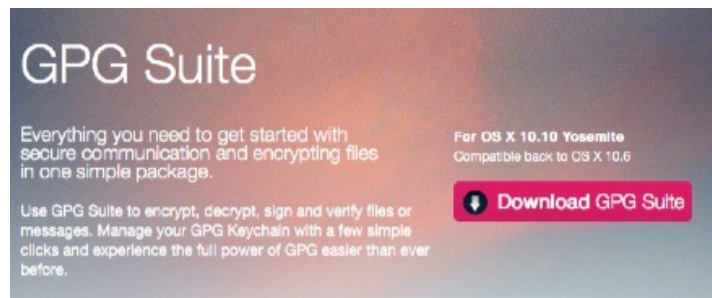


EASY PGP



Open PGP Cheatsheet



Install GPG Tools

The installer will install GPG for Mail, GPG keychain, GPGServices and Mac GPG. With all those installed, you will have everything you need to send and receive encrypted emails.

- **Mac GPG** - This is the brains of the operation.
- **GPG Keychain** - An application to look after your keys.
- **GPG for Mail** - A plug-in to make things easy in your Apple Mail application
- **GPGServices** - This gives you access to GPG within OS X and applications such as the Finder and text based applications. You get access to Services through a right click type action on your mouse or the trackpad equivalent. Ctrl and left click will get you there too.

The Basics of Key Pairs

If I want you to send me an encrypted message I have to give you MY public key. Anything you encrypt with my public key, the only person who can decrypt is ME.

If I'm going to send you an encrypted message you have to give me YOUR Public Key. If I use just that key to encrypt some text or a file, the only person who can decrypt is YOU.

Use Good Passphrases

Get 1Password or Last Pass to look after your passwords / pass phrases for your keys. Use an easy to remember - Hard to crack password to access your password manager. The best place to go to get a good and easy to remember password is the xkcd Password Generator Website.

Encrypt with the public key belonging to the person who is going to decrypt

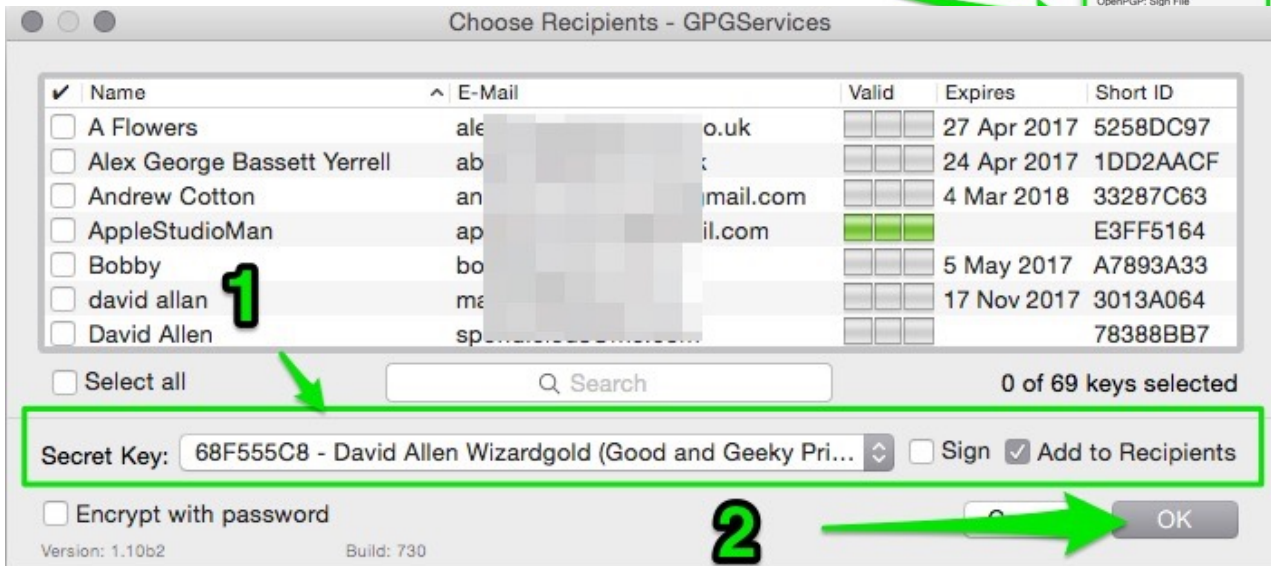
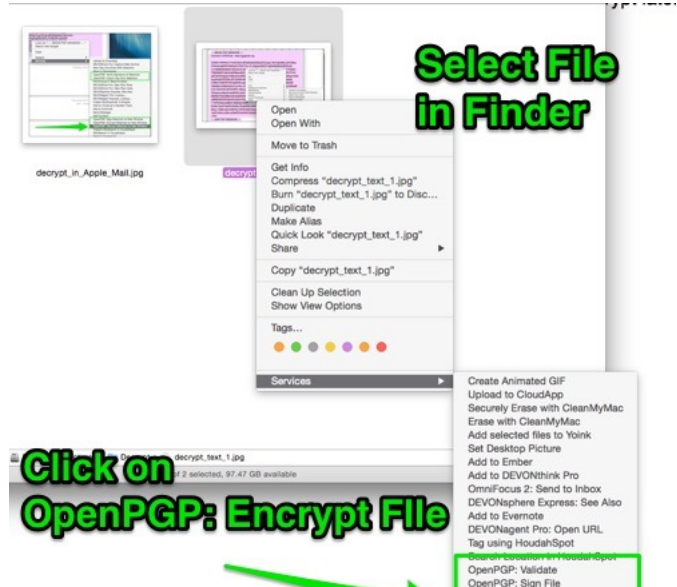
KEY PAIR BASICS

Encrypt Files and Folders - Not Just Emails

Either just to protect your own files on your own computer or files you want to send to recipients. Go to the Finder and do a right click to get to Services in the context sensitive menu. Choose OpenPGP: Encrypt File

Decrypt works the same way - Choose OpenPGP: Decrypt File

Type to enter text



Clean up to maintain security

Don't forget to delete the file you encrypted now you have the encrypted copy.



Sharing your Public Key

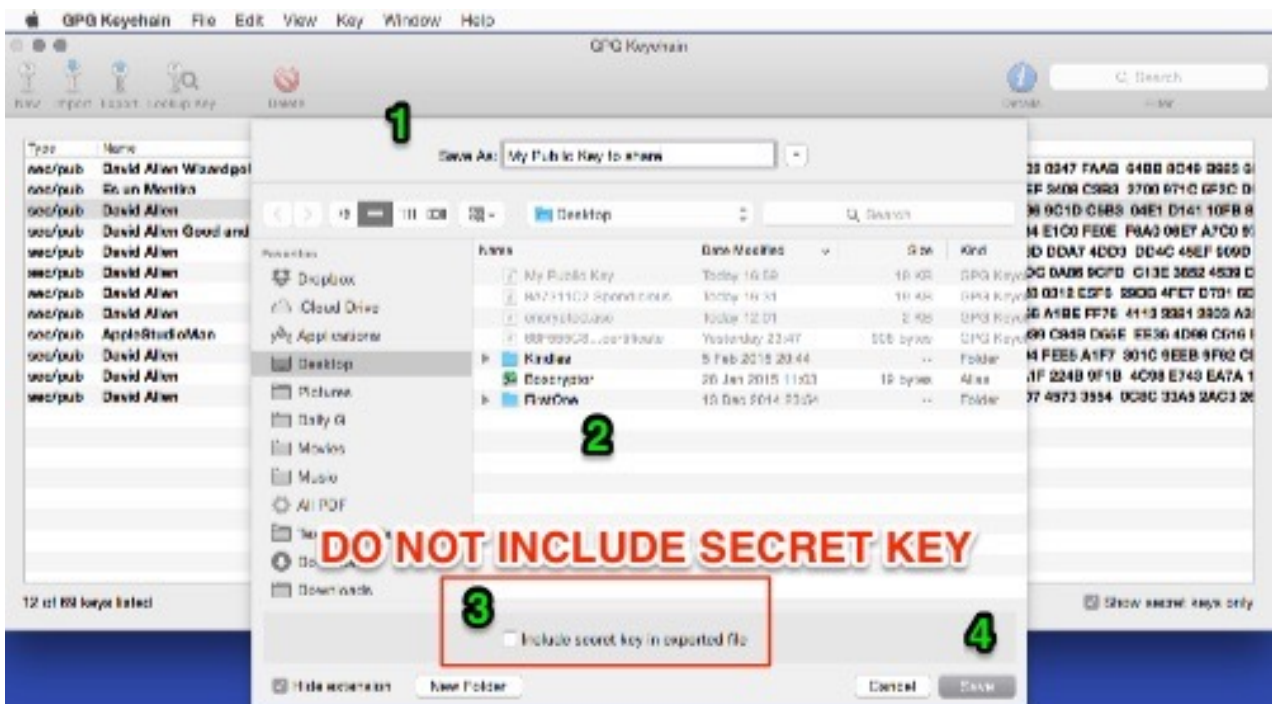
When you make a new Key Pair share the public key to the public key server. This will make it easy for your friends to get your public key and be able to send you encrypted emails.

Or you can send a public key as a block of text or as a .asc file. Add the block of text into a text document using the Services menu. Create the .asc file by exporting out of GPG Keychain.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
Comment: GPGTools - https://gpgtools.org  
  
mQENBFRMuHUBCADlKcQo7PbprsBfTT1ui9wpTa5eKFEldJk56dvmb4F3xL7KenE5-  
laCoG7mb9G8HsnSbuPi4q7MeLU0Ja1C88YTHNNWTA7vwsGEC8c5iWnR7ET10MN1-  
eEOXrYHA7Y3k+KG0W0U8ePUQTT2+lpndd/0RR62A3o56hWEmuRA9KaQdzBYFB/YK-  
Oi+YvNEBvle3Qmq+4vzPc/MTamoUjG3NrRnYrzDNdTWGlLR/ZG4mbhKCGn2XBNTs-  
1oEWvPrWiqKh+59H2whTHytyF584m+UMTF7BGURNggEYeQbk1lsmjxSKxPP71KU+-  
aKtioul49/vAn1o5Aie1TTp4M00nBc52L85ABEBAAG0LkRhdmkIEFsbGVuIChN-
```

About 300 lines of text

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
OXAL6bL6QeEwXoPw3siI7a7J41v9SsBHjc9RM/XshfZCRF/zEn5EvhEZUXTYAgcs-  
cxwFHNLZK5Psp1pMM8Wdh0XkgsHQxS+2dmzUbEw2J+Sjg6XpcXBnVZha98CPFK-  
Zwrsvtp3J+z0NZrgLKU5fPbXHFkKoh+r3rM7Vzo03+3u2T+BJTeHTfubE+T6CAnkM-  
BsssnC1YwZ+rhlobF7JGja9HUU4MdJfmEm5wMSYmDIZAwtdbPtQSPb7GVPPrPaZ0q-  
54thxVt145JX0dKh3/Gg8sTOELUIAQIT6+QE/cNQMuav-  
=DU4N-  
-----END PGP PUBLIC KEY BLOCK-----
```



Don't export with the secret or private key included.

Encrypted Email is Easy

You'll be using the GPG Mail plug-in to automatically encrypt and decrypt your emails. Or use Enigmail plug in if you use Postbox or Thunderbird email clients on your Mac.



Buy the [Good and Geeky Email Privacy and Security Book](#) on Amazon

