**GPG configuration**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrypting and verifying files</td>
<td>55</td>
</tr>
<tr>
<td>Linux</td>
<td>57</td>
</tr>
<tr>
<td>Install GNUPG</td>
<td>57</td>
</tr>
<tr>
<td>Configure the software</td>
<td>58</td>
</tr>
<tr>
<td>Configure GnuPG files</td>
<td>58</td>
</tr>
<tr>
<td>Create your own set of keys</td>
<td>60</td>
</tr>
<tr>
<td>Upload key to keyserver</td>
<td>65</td>
</tr>
<tr>
<td>Import keys</td>
<td>68</td>
</tr>
<tr>
<td>Fetched keys</td>
<td>68</td>
</tr>
<tr>
<td>Manually import keys</td>
<td>69</td>
</tr>
<tr>
<td>Validate keys</td>
<td>71</td>
</tr>
<tr>
<td>Email encryption in Thunderbird on Linux</td>
<td>73</td>
</tr>
<tr>
<td>Settings</td>
<td>73</td>
</tr>
<tr>
<td>Sign and Encrypt emails</td>
<td>76</td>
</tr>
<tr>
<td>Decrypt and Verify emails</td>
<td>78</td>
</tr>
<tr>
<td>Files</td>
<td>81</td>
</tr>
<tr>
<td>Sign and Encrypt files</td>
<td>81</td>
</tr>
<tr>
<td>Decrypt and verify files</td>
<td>82</td>
</tr>
</tbody>
</table>
GPG installation and configuration

Introduction
Before I start explaining how to use GPG you must understand that after the installation and configuration:

- you will have two OpenPGP keys: 1 public, 1 secret;
- the public key is used for encrypting and verifying;
- the secret key is used for decrypting and signing.

You can share your public key with anyone and publish it anywhere you want, but you shouldn’t share your secret key with anyone. Your private key, just like your password, is yours and yours only.

This is how an OpenPGP public key looks like:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2
mQENBFZy+BQBCADIx4Id6gYd2NFNR5XXBwHj/LcYhqT2IbxO5eOLt6VkJWZ7rdF
yTV9IPkggHCl10/QMftcYo3ZMHQSXDITX3YESTO9++umUq2X8wpZ2ZKnqMRbZl
aD0ZQqK9fx9GZGXcVH96x9AWRX/1ChBVoSngHxkBpQYkU6zVO9S1QuRijq0Prlsa
JuZDEr050Wsx8aKvoB1NWjLhiHj4+Q68bVL6g6pVWxq9910DEADgZ62is9A4E8
xVlr3hG3u6v5s15/J2/KZLsgS/k8liQ7e4IF86WWEby/Klm4R1+0vbrf4jU6Ytxq
Lah1Q9fvMMLUnTz7rdzPOcWWUudvQEBASkk0VABEAAG0HE1hcmlsZW5hIEVudXMg
PG1JbnVzQHV3by5jYT6JacEHEAAKsFAlZy+BoXCoAB6ShHOeEfstdt1dn2xAu8z
2s41chJhrRMANIQMzep2RilcG65gupLCAr0LBRi+w30cQ
=XhPL
-----END PGP PUBLIC KEY BLOCK-----
GPG configuration

And this is how an OpenPGP private key looks like:

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: GnuPG v2
IQPGBFZy+BQBCADlIx4zID6gYd2NFNR5KXBwHj/LcYhqT2IbxO5eOLt6VkWz7rdF
yTV9IPkggHctL1Q/QMfcIYo3ZMZHQ5XDlTX3YESTO9++umUq2X8wpZ2ZkJqMRbZl
aD0ZQaK9fx9GZGXcVH969yAWRX/IChBV0sNgHgxKBpQykU6zVO951QuRj/qOPLsa
JuZDEr050WSx8aKaV0B1NLwjlHiHj4+Q6BbVL6gpVWxq9910DEADgZ62Is9A4E8
xVlr3hG3u6Vs15/J2/KZLsgS/k8liQ7e4IF86WWEby/KIm4R1+0vbRI4jU6Yttxq
Lah1Q9fvMMlUnTz7rdzPOcWWWdVQEBASkk0VABEBAAH+BwMCtBYYx760gc3H3Z8c
FgzzNMrgfzeZQjIPPe3tgiBYyk279jcCbxelwAMPGYsPKqjP5B2F4BFjryp5j6
8xJdHFLq5kqMKQAYzj3ugTUyUu0xvLyckpNW57FnNqhpqvgabBl4eN2wPyv
xITaZjVyEmGtEwA0hAzNt6nZGKVzAazpKDOksICvQsFGL7DfRxA=
=1XX3
-----END PGP PRIVATE KEY BLOCK-----
```

Passphrase in this document means a long and complicated password that no one could ever guess or know but you. The passphrase is a part of your secret/private key and prevents anyone but you from using it. Make sure you store the password somewhere safe. That means not on a sticky note underneath your keyboard.

The terms private and secret keys can be used interchangeably.

Validating a key means:
- checking with the owner that the key belongs to them;
- signing the key with your own key.

In emails, when you choose to encrypt, the subject line will always remain in clear text. Only the body of the email will be encrypted. If you want to attach a file, you will have to encrypt it separately and attach that.

Every time you sign, you’ll have to enter your passphrase to unlock your secret key. Your signature is needed to let your recipient know the file/ email sent are really from you and not someone impersonating you.

When you encrypt an email or a file, encrypt it for yourself too if you want to be able to decrypt it later.
Windows

Install GPG4WIN

Install gpg4win:

- for the 32 bit version of Outlook download and install the full version of [Gpg4win 2.3.0](https://www.gpg4win.com)
- for the 64 bit version of Outlook download and install gpg4win-3.0.0-beta128.exe

All the default options for the installation should be fine, just make sure you install all Gpg4win components (fig. 1). Kleopatra is the key manager, GPA is another tool for encryption/decryption, GpgOL is the add-on for Outlook, GpgEX is for encrypting files and the Compendium is the Gpg4win documentation.

![Gpg4win Setup](https://example.com/gpg4win_setup.png)

*fig. 1 Installation process*

After clicking Finish and Reboot check if GpgOL is installed and enabled in Outlook.

If it’s properly installed you should see:

- in Outlook 64bits - two buttons in the far right side of the ribbon, Encrypt and Sign, when you write a new email (fig. 2)
- in Outlook 32bits – a new tab in the far right side of the ribbon called GpgOL (fig. 3)
GPG configuration

fig. 2 – GpgOL in Outlook 64bits

fig. 3 – GpgOL in Outlook 32bits

If you can’t find it, check if the add-on is enabled. In Outlook, go to File → Options → Add-Ins → Manage COM Add-ins / Disabled items → click on Go (fig. 4-7). Make sure that the add-on is not in the disabled items list and that it’s checked in the COM Add-Ins (fig. 7).

fig. 4 Verify Add-on installation

COM Add-ins
Disabled Items

fig. 5 Manage add-ons options
Configure the certificate manager

Configure GPG

Download the organization’s certificate

If you have admin rights, from the keyserver, https://keys.uwo.ca:9000, download UWO’s certificate. Go to Keys → Organization Keys → Organization Certificate → Export → Save File to C:\Users\YOURUSERID\AppData\Roaming\gnupg and rename it uwo.pem (fig. 8).

If you can’t access the server then copy the text below and paste it in a file called uwo.pem. Please note that by the time you read and install this certificate, the information pasted below might be expired.

-----BEGIN CERTIFICATE-----
MIIEIzCCAugAwIBAgIUEWk7SdEsnmTuNlfvIT/A4VmStnJ0wDQYJKoZIhvcNAQEF
GPG configuration

BQAwgZ8xZdANBgNVBAMTBNB3by5jYTEeMBkGA1UEChMMb25zdG9yeS5jb20vY3JlYXRlcyBDb259
-----END CERTIFICATE-----

fig. 8 Download Organization Certificate
Set the keyserver and certificate

Close Outlook and GPG and configure your key manager by adding the following lines in the file
\C\Users\Your User ID\AppData\Roaming\gnupg\gpg.conf:

```
####+--- GPGConf +++++---
keyserver-options ca-cert-file=path\to\this\file\uwo.pem
keyserver-options no-honor-keyserver-url
keyserver-options auto-key-retrieve,verbose,timeout=120
utf8-strings
auto-key-locate local, keyserver
keyserver ldap://keys.uwo.ca
```

Create your own set of keys

Encryption works with keys and you need your own set of keys to make things work.
Open Kleopatra and click on **File → New Certificate → Create a personal OpenPGP key pair** (fig.9-12).

![fig. 9 Kleopatra - New certificate creation](image-url)
Fill in your *Name* and *Email*, click *Next*, *Create Key* and enter your passphrase twice. Make sure your passphrase is strong and unbreakable (fig. 11). This password is what protects your secret key. If someone gets a hold of your secret key, they cannot use it because it’s encrypted with your passphrase. Only your passphrase can unlock your private key.

Make a backup of your secret key, in case you change computers and you want to import your key. Click *Finish* (fig. 12).
Upload your public key to the keyserver

You can export your public key by selecting your name under My Certificates tab in Kleopatra and clicking on File ➝ Export Certificates. Choose an appropriate location, optionally change the name of the file and click on Save. You can view the file content with any text editor. The file starts with “----BEGIN PGP PUBLIC KEY BLOCK----” and ends with “----END PGP PUBLIC KEY BLOCK----”. Upload your public certificate to UWO’s keyserver so that others can find it and encrypt emails and files they want to send to you. Go to http://keys.uwo.ca/vkd/GetWelcomeScreen.event and publish your key twice. Test if the keyserver has successfully received your public key by looking up your certificate in Kleopatra (fig. 13). Click on Lookup Certificates on Server, type in your name and click Search. You can also send someone your public key by email or USB. If you upload your key to the UWO keyserver, anybody can retrieve it from the keyserver directly.
GPG configuration

fig. 13 Lookup your certificate on the keyserver

Importing keys

Manually import keys

Import your keys
If and when you change your computer you can import your key pair into your newly installed GPG. In your old system, in Kleopatra, search for your name, right click and select Export Secret Keys/Export Certificates and browse to where you want the keys to be saved. Copy your keypair onto your new computer, open Kleopatra, click on Import Certificates, browse to the location of your secret key, select the key and click Open. Do the same with your public key.

Import someone else’s public key:
1. If he/ she is a Western user then, in Kleopatra, click on Lookup Certificate on Server, type in their name, click Search, select the user from the list, click Import and OK (fig. 14-15).
2. If the person has sent you their public key via email or other means, save the public key to your computer, open Kleopatra, click on Import Certificates, browse to where you saved the key, click Open and OK.

3. If they have their public key up on a different key server, then go to Kleopatra, Settings, Configure Kleopatra. Because Kleopatra can handle only one OpenPGP entry and several X.509 certificate servers, in the Directory Services options, delete the ldap://keys.uwo.ca:389 OpenPGP server and add the OpenPGP pool of servers hkp://pool.sks-keyservers.net:11371. Click OK and search for this person’s key by clicking on Lookup Certificate on Server (fig 16-18).
GPG configuration

fig. 16 Directory Services in Kleopatra
fig. 17 Changing the keyserver

fig. 18 Certificate lookup
GPG configuration

After you find the person you were looking for, don’t forget to set the OpenPGP server back to ldap://keys.uwo.ca.

Now, after configuring GPG and having your own set of keys, you should be able to send and receive signed and encrypted emails.

Fetched keys

Thanks to the modifications we made to the GPG configuration after installing the software, Kleopatra (the key manager) will automatically import the public key of the users who have sent you a signed email, if it finds them on the keyserver. The retrieved keys will not be automatically validated. You will have to check with the owner to see if the key is actually theirs and when you’re sure that the key belongs to the right person only then you should sign it with your own.

Validate keys

The keys that are in your database, either manually imported or automatically retrieved, will not be validated unless you sign each of them with your secret key. This should be done only after you checked with the owner that that is in fact his/ her key.

Until then, every time you will receive a signed email from someone, the message from the images below will appear (fig. 19-20).

![Decrypt/Verify E-Mail](image)

**Results**

Status and progress of the crypto operations is shown here.

All operations completed.

RE: All the letters of the alphabet: **Decryption succeeded.**

RE: All the letters of the alphabet: **Not enough information to check signature validity.**

Signed on 2016-01-29 14:05 with unknown certificate 0xC68194FA3A962C0.
The signature is invalid: No public certificate to verify the signature

**fig. 19 Verifying signature after fetching key**
You can validate keys by doing the following:

- go to Kleopatra
- right click the key you want to validate
- select *Certify Certificate*
- the new window check the userIDs you want to validate
- check “I have verified the fingerprint”
- click *Next, Certify* and *Finish* (fig. 21-23)
GPG configuration

fig. 21 Certify certificate

fig. 22 Certify certificate
Encrypting emails with Outlook on Windows

Signing and encrypting emails

With GpgOL installed, when you compose a new email you should see the Encrypt and Sign options on the far right of the window (fig. 24).
Enable the *Encrypt and/ or Sign* button before sending the email and keep in mind that the content of the email will be encrypted, but the title will remain in clear text. Kleopatra will automatically encrypt with your public key too so you can be able to read your emails after you send them.

After clicking on Send, a window asking you to select the encryption certificates will appear (fig. 25).

Kleopatra will automatically detect your key and your recipient’s key if you have imported it already (fig. 25).

If you didn’t import your recipient’s key, besides the previously mentioned methods, you can also click on the button with three dots next to the recipient’s email address and import the key from there (fig. 26-28).
When you click on Send, Kleopatra will ask for your passphrase.

A quick recap... emails are:
- encrypted with the recipient’s public key and decrypted with their secret key
- signed with your secret key and verified with your public key.

Please note that Kleopatra will automatically import the public keys of those who have sent you a signed email. You will see the message Not enough information to check signature validity (fig. 29-30) which essentially means that you have to check with the sender that the signed email comes from them and the key is theirs. Only then you can sign it with your key so that future emails coming from them show “Valid signature from ...” if it matches the one you certified (fig. 23).
GPG configuration

Decryption and verifying emails

Kleopatra

Kleopatra for the 64bit version of Outlook automatically detects an encrypted email and asks for your passphrase when you open it. In the 32bit version of Outlook you can decrypt an email by double clicking the email, going to the GpgOL tab and selecting Decrypt and/or Verify. You will be prompted to enter your passphrase (fig. 29).

Because there are many different platforms and many different email clients, Kleopatra doesn’t always detect an encrypted email so you won’t be able to decrypt it just by opening it or clicking on the Decrypt button. If you want to read it or verify the signature you will have to use the GPG tool called GPA.

GPA – GNU Privacy Assistant

In order to decrypt and verify the email, copy and paste the content into GPA’s clipboard and click on Decrypt/ Verify (fig. 30-31). If encrypted, the software will ask for your passphrase and you’ll be able to read the content in clear text.
fig. 30 GPA Keyring manager-click on Clipboard
GPG configuration

**File encryption with GpgEX**

**Signing and encrypting files**

If you want to attach a file to your email you can sign and encrypt it by right clicking the file and choosing *Sign and encrypt* (fig. 32). With signing you’re making sure that if changed by an authorized person the file will show “Bad signature” when verified.

This is the sequence of steps to take: choose what you want to do with the file/ folder (fig. 33), choose for whom you want to encrypt (fig. 34), choose one of your keys (if multiple) to sign it with (fig. 35) and enter your passphrase (fig. 36). The successful encryption will be confirmed or infirmed (fig. 37) as a result. You will see your file/ folder in the same location as the original, but with a different extension and unreadable without the secret key and passphrase.

---

In case the body of the email comes as an attachment, you’ll have to open/ save the attachment, copy and paste the content into GPA and decrypt it.

**fig. 31 Decrypt and Verify with GPA**
fig. 32 Signing and encrypting a file
GPG configuration

![Sign/Encrypt Files dialog box]

**What do you want to do?**

Please select here whether you want to sign or encrypt files.

Selected file:
- C:/Users/menus/Desktop/keys.uwo.ca.jpg

- Archive files with: TAR (PGP@-compatible)
- Archive name (OpenPGP): C:/Users/menus/Desktop/keys.uwo.ca.jpg.tar
- Archive name (S/MIME): C:/Users/menus/Desktop/keys.uwo.ca.jpg.tar.cer

- **Sign and Encrypt (OpenPGP only)**
- Encrypt
- Sign

- Text output (ASCII armor)
- Remove unencrypted original file when done

Next  |  Cancel

*fig. 33 File Encryption options*
For whom do you want to encrypt?

Please select for whom you want the files to be encrypted. Do not forget to pick one of your own certificates.

<table>
<thead>
<tr>
<th>Name</th>
<th>E-Mail</th>
<th>Valid From</th>
<th>Valid Until</th>
</tr>
</thead>
<tbody>
<tr>
<td>uwo.ca</td>
<td><a href="mailto:ciso@uwo.ca">ciso@uwo.ca</a></td>
<td>2010-04-23</td>
<td>2016-03-21</td>
</tr>
<tr>
<td>Peter Dawes</td>
<td><a href="mailto:peterd@uwo.ca">peterd@uwo.ca</a></td>
<td>2009-11-19</td>
<td></td>
</tr>
<tr>
<td>Minime</td>
<td><a href="mailto:marilena_enus@yahoo.com">marilena_enus@yahoo.com</a></td>
<td>2015-12-17</td>
<td></td>
</tr>
<tr>
<td>Meeneemi</td>
<td><a href="mailto:menus@uwo.ca">menus@uwo.ca</a></td>
<td>2015-12-18</td>
<td></td>
</tr>
<tr>
<td>Matthew Feehey</td>
<td><a href="mailto:mfeeney7@uwo.ca">mfeeney7@uwo.ca</a></td>
<td>2012-12-20</td>
<td></td>
</tr>
<tr>
<td>Marilena Enus</td>
<td><a href="mailto:menus@uwo.ca">menus@uwo.ca</a></td>
<td>2015-12-17</td>
<td></td>
</tr>
</tbody>
</table>

Add Remove

<table>
<thead>
<tr>
<th>Name</th>
<th>E-Mail</th>
<th>Valid From</th>
<th>Valid Until</th>
<th>Det.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minime</td>
<td><a href="mailto:marilena_enus@yahoo.com">marilena_enus@yahoo.com</a></td>
<td>2015-12-17</td>
<td></td>
<td>OpenP</td>
</tr>
<tr>
<td>Mari...</td>
<td><a href="mailto:menus@uwo.ca">menus@uwo.ca</a></td>
<td>2015-12-17</td>
<td></td>
<td>OpenP</td>
</tr>
</tbody>
</table>

fig. 34 Choose for whom you want to encrypt
GPG configuration

fig. 35 Choose your key to sign it
fig. 36 Enter your passphrase
Now you can attach the encrypted file to your email.

**Decrypting and verifying files**

When you want to decrypt a file, all you have to do is right click the file, choose *Decrypt and verify* (fig. 38-39), enter your passphrase (fig. 40) and click OK (fig. 41). The new file will be in the location you chose and in a readable format.
<table>
<thead>
<tr>
<th>Open with</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7-Zip</td>
<td></td>
</tr>
<tr>
<td>Edit with Notepad++</td>
<td></td>
</tr>
<tr>
<td>Decrypt and verify</td>
<td></td>
</tr>
<tr>
<td>More GpgEX options</td>
<td></td>
</tr>
<tr>
<td>Scan with OfficeScan</td>
<td></td>
</tr>
</tbody>
</table>

| Share with                      |  |
| Restore previous versions       |  |
| Send to                         |  |
| Cut                             |  |
| Copy                            |  |
| Create shortcut                 |  |
| Delete                          |  |
| Rename                          |  |
| Properties                      |  |

*fig. 38 Decrypt and Verify*
GPG configuration

*fig. 39 Confirm location and input file*
fig. 40 Enter passphrase for decryption
GPG configuration

fig. 41 File successfully decrypted and signature verified

For more details about GPG4Win check the gpg4win-compendium you downloaded when installing the software.
Mac OS

Install GPG Suite

Install GPG Suite from https://gpgtools.org/gpgsuite.html (fig. 42-44).

*fig. 42 GPG Suite installation*
GPG Suite works with the Mac email client. There’s no add-on available for Mac Outlook yet.
After the installation you will have two new applications called Keychain Access (used for password management) and GPG Keychain (stores secret and public keys). The newly installed software will guide you towards creating your set of PGP keys. We will talk about that in the next chapter.

When you try to create a new email, if the add-on was correctly installed and enabled in your email client, you should see three new buttons: OpenPGP, Sign and Encrypt (fig. 45). If not, try installing the software again.

**fig. 45 New buttons in the Mac email client**

Configure the key manager
Create your own set of keys
GPG configuration

In order for the encryption tool to work you need to create your own set of keys. After the installation, GPG Suite will guide you towards creating your key pair. If, by any chance, the wizard didn’t pop-up after the installation, you can manually create your keys by opening up GPG Keychain, click on New or click on File → New Key (fig.46). Enter your name, email address and passphrase and click on Generate Key. The passphrase is used for unlocking your secret key.

fig. 46 Create a new set of keys

Upload your public key to the keyserver
After you create your set of keys you will have to upload your public key to UWO’s keyserver so that people can download it if they wish to send you encrypted files or emails.

Here is how to do it:

- In GPG Keychain, right click your name, click on Export
- Choose where you want to save the public key
- Open your web browser and go to http://keys.uwo.ca (fig. 47)
- Click on Publish Your Key
- Browse to the location of your key and click on Upload (fig. 48)
- Upload your key twice
fig. 47 Publish your public key on the keyservers
Set your keyservers

In order to send encrypted emails or files to someone, you need to have the public key of that person. Public keys are usually stored on keyservers. Some examples of keyservers are: keys.gnupg.net, pgp.mit.edu, keys.uwo.ca. If your recipient uploaded his/her public key on one of the keyservers, then you can retrieve it from there, otherwise they will have to send you their public key via email or USB.

The public key looks something like this (fig. 49):
UWO Security Team

By default GPG Suite comes configured with a pool of keyservers (hkps://hkps.pool.sks-keyservers.net). This pool of keyservers is comprised of many keyservers like pgp.mit.edu etc. but you can modify this setting, and we recommend you do because most Western users have their keys published on the UWO server.

To modify the keyserver setting go to GPG Keychain, click on GPG Keychain → Preferences (fig. 50) and modify the entry hkps://sks-keyservers.net with ldap://keys.uwo.ca (fig. 51).
GPG configuration

![GPG configuration](image)

**fig. 50 GPG preferences**

**Import keys**

**Fetched keys**

GPG will automatically retrieve the public keys of your senders from the keyserver. For those who did not send you a signed email, you will have to import their key manually.
To modify which server to search for keys open GPG Keychain, click on GPG Keychain → Preferences and modify the keyserver entry.

**Manually import keys**

To manually import a public key go to GPG Keychain, click on Lookup Key and type in the first name, full name or email address of the person you are looking for, hit Search Key (fig. 52), choose the right person from the list and click Retrieve Key (fig. 53).

*fig. 52 Manually import keys*
GPG configuration

In GPG Keychain you will see the type of key (sec/pub), the name, email address, date of creation, key ID and validity. In the Validity field green means that the key is fully/ ultimately trusted, yellow means that the validity of the key is unknown (just imported from the keyserver) and red means the key is expired.

**Validate keys**

If you’re sure (you checked with your correspondent) that the fetched/ imported public key is the true key of that person then you can validate it by signing it with your secret key. That simply means that you trust that the owner of the key is truly who he/ she claims to be and every time you will receive a signed email/ file from that person GPG Tools will verify the key with the one you have in your database and if the key doesn’t match you will be notified. In the below screenshots you will see how to validate a key.
The yellow boxes in the Validity field (fig. 54) means that the key is not trusted yet. It was just downloaded from the keyserver.

When you receive a signed email, click on Signed () and you will see that the key is not trusted (fig.55).
GPG configuration

To validate a key do the following:

- Go to Keychain Access, right click the user’s name
- Click on Sign and choose “I have done careful checking” (fig. 56)
- Modify any other values that you need and click on Generate Signature
- If you also trust that this person’s checks on other people’s signatures are accurate you can change the ownertrust to Full from the Details button (right click on the user’s name) (fig. 57)
fig. 56 Validate a public key

fig. 57 Change trust
**GPG configuration**

![GPG Configuration Image]

**fig. 58 Valid key**

Now if you click on Signed() in the email received from this person you will see that the signature is valid (fig. 58).

**Emails and files**

**Sign and encrypt emails with the Mac email client**

Your first signed and encrypted email.

When you want to send a signed and encrypted email, in the new message window enable OpenPGP and click on the Sign and Encrypt buttons (fig. 59). If you don’t have the other person’s public key, you will not be able to encrypt anything for them and the button will be grayed out. In this case you will only be able to sign the email and the other person will be able to verify it.

When encrypting an email, the subject line will remain in clear text. Only the body of the email will be encrypted and if you wish to attach a file, you will have to encrypt it separately and then attach it.
Encrypting and signing a file

You can encrypt and sign a file by doing the following:

- Right click the file
- Go to Services (fig. 60)
- Click Encrypt (fig. 61)
GPG configuration

fig. 60 GPG Services
fig. 61 Encrypt file

- Choose your recipients’ key
- Choose your key
- Enable Signing and Encrypting
- Click OK (fig. 62)

fig. 62 Sign and Encrypt file

- Enter the password (fig. 63)
GPG configuration

fig. 63 Enter passphrase

fig. 64 Encryption confirmation

The resulting file will be located in the same folder as the initial unencrypted file and it will have a “.gpg” extension.

Decrypting and verifying emails
The Mac email client automatically detects an encrypted email and it will ask you for the passphrase to decrypt it when you open it (fig. 65-66).
If for some reason your email client doesn’t recognize an encrypted email (fig. 67), then either right click the body of the email and choose OpenPGP: Decrypt Selection to New Window (fig. 68) or copy and paste the content in a text editor, right click the text and choose OpenPGP: Decrypt Selection to New Window.
GPG configuration

fig. 67 Unrecognized encrypted email

Look up "-----BEGIN PGP MESSAGE-----..." Search with Google

Copy
Share
Speech

OpenPGP: Import Key from Selection
OpenPGP: Sign Selection to New Window
OpenPGP: Encrypt Selection to New Window

OpenPGP: Decrypt Selection to New Window

fig. 68 Right click on the message

fig. 69 Signature verification and decryption

Verification successful

Good signature (Ultimate trust):
“Marilena Enus <menus@uwc.ca>"
If the message still can’t be decrypted, then the issue comes from your sender’s side.

**Decrypting and verifying files**

If you receive an encrypted file you can double click it, enter your passphrase and the decrypted file (fig. 72) will be saved in the same location as the original file and, if signed, the signature will be verified (fig. 71).
GPG configuration

fig. 72 Decryption confirmation
Install GNUPG
This documentation is for Debian distributions and Thunderbird.

The core GNUPG package is installed by default on Ubuntu systems, but if it isn’t, then install it from the command line (fig. 73).

```
marilena@marilena-VirtualBox:~$ sudo apt-get install gnupg
```

Install Thunderbird as your email client with the command `sudo apt-get install thunderbird`.

Configure your email account and install the add-on Enigmail. In Thunderbird, go to Tools → Add-ons and search for Enigmail. From the Available Add-ons click on Install (fig. 74).
GPG configuration

After the add-on installation a new tab called Enigmail will appear in your menu bar.

Configure the software

Configure GnuPG files
Before creating your own set of keys, you need to adjust the gnupg configuration.

In a terminal windows enter the following:

- `apt-get remove gnome-keyring`
- `killall gpg-agent`

Check the version of your gpg-agent with the commands (fig. 75):

```
gpg-connect-agent <<EOT
GETINFO version
EOT
```
Confirm that the gpg agent works (fig. 76):

```
gpg-connect-agent <<EOT
GET_CONFIRMATION Hello
EOT
```

If you receive an error check if your pinentry program is working (fig. 77):

```
pinentry <<EOT
SETDESC Hello World
CONFIRM
EOT
```
GPG configuration

Check the location of the pinentry program:

`whereis pinentry`

Create the gpg-agent.conf and gpg.conf files and type in the following lines:

```
nano .gnupg/gpg-agent.conf
```

```text
pinentry-program /usr/bin/pinentry-gtk-2
use-standard-socket
```

```
nano .gnupg/gpg.conf
```

```text
keyserver-options no-honor-keyserver-url
keyserver-options auto-key-retrieve,verbose,timeout=120
utf8-strings
use-agent
auto-key-locate local,keyserver
keyserver ldap://keys.uwo.ca
```

Change the permissions in the gnupg files:

```
chmod 600 .gnupg/*
```

```
chmod 700 .gnupg
```

Create your own set of keys

Now you can create your own set of keys.

Go To Enigmail → Setup Wizard (fig. 78). A window that will help you configure email with encryption will appear. Leave the default settings unless otherwise required, enter a passphrase (fig. 79) and wait for the software to create the private and public keys for you (fig. 80).
fig. 78 Enigmail setup wizard
GPG configuration

This dialog will create a pair of two keys:
Your public key is for others to send you encrypted emails. You can distribute it to everybody.
Your private key is for yourself to decrypt these emails and to send signed emails. You should give it to nobody.

Your passphrase is a password to protect your private key. It prevents misuse of your private key. The passphrase should be a phrase containing at least 8 characters, digits and punctuation marks. Umlauts (e.g. ä, ö, ñ) and language-specific characters are not recommended.

Account/User ID:
Marilena <menus@uwo.ca> - menus@uwo.ca
Passphrase

Please confirm your passphrase by typing it again

Passphrase quality:

fig. 79 Enter passphrase
In Enigmail \( \rightarrow \) Preferences in the Basic tab click on Display Expert Settings and Menus, go to Keyserver and enter `ldap://keys.uwo.ca, pool.sks-keyservers.net, keys.gnupg.net, pgp.mit.edu` in the Specify your keyservers field and `ldap://keys.uwo.ca` in the Automatically download keys for signature verification field (fig. 81).
GPG configuration

Specify your keyserver(s):

ldap://keys.uwo.ca, pool.sks-keyservers.net, keys.gnupg.net, pgp.mit.edu

Example: sks.dnsalias.net, pgp.mit.edu, ldap://certserver.pgp.com

Always use first keyserver

Automatically download keys for signature verification
from the following keyserver:

ldap://keys.uwo.ca

Now try to send a signed and encrypted email to yourself (fig. 82).
If you receive any errors, then debug the gpg agent and try to find out what causes the error. In a terminal enter the commands:

```
killall gpg-agent
```

```
gpg-agent --debug-level expert --use-standard-socket --daemon /bin/sh
```

**Upload key to keyserver**

Now that everything is working and you have your own keys, you can upload your public key to the server. Go to Thunderbird, click on Enigmail → Key Management, right click your name (fig. 83), choose Export Keys to File → Export Public Keys Only (fig.84), choose a location for the file and click on Save.
GPG configuration

fig. 83 Export your public key
Export your public key only

This is how a public key looks like:
GPG configuration

Now, go to [http://keys.uwo.ca/vkd/GetWelcomeScreen.event](http://keys.uwo.ca/vkd/GetWelcomeScreen.event) and Publish Your Key twice.

**Import keys**

**Fetched keys**

Thanks to our configuration, Enigmail and GnuPG will automatically download the public keys of the people who have sent you a signed email from the keyserver `ldap://keys.uwo.ca`. You can modify this by going to `Thunderbird → Enigmail → Preferences` and changing the entry in the field *Automatically download keys for signature verification from the following server* with the server that you want (fig. 86).
Manually import keys
You can import public keys from the server by going to Enigmail → Key Management → Keyserver → Search for Keys (fig. 87). Type in the name or email address of the person whose public key you need and click on OK. If the search returned the key you were looking for then select the key and click OK to import it (fig. 88). This new key will appear in your local database.
GPG configuration

fig. 87 Search for public keys
You can change the keyserver you wish to manually lookup keys by choosing another keyserver from the drop-down list or just type in the name of the keyserver (fig. 89).
GPG configuration

The keys that are fetched by the software or that you manually import from a server come by default as “untrusted” (fig. 80). That means that you’ll have to check with that person if they actually sent that email and that’s their right key.

After you make sure that the owner of the key is who he/she claims to be, then you can Sign Sender’s Key to validate it (fig. 91 - 92). Every time you receive a signed email from that person, the software will compare the key with the one you validated and if they match, Enigmail will notify you that the key is valid (fig. 93). If the message has been tampered with, you’ll see a “Bad signature” message.
Email encryption in Thunderbird on Linux

Settings
You can modify or check the default settings by going to Thunderbird → Enigmail (fig. 94).
Under *Preferences* (fig. 95), among other things, you can modify your keyserver entries and export your public and secret keys and your GPG configuration files (fig. 96) which you can later import on another machine.
fig. 95 Enigmail preferences
GPG configuration

![Enigmail Preferences](image)

**fig. 96 Backup your keys and settings**

**Sign and Encrypt emails**

To encrypt an email for someone you’ll need their public key. Make sure you have it downloaded in your local database.

In *Thunderbird* when you write a new email, the buttons for signing and encrypting should be in the ribbon (fig. 97). Enable them accordingly before you send the email. If you want to attach a file, it is recommended you encrypt it and sign it separately and then attach it. If you attach an unencrypted file, Enigmail will ask if you want the file to be encrypted for you (fig. 98).
Secret content

fig. 97 Writing a signed and encrypted email
GPG configuration

Encrypting attachments
Enigmail will detect the encrypted email and will ask for your passphrase to decrypt it.

Decrypt and Verify emails
Enigmail will detect the encrypted email and will ask for your passphrase to decrypt it.

If for some reason the add-on doesn’t detect the encryption (fig. 100), then copy and paste the content of the email in a text file. Save it and decrypt it with the command line (fig. 101):

```
gpg /path/to/the/saved/text/file
```

The decrypted message (fig. 102) will be saved in a file in the same location as the encrypted original message file.
fig. 100 No encryption detected
GPG configuration

```
root@marilena-VirtualBox:~

marilena@marilena-VirtualBox:~$ gpg Encrypted Email content

You need a passphrase to unlock the secret key for user: "Marilena Enus <menus@uwo.ca"
2048-bit RSA key, ID 124A304E, created 2015-12-17 (main key ID FBA7403E)

gpg: encrypted with 2048-bit RSA key, ID EEA0D842, created 2012-12-20
  "Matthew Feeney <mfeeney7@uwo.ca>"
gpg: encrypted with RSA key, ID FDAF32F8

gpg: encrypted with 2048-bit RSA key, ID 124A304E, created 2015-12-17
  "Marilena Enus <menus@uwo.ca>"
gpg: Encrypted Email content: unknown suffix
Enter new filename: Decrypted email

gpg: Signature made Tue 12 Apr 2016 12:58:21 PM EDT using RSA key ID 5B3E7D2C

gpg: Good signature from "Matthew Feeney <mfeeney7@uwo.ca>"
  aka "Matthew Feeney <mfeeney7@voicemail.uwo.ca>

marilena@marilena-VirtualBox:~$
```

fig. 101 Decrypting from the command line
Files

Sign and Encrypt files

You can sign and encrypt a file from a terminal windows using the command (fig. 103):

```
gpg --s --e /path/to/your/file
```

Choose your recipients’ keys and your key and hit enter twice. The encrypted file will be saved in the same location as the original file.
En​crypting files from the command line

You need a passphrase to unlock the secret key for user: "Marilena Enus <menus@uwo.ca>"
2048-bit RSA Key, ID F8A7403E, created 2015-12-17

You did not specify a user ID. (you may use "-r")

Current recipients:
Enter the user ID. End with an empty line: mfeeney7@uwo.ca

Current recipients:
2048R/EEA0D842 2012-12-20 "Matthew Feeney <mfeeney7@uwo.ca>"
Enter the user ID. End with an empty line: menus@uwo.ca

Current recipients:
2048R/124A304E 2015-12-17 "Marilena Enus <menus@uwo.ca>"
2048R/EEA0D842 2012-12-20 "Matthew Feeney <mfeeney7@uwo.ca>"
Enter the user ID. End with an empty line:

Decrypt and verify files

When you receive an encrypted file (fig. 104), save it and decrypt and verify it with the command (fig. 105):

```
gpg /path/to/your/file
```
fig. 104 Encrypted file attached

```
marilena@marilena-VirtualBox:~ $ gpg Desktop/Super/ Secret/ File.txt.gpg
You need a passphrase to unlock the secret key for
user: "Marilena Enus <menus@uwo.ca>"
2048-bit RSA key, ID 124A304E, created 2015-12-17 (main key ID F8A7403E)
gpg: encrypted with 2048-bit RSA key, ID EEA0D842, created 2012-12-20
    "Matthew Feeney <mfeeney7@uwo.ca>"
gpg: encrypted with 2048-bit RSA key, ID 124A304E, created 2015-12-17
    "Marilena Enus <menus@uwo.ca>"
gpg: Signature made Tue 12 Apr 2016 02:11:26 PM EDT using RSA key ID 5B3E7D2C
gpg: Good signature from "Matthew Feeney <mfeeney7@uwo.ca>"
gpg:           aka "Matthew Feeney <mfeeney7@voicemail.uwo.ca>"
marilena@marilena-VirtualBox:~ $ 
```

fig. 105 Decrypting a file from the command line