Table of Contents

Mac OS .......................................................................................................................... 2
  Install GPG Suite ........................................................................................................ 2
  Configure the key manager ....................................................................................... 5
    Create your own set of keys .................................................................................... 5
    Upload your public key to the keyserver ............................................................... 5
    Set your keyserver ................................................................................................. 7
  Import keys ................................................................................................................. 10
    Fetched keys ........................................................................................................... 10
    Manually import keys ............................................................................................. 10
    Validate keys ........................................................................................................... 11
  Emails and files .......................................................................................................... 15
    Sign and encrypt emails with the Mac email client ............................................. 15
    Encrypting and signing a file .................................................................................. 17
    Decrypting and verifying emails .......................................................................... 19
    Decrypting and verifying files ................................................................................. 23
Mac OS

Install GPG Suite

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

*fig. 1 GPG Suite installation*
fig. 2 GPG Suite installation

fig. 3 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. 4 New buttons in the Mac email client](image)
Configure the key manager
Create your own set of keys

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 \(\rightarrow\) 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.

![GPG Keychain](image)

fig. 5 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](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. 6 Publish your public key on the keys server
Set your keyserver
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):
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).
fig. 9 GPG preferences

fig. 10 Keyserver 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. 11 Manually import keys
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).
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)
### Validate a public key

**Fig. 15** Validate a public key

### Change trust

**Fig. 16** Change trust
fig. 17 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.
fig. 18 OpenPGP, Sign & Encrypt buttons
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)
Choose your recipients’ key
Choose your key
Enable Signing and Encrypting
Click OK (fig. 62)
- Enter the password (fig. 63)

![fig. 22 Enter passphrase](image)

(fig. 22 Enter passphrase)

![fig. 23 Encryption confirmation](image)

(fig. 23 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.
Unrecognized encrypted email

Right click on the message

Signature verification and decryption
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).

*fig. 30* Verified signature on file

*fig. 31* Decryption confirmation