

Before You Begin

Welcome! The Virtual Security Cloud Labs are your opportunity to gain valuable hands-on experience with professional-grade tools and techniques as you work through the guided lab exercises provided in the on-screen lab manual. The use of virtualization enables you to perform all of the tasks in the lab manual in a live environment without putting your personal device or institution's assets at risk.

Before you begin the guided lab exercises, please review the following preparation checklist.

1. **Run the [System Checker](#).** The System Checker will confirm that your browser and network connection are ready to support virtual labs.
2. **Review the [Common Lab Tasks document](#).** This document provides an overview of the virtual lab environment and outlines several of the recurring tasks you may need to complete your lab exercise.
3. **When you've finished, use the Disconnect button to end your session and create a StateSave.** To end your lab session and save your work, click the Disconnect button in the upper-right corner of the Lab View toolbar. When prompted, assign a name for your StateSave (we recommend using the Section, Part, and Step number where you stopped) and click Continue. Please note that a StateSave will preserve any changes written to disk in your lab session. A StateSave will not preserve any open windows or active processes, similar to restarting your computer.
If you close your browser window without disconnecting, your lab session will automatically end after 5 minutes.
4. **[Technical Support](#) is here to help!** Our technical support team is available 24/7 to help troubleshoot common issues.
Please note that the 24/7 support team is Level 1 only, and cannot assist with questions about lab content or the array of software used in the labs. If you believe you've identified an error in the lab guide or a problem with the lab environment, your ticket will be escalated to the Jones & Bartlett Learning product team for review. In the meantime, we recommend resetting the lab (Options > Reset) or reaching out to your instructor for assistance.

Introduction

As computers, tablets, phones and other “always on” digital devices become increasingly interconnected through unsecure public networks, threats against our privacy and digital security increase in kind. Threats like identity theft and credit fraud threaten our financial security. Digital stalking and online harassment threaten our physical and emotional security. Some suggest that digital surveillance, mass data collection, and data mining by government and commercial entities encroach on our right to free speech, our freedom of association, and our Constitutional protections against unlawful search and seizure.

The need to protect confidential and private information over “public” networks is an ancient one. The solution then, as now, is to encode private data using cryptography. Simply put, cryptography takes human readable information and makes it unreadable “cipher text” which can only be read if one possesses the correct key. Generally speaking, there are three cryptographic standards: symmetric cryptography, asymmetric cryptography, and hybrid cryptography.

With symmetric cryptography the sender and receiver use the same key (or “shared secret”) to encrypt and decrypt a given message. Symmetric cryptography is quite fast and generally easier to implement than asymmetric cryptography. However, while symmetric cryptography does provide confidentiality and integrity, it does not guarantee authenticity. In other words, you do not know for certain who gave you the encrypted message.

With asymmetrical encryption, the receiver has two keys: a private key and a public key. The sender encrypts the message with the receiver’s public key, and the receiver decrypts the message with their private key. While asymmetrical encryption is slower and more complex than symmetrical encryption, it does guarantee the authenticity of the sender.

The hybrid approach is to have the sender encrypt the message with a symmetric key, and then send the message and a copy of the symmetric key using the recipient’s asymmetric public key. The initial message and symmetric key are decrypted using the recipient’s public key, and subsequent messages are then decrypted quickly using the symmetric key. The hybrid approach provides the same full CIA protection as asymmetrical encryption with nearly the same speed as symmetrical encryption.

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 using the receiver’s copy of the keys.

Learning Objectives

Upon completing this lab, you will be able to:

1. Apply the concepts of common cryptographic and encryption techniques to ensure

confidentiality

2. Understand public and private key pairs and basic asymmetric cryptography
3. Generate a public and private key pair
4. Upload a certificate to Directory Services server on the internet
5. Encrypt a data message using a public and private key pair
6. Decrypt a data message using a public and private key pair

Lab Overview

Each section of this lab is assigned at your instructor's discretion. Please consult your instructor to confirm which sections you are required to complete for your lab assignment.

SECTION 1 of this lab has four parts, which should be completed in the order specified.

1. In the first part of the lab, you will create a public and private key pair for the senders account on the vWorkstation 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 vWorkstation desktop using the receiver's public key and the sender's private key, send it to the remote machine, and then decrypt the file.

Using Encryption to Enhance Confidentiality and Integrity

Fundamentals of Information Systems Security, Third Edition - Lab 07

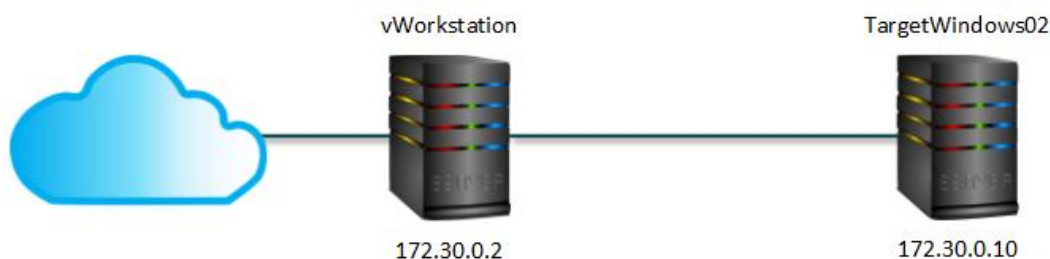
SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will import a new public key and decrypt a file found in the lab.

Finally, you will explore the virtual environment on your own in **SECTION 3** of this lab. You will answer questions and complete challenges that allow you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

Topology

This lab contains the following virtual devices. Please refer to the network topology diagram below.

- vWorkstation (Windows Server 2016)
- TargetWindows02 (Windows Server 2016)



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)

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

SECTION 1:

1. Lab Report file including screen captures of the following;

- the fingerprint generated by the key creation process;
- your name and email address in the Certificate Server Certificate Lookup dialog box;
- the Kleopatra decryption results window and the secret-message.txt file in Notepad;

2. Files downloaded from the virtual environment:

- Secret-message.txt.gpg;

3. Any additional information as directed by the lab:

- none;

4. Lab Assessment (worksheet or quiz - see instructor for guidance)

SECTION 2:

1. Lab Report file including screen captures of the following:

- the fingerprint generated by the key creation process;

- your name and email address in the Certificate Server Certificate Lookup dialog box;
- the Certificate Details dialog box for the imported certificate;
- the successfully decrypted file;

2. Files downloaded from the virtual environment:

- Secure_reply.txt.gpg;
- SC-PublicKey.asc;

3. Any additional information as directed by the lab:

- none.

SECTION 3:

1. Analysis and Discussion
2. Tools and Commands
3. Challenge Exercise

Section 1: Hands-On Demonstration

Note: In this section of the lab, you will follow a step-by-step walk-through of the objectives for this lab to produce the expected deliverable(s).

1. On your local computer, **create** the **Lab Report file**.

Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.

2. **Proceed** with **Part 1**.

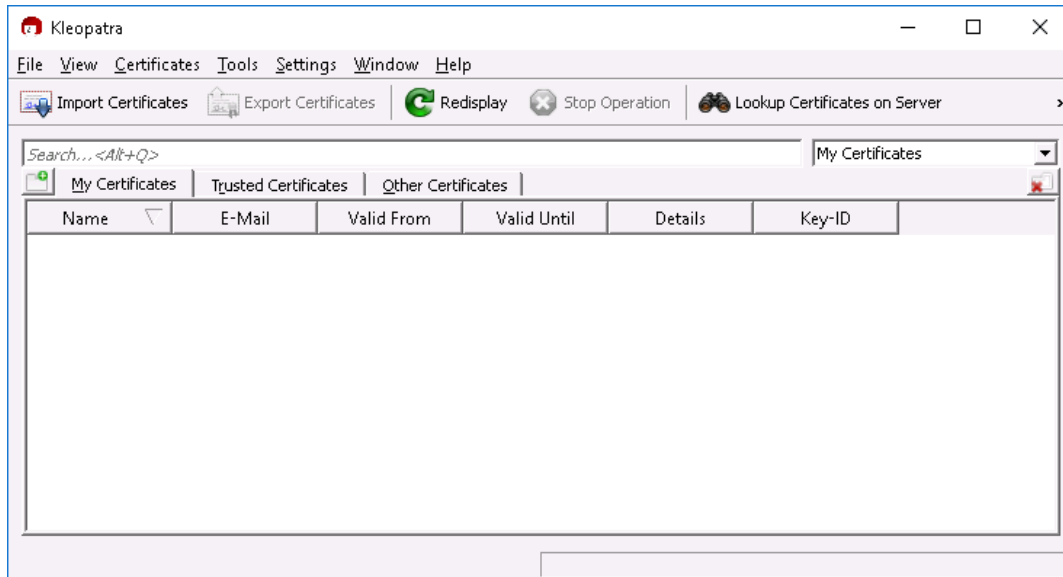
Part 1: Create a Public and Private Key Pair for the Sender

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 encrypt files, which you can then decrypt with your own private key. You only need to provide your public key, never your private key.

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

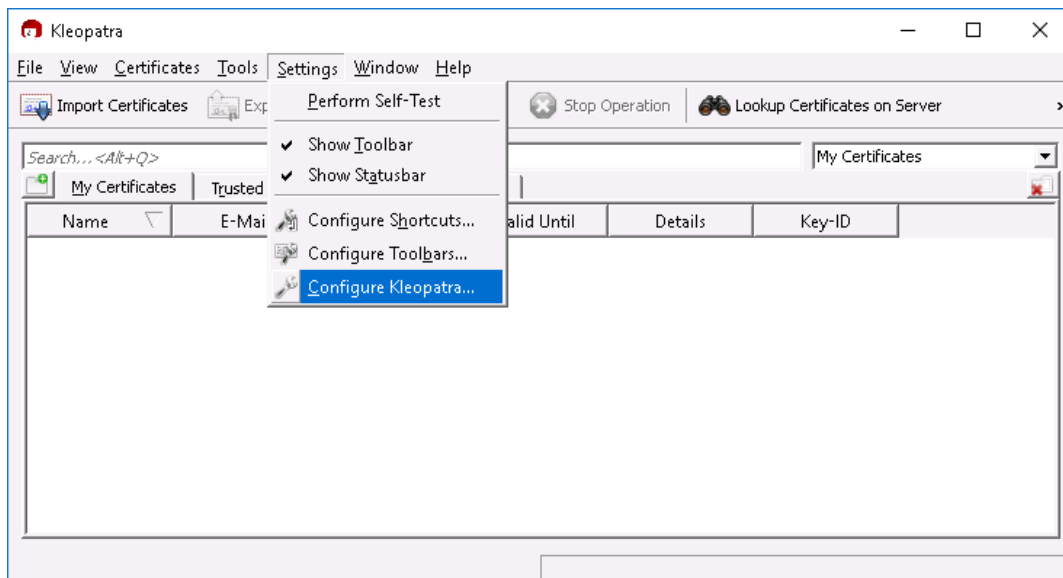
Using Encryption to Enhance Confidentiality and Integrity

Fundamentals of Information Systems Security, Third Edition - Lab 07



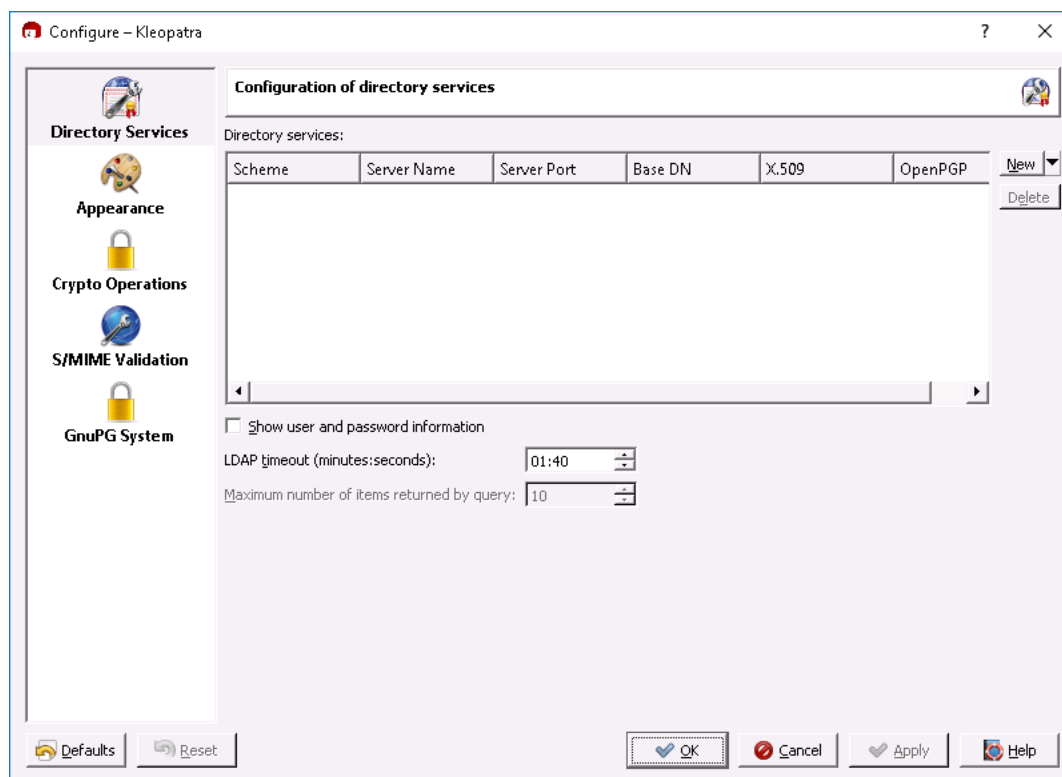
Kleopatra window

2. From the Kleopatra menu bar, **click Settings** and **select Configure Kleopatra** to open the Configure - Kleopatra window.



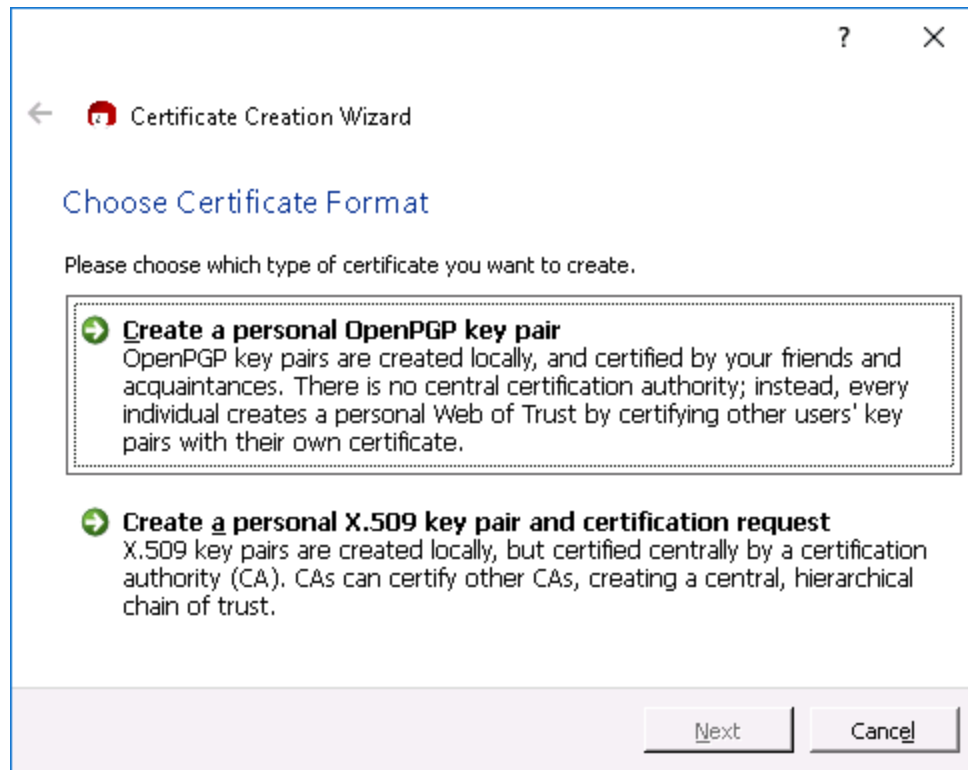
Configure Kleopatra

3. In the Configure - Kleopatra window, **click the New button** in the top right corner to add a new directory services server.



Add directory services

4. In the Configure - Kleopatra window, **click OK** to accept the default server name, keys.gnupg.net, and close the window.
5. From the Kleopatra menu bar, **click File** and **select New Certificate** to open the Certificate Creation Wizard.
6. In the Certificate Creation Wizard, **click the Create a personal OpenPGP key pair** option.



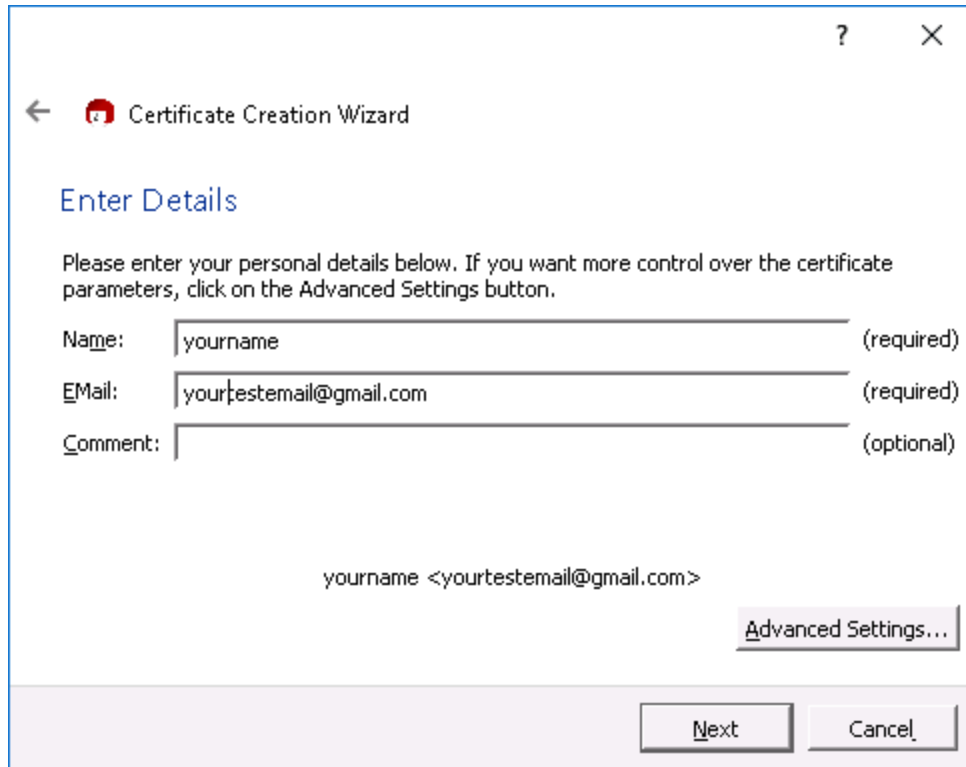
Create a new certificate using Kleopatra

7. At the Enter Details screen, **type** the following information, replacing the placeholder text with your own information, then **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.



The screenshot shows a window titled "Certificate Creation Wizard" with a back arrow and a help icon. The main heading is "Enter Details". Below it, a message says: "Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button." There are three input fields: "Name:" with the text "yourname" and "(required)" to its right; "EMail:" with the text "yourtestemail@gmail.com" and "(required)" to its right; and "Comment:" which is empty and has "(optional)" to its right. Below these fields, the text "yourname <yourtestemail@gmail.com>" is displayed. To the right of this text is a button labeled "Advanced Settings...". At the bottom right of the window are two buttons: "Next" and "Cancel".

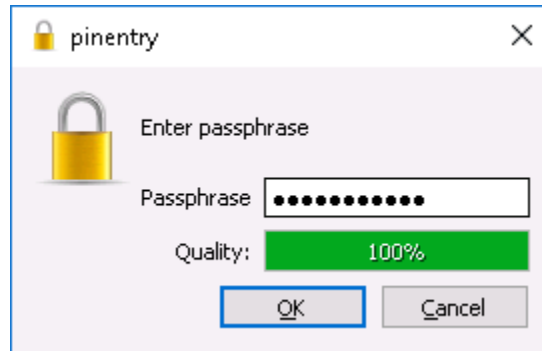
Enter certificate details

8. In the Certificate Creation Wizard, **click** the **Create Key** button.

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*.

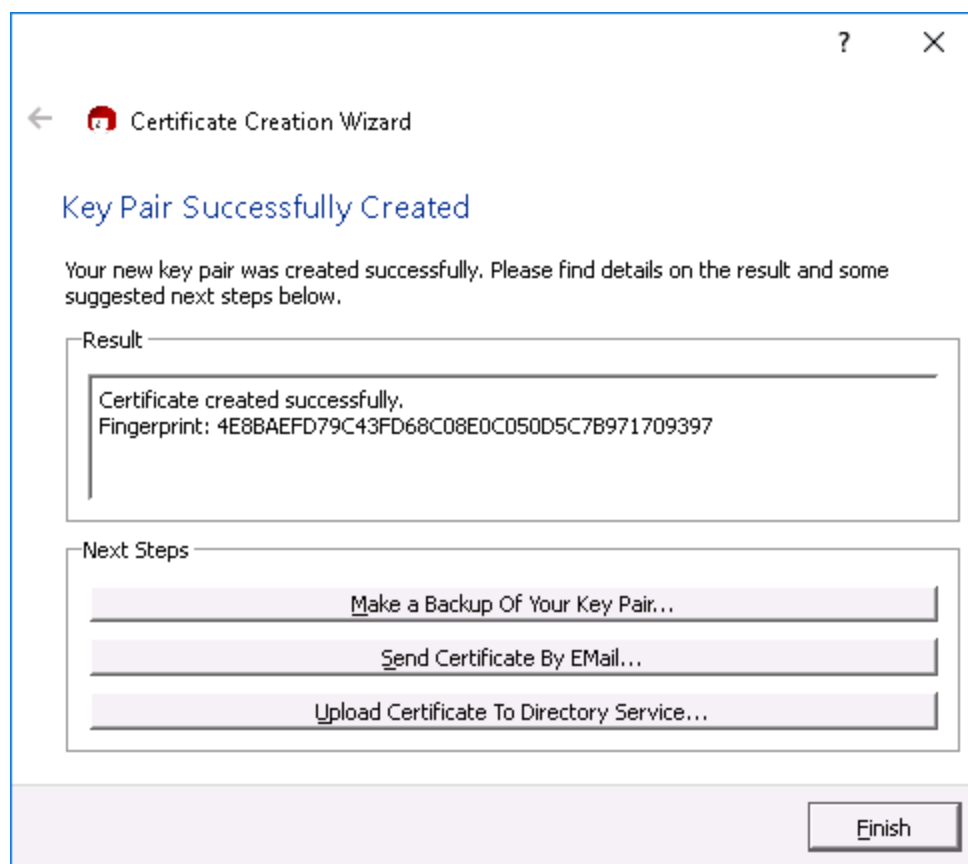


Create a passphrase for the new certificate

10. When prompted to enter the passphrase again, **type 1Tsecurity!** 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.



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. In the Certificate Creation Wizard, **click** the **Upload Certificate to Directory Service** button, then **click Continue** to ignore the warning message.

Please note that the key management server used in this lab exercise is a public directory server, and is known to periodically produce an error message when attempting to export a certificate. If you receive an error message at this step, **click OK** and **repeat step 12**.

If the issue persists, **close** the **Certificate Creation Wizard** and **skip** to **Step 19**. In place of the screen capture required at Step 17, **make a screen capture** of the **Export error**.



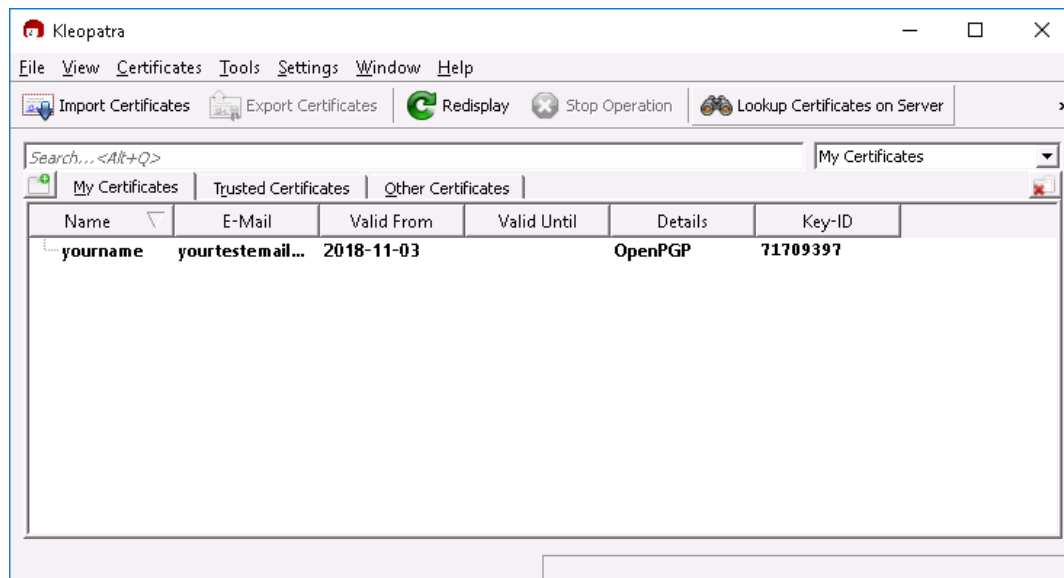
Kleopatra warning message

13. When prompted, **click OK** acknowledge the export process was successful.

14. In the Certificate Creation Wizard, **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. On the Kleopatra toolbar, **click the Lookup Certificate on Server button** to open the Certificate Server Certificate Lookup window and verify the certificate.

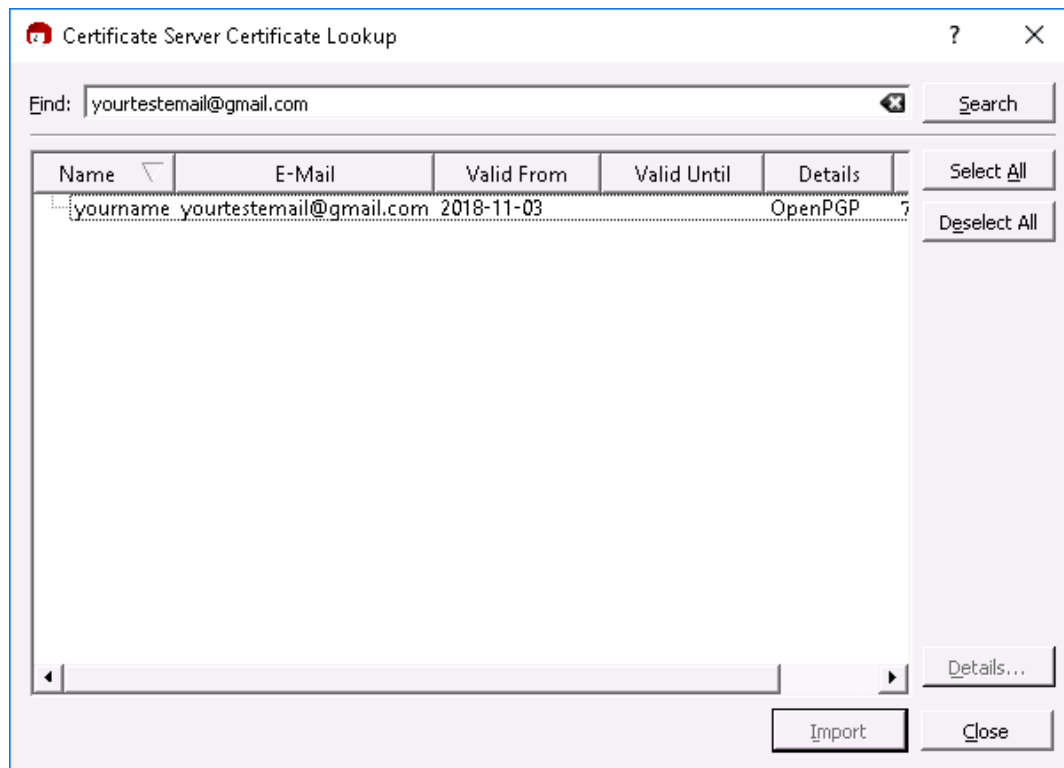


Verify certificate

16. In Certificate Server Certificate Lookup window, in the Find box, **type** the **test email address** you used to create the certificate, then **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.

Remember that this is a Public Directory server, and is not part of the JBL lab environment. If your test email address does not show up after several minutes, we recommend closing the lab, creating a StateSave, waiting an hour and trying again. Please note that because this server is external to the JBL lab environment, Technical Support will not be able to assist with issues related to searching for your certificate.

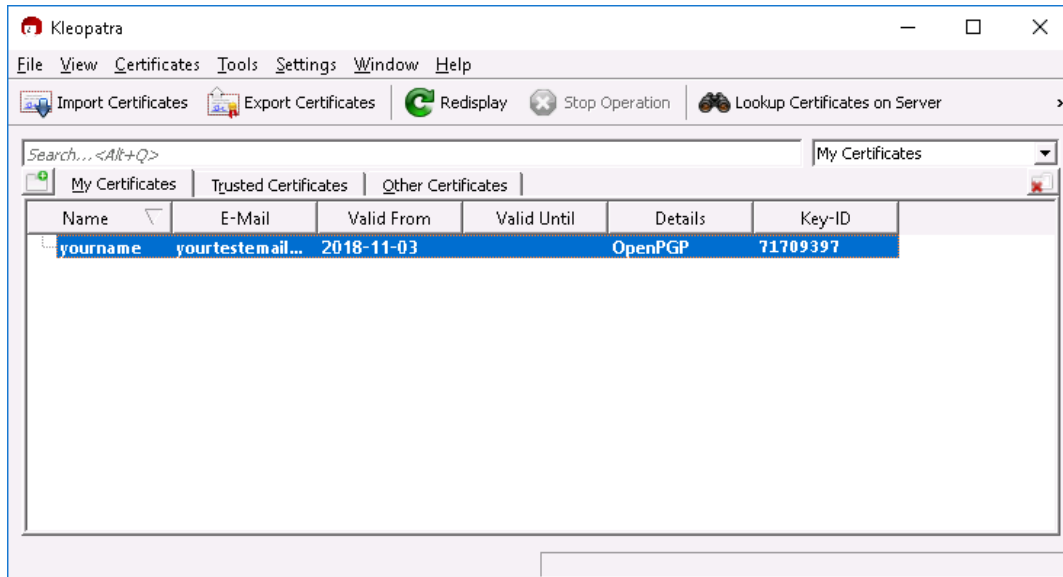


Certificate search

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. In Certificate Server Certificate Lookup window, **click Close** to close the window.
19. In the Kleopatra window, **click your newly created certificate** to select it.

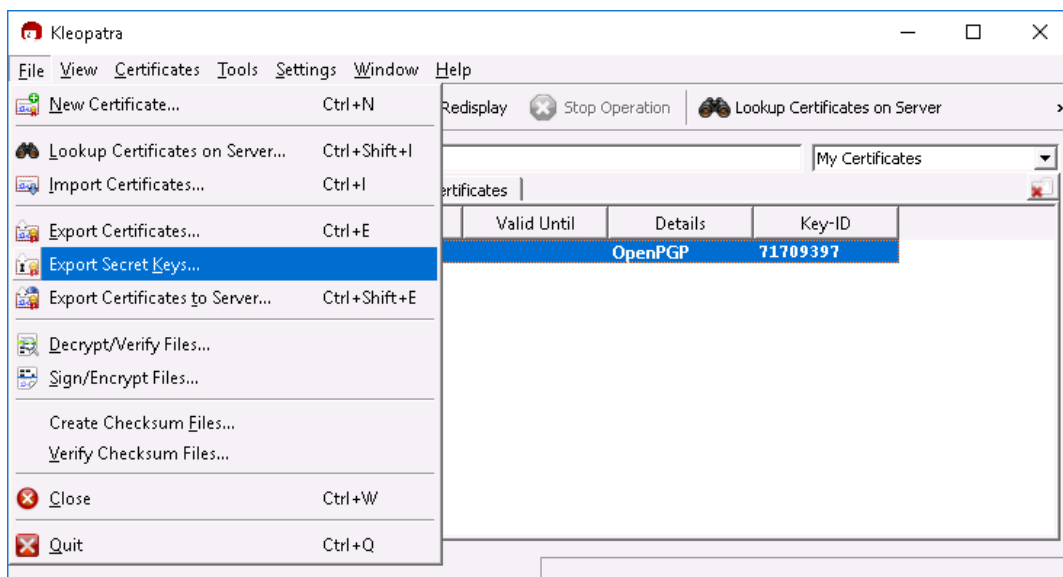
Using Encryption to Enhance Confidentiality and Integrity

Fundamentals of Information Systems Security, Third Edition - Lab 07



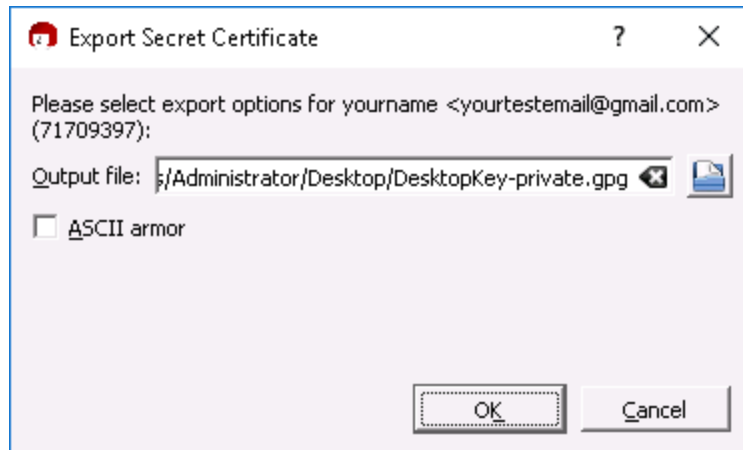
Certificate preview

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



Export certificate

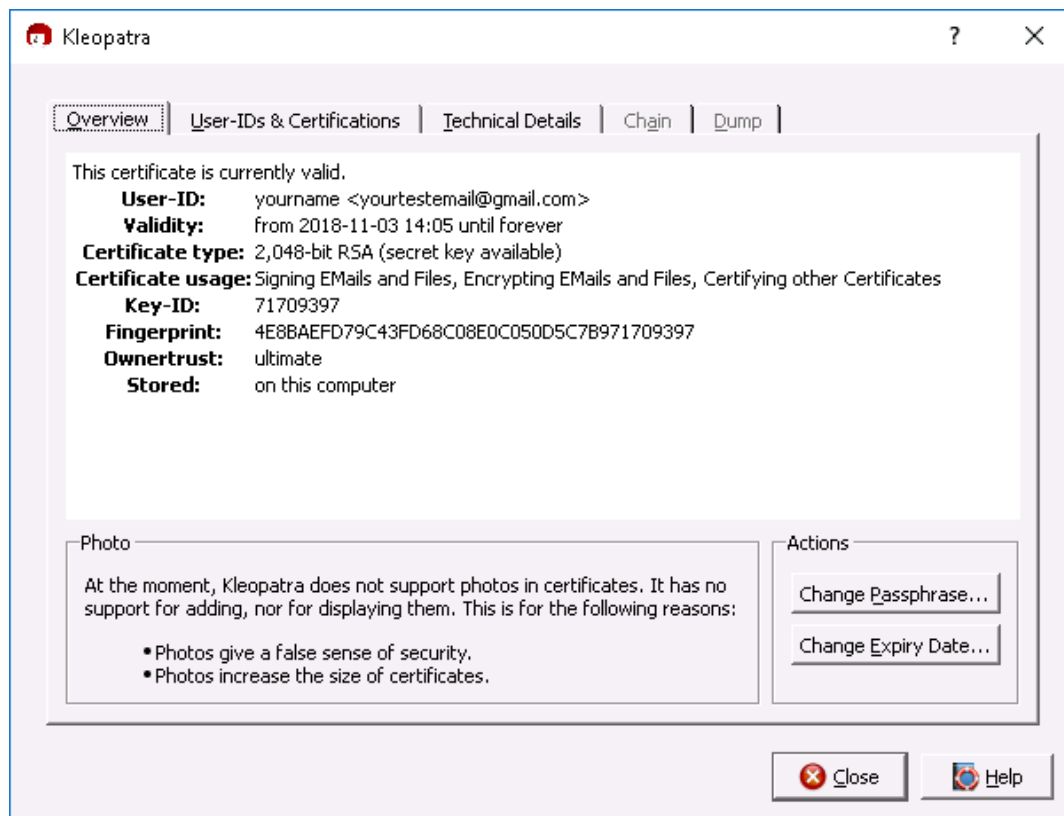
21. In the Export Secret Certificate dialog box, **click** the **Browse** button to open the Save As dialog box, then **navigate** to the vWorkstation desktop (**This PC > Users > Administrator > Desktop**), **type** **DesktopKey-private** in the File Name box, and **click** **Save** to return to the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



Export Secret Certificate

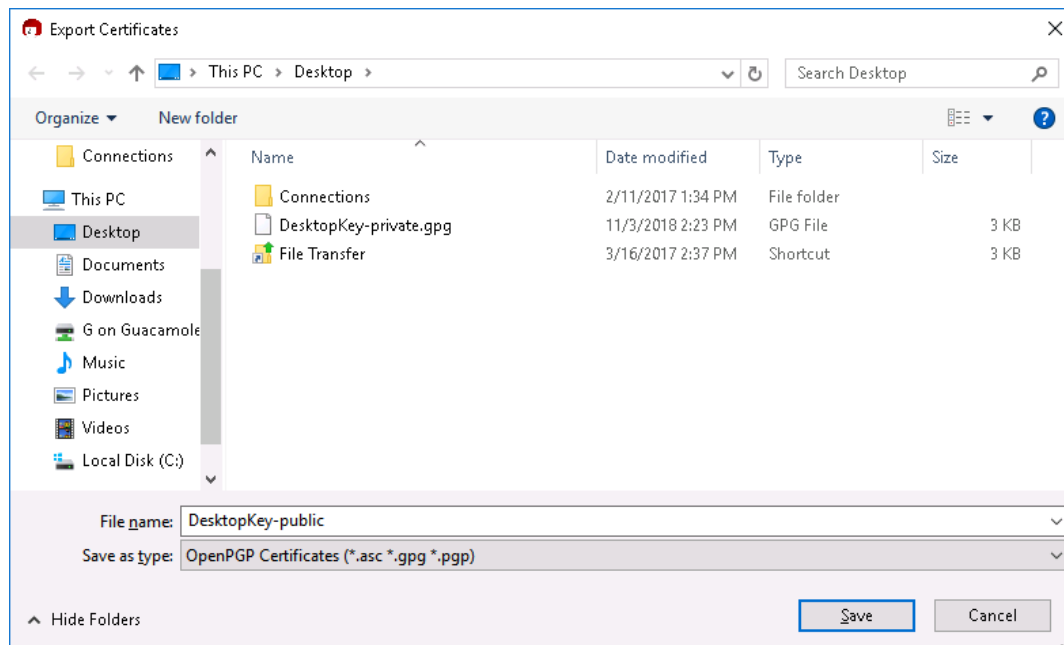
22. In the Export Secret Certificate dialog box, **click** **OK** to save a copy of your private key and close the dialog box.
23. When prompted, **click** **OK** to acknowledge the export process is completed.
24. In the Kleopatra window, **double-click** the **certificate** you created to view all details related to the certificate:

Note that the key 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 when creating a new certificate by clicking the Advanced Settings button on the Enter Details.



Certificate details

25. In the Certificate details window, **click Close** to close the window.
26. In the Kleopatra window, with your certificate highlighted, **click the Export Certificates button** on the Kleopatra toolbar to save a copy of your public key.



Export the public key

27. **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 set of keys on the remote TargetWindows02 desktop. You will use this key later in this lab to encrypt a file.

1. On the vWorkstation desktop, **double-click** the **Connections folder**.
2. In the Connections folder, **double-click** the **TargetWindows02 RDP shortcut** to open a remote connection to the TargetWindows02 machine.

If prompted, **type** the following credentials and **click OK**.

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

The remote desktop opens with the IP address of TargetWindows02 (172.30.0.10) in the title bar at the top of the window.

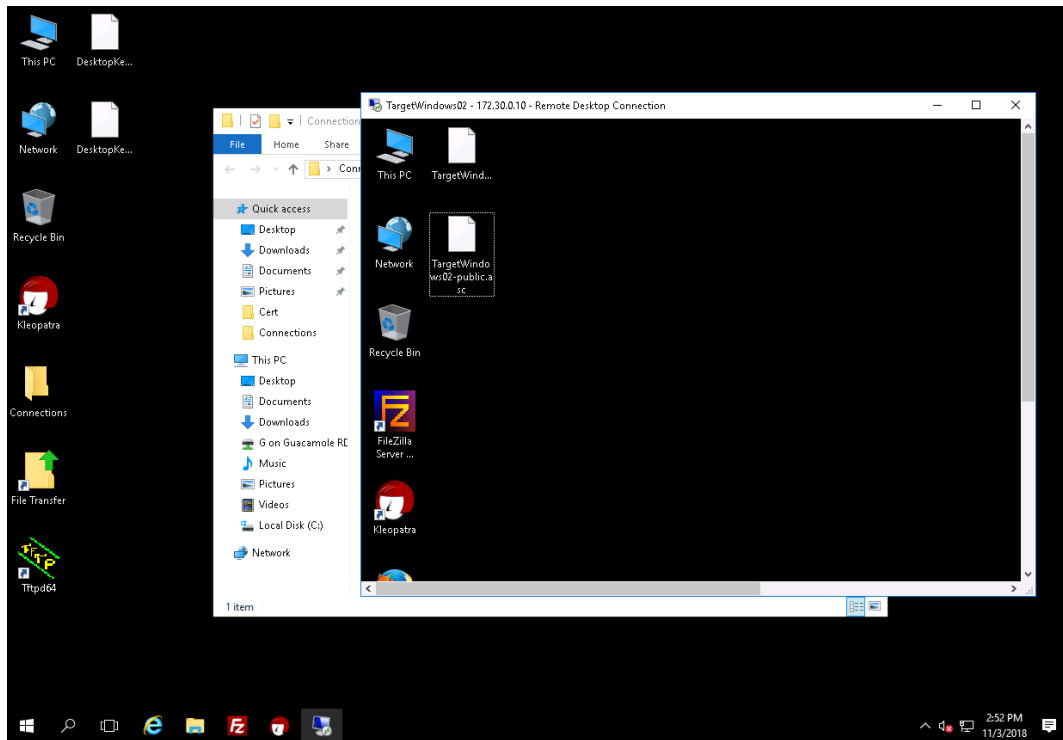
3. On the TargetWindows02 desktop, **double-click** the **Kleopatra icon** to open the Kleopatra component of the GPG4Win application.
4. **Repeat Part 1, Steps 5-10** to create a personal OpenPGP key pair using the following information:
 - Name: **TargetWindows02**
 - EMail: **TargetWindows02@securelabsondemand.com**
 - Pinentry Passphrase: **1Tsecurity!**
5. When the key pair has been successfully created, **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.
 - File name: **TargetWindows02-private.gpg**
7. **Repeat Part 1, Steps 26-27** to export a copy of the public key and save it 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. On the TargetWindows02 RDP title bar, **click** the **Restore down button** to reduce the size of

the remote connection window and display both vWorkstation and TargetWindows02 desktops.

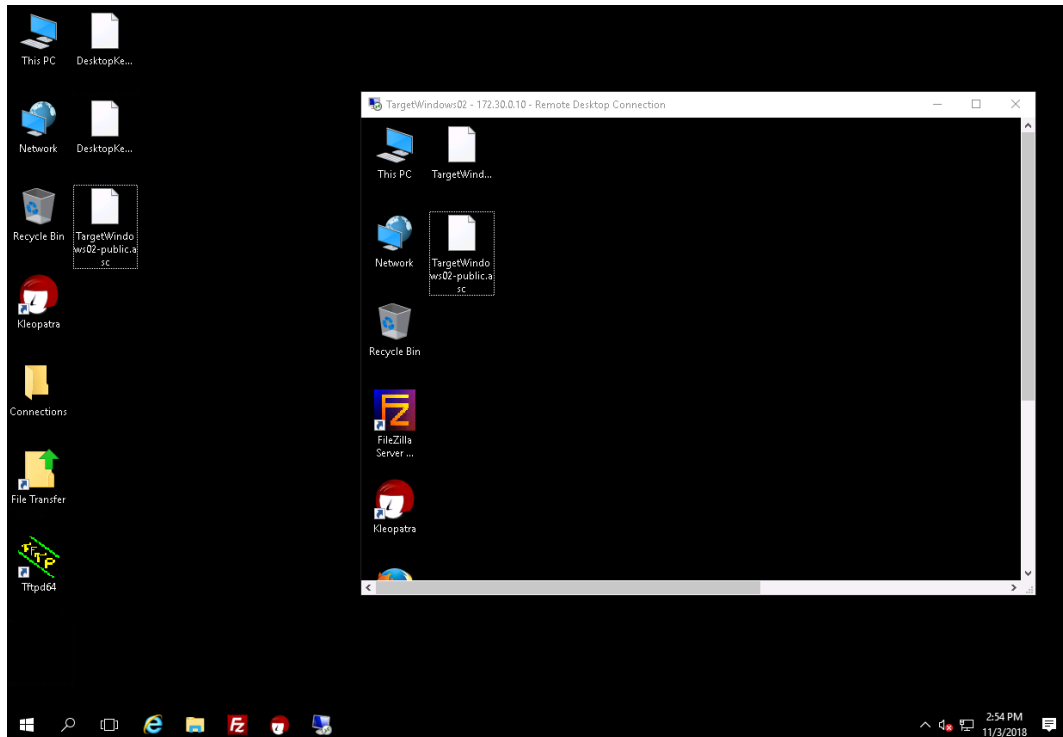


Display both virtual machines

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

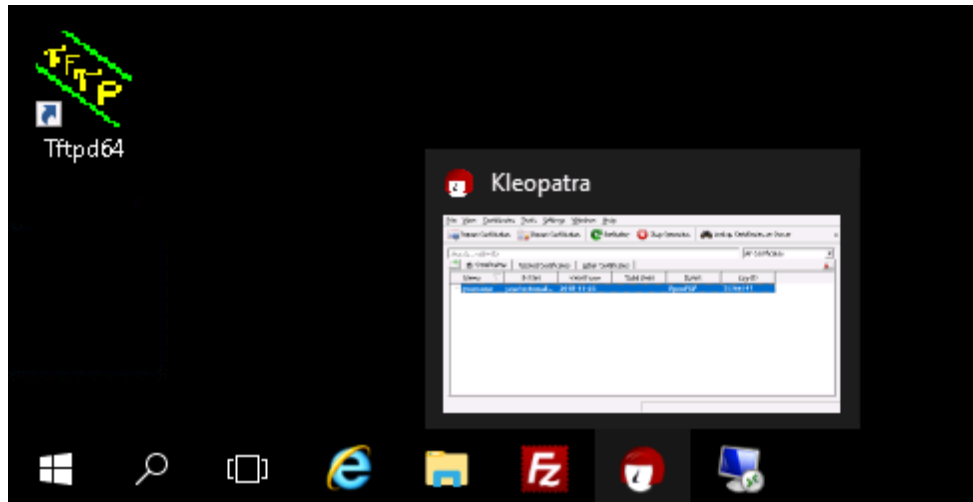
If necessary, **reposition** the **windows** so that the public and private keys for both machines are visible.

3. On the TargetWindows02 desktop, **right-click** the **TargetWindows02-public.asc** file and **select Copy** from the context menu to copy it to the Windows clipboard.
4. On the vWorkstation desktop, **right-click** any empty space and **select Paste** from the context menu to copy the file to the vWorkstation desktop.



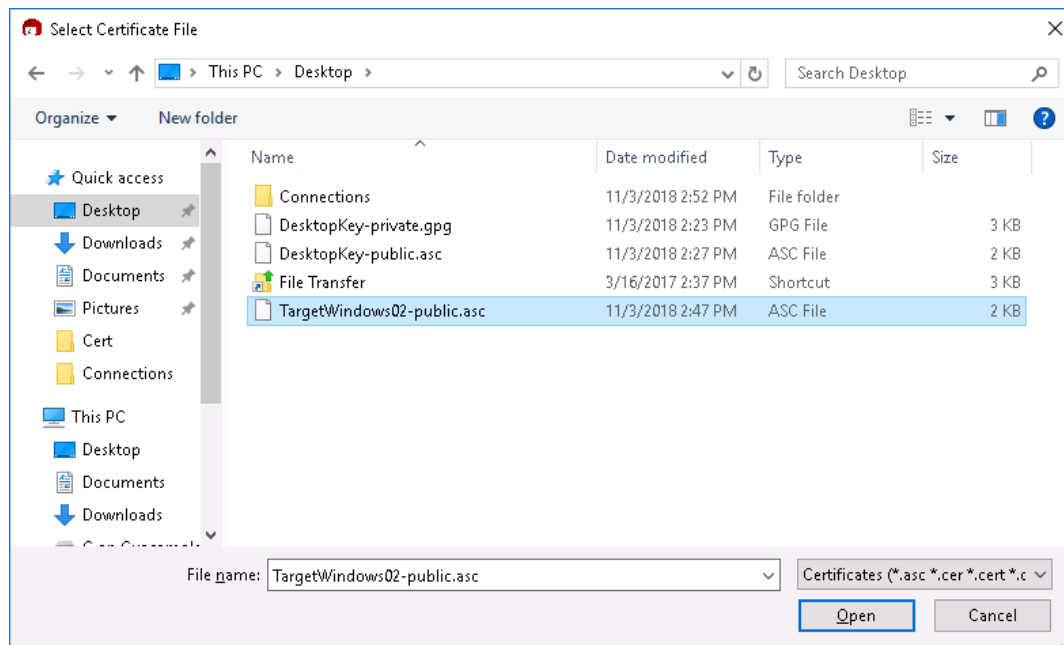
Transfer the public key

5. **Minimize** the **remote TargetWindows02 connection**.
6. On the vWorkstation taskbar, **click** the **Kleopatra icon** to restore the Kleopatra window.



Kleopatra icon

7. On the Kleopatra toolbar, **click** the **Import Certificates** button to open the Select Certificate File dialog box.
8. In the Select Certificate File dialog box, **navigate** to the Desktop (**This PC > Desktop**), then **select** the **TargetWindows02-public.asc** file and **click Open** to import the file.



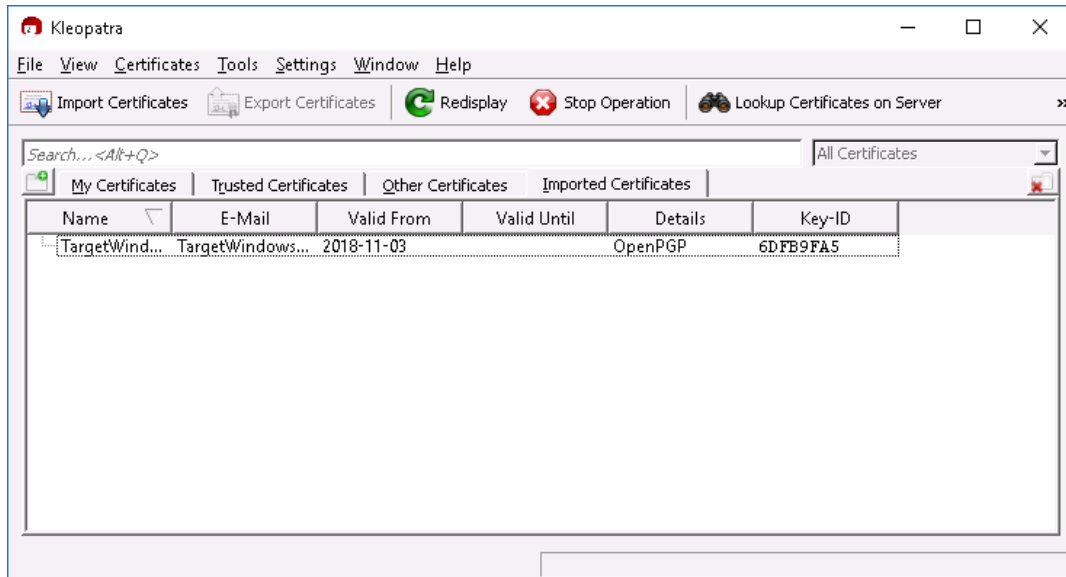
Import the receiver's public file

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.

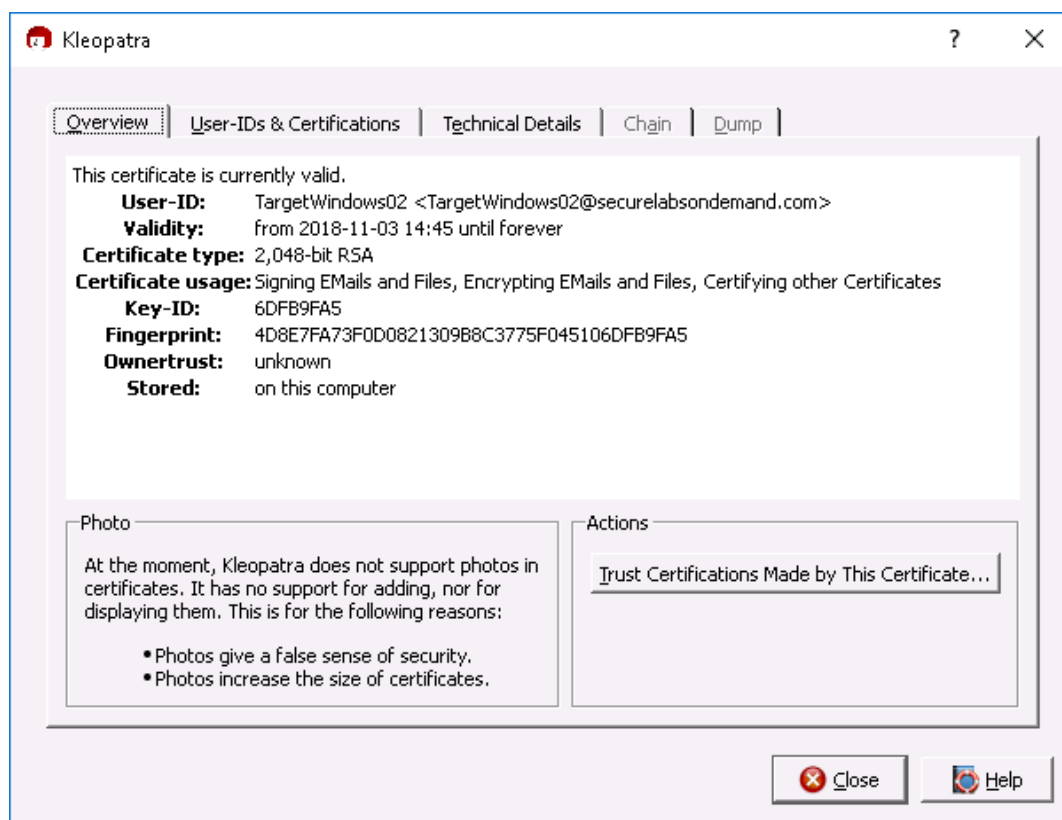
Using Encryption to Enhance Confidentiality and Integrity

Fundamentals of Information Systems Security, Third Edition - Lab 07



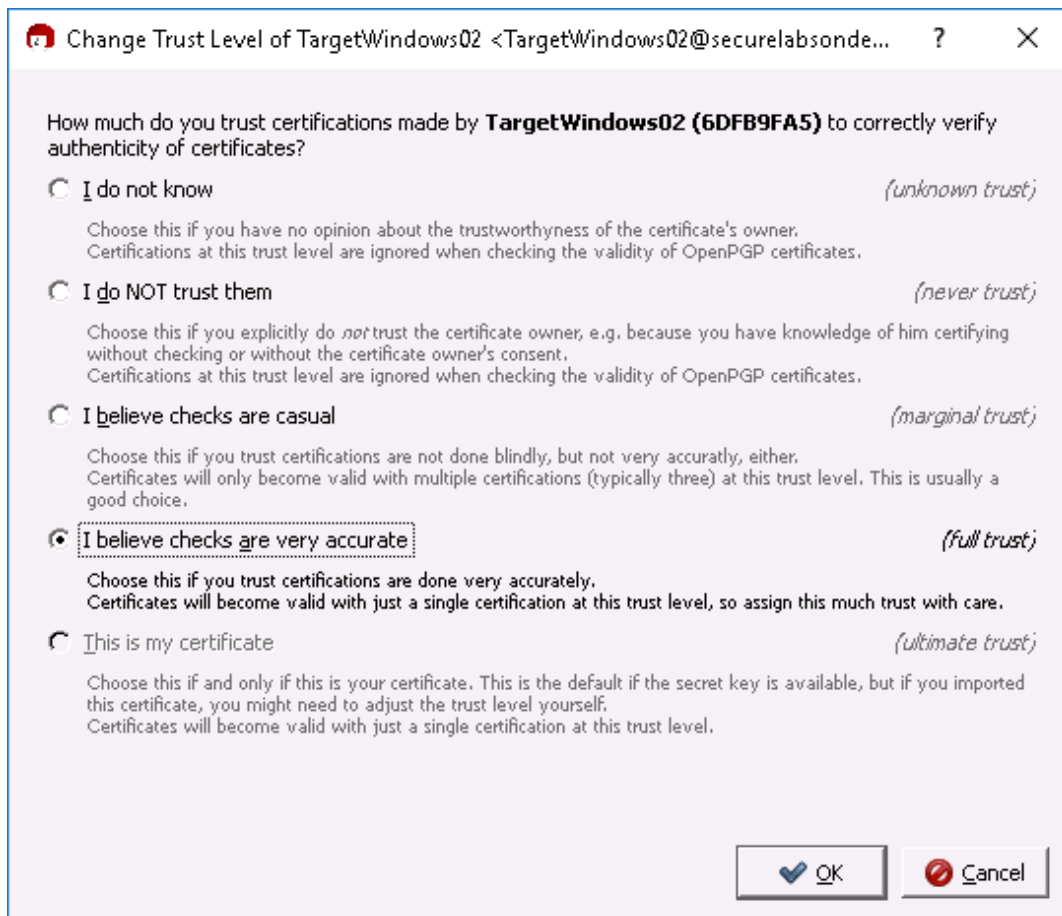
Imported Certificates tab

10. In the Kleopatra window, **double-click** the **TargetWindows02 certificate** to open the Certificate Details window.



Trust Certificates button

11. In the Certificate Details window, under Actions, **click** the **Trust Certificates made by this Certificate** button to open the Change Trust Level window.
12. In the Change Trust Level window, **select** the **I believe checks are very accurate radio button** to assign full trust to certificates made by TargetWindows02.



Confirm trust level

13. In the Change Trust Level window, **click OK** to close the window.
14. When prompted, **click OK** to close the *Owner trust changed successfully* dialog box.
15. In the Certificate Details window, **click the Close button** to close the window.

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.

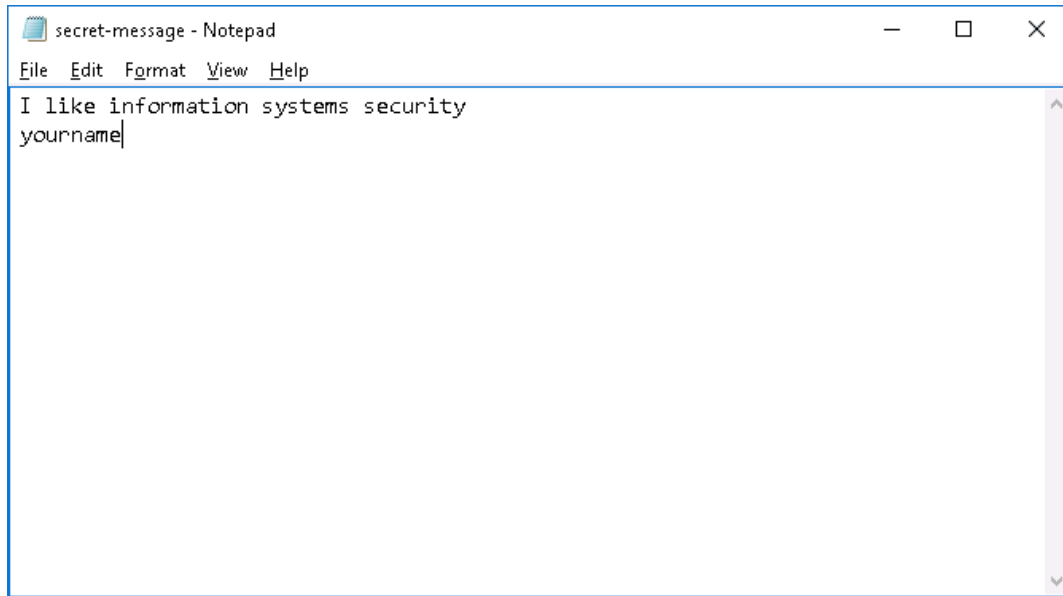


Create a new text document

2. With *New Text Document* highlighted, **type** **secret-message** and **press Enter** to name the new file.
3. On the vWorkstation desktop, **double-click** the **secret-message icon** to open the file in the Notepad application.
4. In the Notepad window, **type** **I like information systems security**, then **press Enter** and **type** **yourname**, replacing *yourname* with your own name.

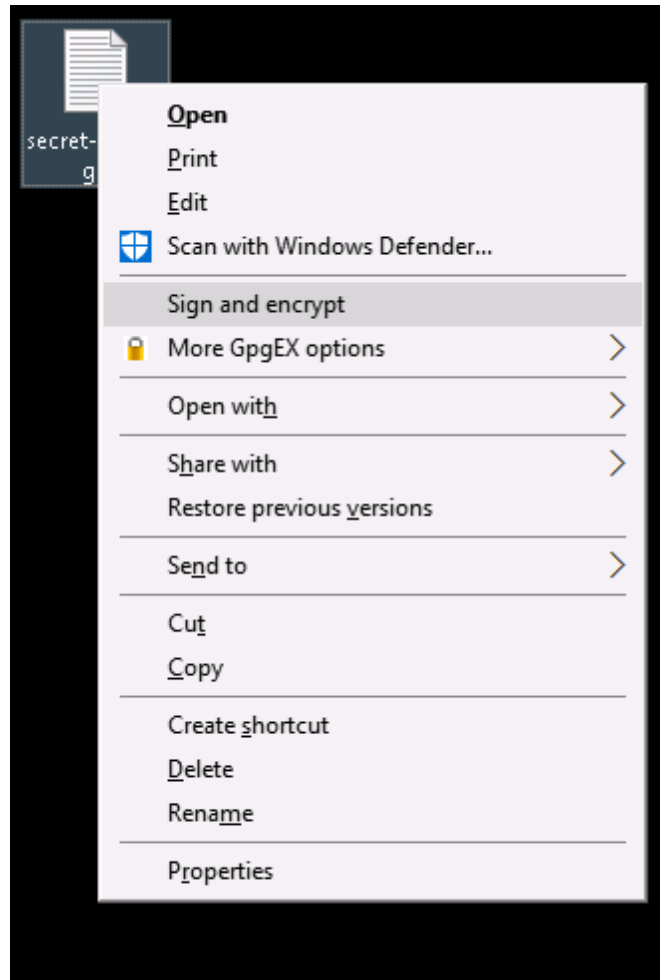
Using Encryption to Enhance Confidentiality and Integrity

Fundamentals of Information Systems Security, Third Edition - Lab 07



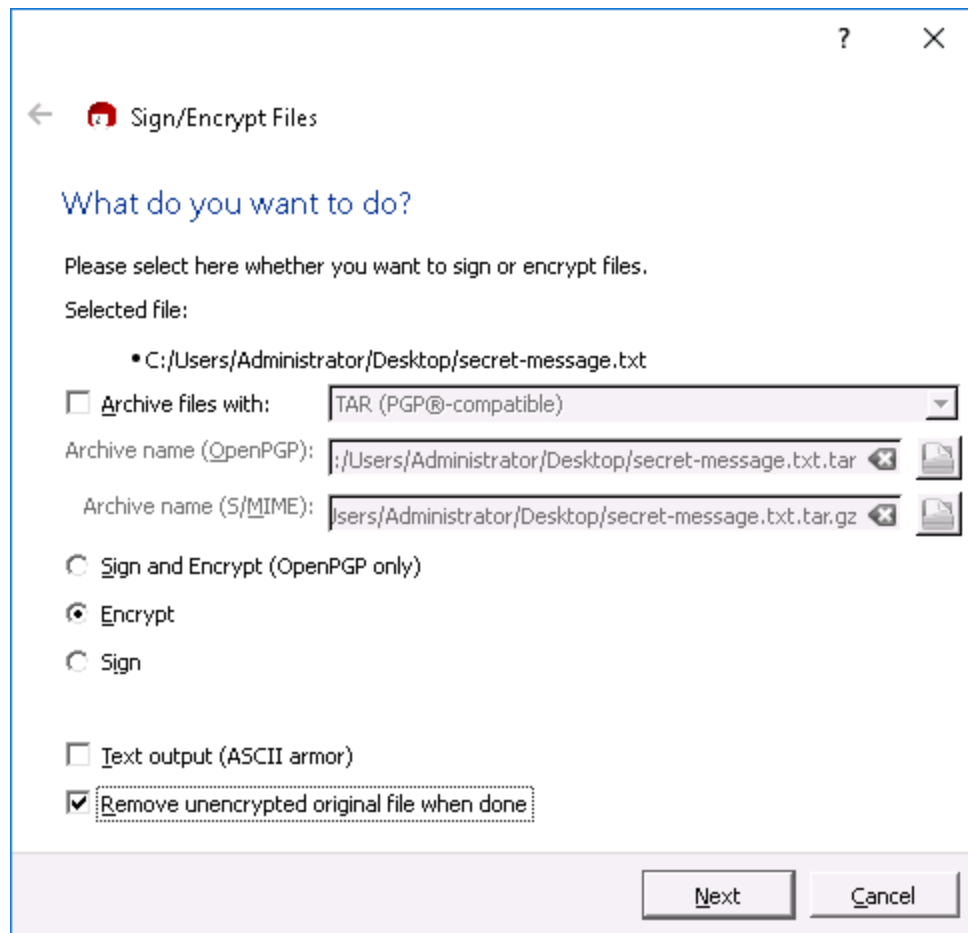
Create secret-message.txt

5. On the Notepad menu bar, **click File > Exit**, then **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 to open the Sign/Encrypt Files dialog box.



Sign and encrypt option

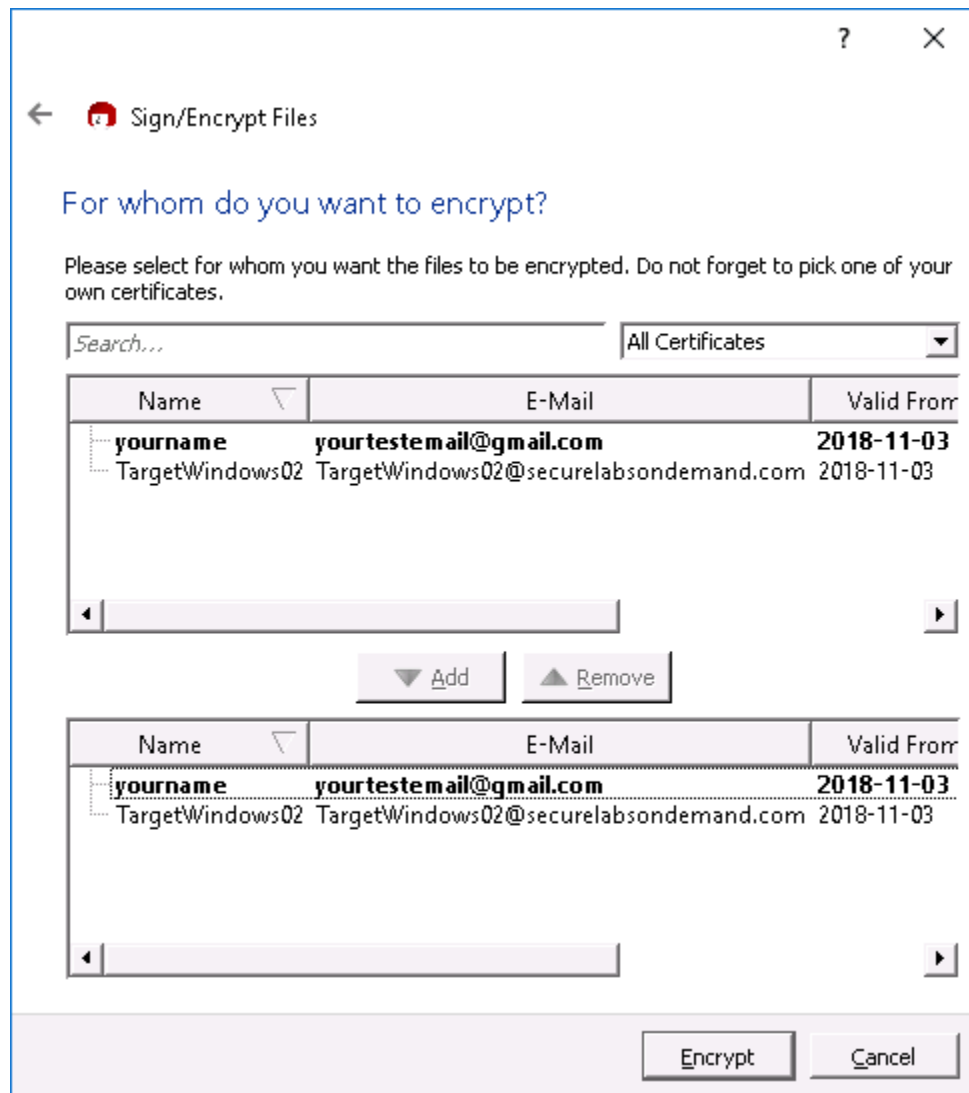
7. In the Sign/Encrypt Files dialog box, **click** the **Remove unencrypted original file when done** **checkbox** and **click Next** to continue.



Replace the unencrypted file

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

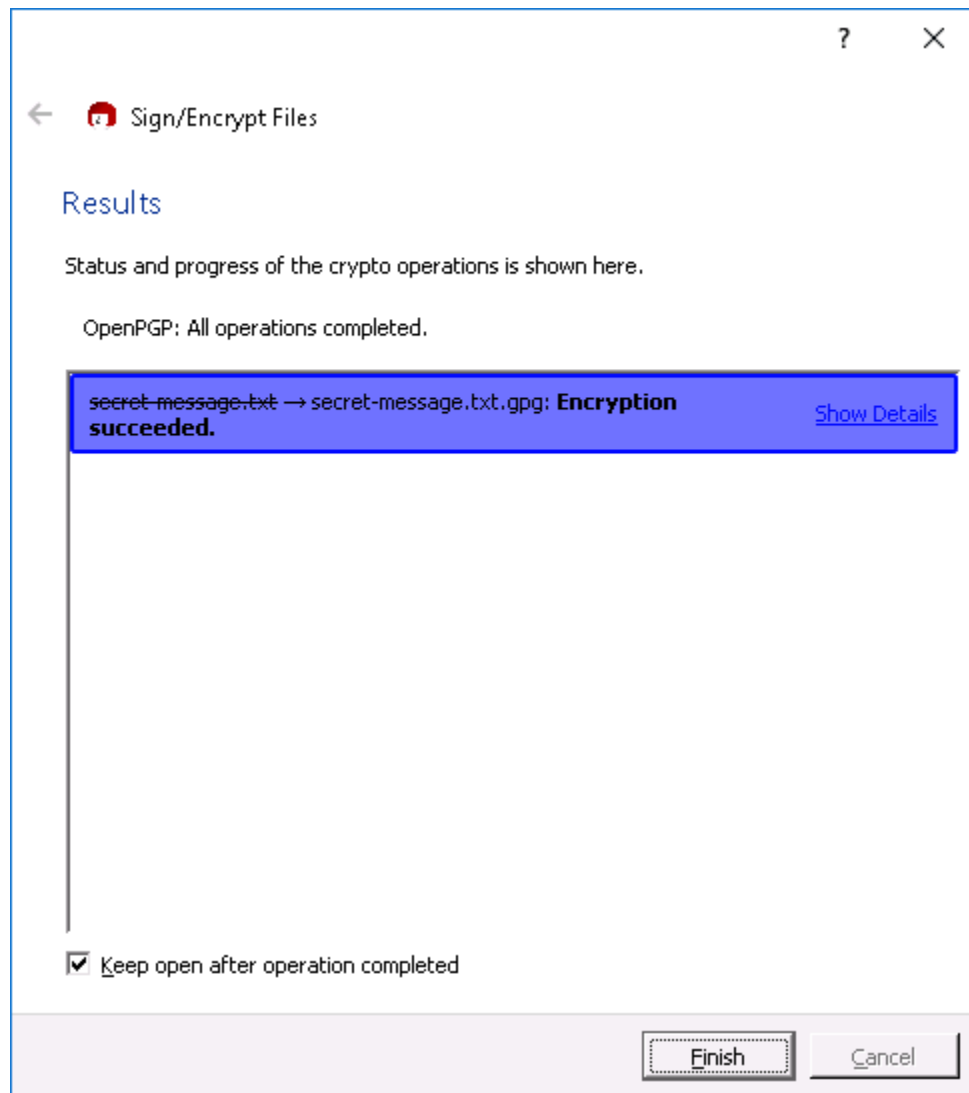
Selecting both certificates will tell Kleopatra to use the TargetWindows02 (receiver's) public key and your (sender's) private key to encrypt the message. Adding both keys will allow both the sender and the receiver to decrypt the file.



Add sender's and receiver's certificates

9. In the Sign/Encrypt Files dialog box, **click the Encrypt button** to continue.

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



Successful encryption

10. In the Sign/Encrypt dialog box, **click** the **Finish** button.

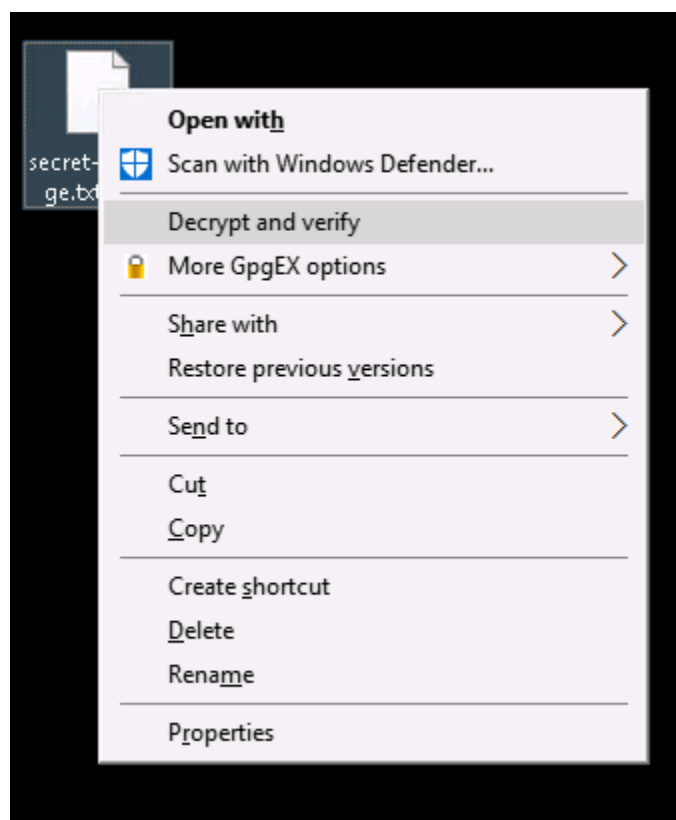
11. **Close** the **Kleopatra** window.

Note: In the next steps, you will transfer 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 context menu.
13. **Restore** the **remote TargetWindows02** connection.
14. On the TargetWindows02 desktop, **right-click** any empty space and **select Paste** from the context menu to copy the secret-message.txt.gpg file to the TargetWindows02 desktop.

Note: In the next steps, you will decrypt the file you just transferred. You can verify that the 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 **remote TargetWindows02** connection.
16. On the TargetWindows02 desktop, **right-click** the **secret-message.txt.gpg** file and **select Decrypt and verify** from the context menu to open the Decrypt/Verify Files dialog box.



Decrypt and verify

17. At the bottom of the Decrypt/Verify Files dialog box, **click** the **Decrypt/Verify** button to decrypt the secret-message file.

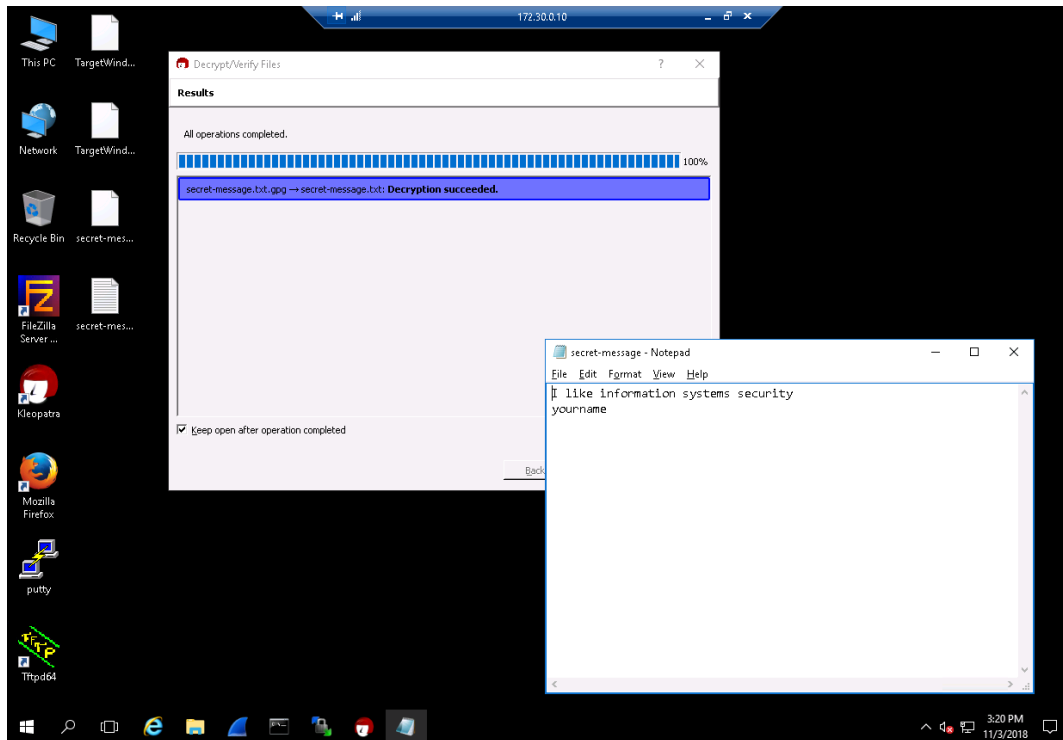
18. When prompted, **type 1Tsecurity!** (the passphrase you used when you created the encryption file) and **click OK**.

Do not close the dialog box.

19. If necessary, **reposition** the **Decrypt/Verify Files dialog box** so that both the original encrypted file and the new secret-message file are visible on the TargetWindows02 desktop.

20. On the TargetWindows02 desktop, **double-click** the newly decrypted **secret-message** file to open the file in Notepad.

21. **Reposition the open windows** so that the Decrypt/Verify Files dialog box and the Notepad window are visible.



Decrypted message

22. **Make a screen capture** showing the **Kleopatra decryption results window** and the **secret-message.txt** file in **Notepad**, 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**

Section 2: Applied Learning

Note: **SECTION 2** of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will import a new public key and decrypt a file found in the lab.

Please confirm with your instructor that you have been assigned Section 2 before proceeding.

1. On your local computer, **create** the **Lab Report file**.
Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.
2. If you already completed Section 1 of this lab, you will need to reset the virtual environment before beginning Section 2. To reset the virtual environment, complete one of the following options.
 - a. **Click Options > Reset Lab** to restore all virtual machines to their base state. This will take several minutes to complete. If you do not see the vWorkstation desktop after five minutes, **click Options > Reload Lab** to reload your lab connection.
 - b. **Click Disconnect**, then **select Discard Changes** to end your lab session without creating a StateSave. If you previously created a StateSave, delete the StateSave at the launch page, then start a new lab session.
3. **Proceed with Part 1.**

Part 1: Create a Public and Private Key Pair

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 encrypt files, which you can then decrypt with your own private key. You only need to provide your public key, never your private key.

1. From the vWorkstation desktop, **open** the **Kleopatra** component of the GPG4Win application.
2. **Create** a new **Directory Services server**, accepting the default server, **keys.gnupg.net**.
3. **Create a new personal OpenPGP key pair certificate** using the following information.
 - 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.

4. When prompted for a passphrase, **type 1Tsecurity!**.

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.
5. **Make a screen capture** showing the **fingerprint generated by the key creation process** and **paste** it into your Lab Report file.
 6. **Upload** the **Certificate** to Directory Services, then **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.

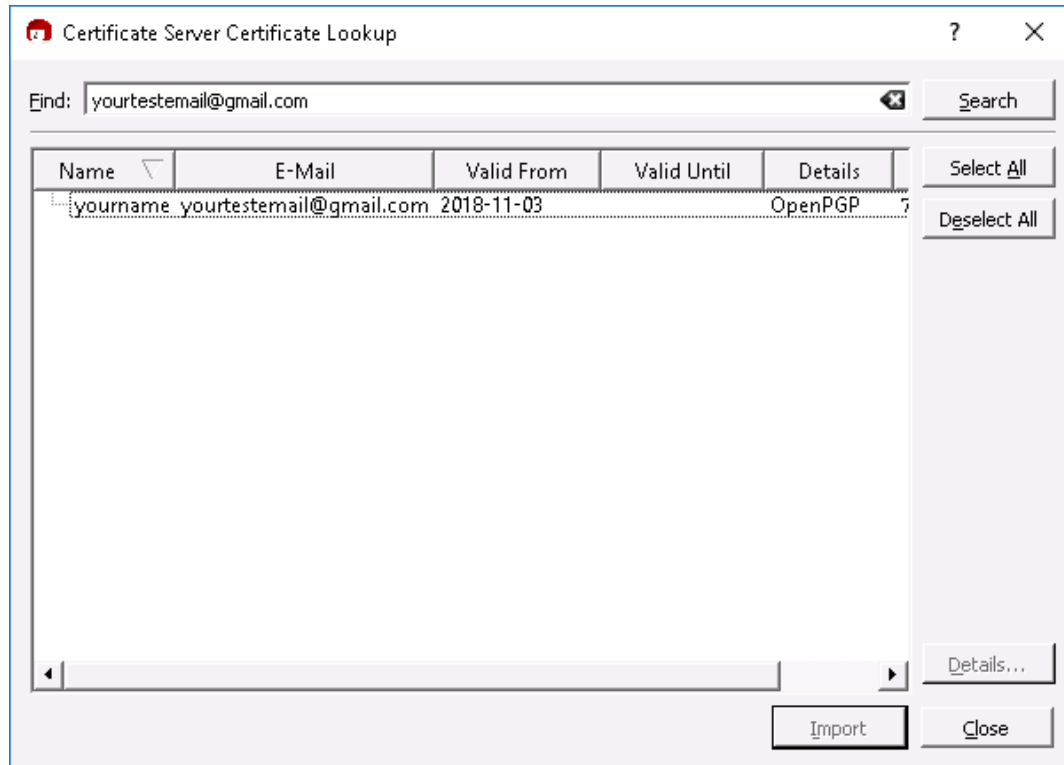
Note: Please note that the key management server used in this lab exercise is a public directory server, and is known to periodically produce an error message when attempting to export a certificate. If you receive an error message at this step, click OK and repeat step 6.

If the issue persists, close the Certificate Creation Wizard and skip to step 11. In place of the screen capture required at Step 9, make a screen capture of the Export error.

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

8. **Search** for the *test email address* you used to create the certificate to confirm the certificate was uploaded to the Public Directory Server.

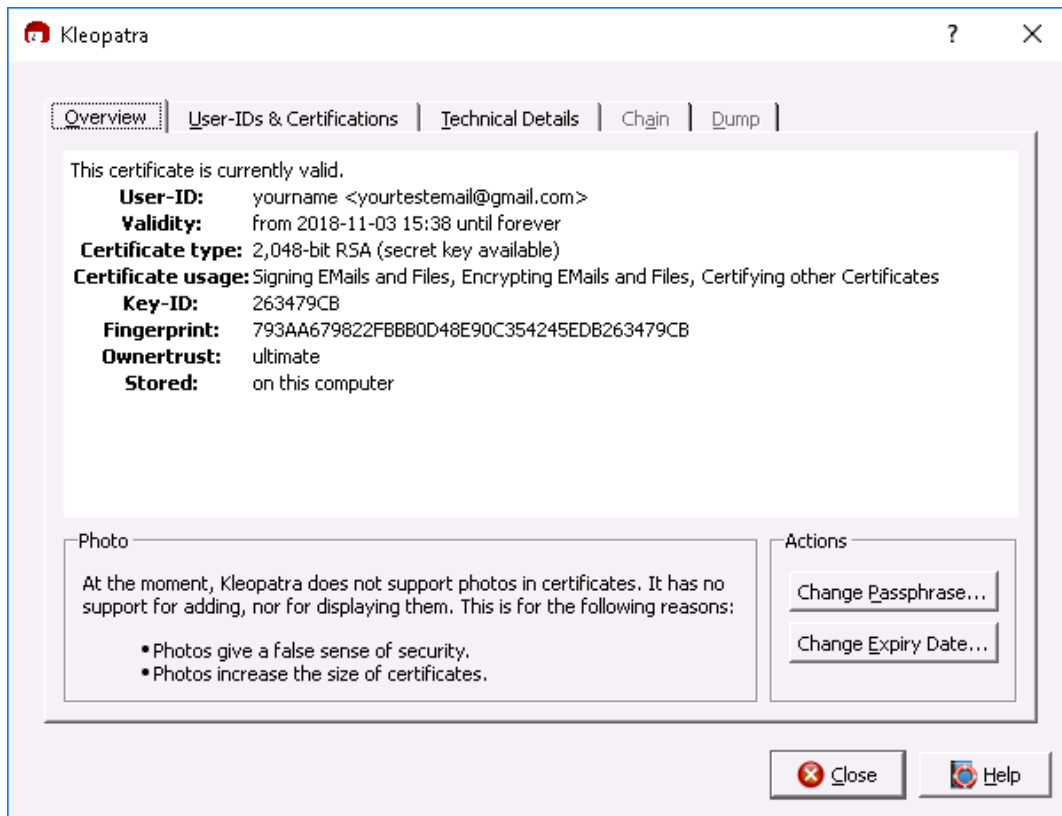
This process may take several minutes; you may click the Search button repeatedly to refresh the results of this screen. When your test email address appears in the search results section, adjust the column widths so that your name and email address are visible in their entirety.



Certificate search

9. **Make a screen capture** showing **your own email address** in the Certificate Server Certificate Lookup window and **paste** it into your Lab Report file.
10. **Close** the **Certificate Lookup**.
11. **Select your certificate**, then **select File > Export Secret Keys** and **save** your private (secret) key to the vWorkstation desktop as **DesktopKey-private.gpg**.
12. In the Kleopatra window, **double-click your certificate** to view all details related to the certificate:

Note that the key 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.



Certificate details

13. **Close the Certificate details.**
14. **Select your certificate**, then **select File > Export Certificates** and **save** your public key to the vWorkstation desktop as **DesktopKey-public.asc**.

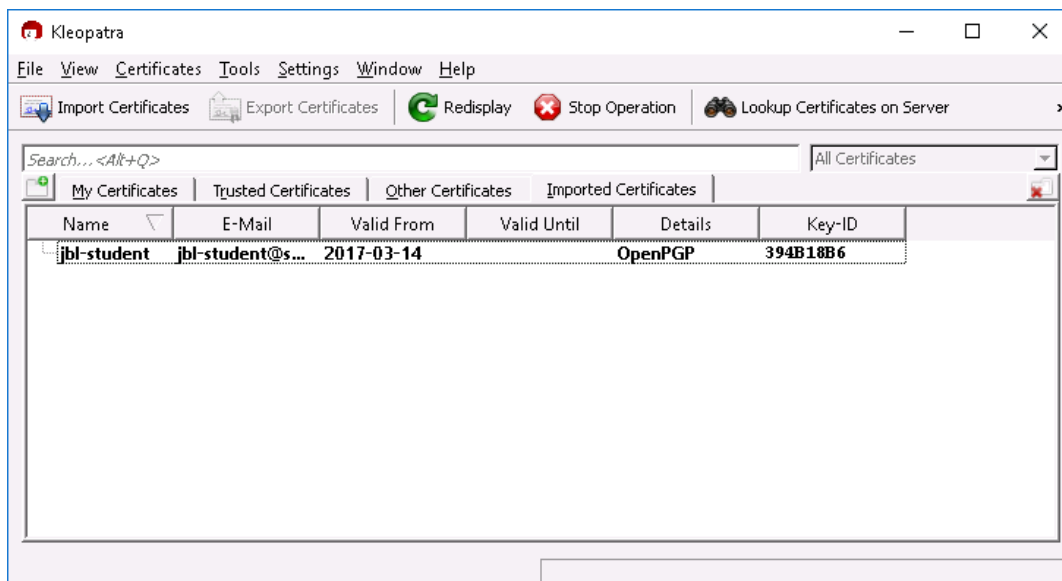
Part 2: Import Another Private Key

Note: In the next steps, you will import another private key stored on the vWorkstation machine and import it into Kleopatra. This key is the Student Certificate and is used to encrypt and decrypt message between the two machines in the lab.

1. **Import the SC-PrivateKey.gpg** (the student certificate) from the Cert folder (**This PC > Local**

Disk (C:) > Cert).

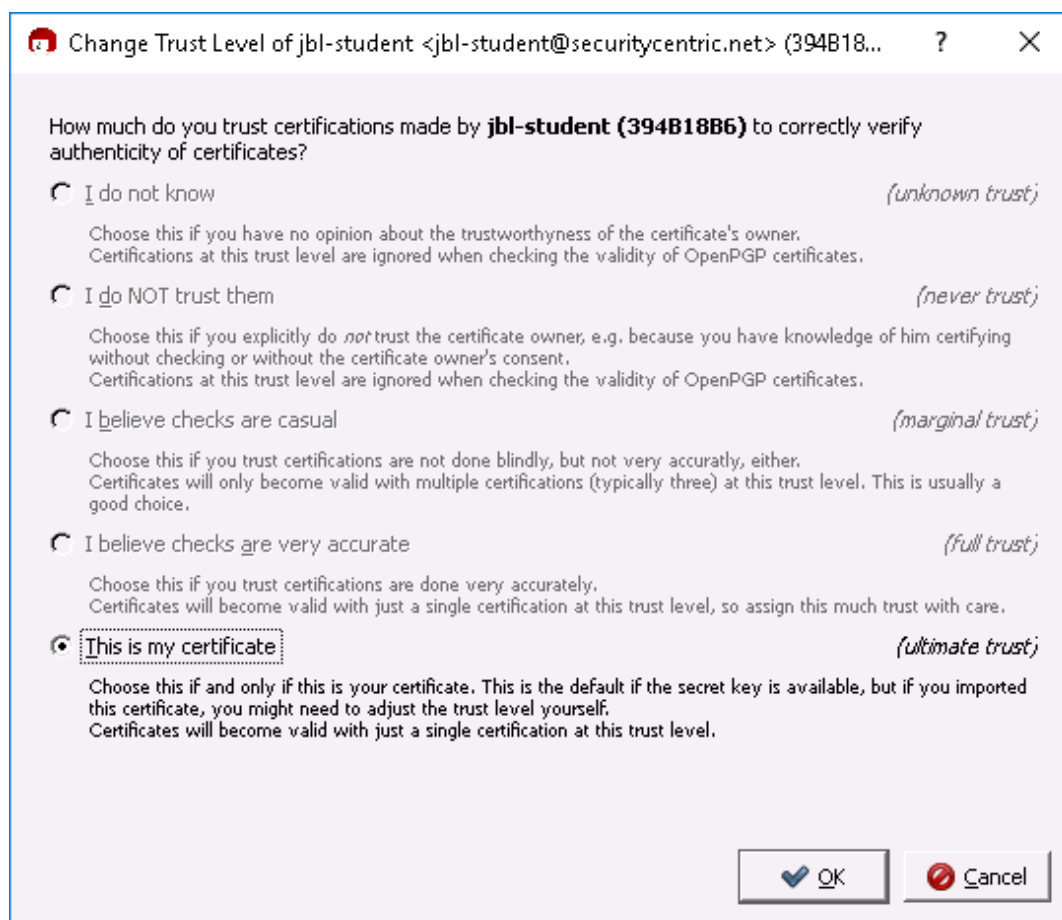
The new certificate will appear as a new line item on the Imported Certificates tab of the Kleopatra application.



Imported Certificates tab

2. **Export** the **public key** for the imported certificate to the vWorkstation desktop as **SC-PublicKey.asc**.
3. **Change** the **Trust Level** for this certificate.

Notice that only the This is my certificate option is available. This is a private key created by the vWorkstation, so this is the correct option.



Trust imported certificate

4. **Make a screen capture** showing the **Certificate Details** for the **student certificate** and **paste** it into your Lab Report file.

Part 3: Decrypt a File with the Imported Certificate

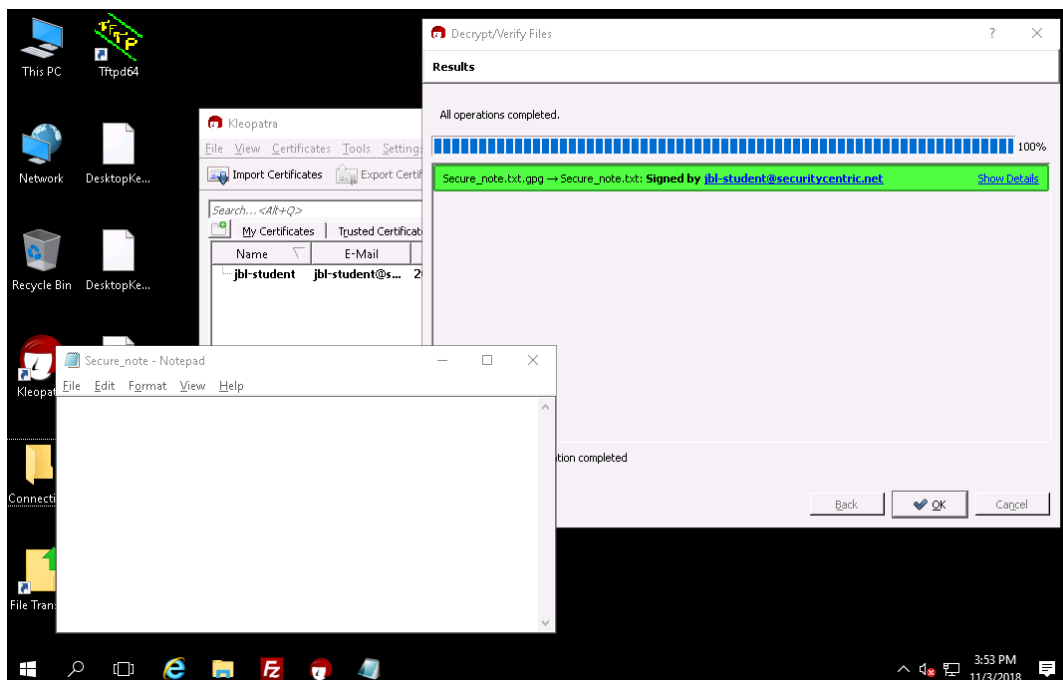
Note: In the next steps, you will decrypt a file stored on the vWorkstation using the imported key. You also will download the key as a deliverable for this lab.

1. **Decrypt and verify** the **C:/Key/Secure_note.txt.gpg** file.

Using Encryption to Enhance Confidentiality and Integrity

Fundamentals of Information Systems Security, Third Edition - Lab 07

- When prompted, **type 1Tsecurity!** (the passphrase associated with the encrypting key) and **click OK**.
- Without closing the Decrypt/Verify files dialog box, **open** the newly decrypted **Secure_note.txt** file in Notepad.
- Reposition** the **open windows** so that the Decrypt/Verify Results window and the decrypted Secure_note.txt file in Notepad are visible.



Window arrangement for screen capture (secure_note contents redacted)

- Make a screen capture** showing the **Kleopatra decryption results window** and the **Secure_note.txt file in Notepad**, and **paste** it into the Lab Report.
- Close** the **Notepad window**, **Decrypt/Verify Files dialog box**, and the **File Explorer window**.

Part 4: Encrypt a Reply Using the Imported Certificate

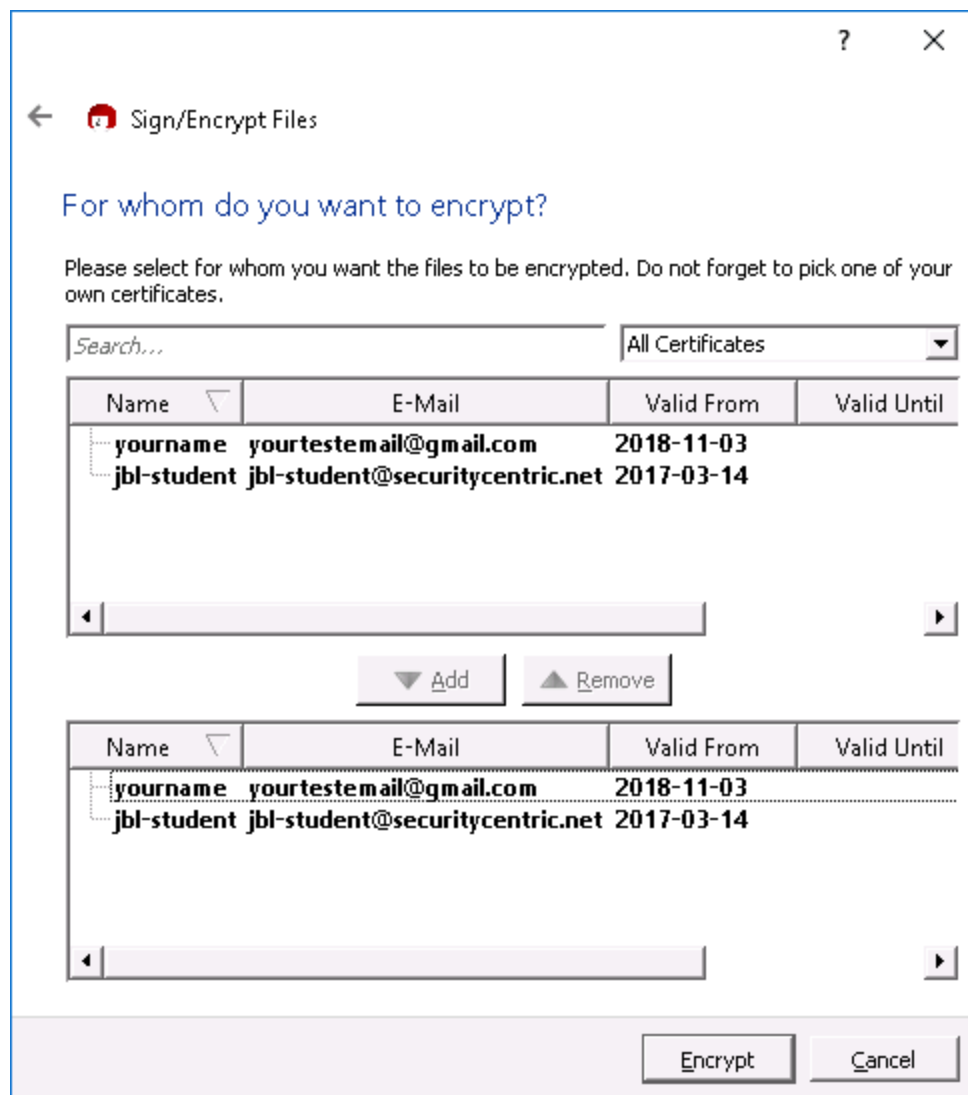
Using Encryption to Enhance Confidentiality and Integrity

Fundamentals of Information Systems Security, Third Edition - Lab 07

Note: In the next steps, you will create a file on the vWorkstation that responds to the encrypted message from Part 3. You will encrypt your reply using the keys you imported earlier in this lab.

1. On the vWorkstation desktop, **create a new text file titled Secure_reply.txt**, then **open the text file** and **type a reply** to the decrypted Secure_note.txt.
2. **Encrypt the Secure_reply.txt file** using the imported certificate and the personal certificate that you created in Part 1 of this lab.

Selecting both certificates will tell Kleopatra to use the imported key and your personal key to encrypt the message. Adding both keys will allow both certificates to decrypt the file.



Encrypt the Secure_reply.txt file

3. Close Kleopatra.

Note: This completes Section 2 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.

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

- **Secure_reply.txt.gpg**
- **SC_PublicKey.asc**

Section 3: Lab Challenge and Analysis

Note: The following questions are provided to allow you the opportunity for independent, unguided research, similar to what you will encounter in a real situation. Some questions will challenge you to find command line syntax for tasks you performed in the lab, others may ask you to extend your learning from the lab. Use screen captures where possible to illustrate your answers.

Part 1: Analysis and Discussion

1. What is the difference between RSA and DSA encryption?
2. Would it be possible to encrypt the secret-message.txt file using only the TargetWindows02 (receiver's) public key? What would be the ramifications of doing this?

Part 2: Tools and Commands

1. PGP encryption can be performed from the command line as well. What is the PGP command line syntax to encrypt the my-message.txt file for a specific user (Sean) and save the output as secret-message.txt.gpg?
2. What is the command line syntax to generate a revocation certificate?

Part 3: Challenge Exercise

Install Kleopatra on your own local machine from <https://www.gpg4win.org/>. Using what you learned in the lab, configure Directory Services, create your own personal OpenPGP key pair, and upload the certificate to Directory Services. Import the certificate provided by your instructor and use both to encrypt a copy of your Lab Report showing screen captures that illustrate the steps you used to complete this challenge. Send the encrypted file and your public key to your instructor via email.