Document Signing (in Ubuntu)

Users will get 2 certificates from CA-
1.   User certificate for document/signing purpose.
2.   CA's root certificate, used to verify/authorize the user certificate.

User certificate will be in PKCS12 format. Also, user will set a password to import/export the certificate. File name will be, for example, testuser.p12.

CA's certificate will be in DER/PEM format. File name will be, such as, rootCA.crt.

User will first import the certificate into Mozilla Firefox browser. Open Firefox, click on Edit-> preferences.
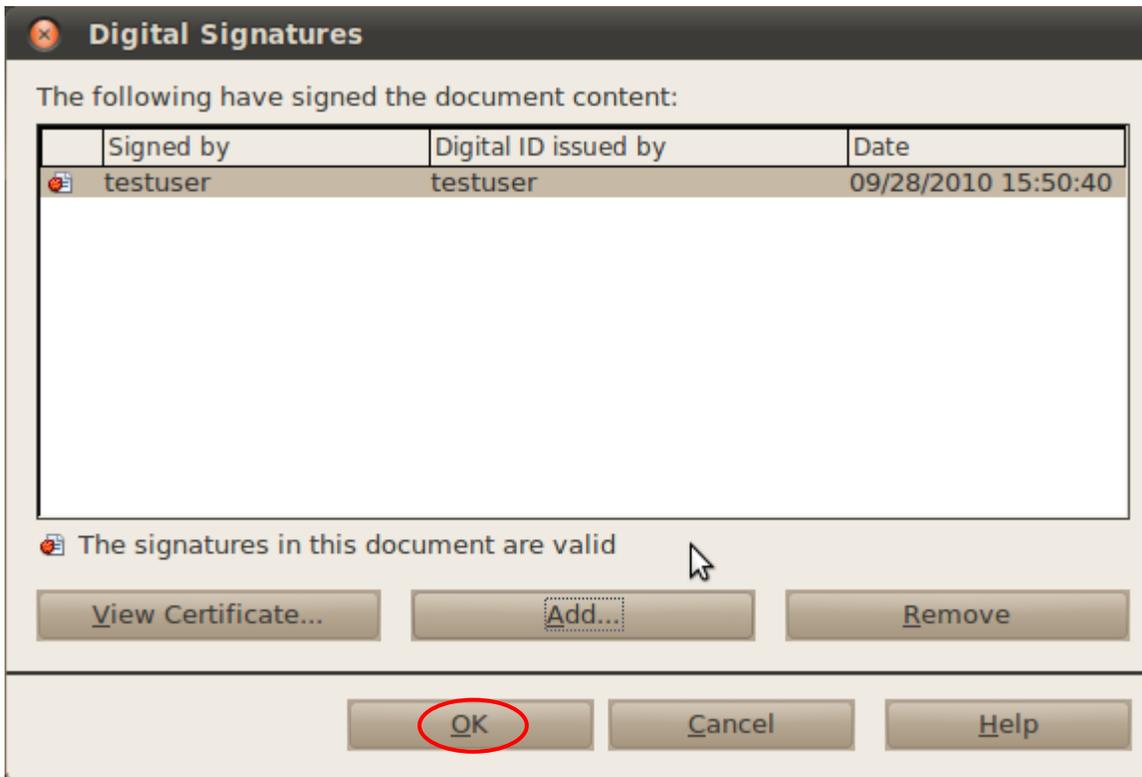
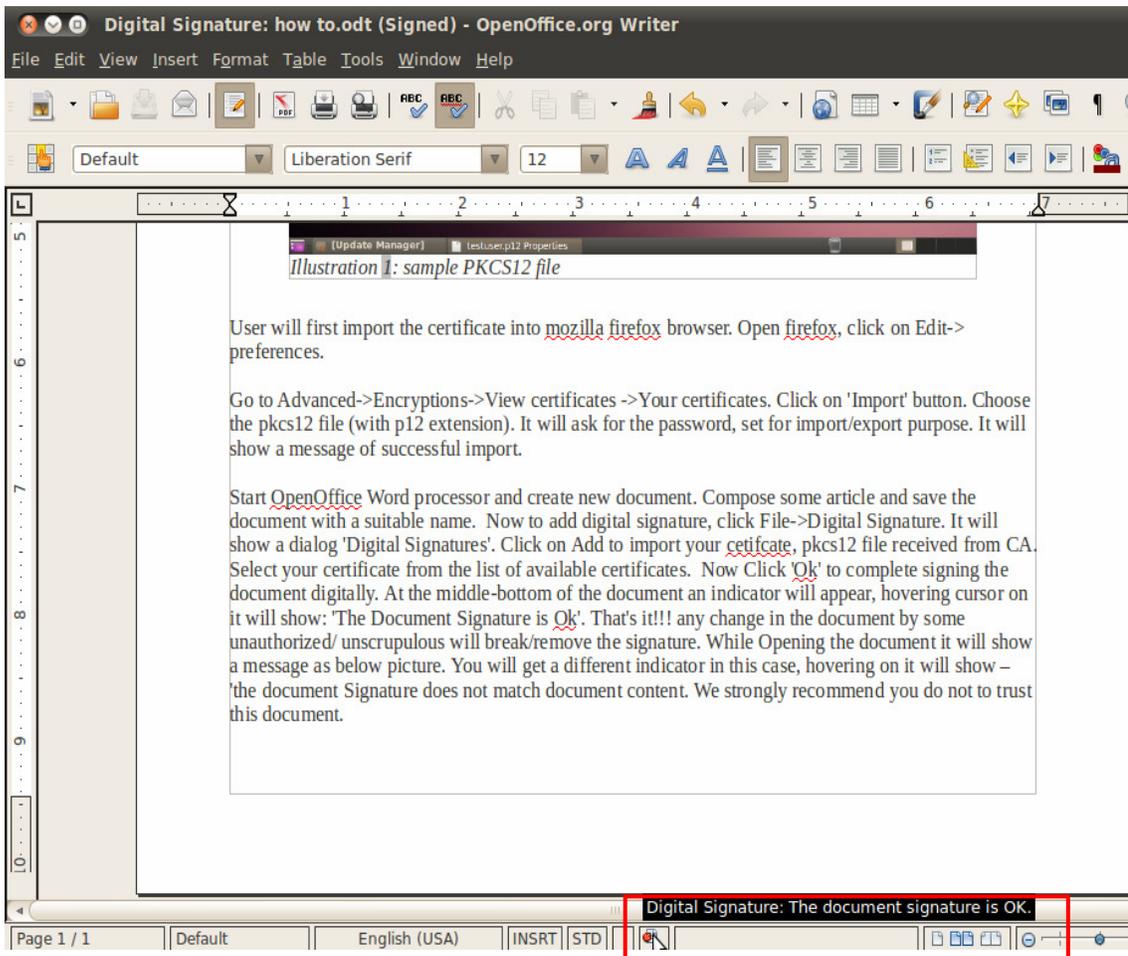Go to Advanced->Encryptions->View certificates ->Your certificates. Click on 'Import' button.

Choose the pkcs12 file (with p12 extension). It will ask for the password, set for import/export purpose.

Upon entering password, It will show a message of successful import.

Start OpenOffice Word processor and create new document. Compose some article and save the document with a suitable name. Now to add digital signature, click File->Digital Signature.

It will show a dialog 'Digital Signatures'. Click on Add.

Digital Signatures

The following have signed the document content:

Signed by	Digital ID issued by	Date

View Certificate...   Add...   Remove

OK   Cancel   Help

Select your certificate from the list of available certificates. Now Click 'Ok' to complete signing the document digitally.

Digital Signatures

The following have signed the document content:

	Signed by	Digital ID issued by	Date
	testuser	testuser	09/28/2010 15:50:40

The signatures in this document are valid

View Certificate...	Add...	Remove

OK	Cancel	Help

At the middle-bottom of the document an indicator will appear, hovering cursor on it will show: 'The Document Signature is Ok'.
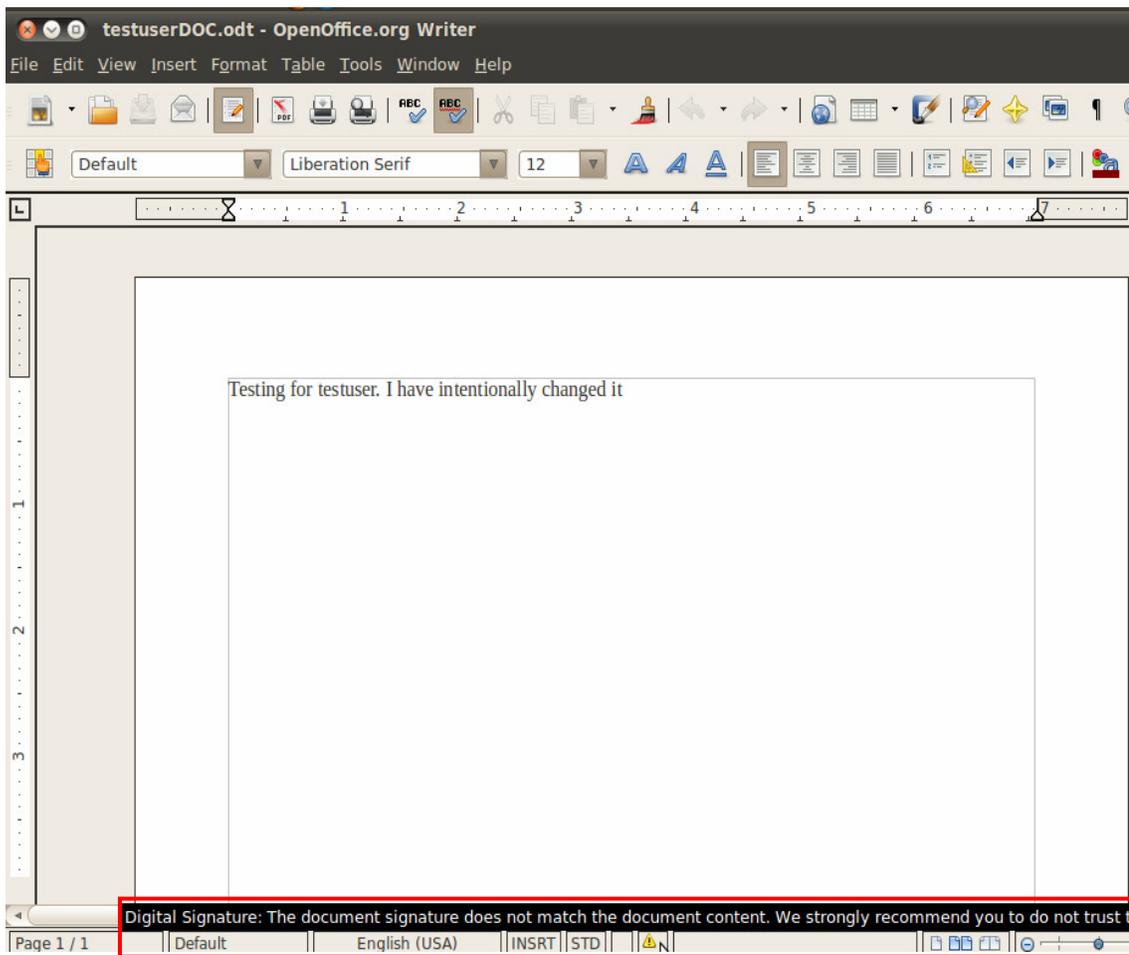
Illustration 1: sample PKCS12 file

User will first import the certificate into mozilla firefox browser. Open firefox, click on Edit-> preferences.

Go to Advanced->Encryptions->View certificates ->Your certificates. Click on 'Import' button. Choose the pkcs12 file (with p12 extension). It will ask for the password, set for import/export purpose. It will show a message of successful import.

Start OpenOffice Word processor and create new document. Compose some article and save the document with a suitable name. Now to add digital signature, click File->Digital Signature. It will show a dialog 'Digital Signatures'. Click on Add to import your cetifcate, pkcs12 file received from CA. Select your certificate from the list of available certificates. Now Click 'Ok' to complete signing the document digitally. At the middle-bottom of the document an indicator will appear, hovering cursor on it will show: 'The Document Signature is Ok'. That's it!!! any change in the document by some unauthorized/ unscrupulous will break/remove the signature. While Opening the document it will show a message as below picture. You will get a different indicator in this case, hovering on it will show – 'the document Signature does not match document content. We strongly recommend you do not to trust this document.

 That's it!!! any change in the document by some unauthorized/ unscrupulous will break/remove the signature. While Opening the document it will show a message as below

picture.

You will get a different indicator in this case, hovering on it will show – 'the document Signature does not match document content. We strongly recommend you do not to trust this document.'

Email signing (Ubuntu)

We will show email signing with Evolution mail client, shipped as default mail client with Ubuntu 10.04.

Open Evolution mail Client from the top-right corner of your Ubuntu Desktop.

At first we need to import the pkcs12 files for signing mail with digital signature. Now go to Edit->preferences->certificates->Your Certificates. Click on the Import button.

Choose your pkcs12 file from Ubuntu file system. It will ask for 2 passwords – 1 for evolution mail client security purpose and 1 for import/export purpose.

Upon entering valid passwords, it will successfully import the certificate into evolution system.

Clicking on view will show the certificate details.

Certificate Viewer: testuserMailCSR

General | Details

This certificate has been verified for the following uses:

SSL Client Certificate
SSL Server Certificate
Email Signer Certificate
Email Recipient Certificate

Issued To
Common Name (CN)   testuser@UbuntuOS.com
Organization (O)   BCC
Organizational Unit (OU) CCA
Serial Number   08
Issued By
Common Name (CN)   rootCA
Organization (O)   BCC
Organizational Unit (OU) CCA
Validity
Issued On   14/08/2010
Expires On   14/08/2011
Fingerprints
SHA1 Fingerprint   E3:5B:CA:68:02:FA:A2:38:45:D0:2A:23:47:0A:2A:3A:91:A7:E1:EB
MD5 Fingerprint   40:20:65:67:2E:13:0E:AE:77:C6:21:F6:CD:F7:E1:09

Close

Now users need to import CA's certificate also into the evolution system. go to Edit->preferences->certificates->Authorities. It will show available root CA certificates.

Evolution Preferences

Your Certificates | Contact Certificates | Authorities

You have certificates on file that identify these certificate authorities:

Mail Accounts

Contacts

Mail Preferences

Composer Preferences

Network Preferences

Calendar and Tasks

Certificates

Help

Certificate Name   View

+ ABA.ECOM, INC.   Edit
+ AC Camerfirma SA CIF A82743287
+ AddTrust AB   Import
+ America Online Inc.
+ AOL Time Warner Inc.   Delete
+ AS Sertifitseerimiskeskus
  Autoridad de Certificacion Firmaprofesional CIF A62634068
+ Baltimore
+ BCC
+ beTRUSTed
+ Buypass AS-983163327
+ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmet
+ Certplus
+ certSIGN
+ Chunghwa Telecom Co., Ltd.
+ CNNIC
+ Comodo CA Limited
+ COMODO CA Limited
+ ComSign
+ Cybertrust, Inc
+ Deutscher Sparkassen Verlag GmbH

Click on the Import button. Choose CA's certificate DER/PEM file from Ubuntu file system. It will show a message for trusting CA. Check 'Trust this CA to identify web sites' and 'Trust This CA to identify email users'.

Click Ok and it will successfully import the CA certificate into evolution system. Clicking on view will show the certificate details.

Still another step remains: go to Edit->preferences->Mail Accounts.
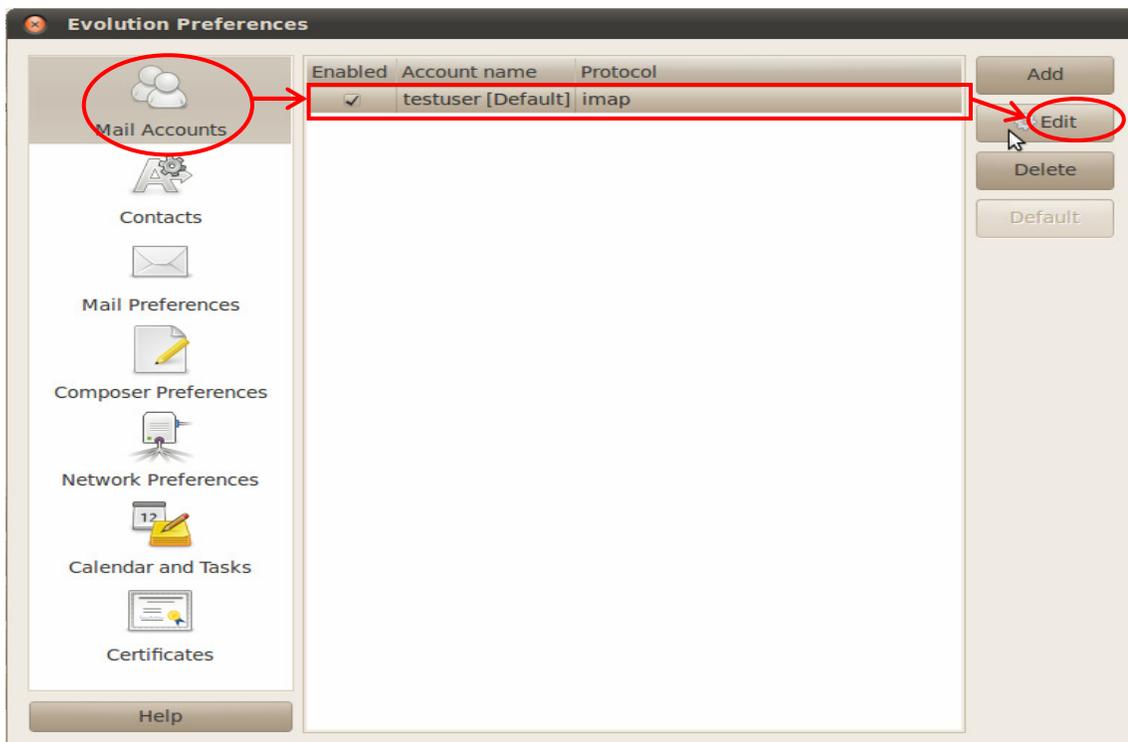
It will show user account details. Choose your user account and click on 'Edit' button. Next, click on 'Security' tab. It will show certificate status of your mail account.
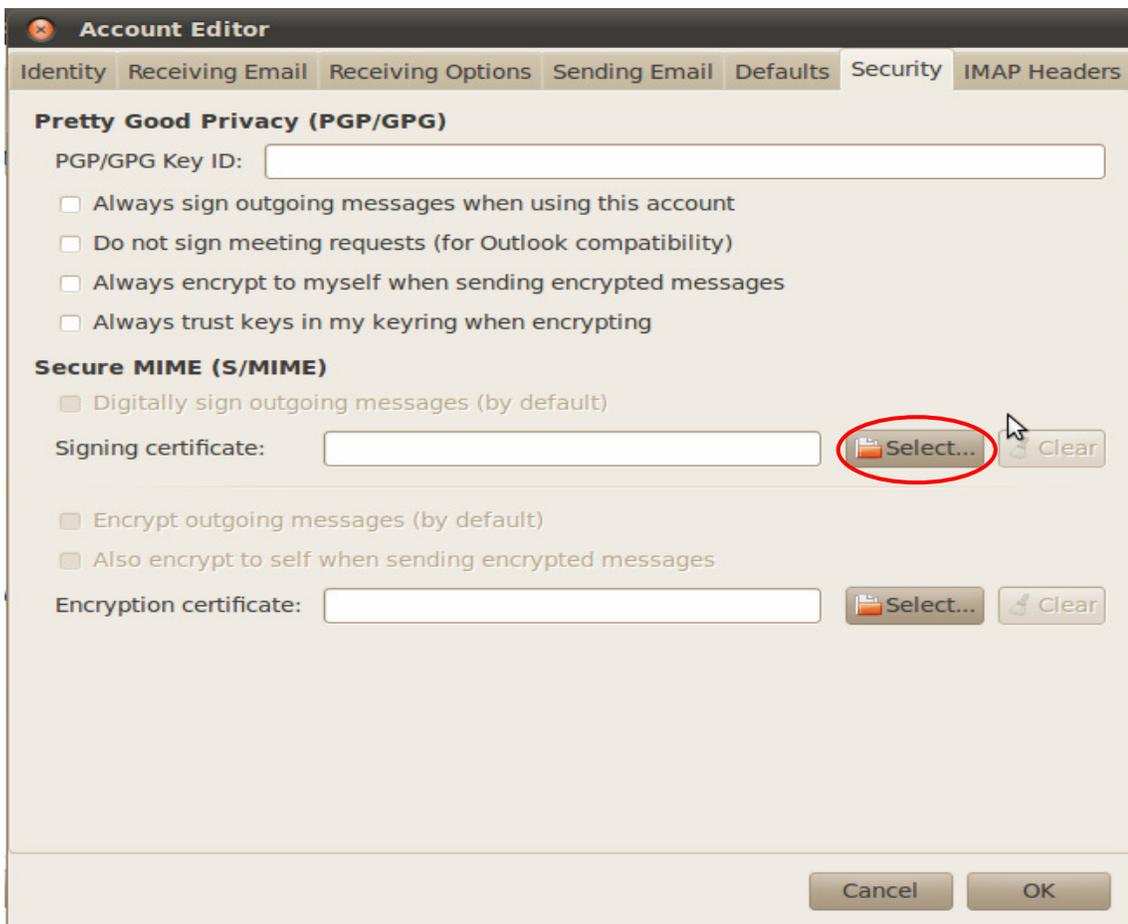
Now, click on 'Select' button and choose your certificate for mail signing.

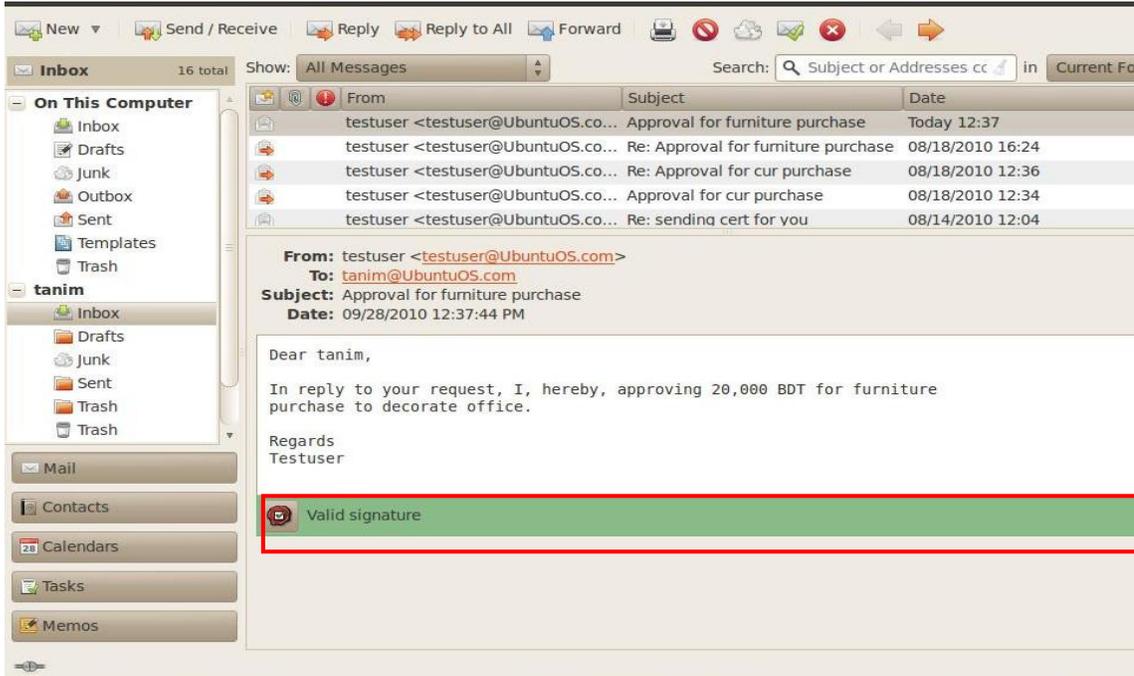Yes, your mail account is now enabled to send digitally signed mails!!!

Now compose a new mail. Click on Security and again click on 'S/MIME Sign'. The option will be checked as shown below.
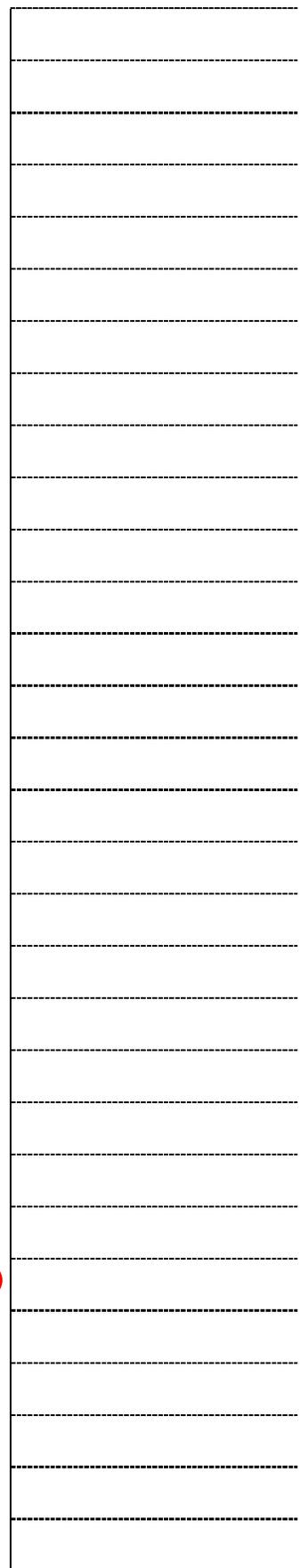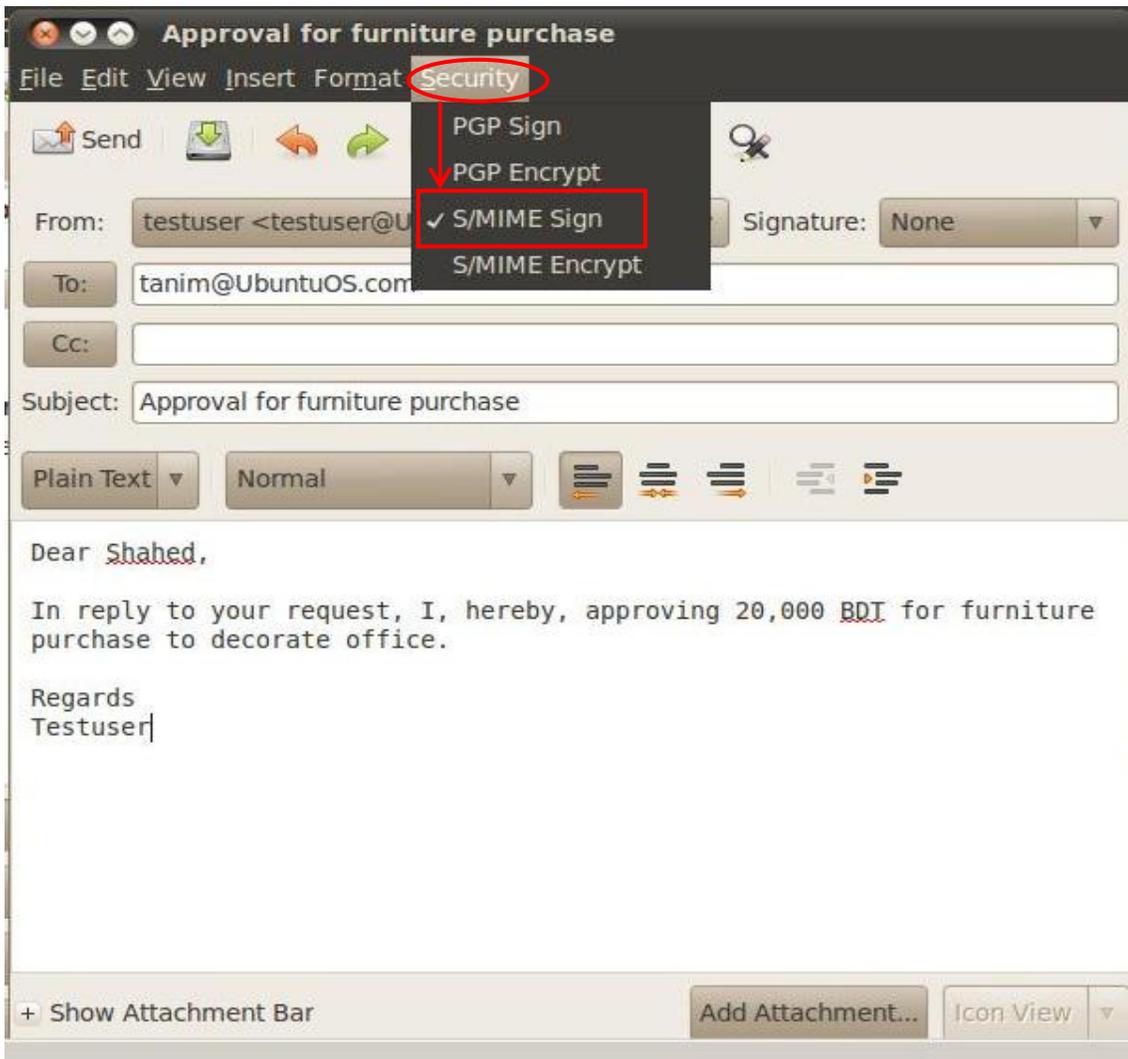
Now send the mail and it will send the mail by digitally signing!!!
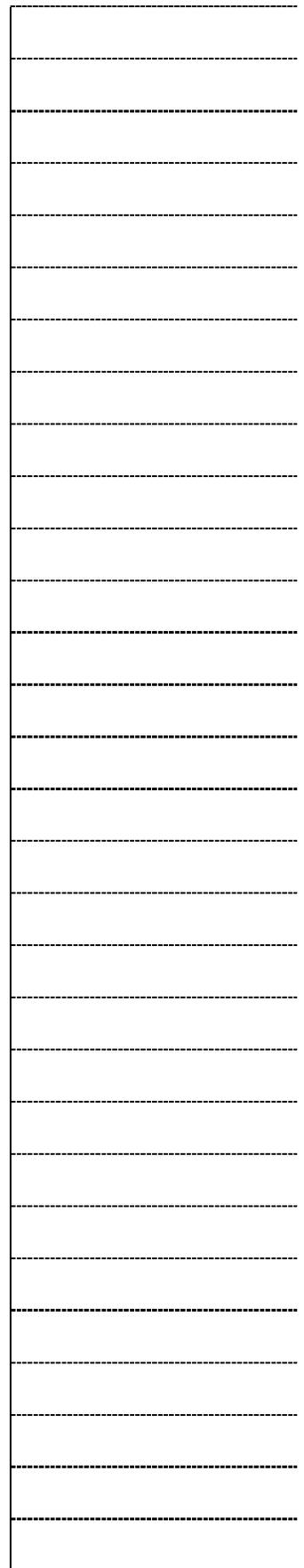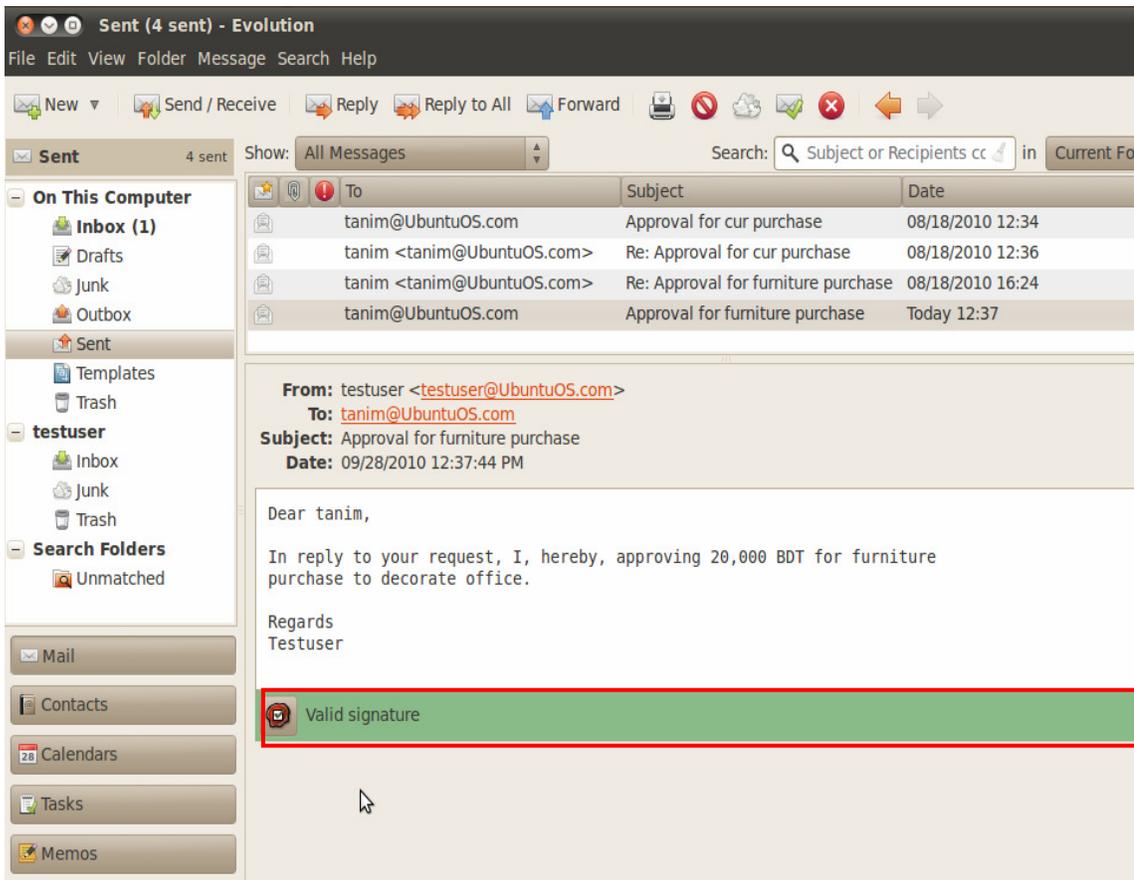
At the receiving end, user will configure his/her Evolution mail client as described above. When he/she receives the mail,

it will also indicate if the signature is valid or some unscrupulous user have tampered with it. If it's being changed by some intermediate hacker/cracker, it will show a red colored warning -