



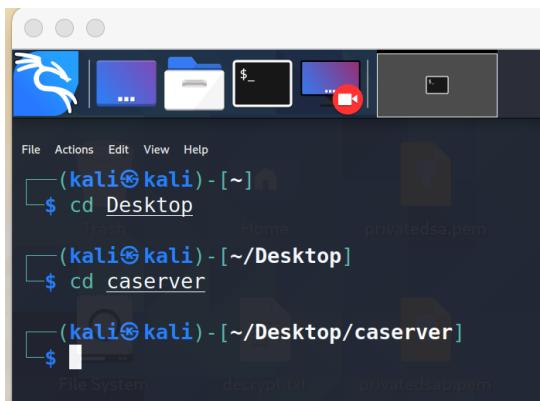
Secure Email Service

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

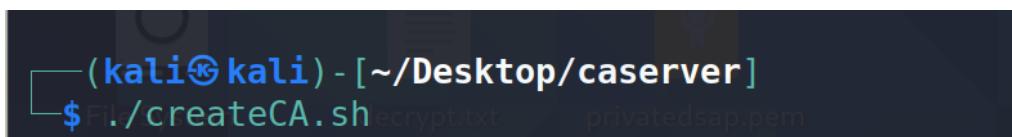
1. Start Kali Linux and Go to the terminal.
2. Give path to the “caserver” folder.



A screenshot of a terminal window on Kali Linux. The window title is '(kali㉿kali)-[~]'. The terminal shows the following command history:
\$ cd Desktop
\$ cd caserver
\$ ls

The current directory is ~/Desktop/caserver. There are three files visible: 'privatedsa.pem', 'decrypt.txt', and 'privatedsap.pem'.

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



A screenshot of a terminal window on Kali Linux. The window title is '(kali㉿kali)-[~/Desktop/caserver]'. The terminal shows the following command:
\$./createCA.sh

The command has been entered but not yet run.



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]:
Organization 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]:
Organization 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.

```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Enter Export Password: User 01 Password
Verifying - Enter Export Password: Verify User 01 Password
ALL DONE
```

Figure 3

```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Enter Export Password: User 02 Password
Verifying - Enter Export Password: Verify User 02 Password
ALL DONE
```

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/>

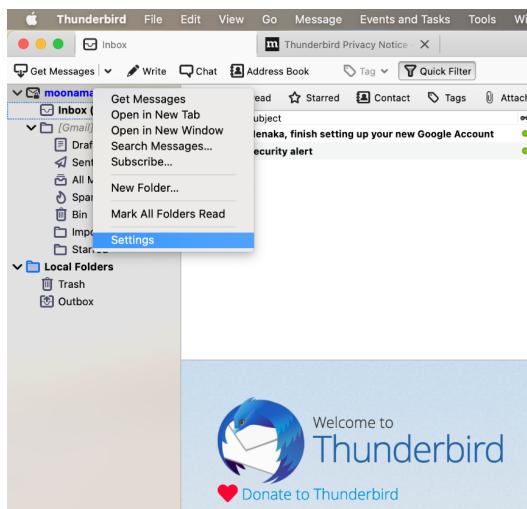
2. Set Up “User 02” gmail address in Thunderbird.



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

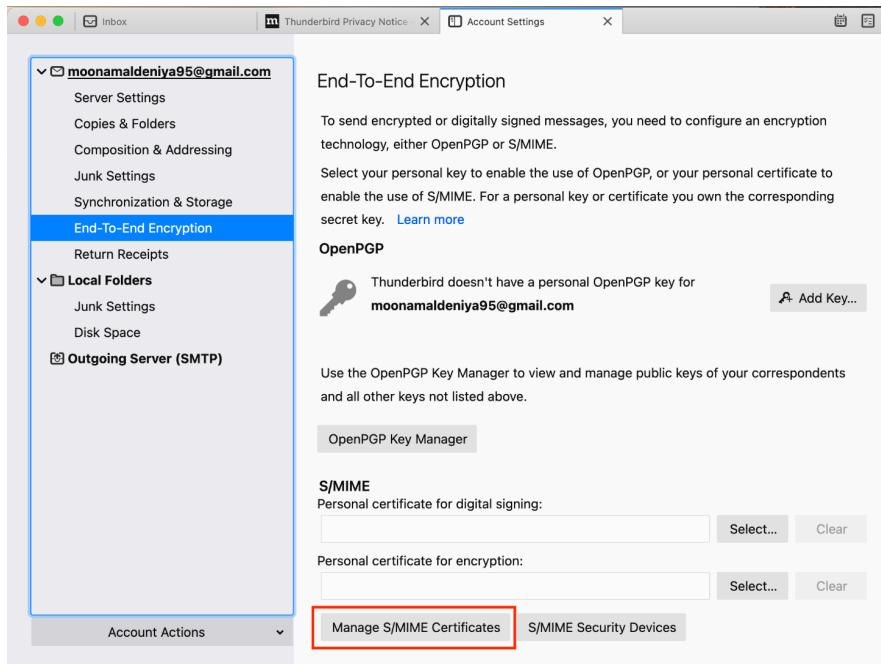
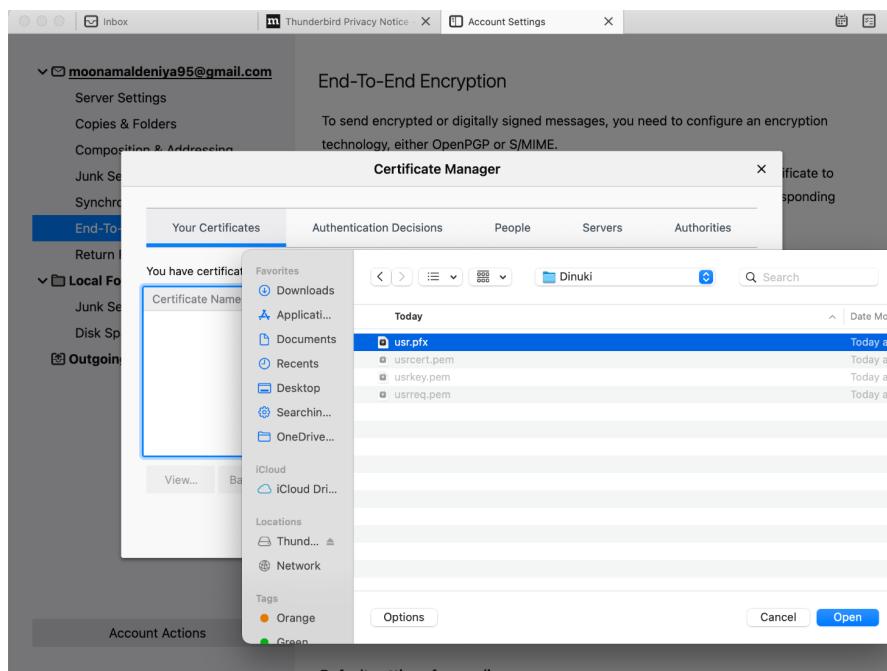
- you have to create S/MIME for both Users

1. Go to the gmail “Settings” in thunderbird



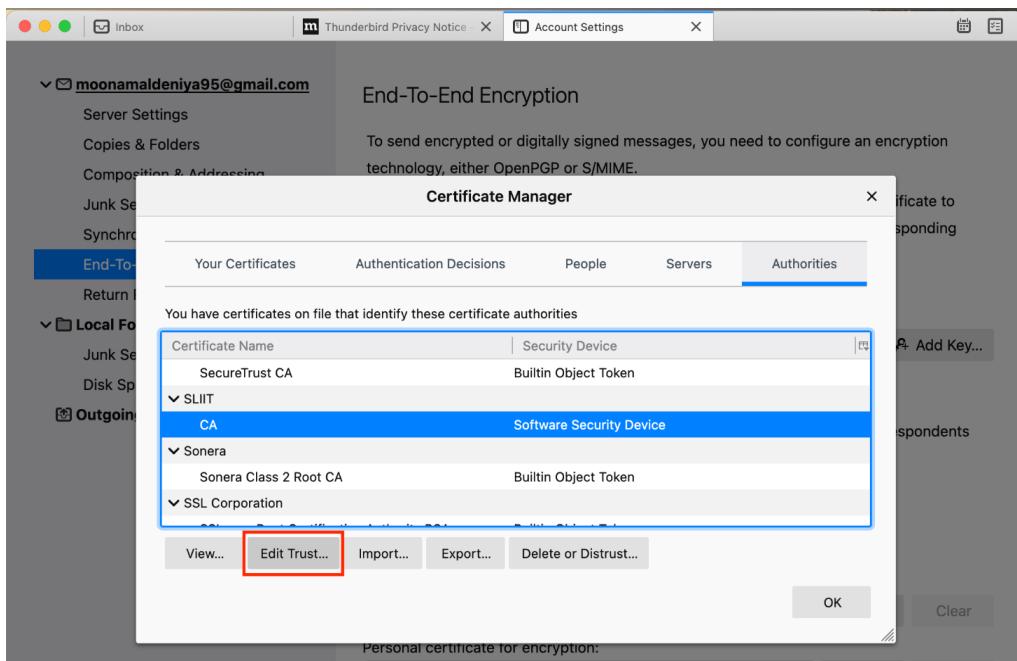
2. Select “End-To-End Encryption”



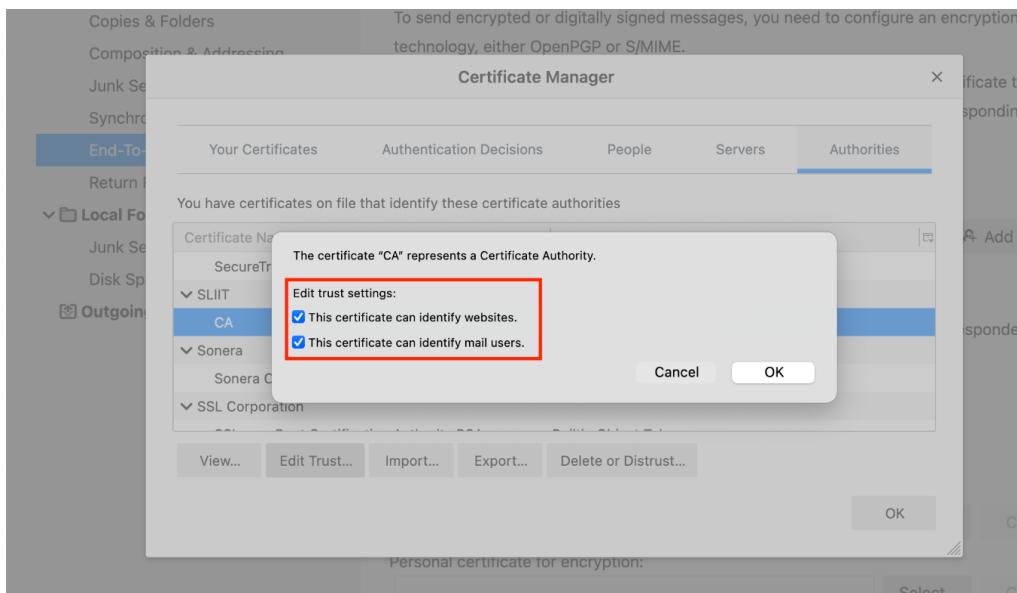
**3. Click “Manage S/MIME Certificates”****4. Click “Your Certification” and import the User “usr.pfx” file using “Import” Button.**



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

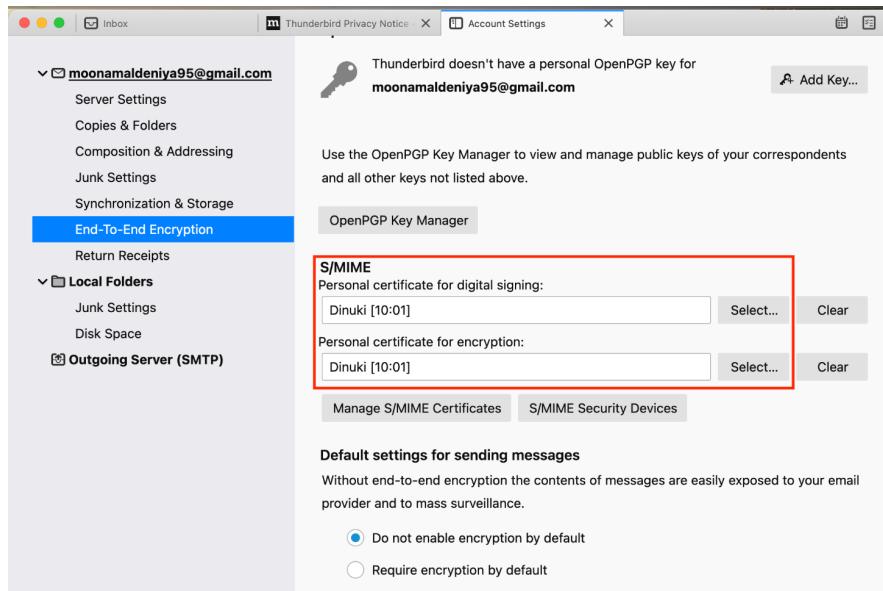


6. Give permission to identify websites and mail users

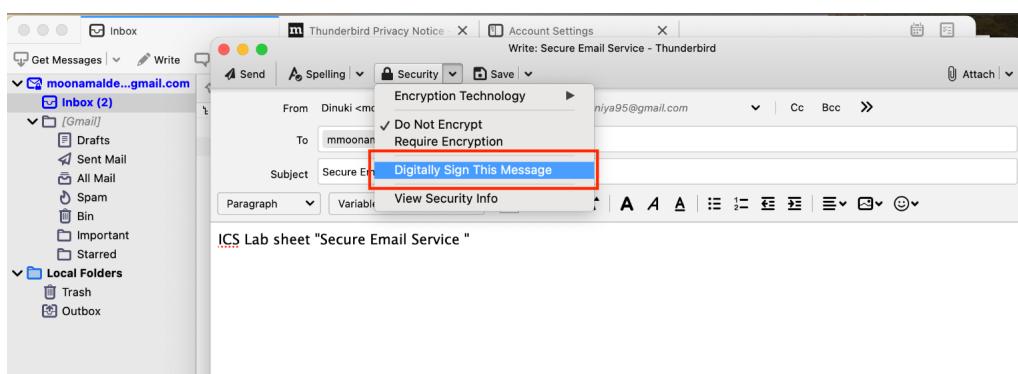




7. Go back to “End-To-End Encryption” in “Settings” and select your certification for “Personal Certification for digital signing” and “Personal Certification for encryption”



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”

A screenshot of an email client interface. The top header shows the From field as "menaka <mmoonamaldeniya@gmail.com>" and the Subject as "Secure E-mail service". The recipient is "To Me". The time is 16:17 and the S/MIME status is shown. The main body of the email is titled "Reply to secure Email services". On the right side, there is a "Message Security - S/MIME" panel. It contains a section titled "Message Is Signed" which states "This message includes a valid digital signature. The message has not been altered since it was sent." Below this, it shows "Signed by: menaka", "Email address: mmoonamaldeniya@gmail.com", and "Certificate issued by: CA". A red box highlights the "View Signature Certificate" button. Another section below is titled "Message Is Not Encrypted" with the note "This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit."

10. you can see certification details.

A screenshot of a certificate details page. The title is "Certificate". At the top, there is a search bar with the name "menaka". The page displays two sets of certificate details. The first set is for the "Subject Name" and includes fields for Country (LK), State/Province (Western), Organization (SLIIT), Organizational Unit (FOC), Common Name (menaka), and Email Address (mmoonamaldeniya@gmail.com). The second set is for the "Issuer Name" and includes fields for Country (LK), State/Province (Western), Locality (Colombo), Organization (SLIIT), Organizational Unit (FOC), Common Name (CA), and Email Address (CA@gmail.com). Both sets also show "Validity" information. The "Not Before" date is 4/24/2021, 3:20:12 PM (India Standard Time) and the "Not After" date is 4/24/2022, 3:20:12 PM (India Standard Time). At the bottom, there is a "Public Key Info" section with the "Algorithm" listed as RSA.