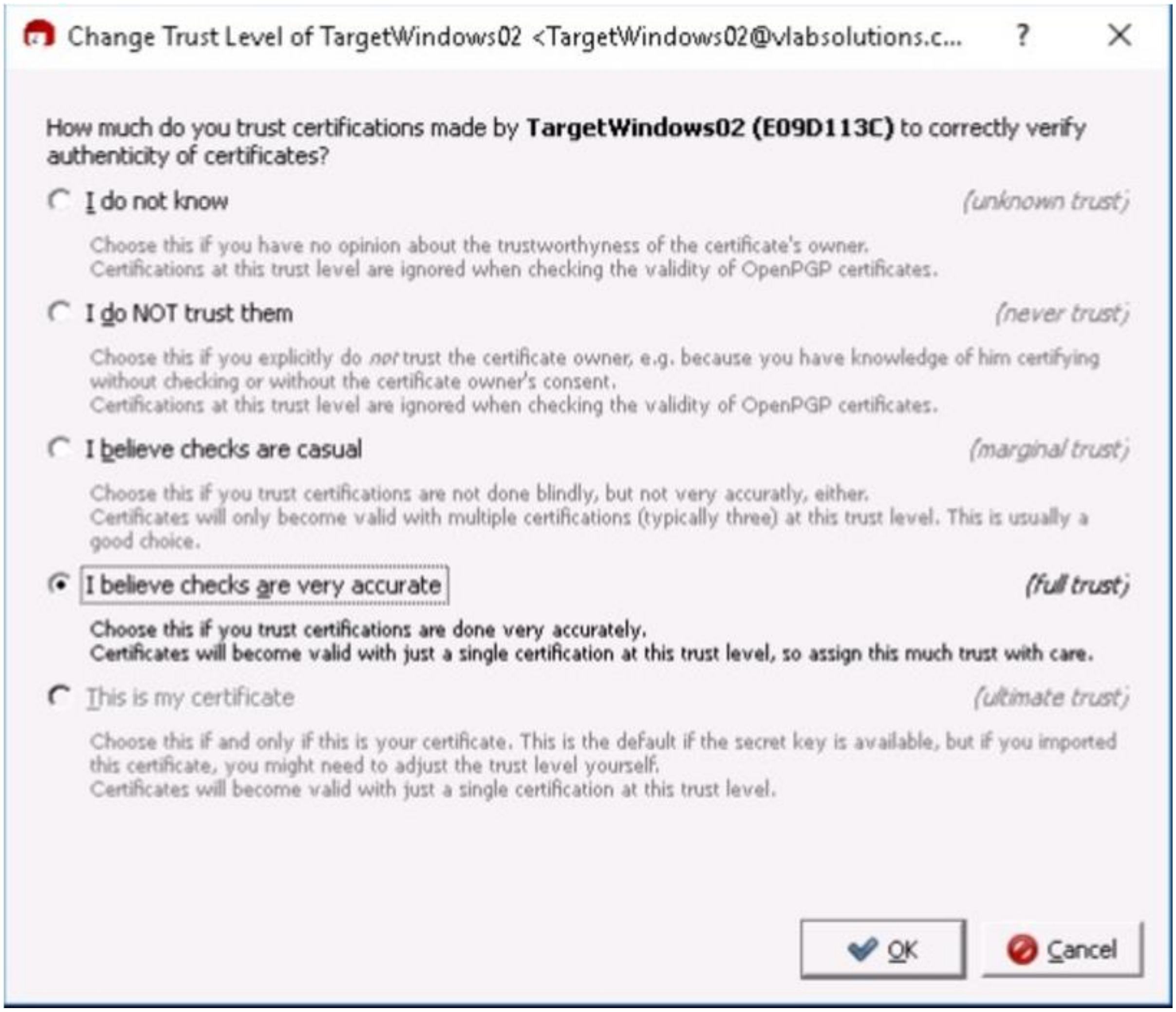
At the moment, Kleopatra does not support photos in certificates. It has no support for adding, nor for displaying them. This is for the following reasons:

- Photos give a false sense of security.
- Photos increase the size of certificates.

Figure 25 Trust Certificates button

11. **Click** the **Trust Certificates made by this Certificate button** in the Actions section of the dialog box.

12. In the Change Trust Level dialog box, **select** the **I believe checks are very accurate radio button**.



Change Trust Level of TargetWindows02 <TargetWindows02@vlabsolutions.c...

How much do you trust certifications made by **TargetWindows02 (E09D113C)** to correctly verify authenticity of certificates?

○ I do not know *(unknown trust)*

Choose this if you have no opinion about the trustworthyness of the certificate's owner.
Certifications at this trust level are ignored when checking the validity of OpenPGP certificates.

○ I do NOT trust them *(never trust)*

Choose this if you explicitly do *not* trust the certificate owner, e.g. because you have knowledge of him certifying without checking or without the certificate owner's consent.
Certifications at this trust level are ignored when checking the validity of OpenPGP certificates.

○ I believe checks are casual *(marginal trust)*

Choose this if you trust certifications are not done blindly, but not very accuratly, either.
Certificates will only become valid with multiple certifications (typically three) at this trust level. This is usually a good choice.

● I believe checks are very accurate *(full trust)*

**Choose this if you trust certifications are done very accurately.**
**Certificates will become valid with just a single certification at this trust level, so assign this much trust with care.**

○ This is my certificate *(ultimate trust)*

Choose this if and only if this is your certificate. This is the default if the secret key is available, but if you imported this certificate, you might need to adjust the trust level yourself.
Certificates will become valid with just a single certification at this trust level.

Figure 26 Confirm trust level

13. **Click OK** to close the dialog box.

14. **Click OK** when the process is complete.

15. **Click** the **Close button** to close the Certificate Details dialog box.

## Part 4: Encrypt and Decrypt a File from the Sender

> **Note:** In the next steps, you will create a file on the vWorkstation and encrypt it using the keys created earlier in this lab. You also will transfer the file to the TargetWindows02 desktop (the receiver) and decrypt it.

1. On the vWorkstation desktop, **right-click** any **empty space** and **select New > Text Document** from the context menu.

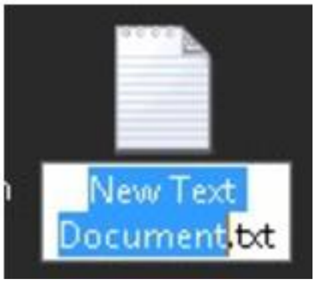
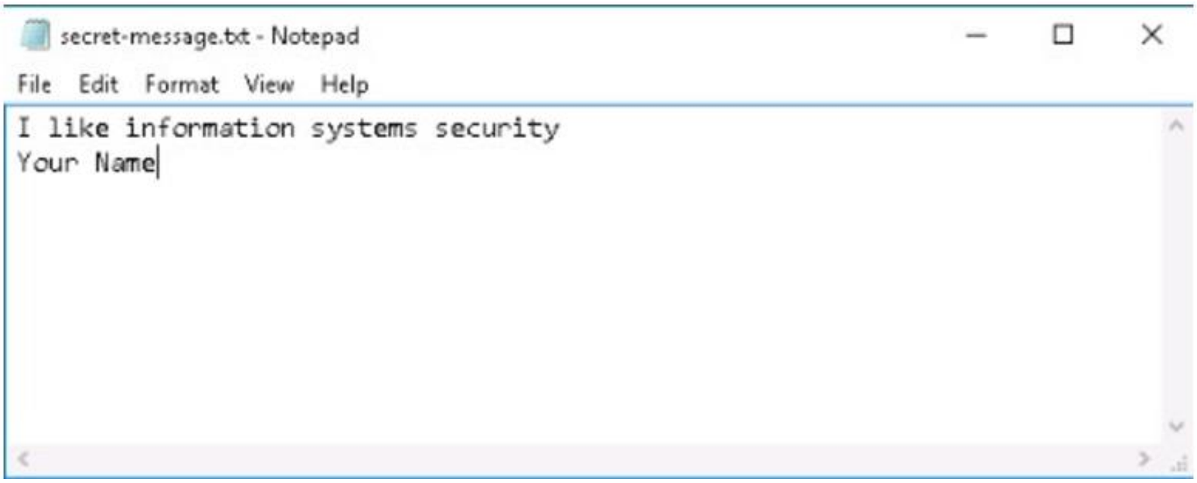


Figure 27 Create a new text document

2. With *New Text Document* highlighted, **type secret-message** and **press Enter** to name the new file.

3. **Double-click** the **secret-message.txt icon** to open the file in the text editor.

4. In the Notepad window, **type I like information systems security**, **press Enter**, and **type *Your Name***, where Your Name is your own name.



```
I like information systems security
Your Name
```

Figure 28 Create secret-message.txt

5. From the Notepad menu, **click File > Exit**, and **click Save** when prompted to save the file and close Notepad.

6. On the vWorkstation desktop, **right-click** the **secret-message.txt file** and **select Sign and Encrypt** from the context menu.

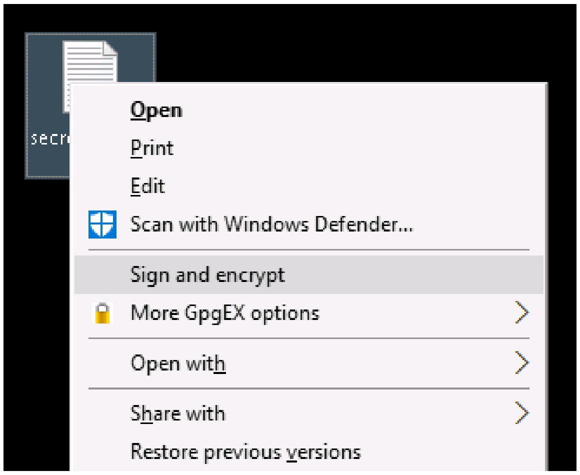
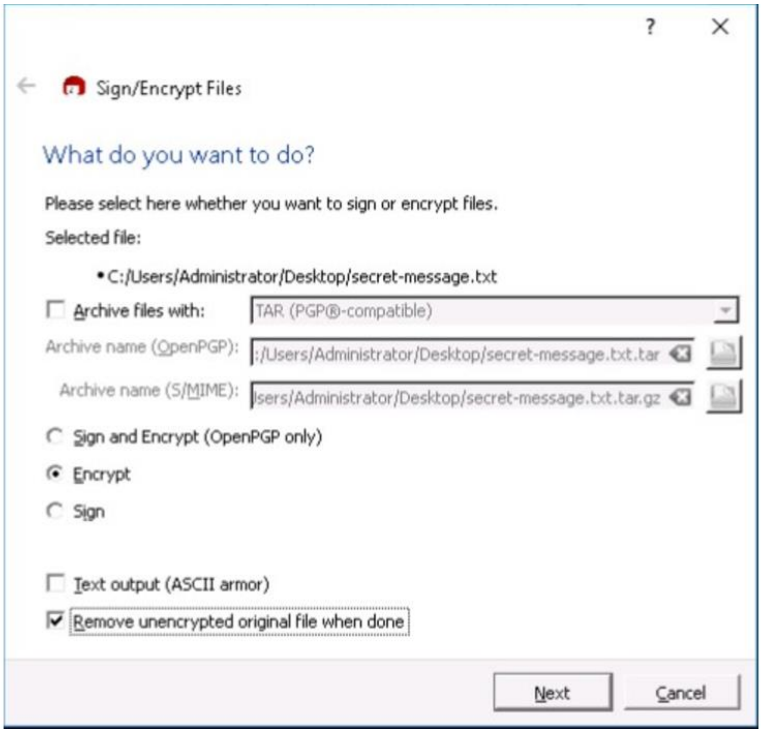


Figure 29 Sign and encrypt option

7. In the Sign/Encrypt Files dialog box, **click** the **Remove unencrypted original file when done checkbox** and **click Next** to continue.



Sign/Encrypt Files

What do you want to do?

Please select here whether you want to sign or encrypt files.

Selected file:

- C:/Users/Administrator/Desktop/secret-message.txt

□ Archive files with: TAR (PGP®-compatible)

Archive name (OpenPGP): :/Users/Administrator/Desktop/secret-message.txt.tar

Archive name (S/MIME): lsers/Administrator/Desktop/secret-message.txt.tar.gz

○ Sign and Encrypt (OpenPGP only)

● Encrypt

○ Sign

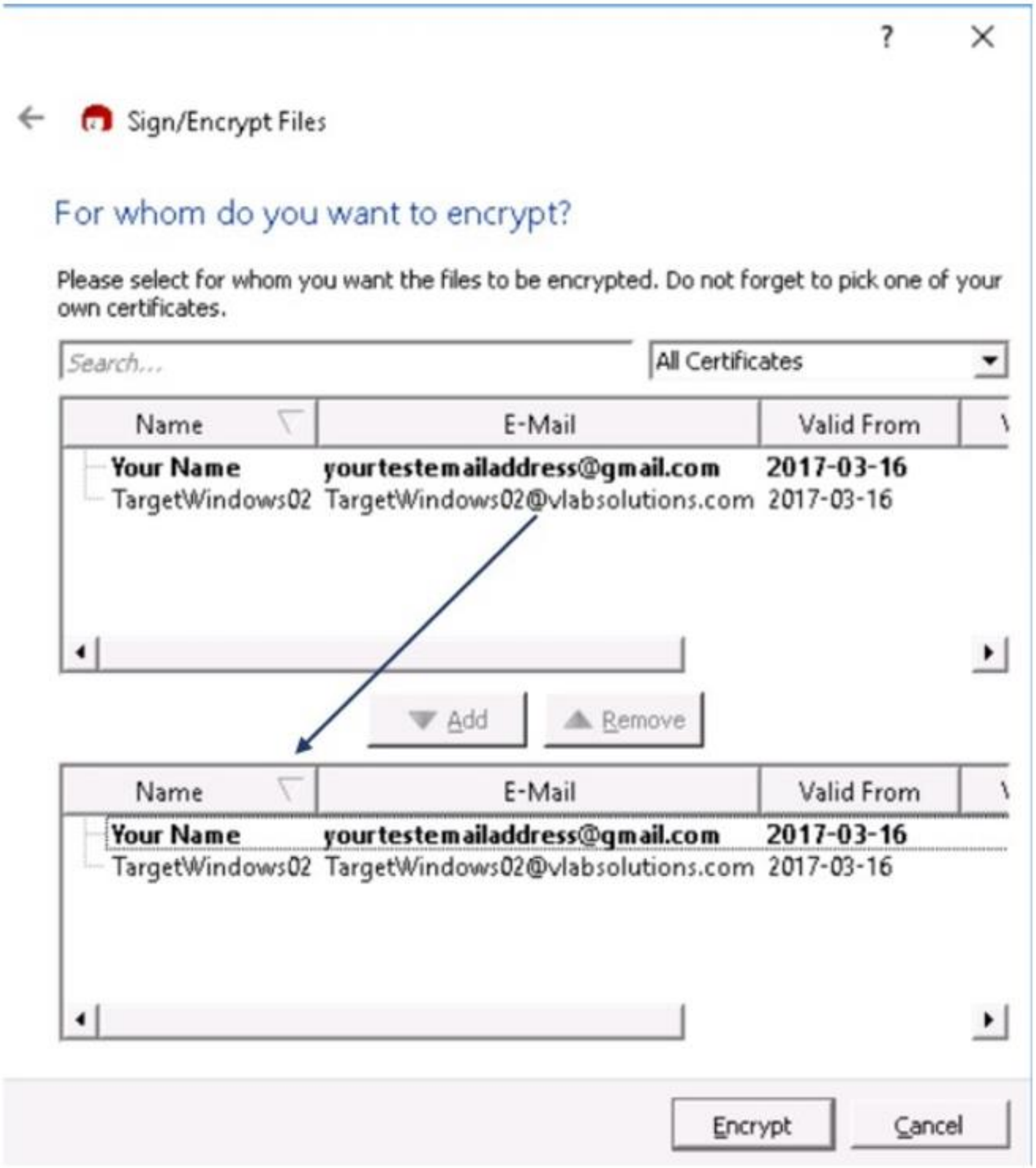
□ Text output (ASCII armor)

☑ Remove unencrypted original file when done

Figure 30 Replace the unencrypted file

8. In the Sign/Encrypt dialog box, **click** both the **TargetWindows02** certificate and the **personal** certificate that you created in Part 1 of this lab, and then **click** the **Add button**.

   Selecting both certificates will tell Kleopatra to use the TargetWindows02 (receiver's) public key and your (sender's) private key to encrypt the message. Adding both keys will allow both the sender and the receiver to decrypt the file.



Sign/Encrypt Files

For whom do you want to encrypt?

Please select for whom you want the files to be encrypted. Do not forget to pick one of your own certificates.

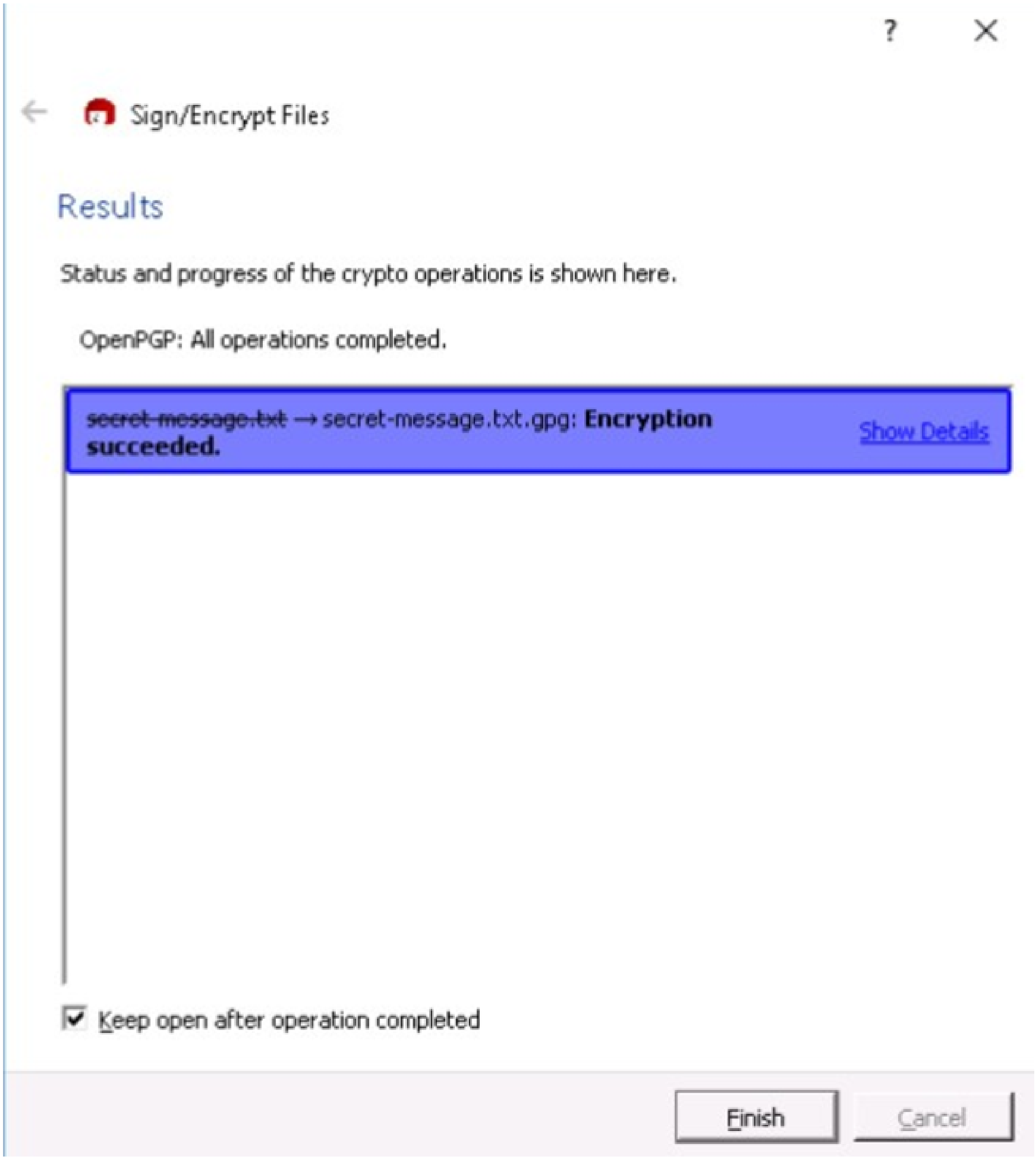
| Name | E-Mail | Valid From |
|---|---|---|
| **Your Name** | **yourtestemailaddress@gmail.com** | **2017-03-16** |
| TargetWindows02 | TargetWindows02@vlabsolutions.com | 2017-03-16 |

| Name | E-Mail | Valid From |
|---|---|---|
| **Your Name** | **yourtestemailaddress@gmail.com** | **2017-03-16** |
| TargetWindows02 | TargetWindows02@vlabsolutions.com | 2017-03-16 |

Figure 31 Add sender's and receiver's certificates

9. **Click** the **Encrypt button** to continue.

   When the secret-message.txt is successfully encrypted, Kleopatra will delete the original file and replace it with an encrypted (.gpg) file: secret-messsage.txt.gpg.



Results

Status and progress of the crypto operations is shown here.

OpenPGP: All operations completed.

~~secret-message.txt~~ → secret-message.txt.gpg: **Encryption succeeded.**

☑ Keep open after operation completed

Figure 32 Successful encryption

10. **Click Finish**.

11. **Close** the **Kleopatra window**.

**Note:** In the next steps, you will upload the encrypted secret-message.txt.gpg file from the vWorkstation to TargetWindows02.

12. On the vWorkstation desktop, **right-click** the **secret-message.txt.gpg file** and **select Copy** from the shortcut menu.

13. **Restore** the **TargetWindows02 connection**.

14. **Paste** the copied file to the TargetWindows02 desktop.

**Note:** In the next steps, you will decrypt the file you just transferred. You can verify that integrity of encrypted files is maintained during transmission by comparing the decrypted file's contents with the file you created earlier in the lab. You will then make a screen capture of the successful file decryption for use as a deliverable in this lab.

15. **Maximize** the **TargetWindows02 window**.

16. On the TargetWindows02 desktop, **right-click** the **secret-message.txt.gpg file** and **select Decrypt and verify** from the context menu.

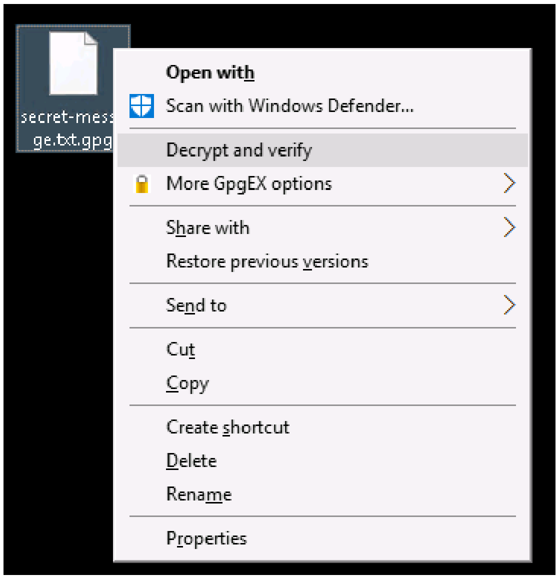


Figure 33 Decrypt and verify

17. **Click** the **Decrypt/Verify button** at the bottom of the Decrypt/Verify Files dialog box.

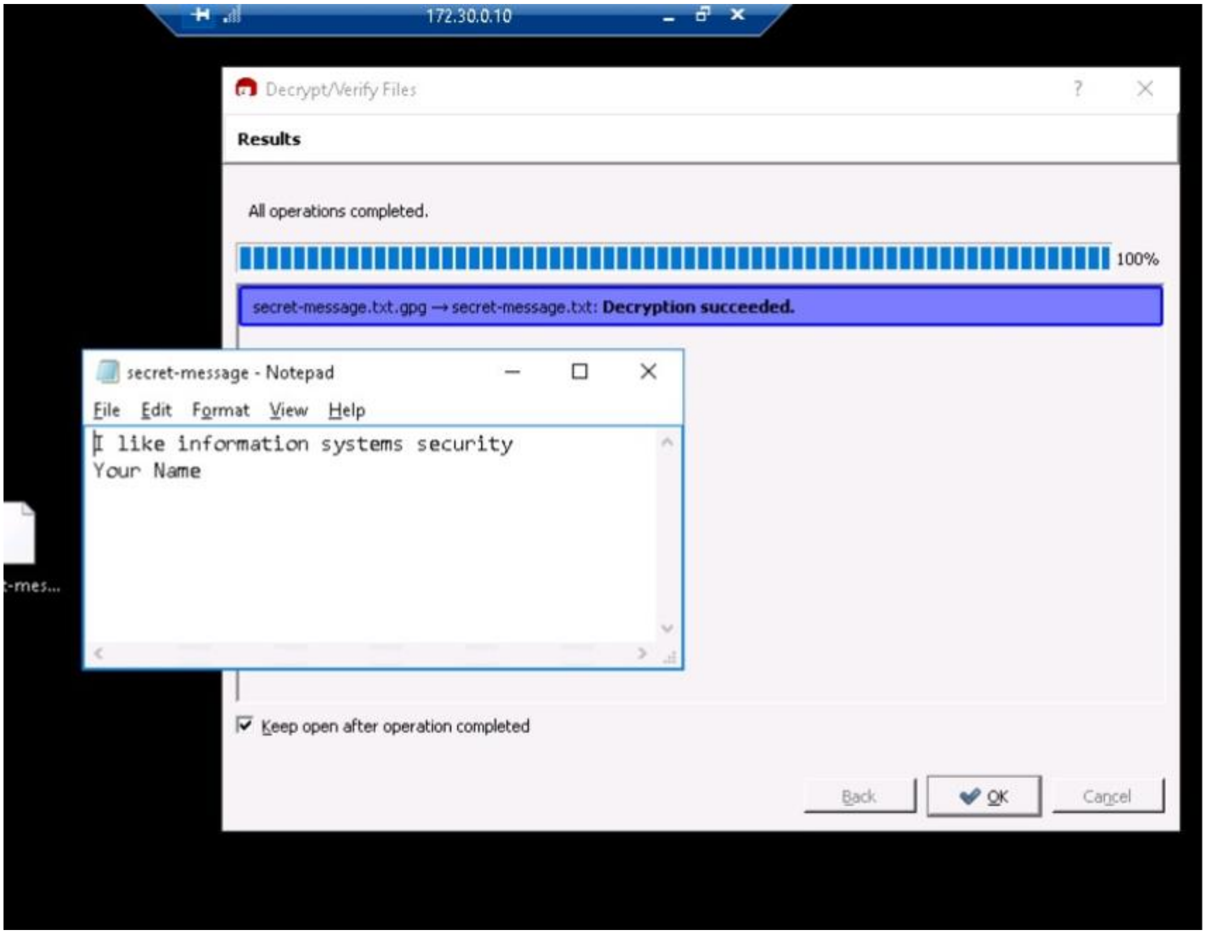
18. When prompted, **type 1Tsecurity!** (the passphrase you used when you created the encryption file) and **click OK**.

Do not close the dialog box.

19. **Reposition** the **Decrypt/Verify Files dialog box** so that both the original encrypted file and the new secret-message.txt file are visible.

20. **Double-click** the newly decrypted **secret-message.txt** to open the file in Notepad.

21. **Reposition** the **open windows** so that the Decrypt/Verify Results window and the decrypted secret-message.txt file in Notepad are visible.



All operations completed.

100%

secret-message.txt.gpg → secret-message.txt: **Decryption succeeded.**

```
I like information systems security
Your Name
```

☑ Keep open after operation completed

Figure 34 Decrypted message

22. **Make a screen capture** showing the **Kleopatra decryption results window, the secret-message.txt file in Notepad**, and the **TargetWindows02 title bar**, and **paste** it into the Lab Report.

23. **Close** any **open windows**.

24. **Close** the **remote TargetWindows02 connection**.

**Note:** This completes Section 1 of this lab. In the next steps, you will use the File Transfer folder to move any files from the vWorkstation to your local system that are to be submitted as part of your lab deliverables. Refer to the instructions in the Common Lab Tasks document for more information on how to use this function.

25. On the vWorkstation desktop, **drag and drop** the following files into the File Transfer folder to complete the download to your local computer.

    - **secret-message.txt.gpg**

## Part 5: Challenge Question

1. What is the difference and tradeoffs between X.509 and PGP certificate types? (Discuss them in 200 words.)