Generate encrypted files with this pictorial tutorial in minutes. Anyone with basic computer skills can do this right now.

The FREE GnuPG program is an updated offshoot of the old PGP encryption system invented over 20 years ago and is still the best game in town. Good enough that there isn't enough computer power in all the government agencies in the world to crack it. It is bullet proof as long as your computer is secure enough that the encryption keys aren't stolen out of it. (This is not the encryption system that has recently made news (April 2014) as being hacked.) For ultimate safety (journalists, opposition candidates) should use a separate computer to store keys and generate encrypted files to transfer by memory devise to a connected computer.

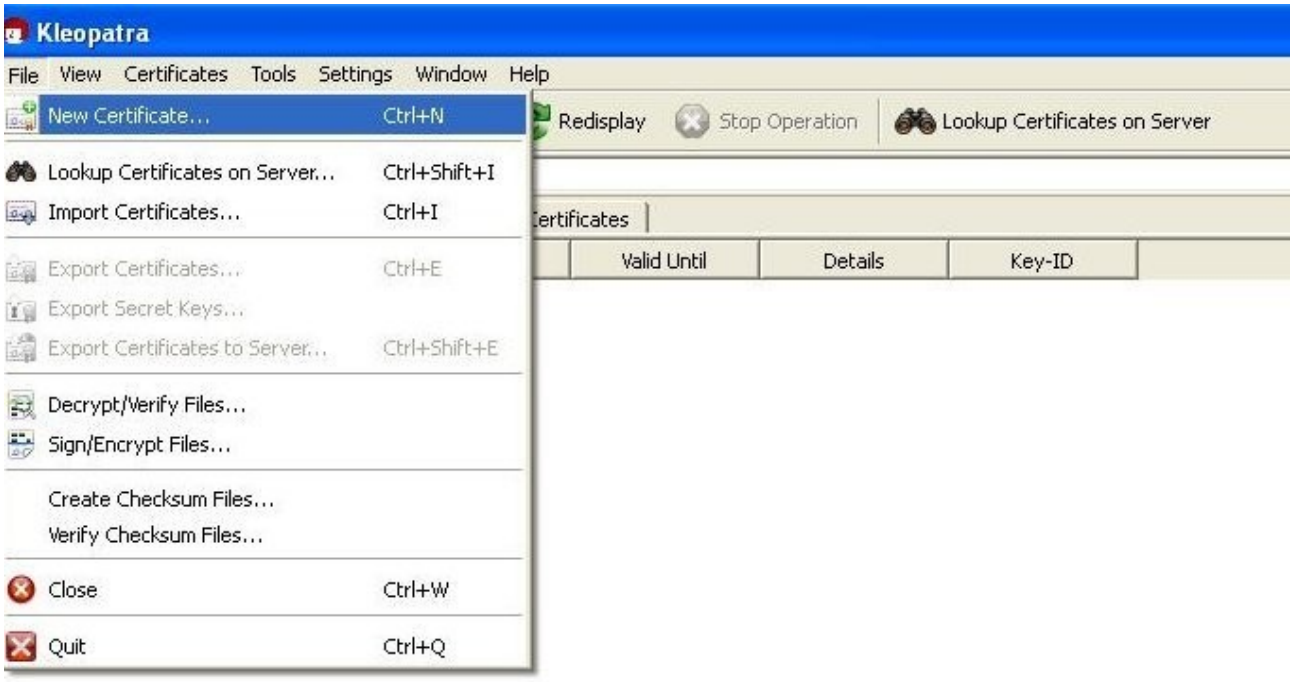
Gnupg is interoperable with the other PGP programs that you have to pay for.

CTRL-Click on the image above or on this link to go to www.gnupg.org to download.
(no one receives any reward for directing anyone to this free program, this is a recommendation only)

If you can attach files to an email and save files received, you have the skills required to do this.

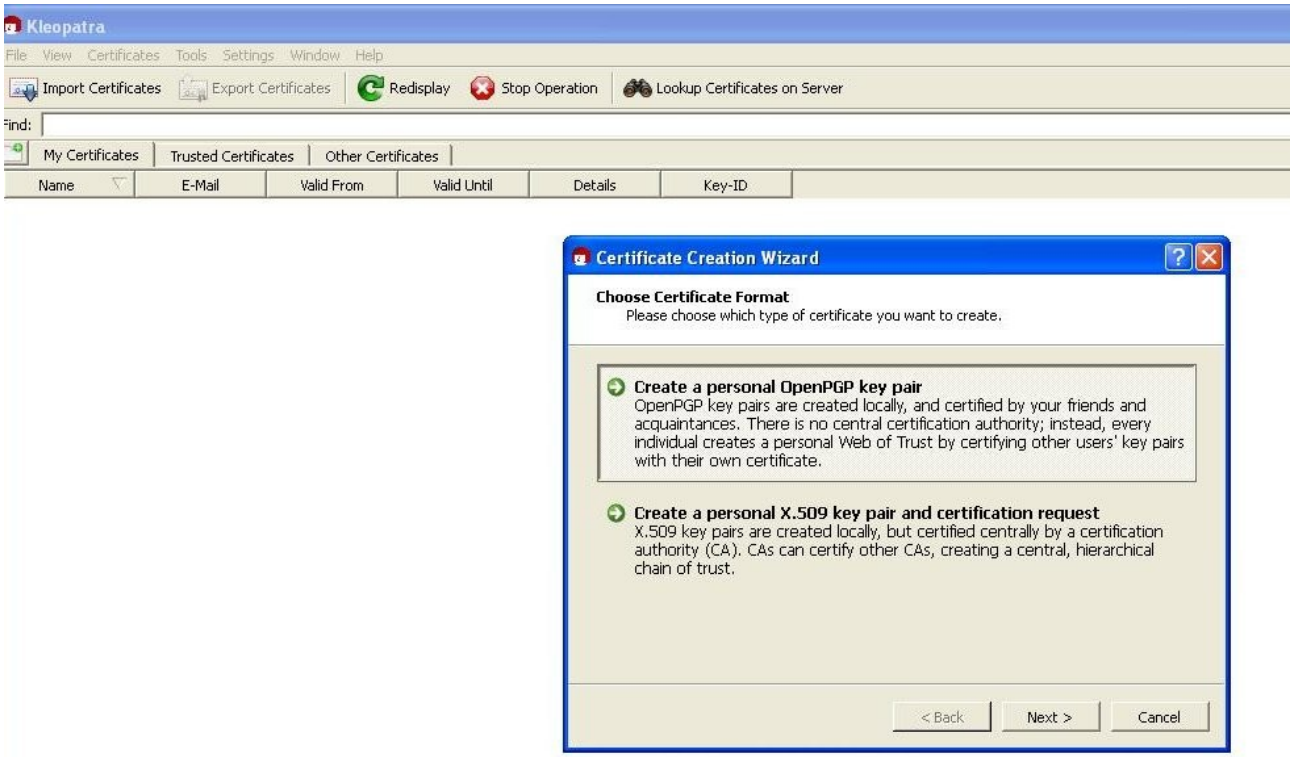
The problem with encryption programs was the belief that only a geek knew how to use them. The PG4win system (also versions for Apple and Linux) incorporates features that eliminate the 'command line' structure that makes the non Geek community run for cover. There is an instruction manual that downloads with the program but it makes a common mistake, I think. It expects you to read and retain every detail of it's operation at once! This tutorial doesn't attempt to teach you every detail of the program in one huge gulp but rather to do a basic operation that is fully functional and useful and then you have enough understanding to delve into the the other stuff at leisure, or maybe not because if just being able to communicate across the web with known correspondents or guard documents stored on your computer is enough... this one lesson may do it for you.

This tutorial assumes you have already downloaded and installed the Gnu PG which is very compact and intuitive, or maybe you want to see if it is worth the effort before you bother. In any case, let us begin..... *The following images are cropped screenshots for easier viewing. This demo was done on XP but the program is suitable for win7, vista etc... The appearance may vary slightly in those other windows systems but the functions are the same.*

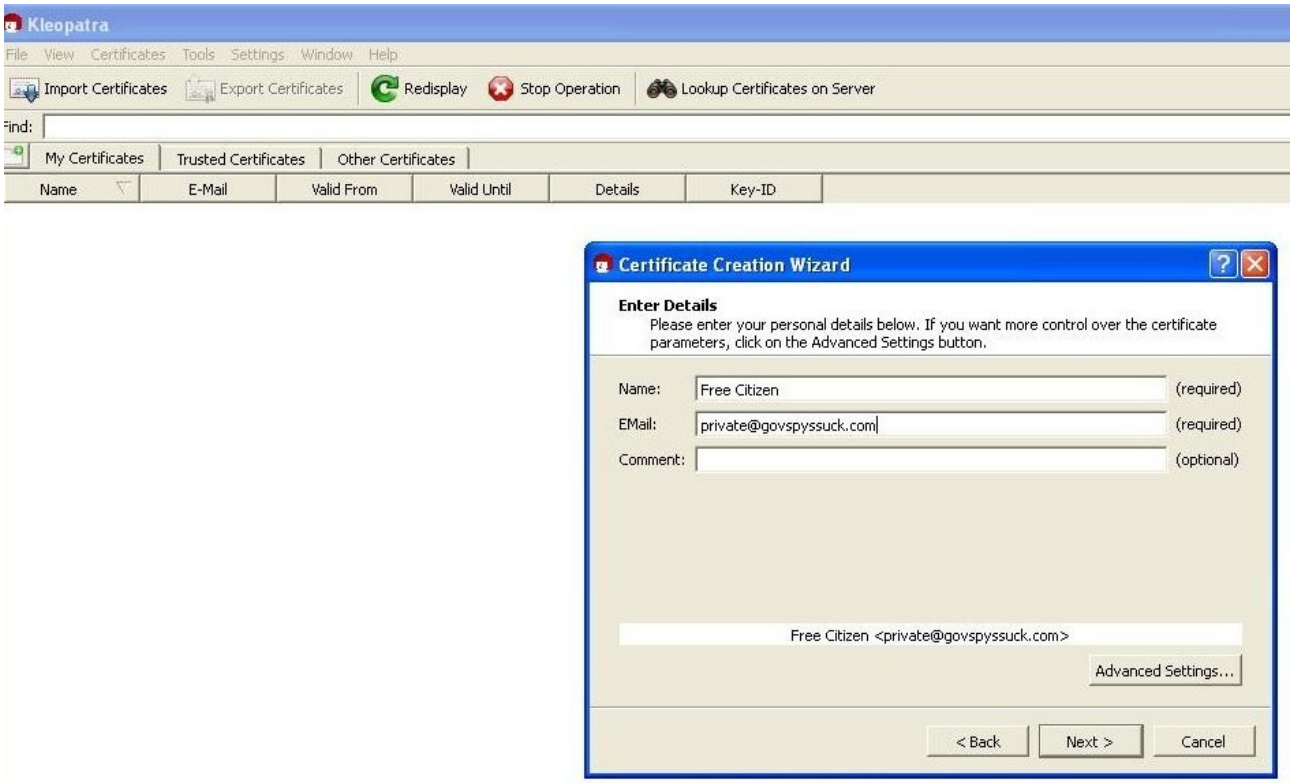


The Front End or the face of the program that you work in is called “Kleopatra”. When you install GnuPG a short cut to open Kleo is installed on your start menu or your desktop if you choose. Open as any other program and this is what you see above. Since the first thing you need to do is create a set of keys, click on *File>New Certificate.*

…….

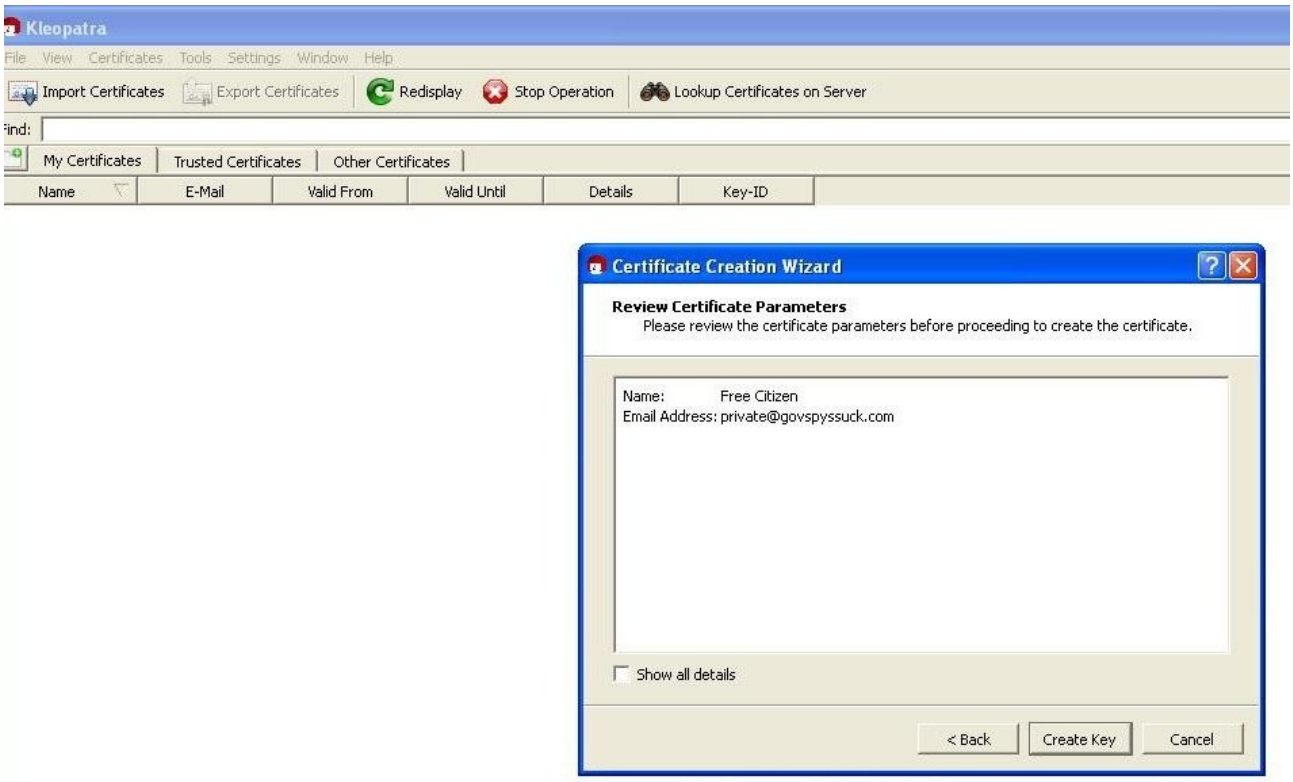


On the new popup window, select *Create Personal PGP key pair.* You will generate two keys, a public and private key set. The public key is the one you can give to anyone because it allows the other person to encrypt a document (or photo or any other digital data) to send to you that only you can open because you have the secret-private key that ***you give to no one***. Click *Next.*



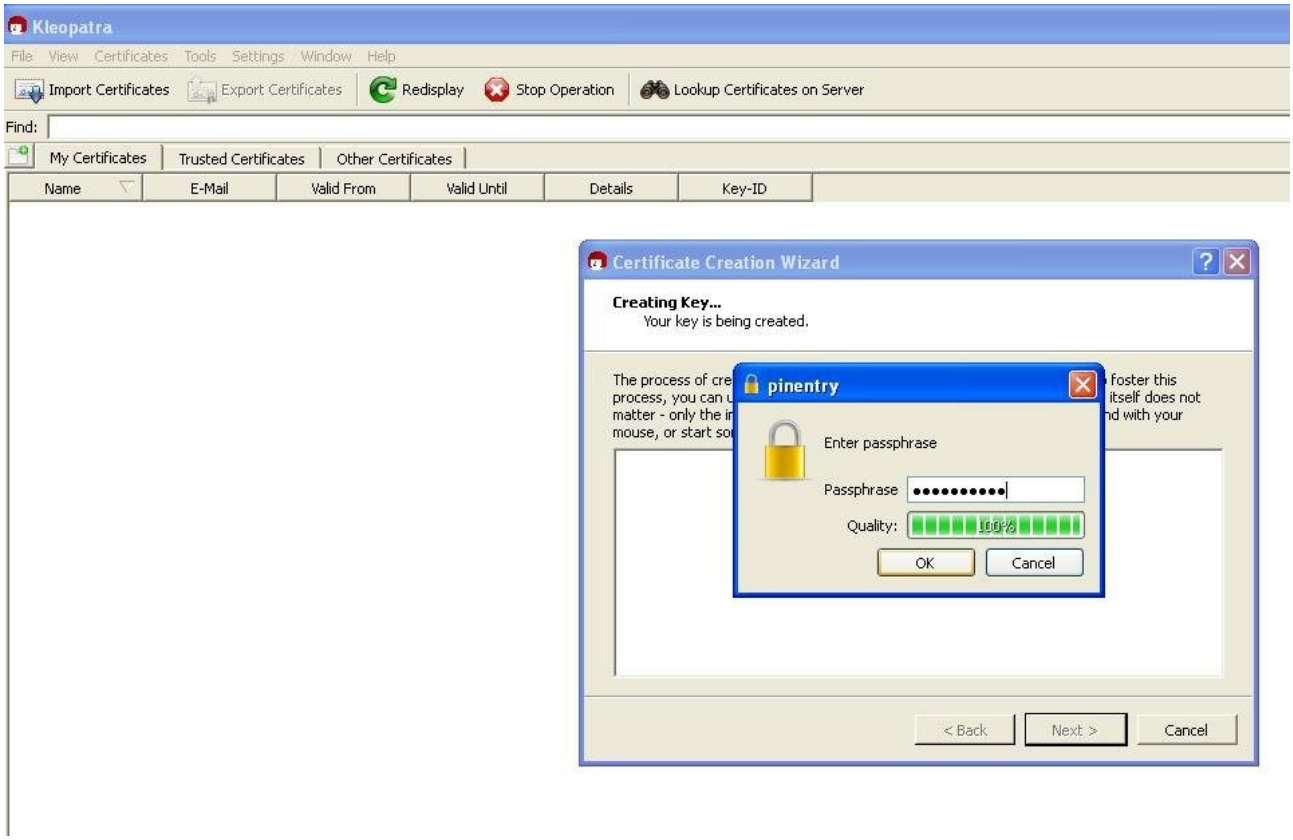
Enter your details in the next popup as shown, or at least those you wish to reveal. Click *Next.*

…….



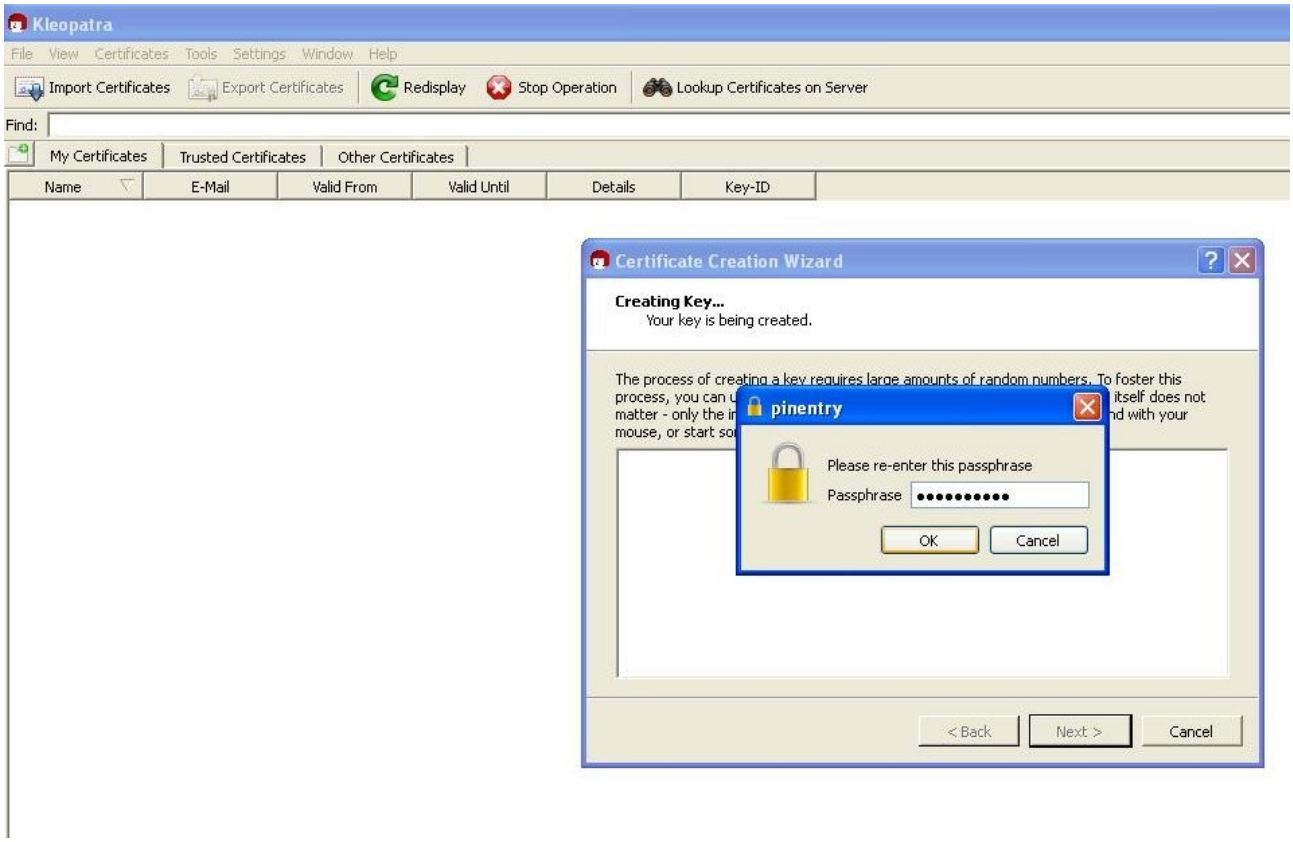
New window appears. Check details and if you approve, click *create key.*

…….

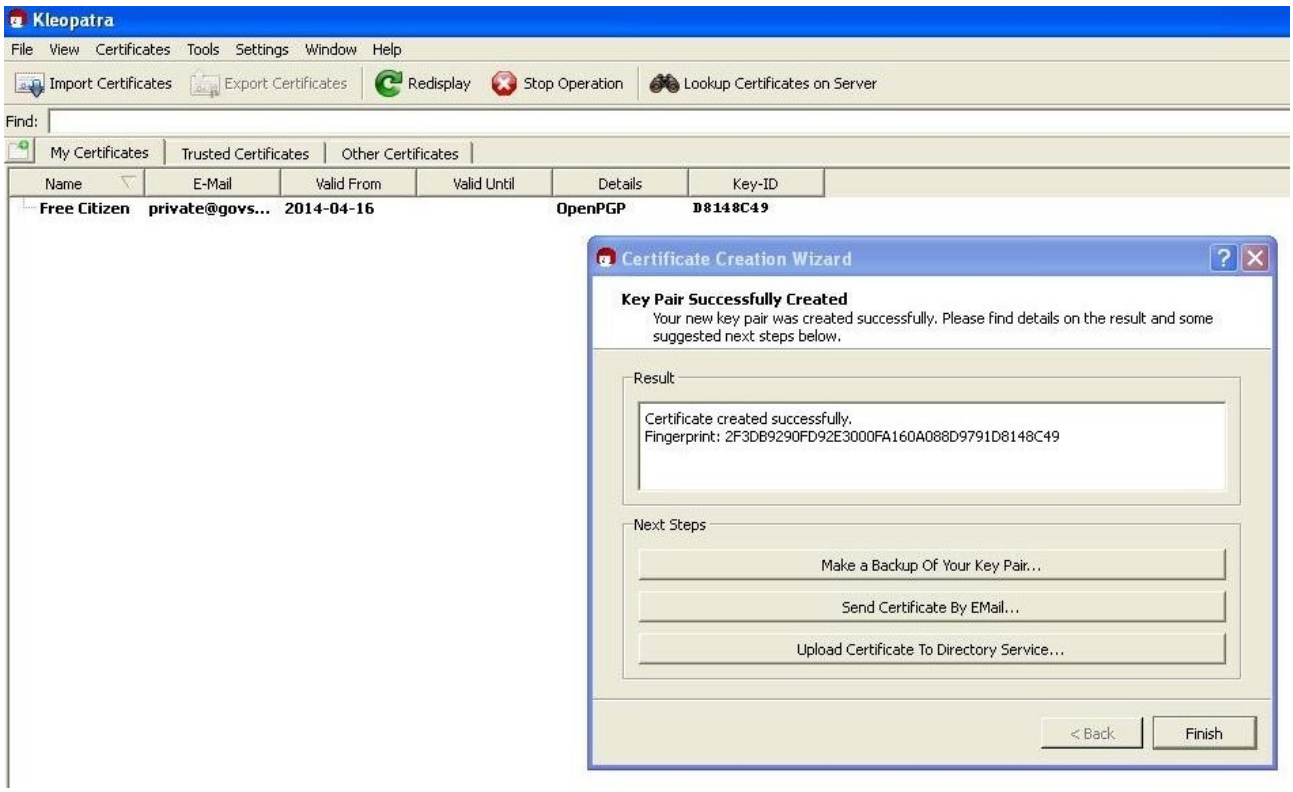


Now the business end of your secret key. Besides the digital file the private key needs an interface, your command, your pass phrase. Make it a good one! Several words, perhaps upper and lower case and numbers would be terrific. Something you will remember or already know that IS NOT a piece of publicly available information. Click *OK*

.....

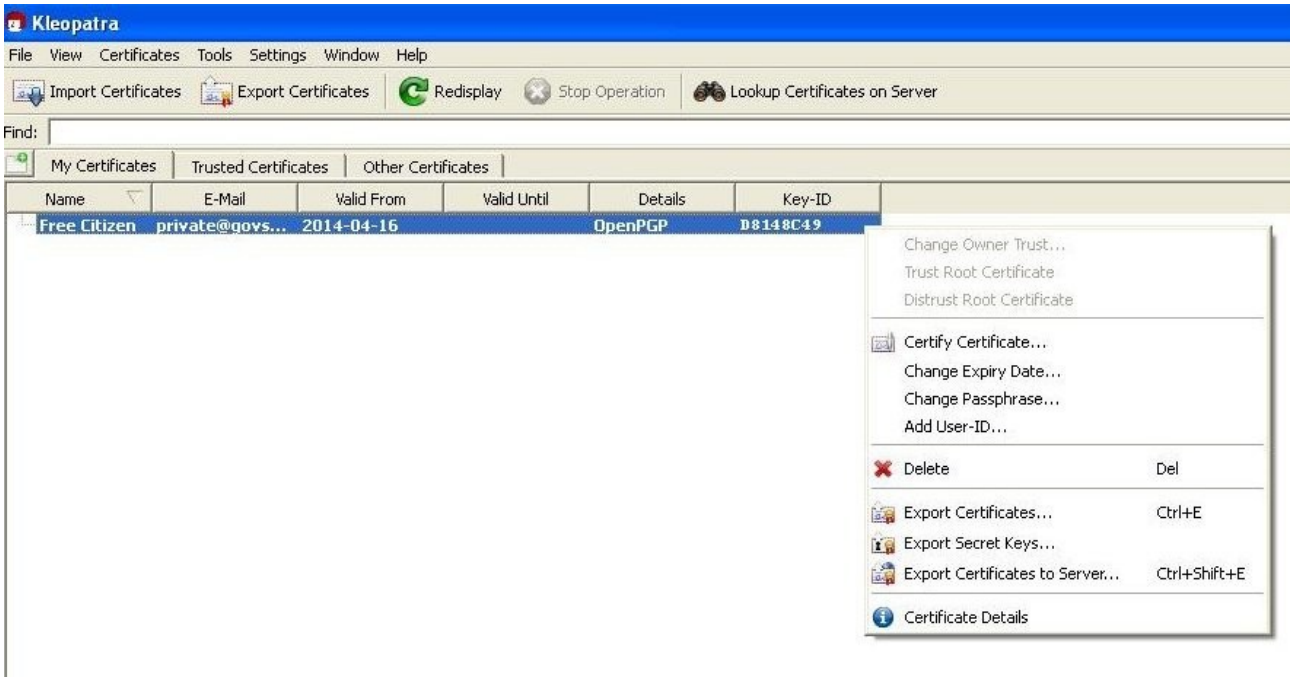


And then you will be asked to repeat it to make sure you have it in correctly. While you are doing that the program is generating your key set. Click *OK* again and then *Next.*

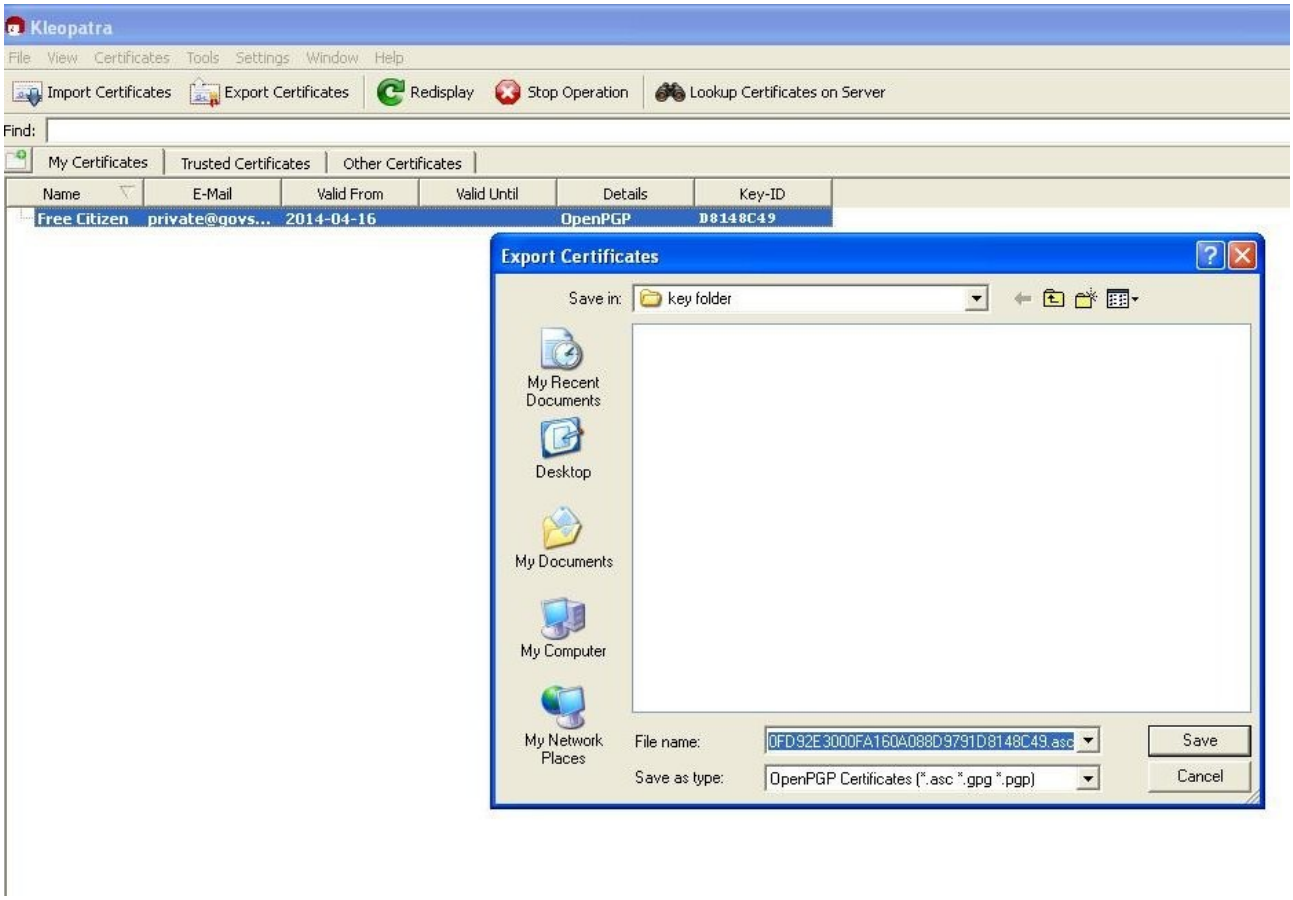


Viola! Your new key set shows up on your Kleopatra window under the heading of *My Certificates* and another popup that asks you to *Make a backup*.. don't bother. I have another way I want to show you how to do that later. Ditto with *Send Certificate by email. Upload to Directory Service* is not needed to communicate with a known person. The directory service is like a public phone book for certificates. This could be useful to some people, sometimes and the manual that comes with the program is always there for that but not right now. Click *Finish.*

.....

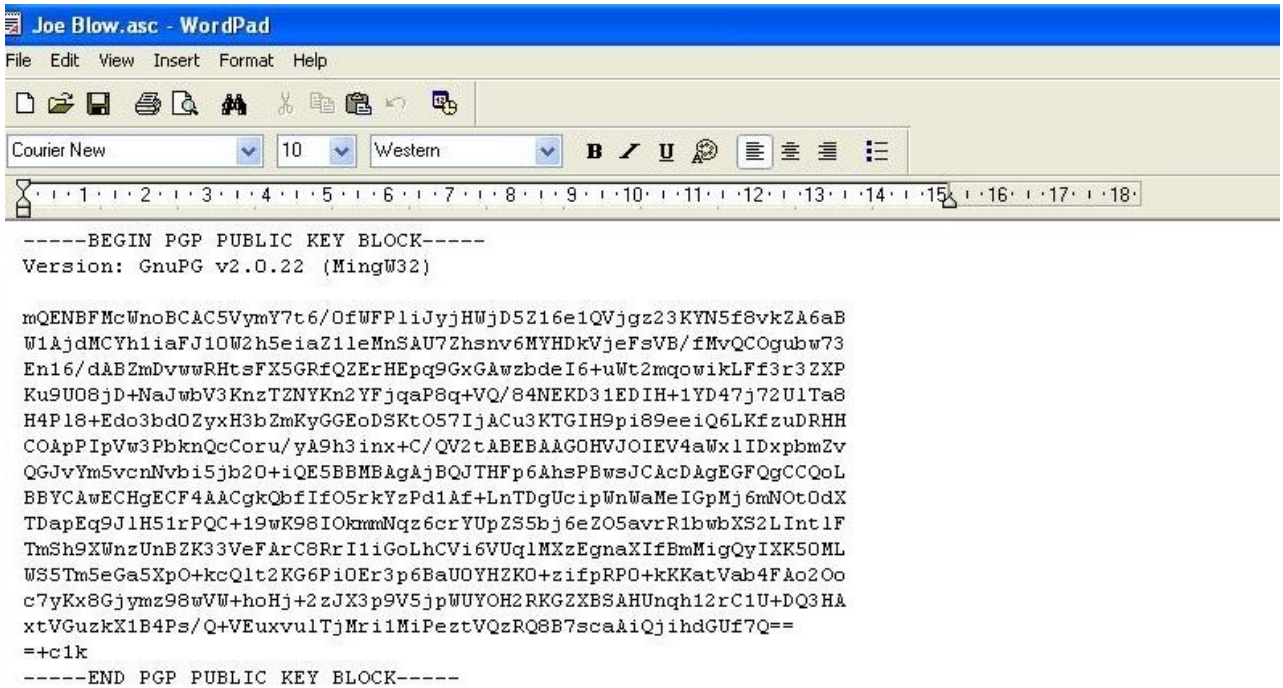


This is why I wanted you to wait on the previous step. By selecting (clicking on) a certificate in the window and right clicking, all those functions and more are available. Get used to the right click. Right now we need to click to select, *export certificate*-your public key, so you can send it off to a mate so they can send you a private message.

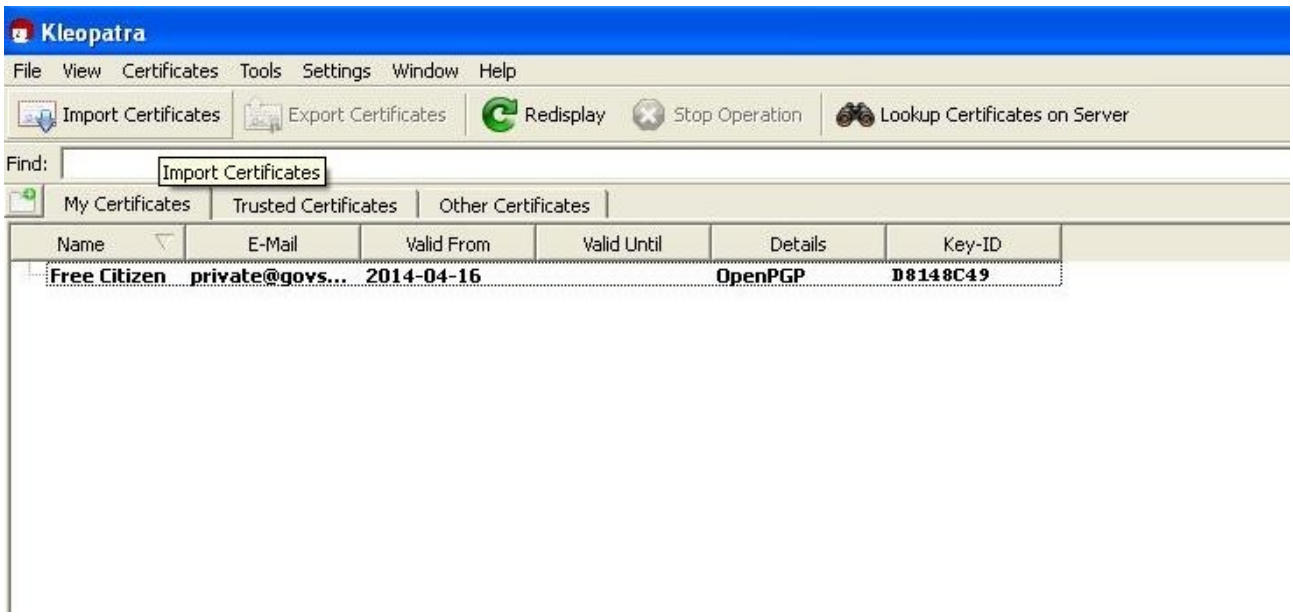


I created a folder in My Documents to store my certificate-public key so I found that folder on the browser popup, Click *Save.* You can rename the file but make sure you don't change the file type. Leave the ".asc" Now that you have this in a documents folder you can send it via email as a normal attachment to your mate Joe.

.....

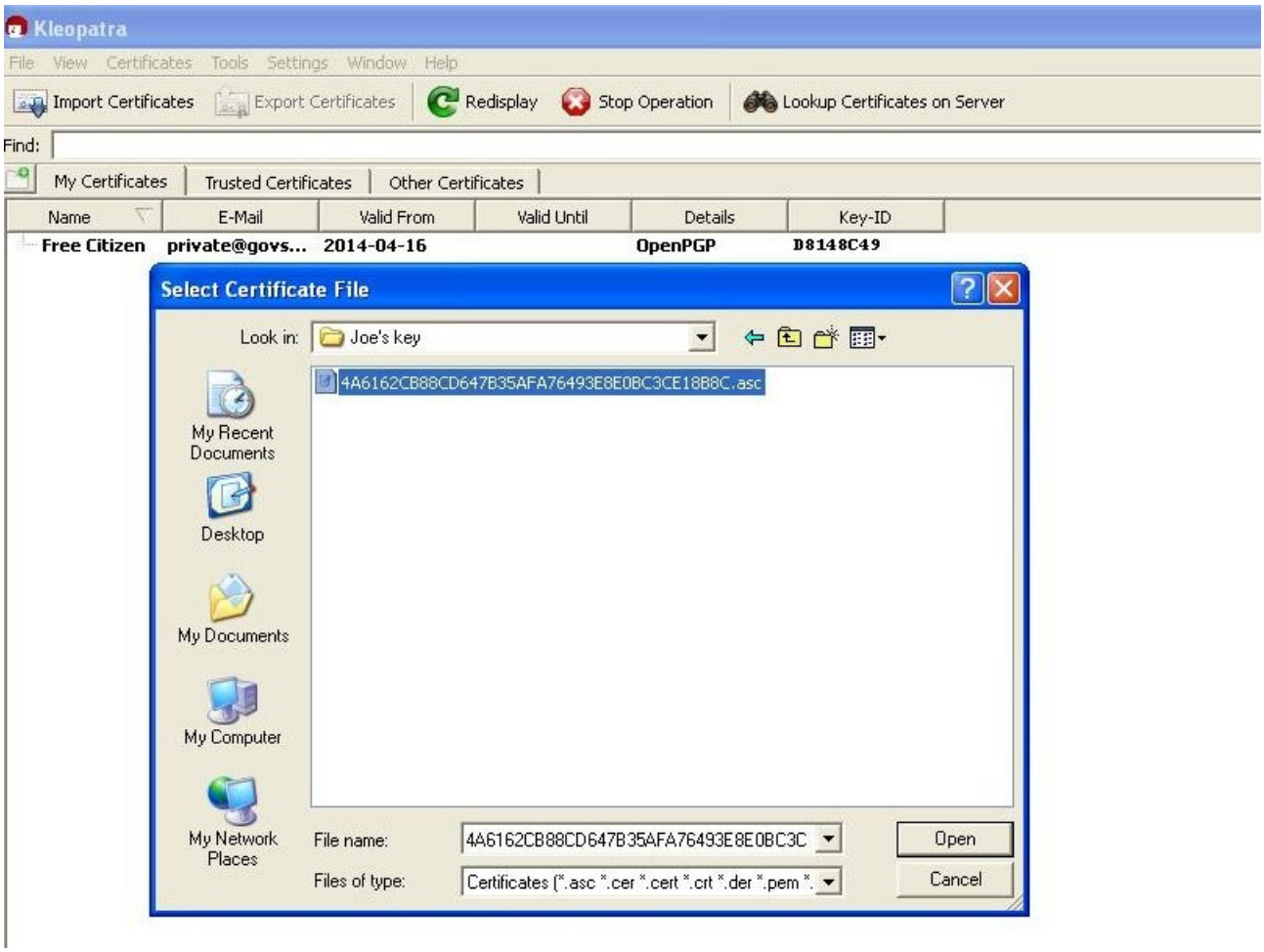


Here is what a public key looks like when viewed in a **text editor** like Windows Word Pad. If you open it in a word processor it may distort the formatting and saving it that way makes it useless.

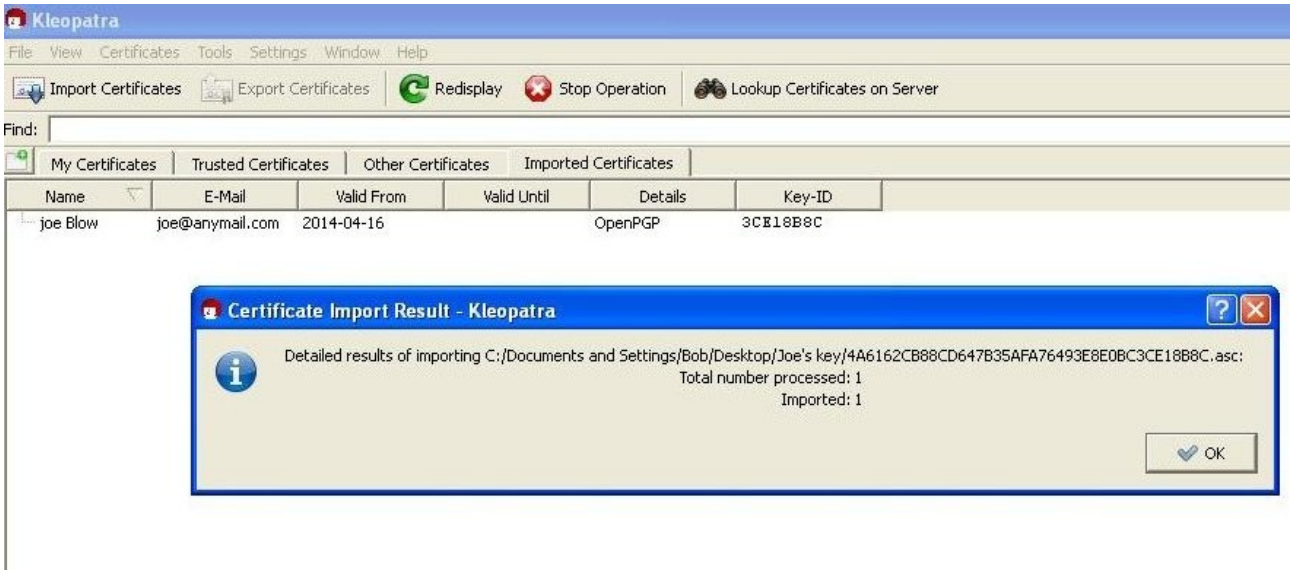


While you were sending your public key to Joe, he was sending his to you! You made another folder in your Documents called Joe's Key and saved it there from his email. Open Kleopatra again and click on *Import Certificates*.

…….

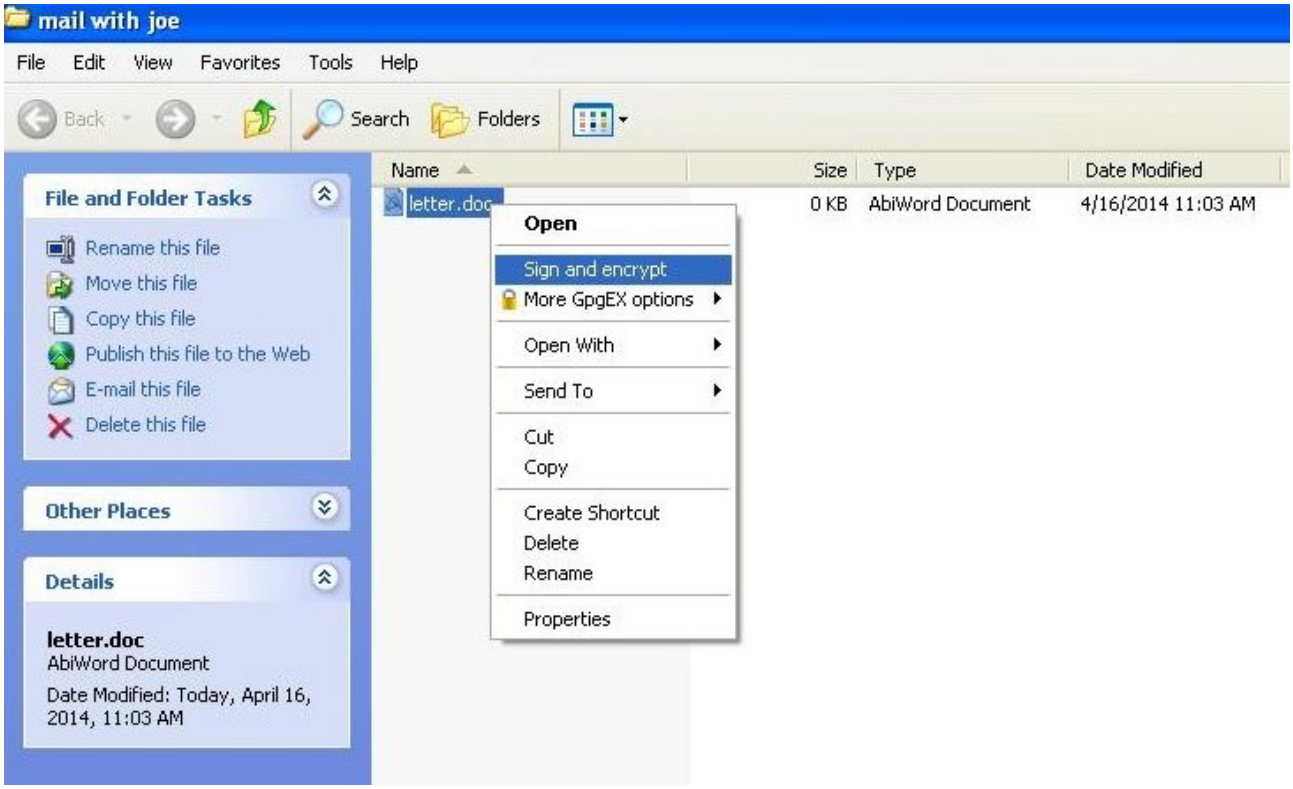


The file browser window opens again and you find the file (*My documents>Joe's key*) and open it and there is Joe's key. Select the file by clicking on it and then click on *Open*.

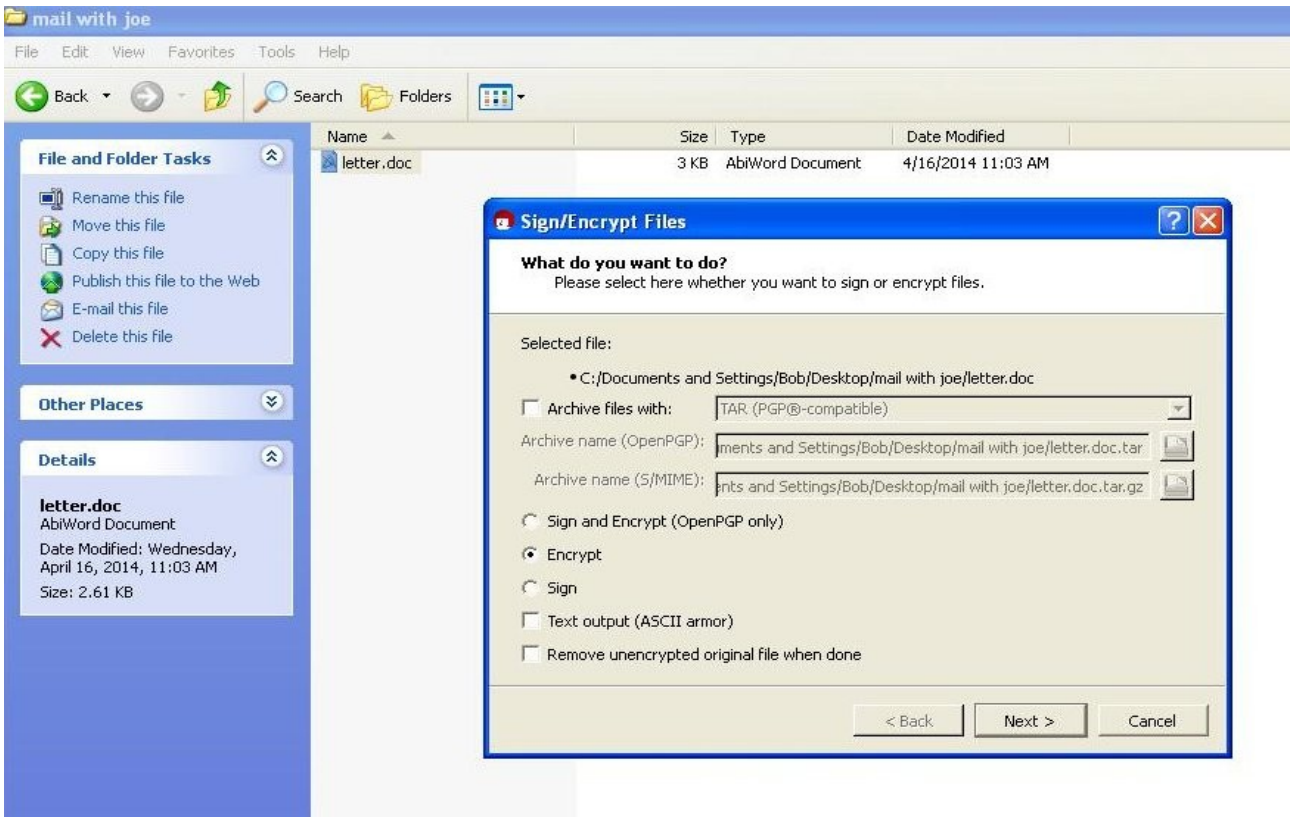


Then another window pops up that confirms it was imported and on Kleopatra, under the heading of *Imported Certificates*, it shows the details of Joe's Key. All the hard work is now done and you are ready to exchange encrypted files with Joe. It is so easy... click *OK*

….....

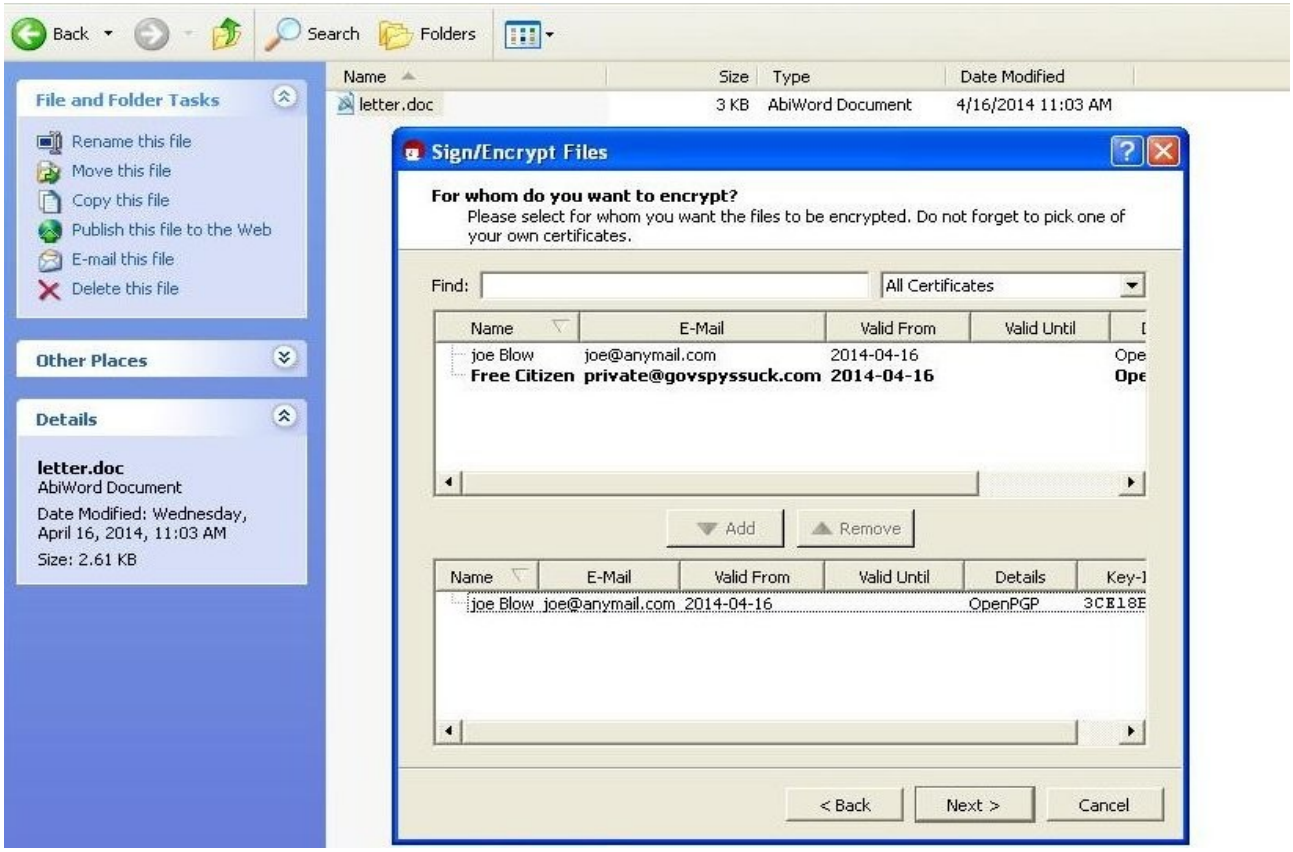


You can write a letter to joe and save it somewhere, anywhere. Right click on it and check the drop down window. Select *Sign and Encrypt.*

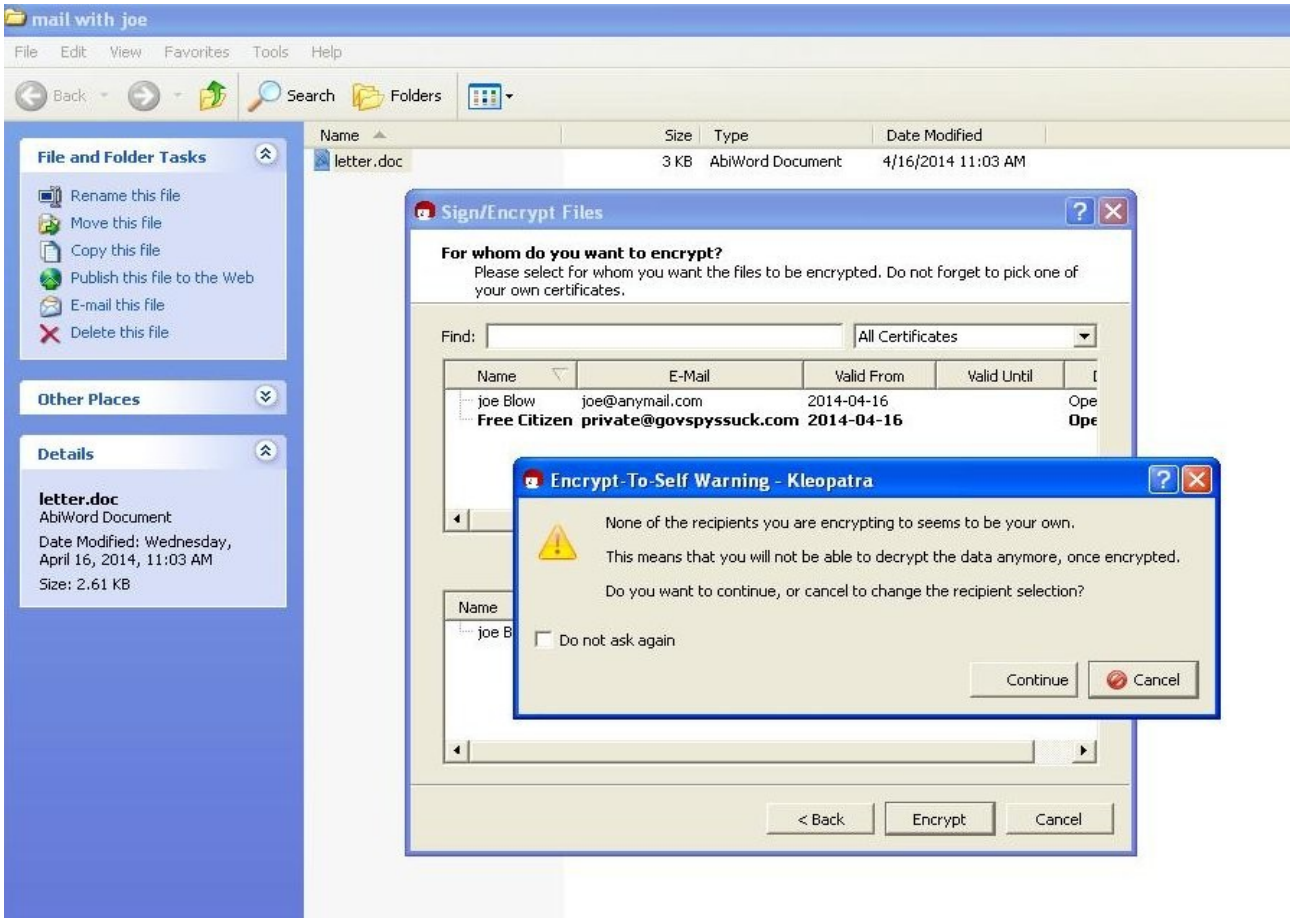


The next popup gives choices, select *Encrypt* and *Next*

.....

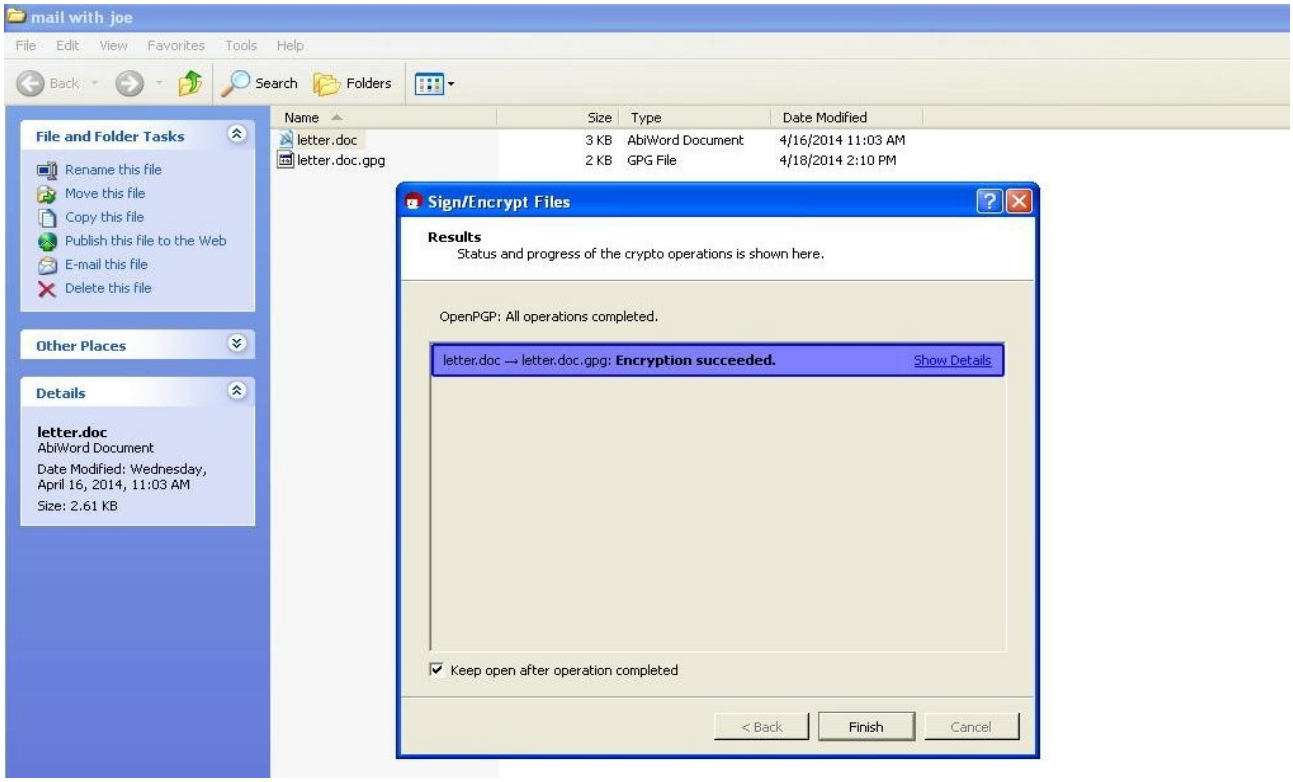


Now the window asks who you want to encrypt it for. You only have two certificates in *ALL Certificates*, yourself and Joe. You already have a copy of the unencrypted document so just select Joe's certificate and the *ADD* button highlights, click on that button and Joe's certificate appears in the bottom-recipients window. Click *Next*. So, to recap; *select>Add>Next*

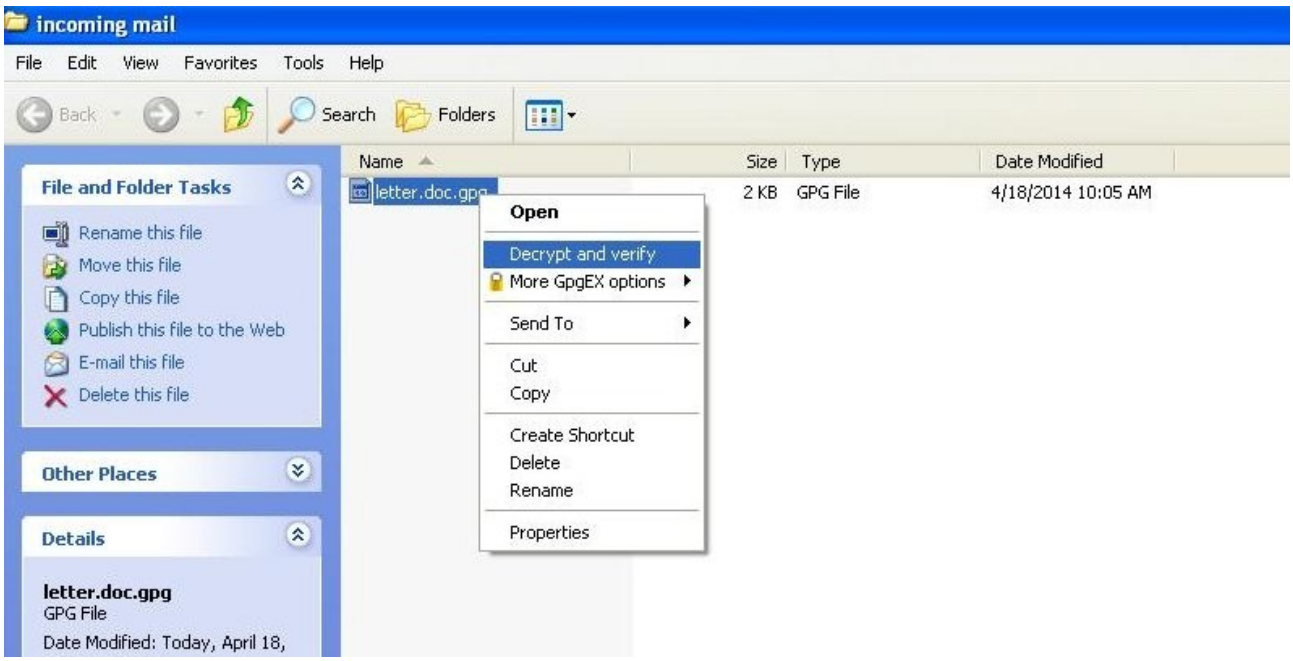


The next window reminds you that you didn't encrypt for yourself but like I say, you already had a copy. Click *Continue* and then *Encrypt.*

…….

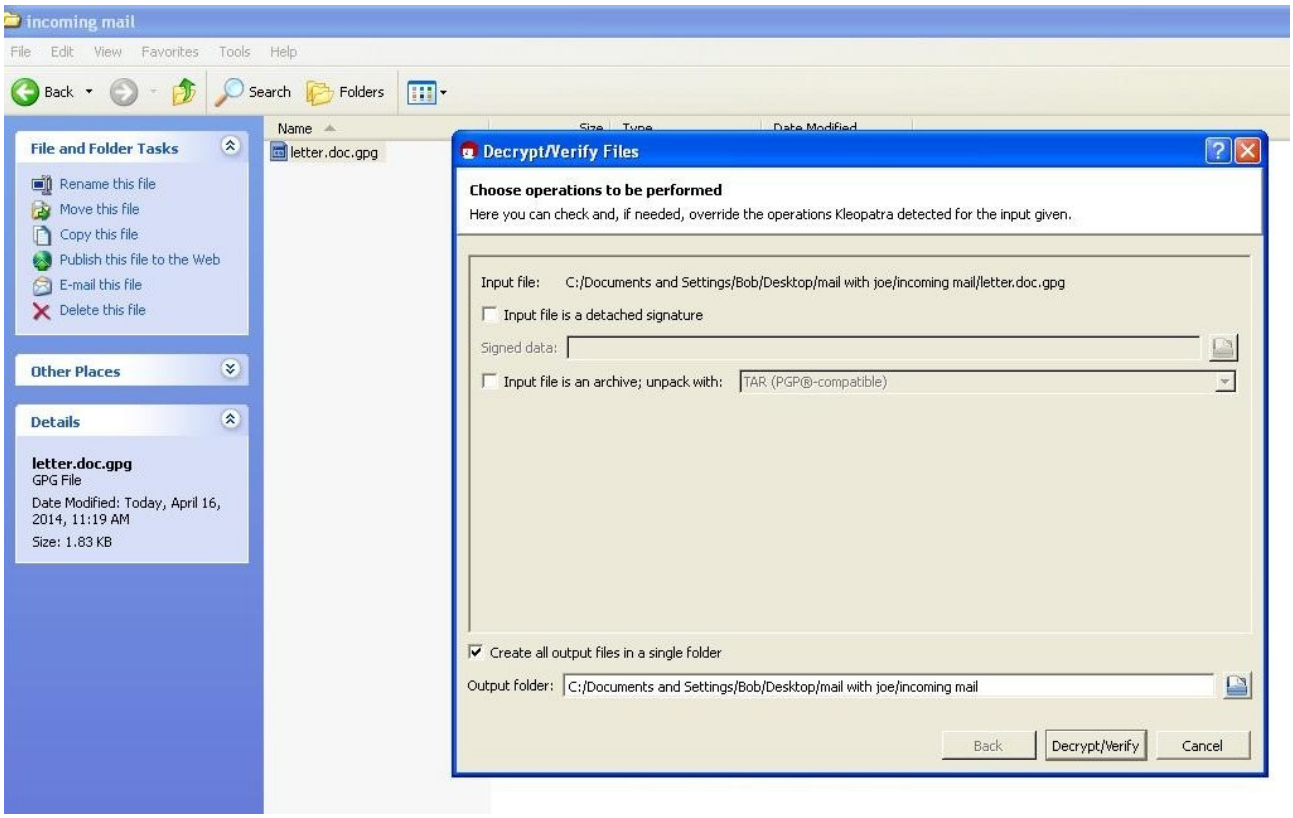


Done! The encrypted file is ready to attach to a mail, to send to Joe. Only he can open it and you have the original doc to refer to. Make sure you attach the right one! Click *Finish.*

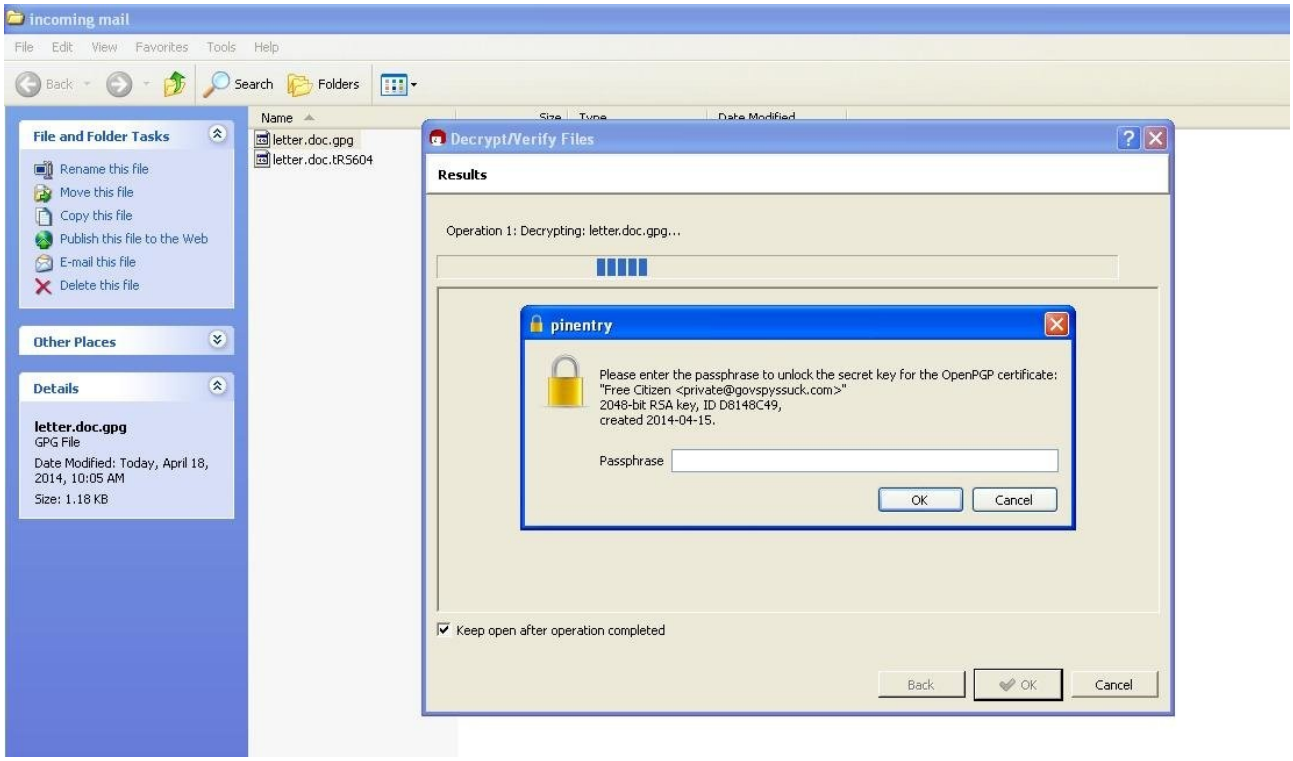


While you were sending your letter to Joe, he was firing one off to you so you saved it to a folder and now right click on the document. Select *Decrypt and verify* from the drop down menu.

…….

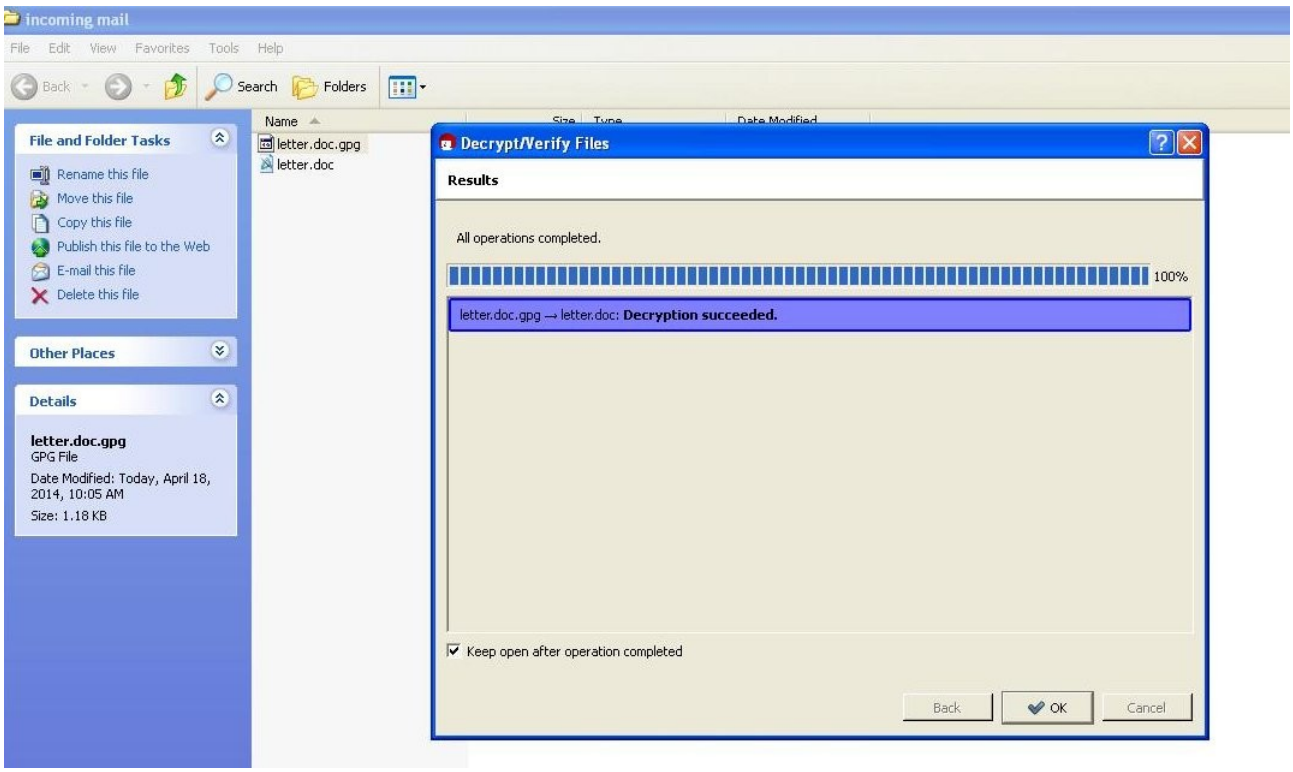


Accept the default setting on the next window, *Create all output files in a single folder*..... and click *Decrypt/Verify.*



Now you need your pass phrase, type it in and click *OK*. If you have other files to decrypt as well, the program will save the pass for the session.

.....



Success! You now have the original encrypted file and the decrypted file, ready to open in your word processor in the same folder. Click *OK*.

You have created keys, sent and received files in privacy. Please say Thank You, It's all I get out of this...

As time permits this tutorial may expand but I think most of you will do OK with this start. You will probably be OK on your own with the confidence of success this far.

One final note on security, if you worry your public key may be altered in transit to your intended recipient, take a screen shot of it before shipping. Send the screenshot along with the text/.asc file and the recipient can compare the two visually. To take a screen shot on a Windows computer, look for the key on your keyboard that says "PrtSc" (stands for *Print Screen*) or similar, usually on top row next to the F12 key. Open the asc doc and press that key to take the shot, then open a photo editing program like Windows Paint, see your start menu, if it doesn't show there, click on All *Programs>Accessories>Paint.* Once opened the pic should be on the clipboard so click on edit>paste. That should get it on the screen, then click *File>save* as and browse for a location and save.

OK... A second final note... there is always the concern that agencies like the US NSA will impersonate a site like www.gnupg.org so people download their corrupted program instead of the real deal. There is a verification program to test that but that is another lesson. Chances are you are ok unless you are in the US but before transmiting really sensitive material you might consider doing it.

OOPHS! I thought of another one. Your secret keys are only as secure as your computer. Make sure it is password protected and do not give the password to anyone! So far the government can't legally force you to reveal it.... so far.

OK, OK... a forth final note... The Australian government is currently debating a proposal from their spy agencies to require anyone to produce their private keys on demand. The agencies have apparently become so comfortable intruding on citizens privacy they are now considering it a right. The trajectory of this kind of intent should finally wake the majority dumb bastards up.... but I doubt it. Make all the noise you can as the government knows (SMH poll showed 94% against increasing their powers last year) people don't want to give up more rights.

From the United Nations Universal Declaration Of Human Rights;

Article 12.

- No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.