Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 8
Year 2, Semester 1

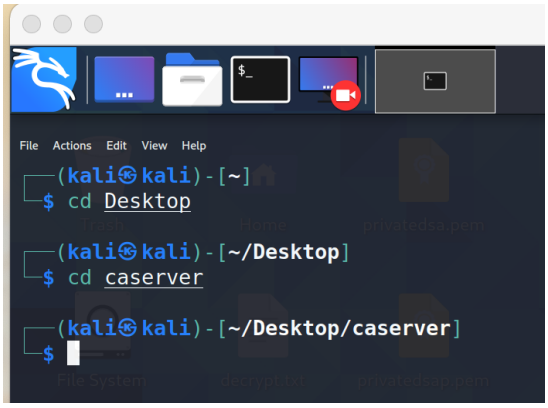
Secure Email Service

Objectives:

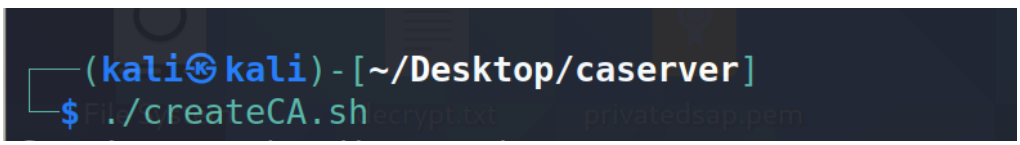
- Use kali linux for creating Certification Authority (CA) and Users Private key, Public key and Pfx files.
- Need two user email addresses (Create two gmail addresses or you can use existing two gmail addresses that you own)
- Use Thunderbird for sending email between two users,import certifications and assign Digital Signature to each user.
- Download "caserver" folder from courseweb "lab 08 Resources"

Create Certification Authority

1. Start Kali Linux and Go to the terminal.
2. Give path to the "casever" folder.



3. Run "createCA.sh" script in "caserver" folder using "./createCA.sh" command



Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 8
Year 2, Semester 1

Create User Certification,Private Key and Public Key

1. Run "createUserCert.sh" script in "caserver" folder using "./createUserCert.sh" command.
2. You have to create two user certifications because of that you have to run "createUserCert.sh" twice.
3. To both users you have to give their user name and gmail address respectively like below figure 1 and figure 2

```
┌──(kali㉿kali)-[~/Desktop/caserver]
└─$ ./createUserCert.sh
Generating a RSA private key
...+++++
.........+++++
writing new private key to 'usrkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
County Name [LK]:
Province Name [Western]:
Locality Name [Colombo]:
Oganization Name [SLIIT]:
Organization Unit Name [FOC]:
Common Name (e.g. server FQDN or YOUR name) []: USER 01 NAME
Email Address []: USER 01 Gmail address
```

Figure 1 : User 01 name and Gmail address

```
┌──(kali㉿kali)-[~/Desktop/caserver]
└─$ ./createUserCert.sh
Generating a RSA private key
...+++++
.........+++++
writing new private key to 'usrkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
County Name [LK]:
Province Name [Western]:
Locality Name [Colombo]:
Oganization Name [SLIIT]:
Organization Unit Name [FOC]:
Common Name (e.g. server FQDN or YOUR name) []: USER 02
Email Address []: USER 02 Gmail Address
```

Figure 2 : User 02 name and Gmail address

4. You have to put an Export password for both Users like below Figure 3 and Figure 4.

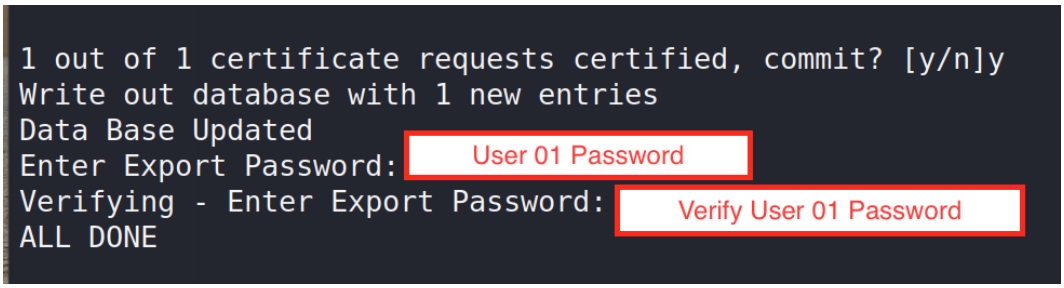


Figure 3

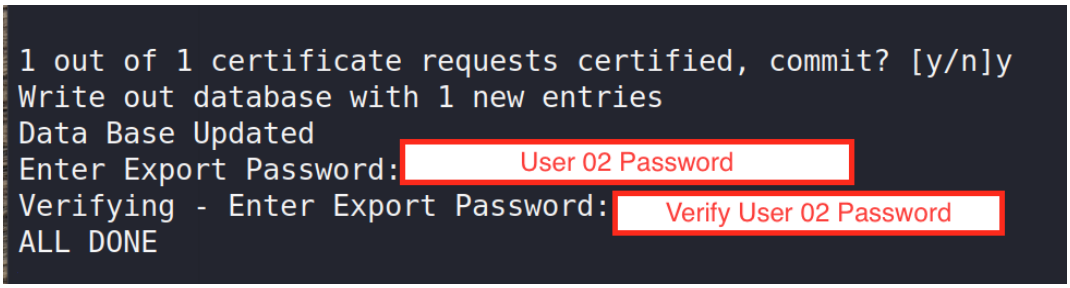


Figure 4

Thunderbird

(Kali Linux Virtual Environment)

1.Download and Execute Thunderbird in Kali Linux

- Download Link - https://www.thunderbird.net/en-US/

2. Set Up "User 01" gmail address in Thunderbird.

(Windows)

1.Download and Open Thunderbird in Windows

- Download link - https://www.thunderbird.net/en-US/

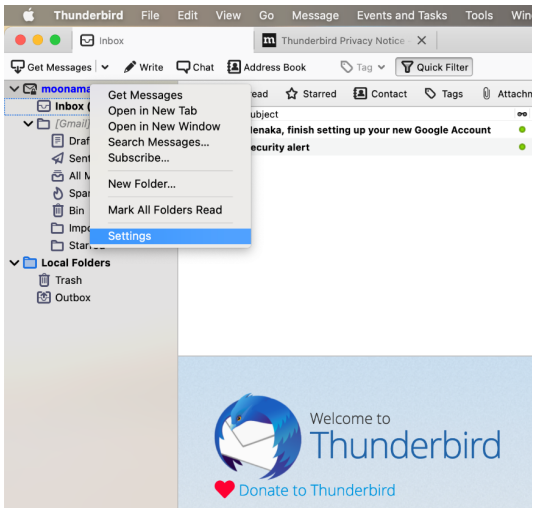
2. Set Up "User 02" gmail address in Thunderbird.

Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 8
Year 2, Semester 1

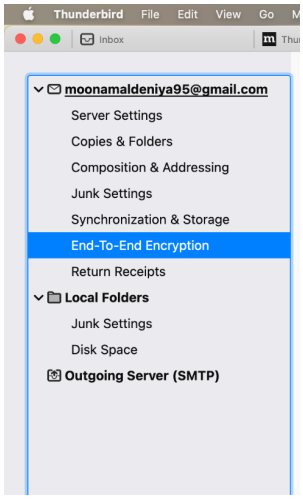
S/MIME (Personal Certificate for Digital Signing and Encryption)

- you have to create S/MIME for both Users

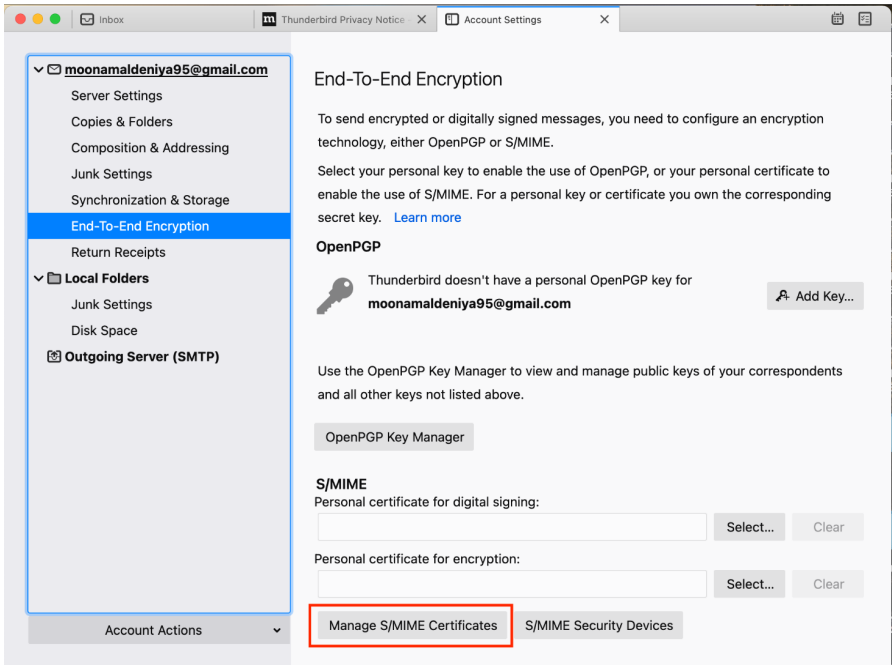
1. Go to the gmail "Settings" in thunderbird



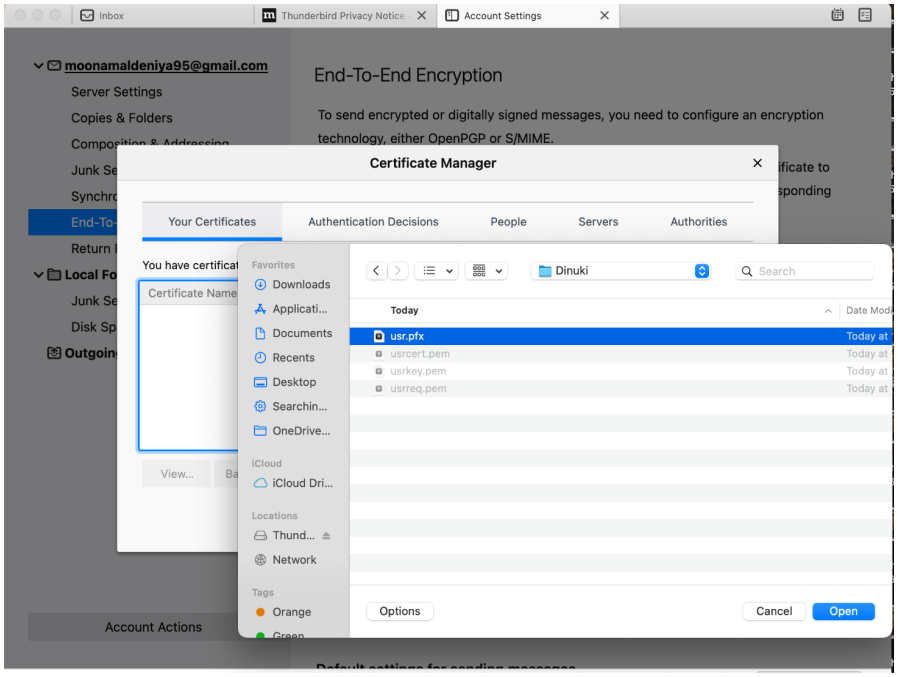
2. Select "End-To-End Encryption"



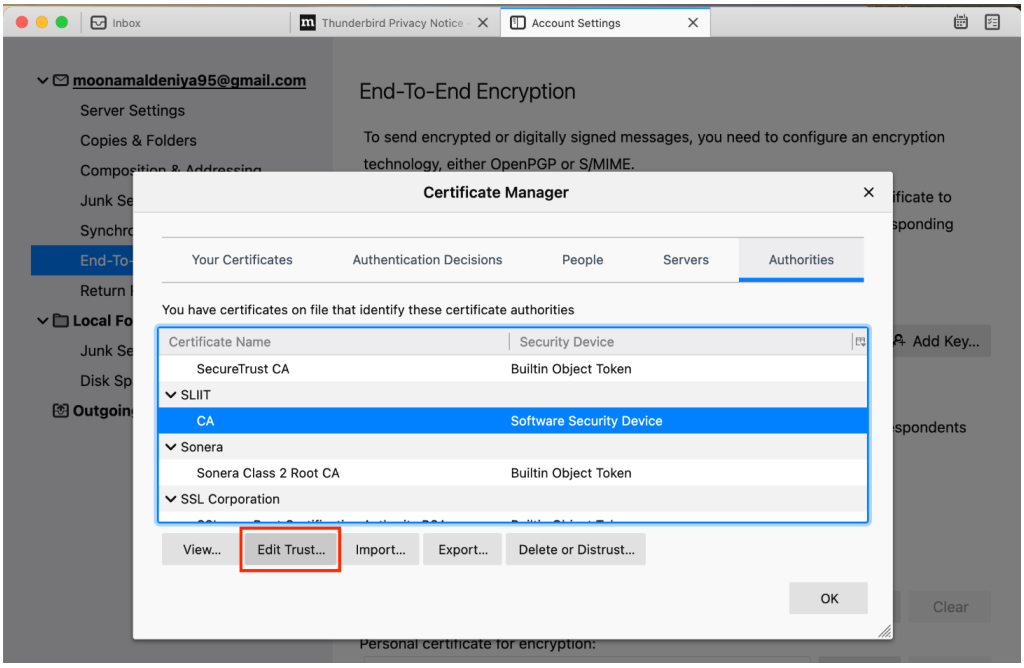
3. Click "Manage S/MIME Certificates"



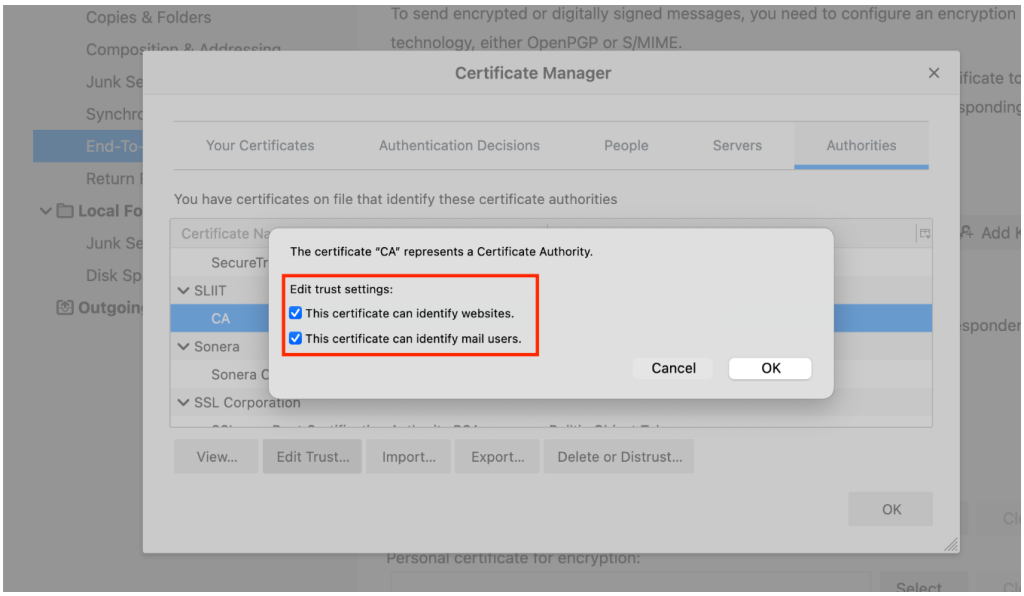
4. Click "Your Certification" and import the User "usr.pfx" file using "Import" Button.



5. Go to the "Authorities" and Find your Certification Name and Click "Edit Trust".

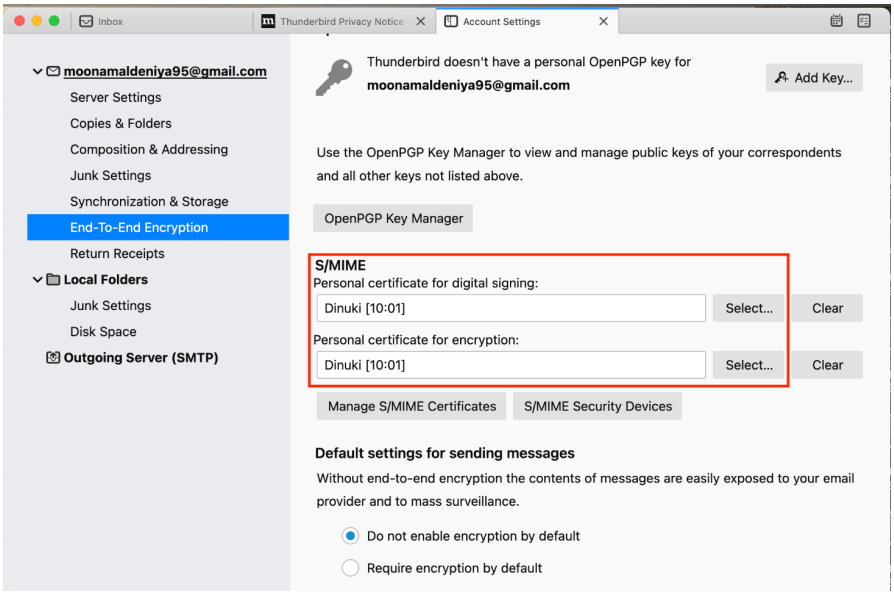


6. Give permission to identify websites and mail users

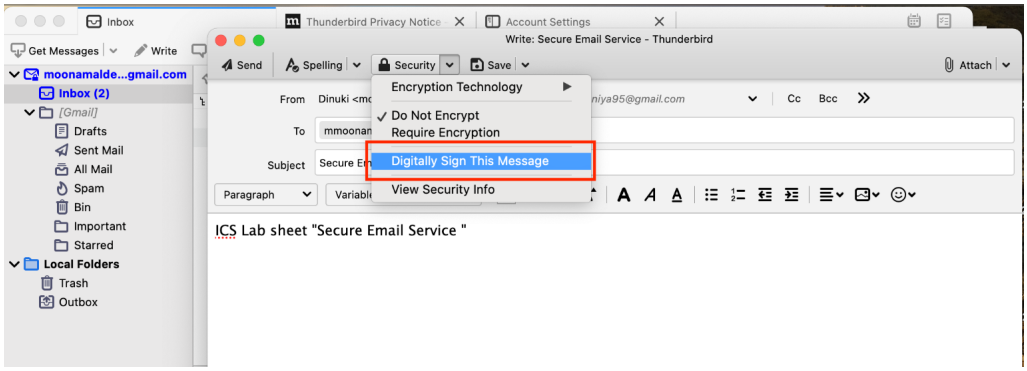


Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 8
Year 2, Semester 1

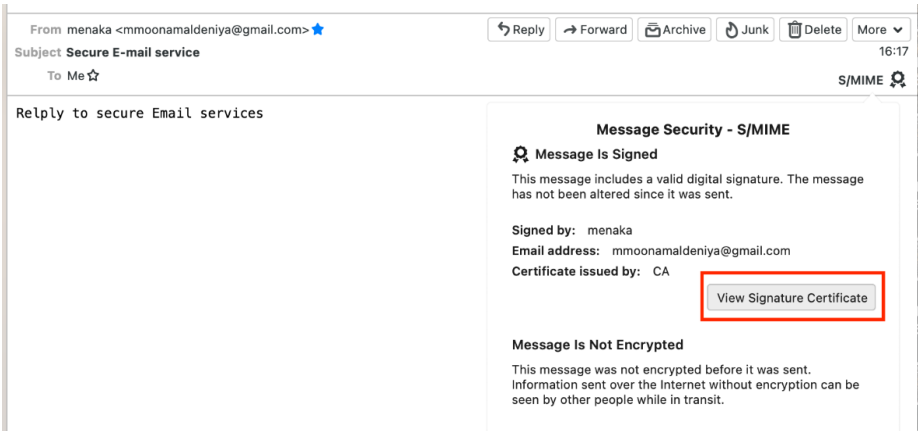
7. Go back to "End-To-End Encryption" in "Settings" and select your certification for "Personal Certification for digital signing" and "Personal Certification for encryption"



8. Now "User 01" can send an Email to "User 02" or vice versa before you send the mail go to the "security" and select "Digitally Sign This Message"



9. After you send the Email your Email is Signed and you can view the certification by clicking "View Signature Certificates"



10. you can see certification details.