What is GPG?

See description here

GPG for Windows users

There are several applications under the Windows operating system which allow you to generate a gpg key pair. Among the best known is Gnu4win with its module called [Kleopatra]. Gpg4win is a free distribution encryption software which allows the encryption of files and the sending of documents through email using public key cryptography for data encryption and digital signatures.

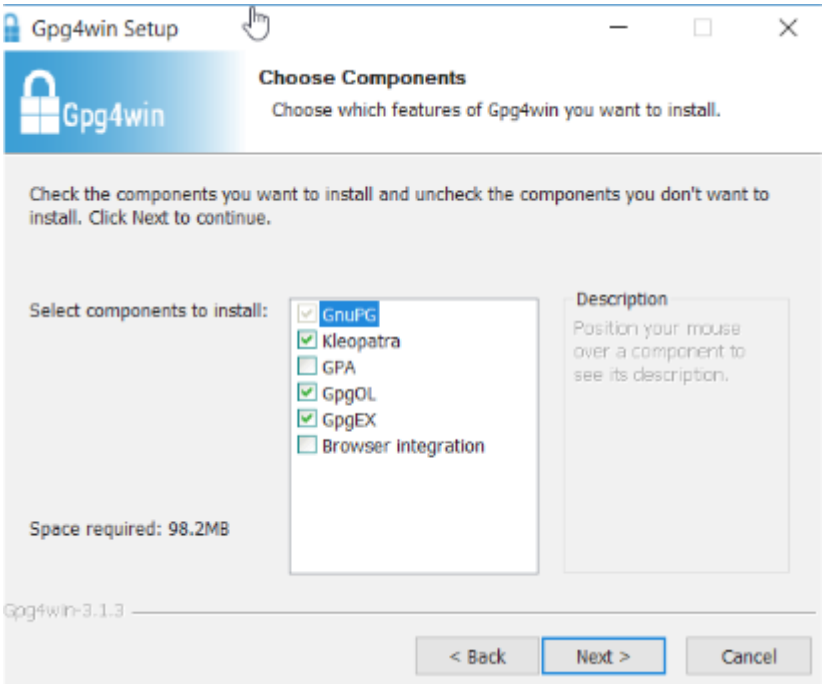
Supports cryptography OpenPGP and S/MIME (X.509) standards.

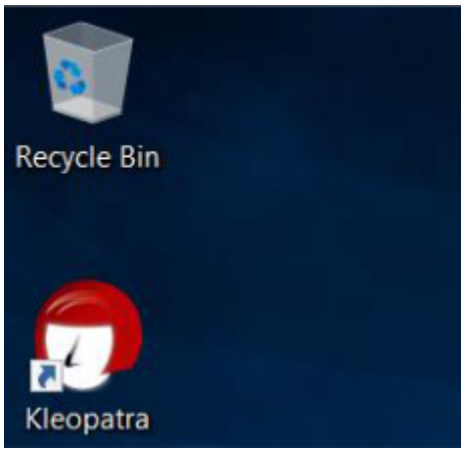
It consists of several modules, including:

- GnuPG : the basic encryption tool
- Kleopatra : certificate manager for OpenPGP y X.509
- GPA : an alternative certificate manager (GNU) for OpenPGP and X.509

GPG4win installation

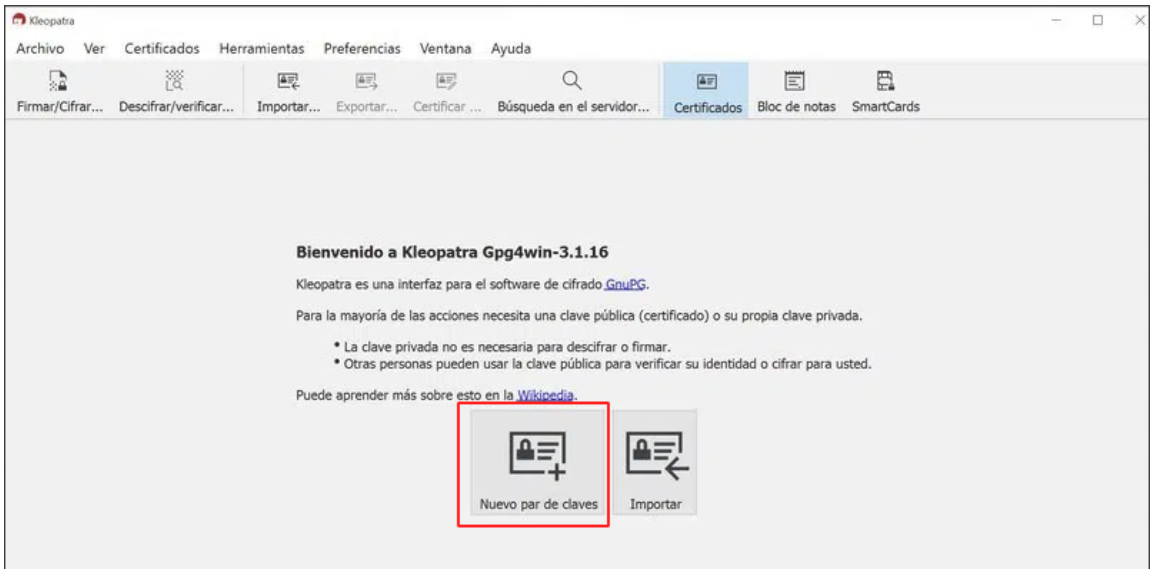
On the project website download the latest version of the software. Open the installer and authorize the changes if necessary. Follow the steps indicated with the Next button.





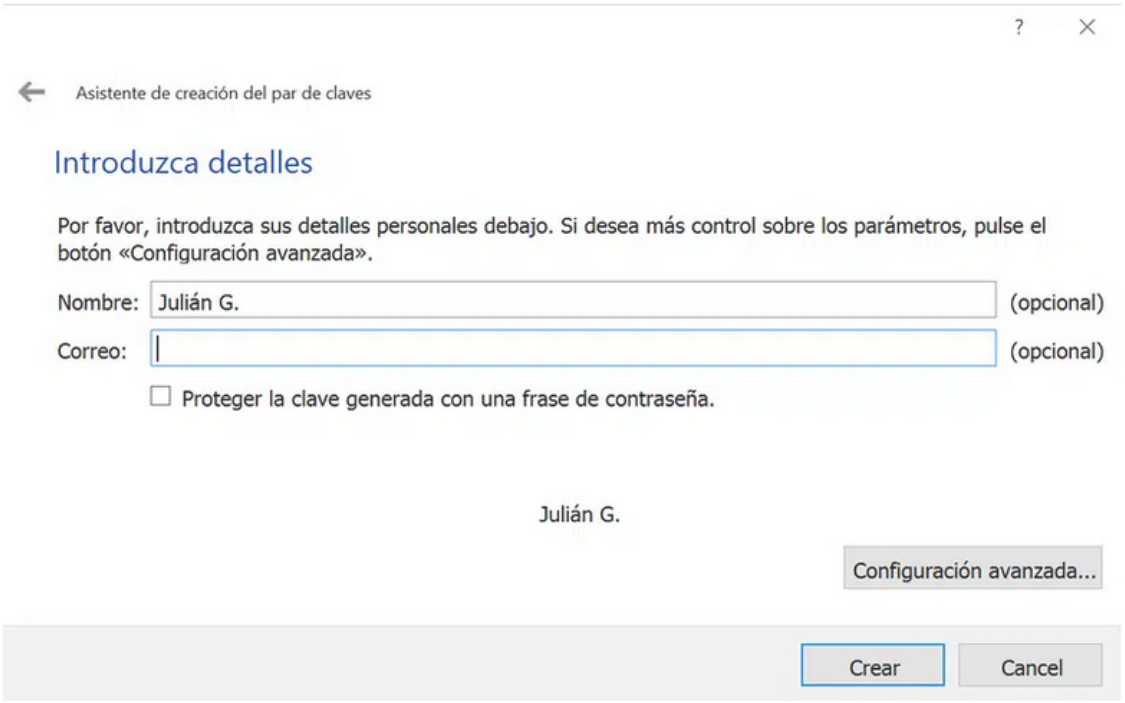
Generate a key pair (public and private)

Once Gpg4win is installed we are going to use the *Kleopatra* module to generate a new gpg key pair. To do this, from the files tab we select *New Certificate* which will open the certificate generation wizard.

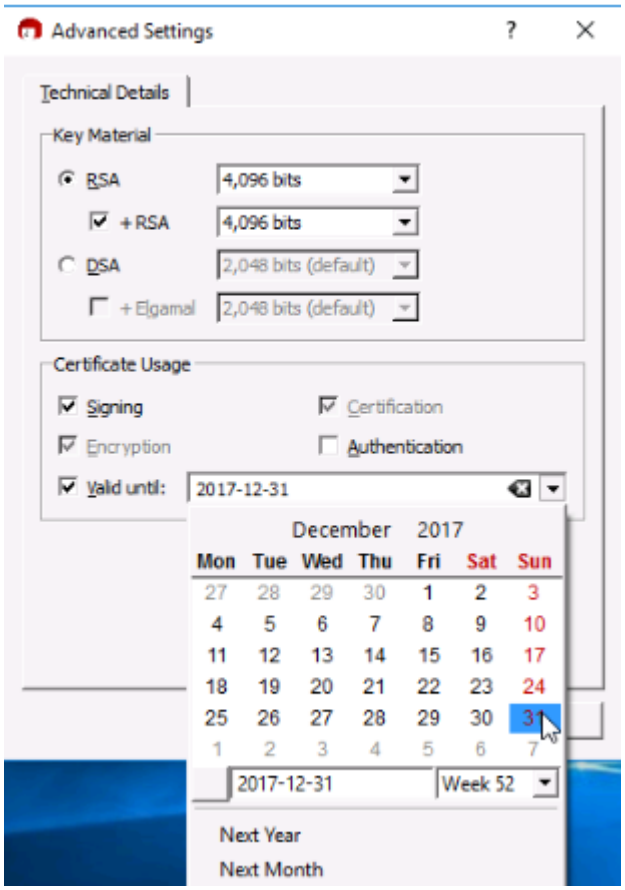


Click on *Create a personal OpenGPG key pair*

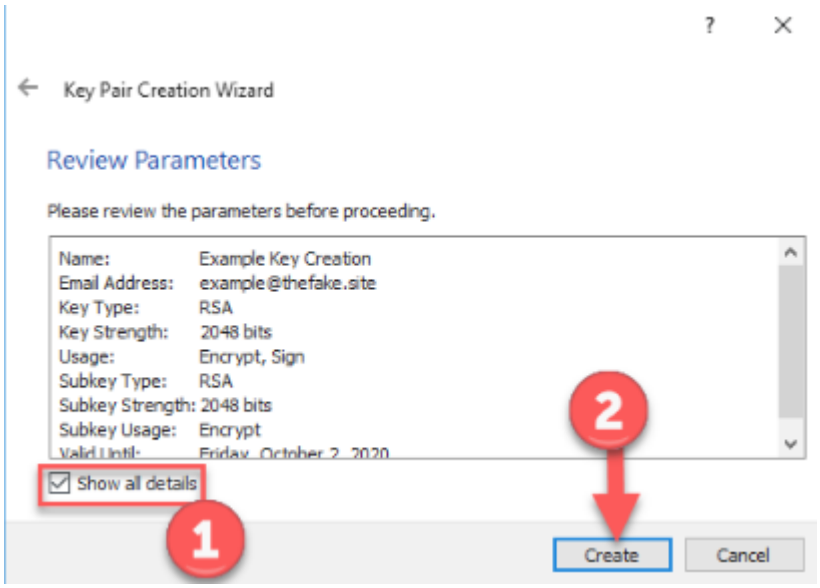
Enter the required data



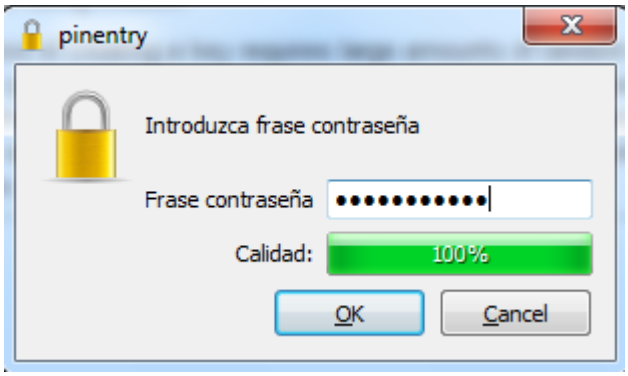
In the *Advanced Settings* tab, indicate a 4096 bits key length and an expiration date no more than 2 years.



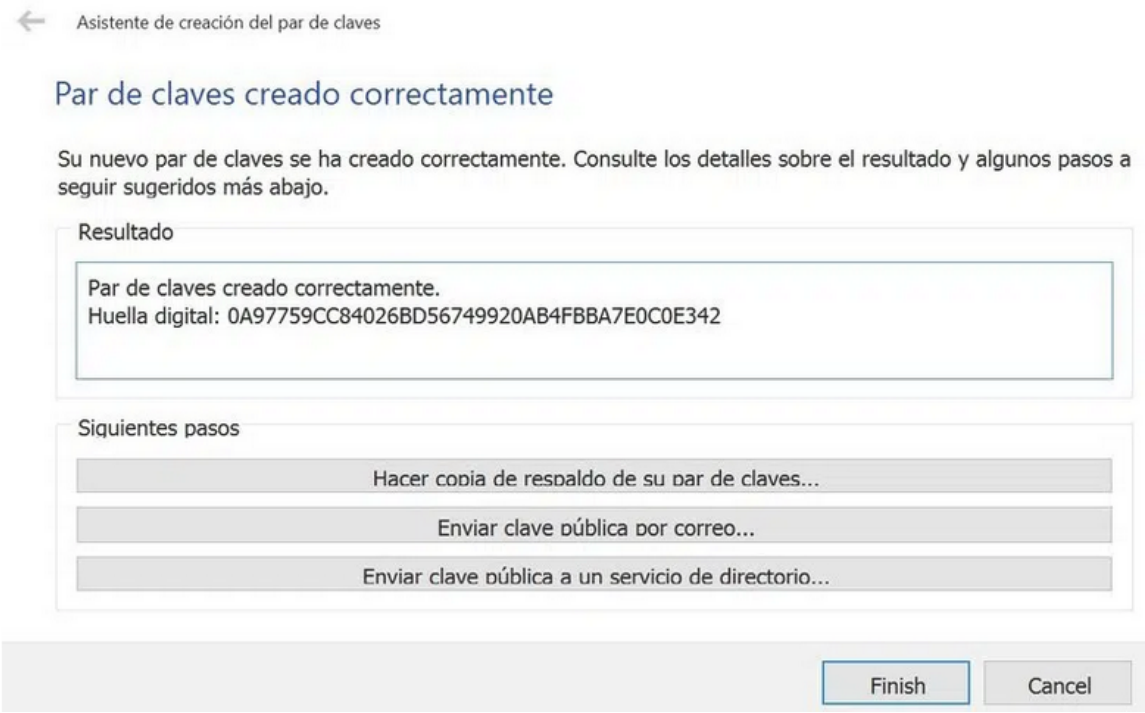
Confirm the entered values and generate key pair by clicking on *Create Key*.



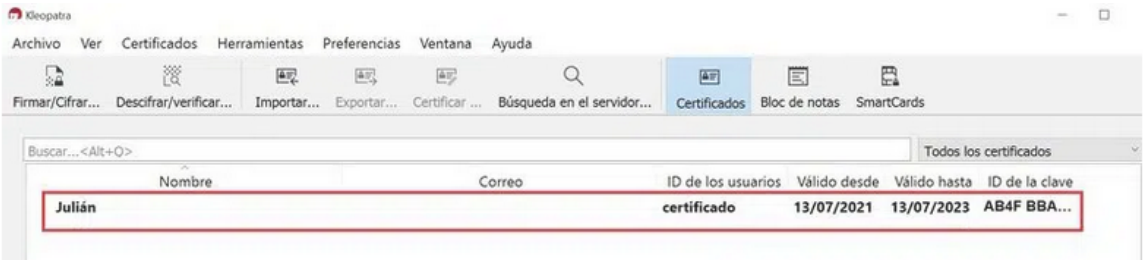
Enter a password that you remember for your private key. This password will be used to decrypt the files that you receive encrypted with your public key.



Clicking **OK** you will see your public / private key pair have been generated correctly.

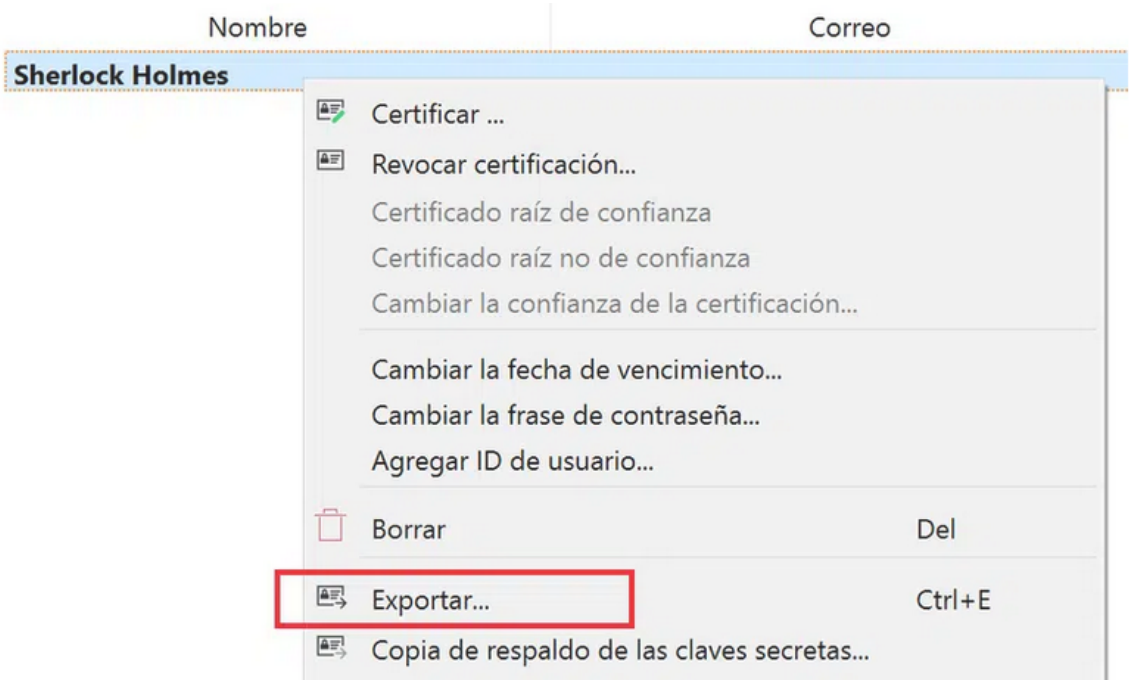


You can check your certificates in the tabs *My Certificates*.



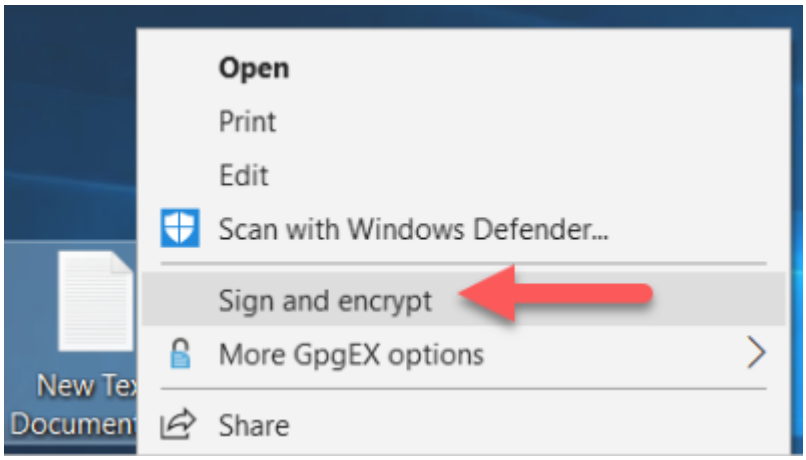
Export the public key

When exporting the public key a text file is generated. As a general rule, it is saved with the extension *.asc*. You can send this file by email or publish it on a public key server as *REDIRIS* where anyone can download it.



You will get a file of this type :

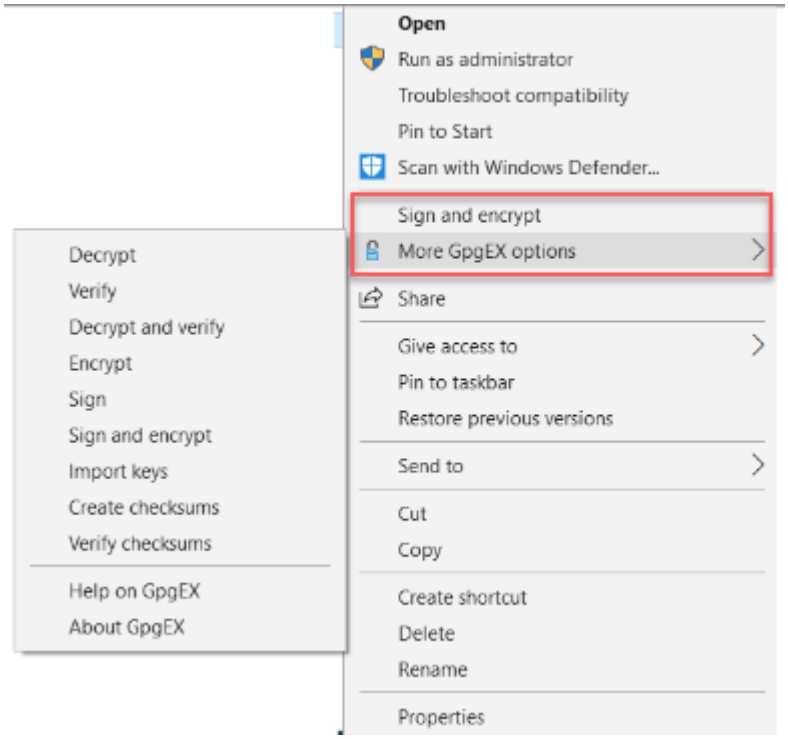
Encrypt files with the public key.



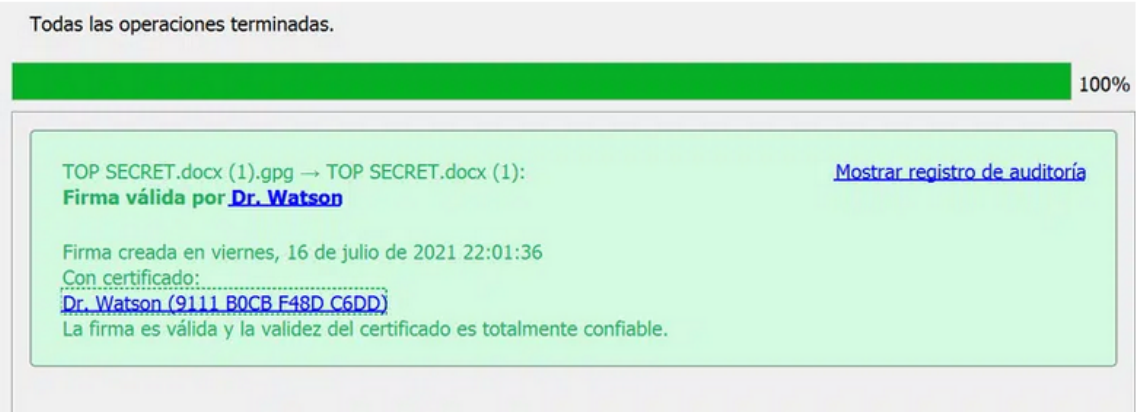
Decrypt files with private key

Only if a * .gpg * file has been encrypted with your public key and has the private key as well as your password, will you be able to decrypt its content .

You can use the context menu *Decrypt and verify* to recover the original file. It is also possible to do this from the Kleopatra.



It will have the same name without the gpg extension.



IMPORTANT NOTE: If you change computers or use a different one, make sure you have your key pair in a safe place. Without them you will not be able to decrypt the content of the file. Therefore, we recommend making a backup of the GPG key pair