



Sending Encrypted and Digitally Signed emails

Pre-requisites:

1. Thunderbird1.5 or greater has to be installed.
2. Sendmail has to be installed. (It is already in linux.)
3. Dovecot has to be installed.
4. Openssl has to be installed. (It is already in linux.)

Configuration of dovecot

You have to configure Dovecot with 'dovecot.conf' file. When you have installed Dovecot it has also installed a '/usr/local/etc/dovecot-example.conf' file. Which You'll have to rename to /usr/local/etc/dovecot.conf.

In the file '/etc/dovecot.conf' change the value of 'protocols' to 'protocols = pop3'.

Authentication

You'll probably be using PAM authentication. See the PAM page for how to configure it

A typical configuration with Linux would be to create '/etc/pam.d/dovecot' which contains:

auth	required	pam_unix.so
account	required	pam_unix.so

Pre-setup:

1. Start the sendmail.
2. Start the dovecot.
3. Create pki directory (mkdir pki)
4. Create public,private,client directories under pki
5. Create self-signed CA certificate.
6. Create server certificate signed by CA and create PKCS12 file.
7. Create client certificate signed by CA

To start the sendmail:

First login in system as root and check the status of sendmail by the command

/sbin/service sendmail status

if **sendmail is running , sm-client is running** then sendmail is running on your machine

if **sendmail is stopped, sm-client is stopped** then we have to start the sendmail by the command

/sbin/service sendmail start

To start the dovecot:

Login in system as root and start the dovecot by the following command.

/usr/local/sbin/dovecot

Creation of self signed CA certificate:

Create private key for CA, ca.key in the directory private with the following command:

openssl genrsa -des3 -out private/ca.key 1024

Enter pass phrase for private/ca.key : 'ca-password'

Verifying- Enter pass phrase for private/ca.key : 'ca-password'

After that you can self-sign your CA certificate for a long period of time if you wish. Specify

Some information regarding your country, location, etc...

openssl req -new -x509 -key private/ca.key -out public/ca.crt -days 3600

```
Enter pass phrase : 'ca-password'
Country          : IN
State            : Karnatka
Locality         : Bangalore
Organization     : C-DAC
Organization unit : CNIE
Common Name      : CA
Email address    : ca@hgdrd1.cdacbangalore.in
```

Create server certificate signed by CA and create PKCS12 file

First you generate the your private key encoded (-des3), and protected with a strong password.

```
openssl genrsa -des3 -out private/yourname.key 1024
```

```
Enter pass phrase for private/ca.key : 'your-password'  
Verifying- Enter pass phrase for private/ca.key : 'your-password'
```

Then you can create your certificate signing request (csr). We can send it to CA for signing

```
openssl req -new -key private/yourname.key -out yourname.csr
```

```
Enter pass phrase : ' your-password'  
Country : IN  
State : Karnatka  
Locality : Bangalore  
Organization : C-DAC  
Organization unit : CNIE  
Common Name : Abhijit  
Email address : abhijit@hgdrd1.cdacbangalore.in
```

This is the way you can sign your server certificate with your CA:

```
openssl x509 -req -days 360 -in yourname.csr -CA public/ca.crt -CAkey  
private/ca.key -CAcreateserial -out public/yourname.crt
```

```
Enter pass phrase: 'ca-password'
```

Client certificate creation and signing

Now, we will create our client private key and our CSR (Certificate Signing Request) in one command with openssl:

```
openssl req -new -newkey rsa:1024 -nodes -out client/client.req -keyout  
client/client.key
```

Then sign the csr with your own CA (you will have to specify the pass-phrase of the CA):

```
openssl x509 -CA public/ca.crt -CAkey private/ca.key -CAserial public/ca.srl -req
```

-in client/client.req -out client/client.pem -days 100

```
Enter pass phrase      :      'ca-password'  
Country               :      IN  
State                 :      Karnataka  
Locality              :      Bangalore  
Organization          :      C-DAC  
Organization unit     :      CNIE  
Common Name          :      Clinet-name  
Email address         :      client@hgdrd1.cdacbangalore.in
```

Export client certificate as keychain in pkcs12/java keystore

**openssl pkcs12 -export -clcerts -in client/client.pem -inkey
client/client.key**

-out client/client.p12 -name your_certificate_client_name

Adding account to thunderbird email client

- Open Thunderbird, and goto 'Edit'->'Account Settings'.
- Select 'Email account,' and click 'Next.'
- Enter your user name in the 'Your Name:' field. Enter your host email address in the 'Email Address:' field, and click 'Next.'
(Here e-mail address will be [username@yourhostname.domainname](#))
- Select the type of incoming server name.(If you are running pop server select 'pop' radio button. If you are running IMAP server select 'IMAP' radio button.), and enter your incoming server name (Here it will be your host name only).
- Enter your username in 'Incoming user name' text box and click 'Next'
- Enter your username in 'Account Name' text box and click 'Next'
- Verify your account information in the dialogue box, and click 'Finish.'
- In 'Account Settings' window select 'Outgoing Server(SMTP)' and select 'Add'.
- Enter some description in 'Description' text box , enter 'Server Name'(Here it is your host name.) and then enter your user name and select 'No' radio button for 'Use Secure Connection' field. Then select 'OK' button.

Importing Certificates to Thunderbird email client:

- Set Master password
Goto 'Edit'->'Preferences'->'Passwords'->'Change Master Password' and enter the master password. Click 'OK' button.
- Goto 'Edit'->'Preferences'->'Security'->'View Certificates'->'Authorities' then click on 'Import' to import CA certificate. Then import CA certificate created by you earlier.
- Then select 'Your Certificate' tab. Then 'Import' your certificate i.e. Server certificate created earlier.
- Then select 'Other People's' tab. Then 'Import' client certificate created by you earlier.
- Now you are ready to send/receive encrypted digitally signed mails from your trusted clients.

Sending Digitally signed and encrypted mails from thunderbird email client:

- Click on 'write' then you will get write pad and then enter required information in that pad.
- Then choose 'security' pulldown menu. Then select 'Encrypt this Message' radio button and select 'Digitally Sign This Message'.
- Then send the message...