What is GPG?

GNU Privacy Guard (GnuPG o GPG)is an encryption and digital signature tool that implements the OpenPGP standard. GnuGPG allows you to encrypt and sign both data and communications (emails for example). It has a versatile key management system, along with access modules for all types of public key directories. Also known as GPG, it is a command line tool with functions for easy integration with other applications.

GPG encrypts messages using user-generated asymmetric individual key pairs. Public keys can be shared with other users in many ways, an example of this is by depositing them on key servers.

IMPORTANT: NEVER SHARE YOUR PRIVATE KEY, KEEP IT SECURELY AND ONLY FORWARD OR PUBLISH THE PUBLIC KEYS ON A SERVER.

GPG for macOS users

There are two ways to install gpg on macOS:

- Install the GPG Suite
- Install GPG using Homebrew package manger

We recommend installing `gpg` via Homebrew and using it via the terminal, e.g. iTerm.

Generate user key-pair

```
gpg --gen-key
```

Some questions must be answered in order to generate the key pair:

- Key type. RSA-RSA is the default.
- Expiration time: How long the key shoud be valid.
- User data (Real name, email, comment) . This data is used to identify the key in public key servers and when it's sent to other users.
- Password: It is possible to protect the key file with a password.

Export public key

```
gpg --armor --output myname_public_key.asc --export 'Name Surname'
```

Import public key

```
gpg --import johndoe.asc
```

We can check the list of public key in our databes with this command:

```
gpg --list
```

Encript files

```
gpg --encrypt --recipient 'Name Surname' file.txt
```

Decrypt files

```
gpg --output file.txt --decrypt file.txt.gpg
```

Usefull links

- <https://www.madboa.com/geek/gpg-quickstart/>