Lab 7 PKI: Web Of Trust Key Signing

Table of Contents

Summary

In this portion of the lab, you will be signing each other's keys in order to help establish a web of trust. You should have exchanged contact information with the student on your left and the student on your right. Remember that you will not be sending two separate keys to the students, you will first need to send the key to the student on your left, have that student send back that signed key. Once you received that signed key, you must send that signed key to the student on your right, have them sign it and send it back to you. You will learn how to sign the keys your receive with the following instructions. If you have any issues about who you are sending your key to, let me us know as soon as possible.

Concept for Lab: https://www.gnupg.org/gph/en/manual/x56.html

MUST READ for Linux/Mac

- Before you send/exchange your .asc files, you must export your key again with ASCII Armor
  - Open a Terminal, go to a directory of your choosing
  - "sudo gpg2 --output <yourname>.asc --armor --export <hawaii.edu email>"
    - If you choose the directory where an existing .asc file is just overwrite it.

Linux/Mac Signing Tutorial

Step 1: Importing the public key

- After you download the .asc file from your partner
- Open a terminal
- Direct terminal to the directory where you downloaded the .asc file
- Type “sudo gpg2 --import <name of asc file>.asc
- Type “sudo gpg2 --list-keys”
    - You will see the public key you just imported as well as their email

Step 2: Signing the Public Key

- Type “sudo gpg2 --edit-key <email of partner>”
    - At the new prompt type “sign”
    - Type “y” to sign the public key with your private key
    - Type “quit”
    - Type “y” to save changes
- Type “sudo gpg2 --check-signature <email of partner>
    - You should see your signature on the key
- Export the key and email it back to your partner
    - Remember to use:
        - “sudo gpg2 --output <your partner’s name>.asc --armor --export <your partner’s hawaii.edu email>”

Step 3: Repeat Step 1 and 2 for your other partner’s signed key

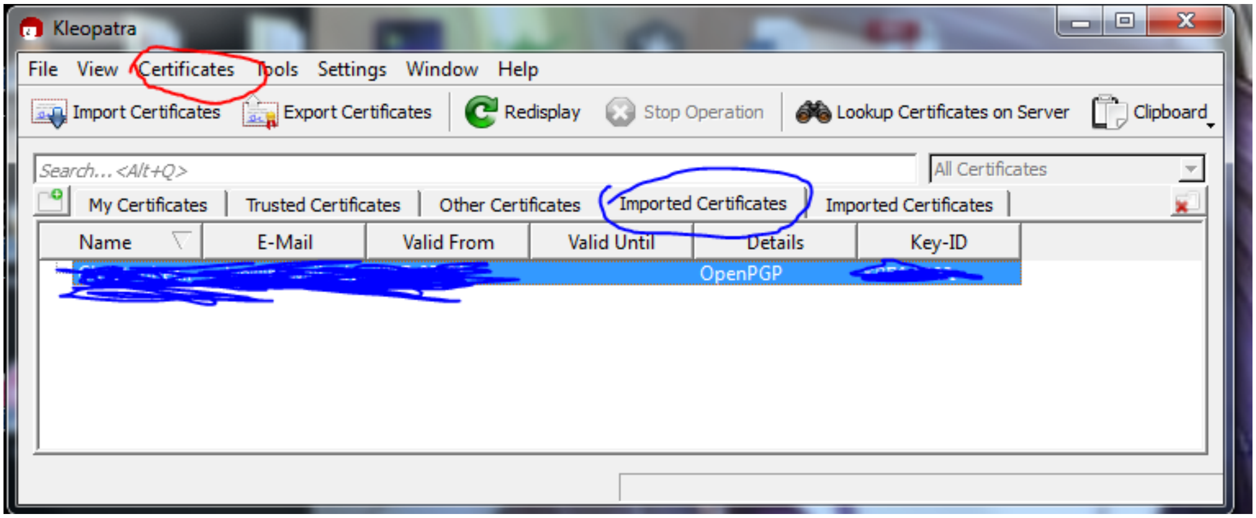
Windows Signing Tutorial

Step 1: Importing someone else’s public key

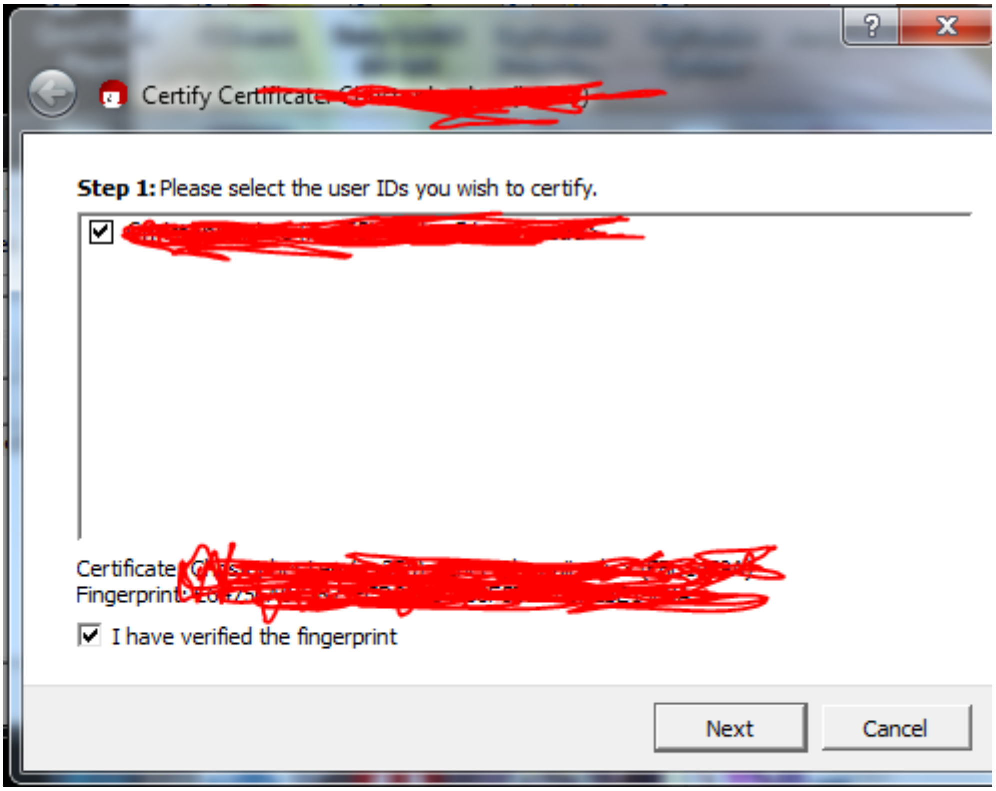
- After you download the .asc file from your partner
- Open a Kleopatra
- Click “Import Certificates” in the top left corner
- Go to directory with the downloaded asc file
- Select your partner’s .asc file
- When prompted press “okay”

Step 2: Signing the Public Key

- In Kleopatra



  - Under the tab “Imported Certificates”
  - Highlight the imported certificate
  - On the top, click the Certificates (Circled Expertly in Red)
    - Select “Certify Certificate”
    - See next picture



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

☑ [redacted]

Certificate
Fingerprint [redacted]

☑ I have verified the fingerprint

- Check the two boxes at the next prompt
- In the next page, make sure “Certify For Everyone To See” is selected, uncheck the additional box that says to send certificate to key server and select “Certify” in the bottom
- Click Finish in the next prompt
- Check your signature by right clicking your partner’s certificate and select “Certificate Details”
  - Go to Tab “User-IDs & Certifications”
  - Highlight the certificate in that tab
  - Click “Load Certifications (may take a while)”
  - You should see your signature/email below the chain of the highlighted certificate
- Export the certificate and email it back to your partner

Step 3: Repeat Step 1 and 2 for your other partner’s signed key