

Waysact data protection and security

Waysact has made significant investment in our technology to help keep your donor data secure. One of the many ways we help ensure the security of your donors' information is by encrypting the files you export from Waysact with a unique encryption key that you create.

Once you have downloaded the GPG program and create your key (which is really just a very long string of numbers, characters and letters) there will actually be two keys created (this is your 'key pair'). One is your private key that you keep private and secure. The other is your public key, which you send to us securely (via https) so we can encrypt your files with it.

When you go to decrypt a Waysact export file, the GPA program will only decrypt the file if the private key on your computer and the public key encrypting the file are a matching 'key pair'.

This document will provide you with step-by-step instructions on how to download the GPA program, create your unique encryption key and use your key to open an encrypted file.

Best practice for key management

Before we start, there are some important points to consider when creating your unique encryption key.

To follow best practice, please consult with your IT Department and read this important information about creating and maintaining keys:

- When creating a passphrase (which is the password for your key) make the passphrase as strong as possible by:
 - using a combination of upper and lower case letters, numbers and special characters,
 - avoiding common passwords, or ones that would be easy for other people to guess, and
 - making your password at least 7 characters long.

While it is important to choose a secure passphrase, there is no 'password reset' facility so make sure you choose something you will easily remember – otherwise you will have to start from scratch and create a new key pair.

- Your key should be stored in a safe location where it is easy for you to retrieve

it. When storing your key, you should consider who else will have access to that location. Your IT Department may be able to provide you a secure location with restricted access, for example an encrypted drive or vault.

- Someone in your organisation should be overseeing the management of the keys, ensuring that :
 - keys are being stored securely,
 - procedures are in place to ensure the key has a defined lifetime (for example, a timeframe of anywhere up to a maximum of 2 years) and someone will be responsible for overseeing this and changing the key after that period of time,
 - keys are changed immediately if someone who has had access to them leaves the organisation, and
 - keys are changed immediately if it is suspected that someone has had unauthorised access to a private key.

The person responsible for management of the keys should also ensure that there is a policy around distributing keys securely and that anyone who has access to the keys formally acknowledges their responsibilities to ensure the security of the key data.

Installing GnuPG tools for Windows

GPA is free, open source encryption software: visit www.gpg4win.org

1. Select **Download Gpg4win**.



2. Select the most recent release of Gpg4win at the top of the next page and click **Run** or **Save**.



3. Select your language and click **OK**.



4. Click **Next** to continue with the installation.



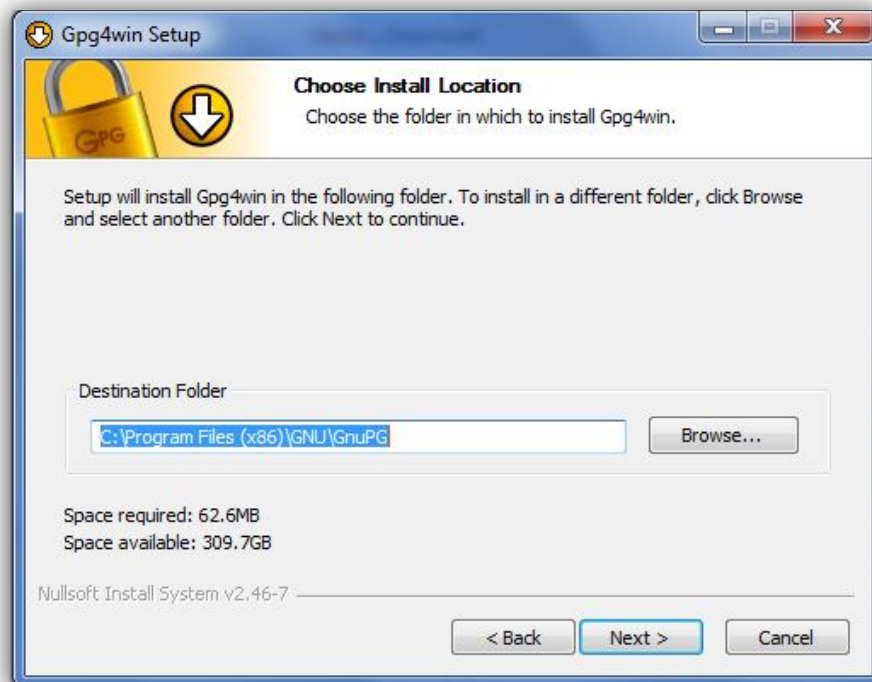
5. Click **Next** to accept the License Agreement.



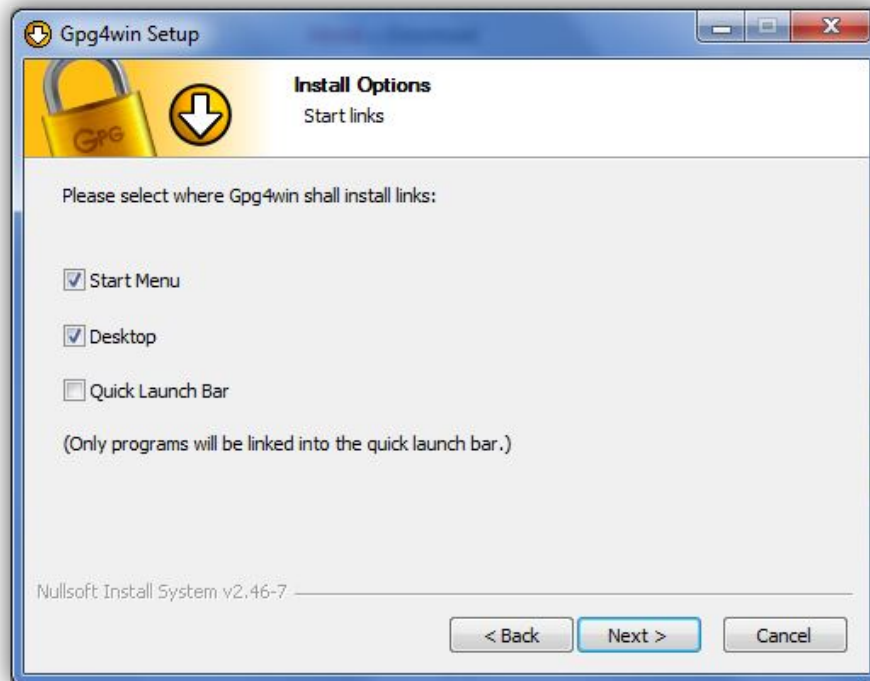
6. Untick everything leaving only GPA (and GnuPG) ticked. Click *Next*.



7. Choose to install in the default location by clicking *Next*.



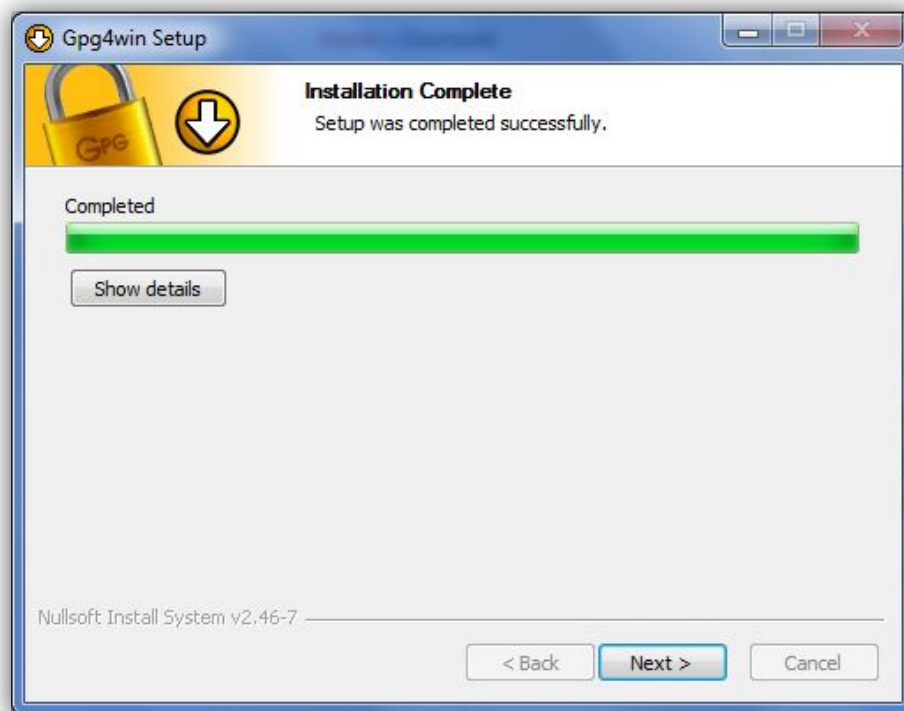
8. Tick *Start Menu* and *Desktop* to install a desktop icon (recommended).



9. Click *Next* to create a shortcut for the Start Menu.



10. Click *Next* to continue with the installation.



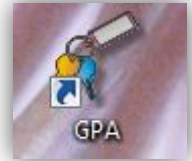
11. Click *Finish* to complete the installation.



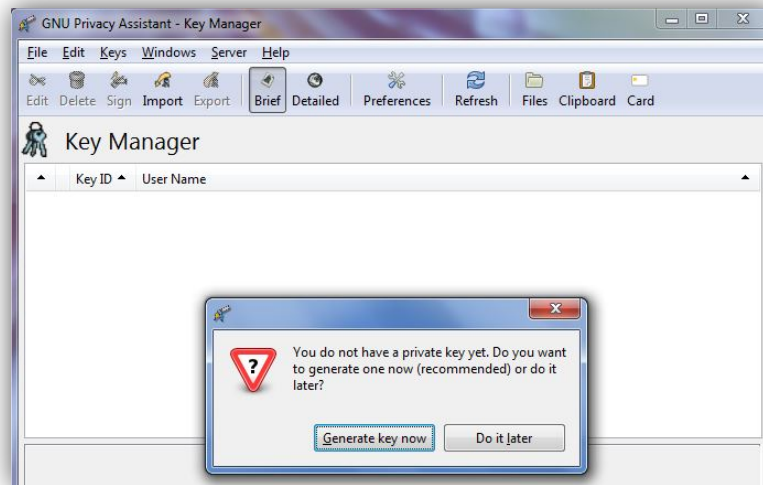
Congratulations – you have now successfully installed GPA on your computer!

Creating your key

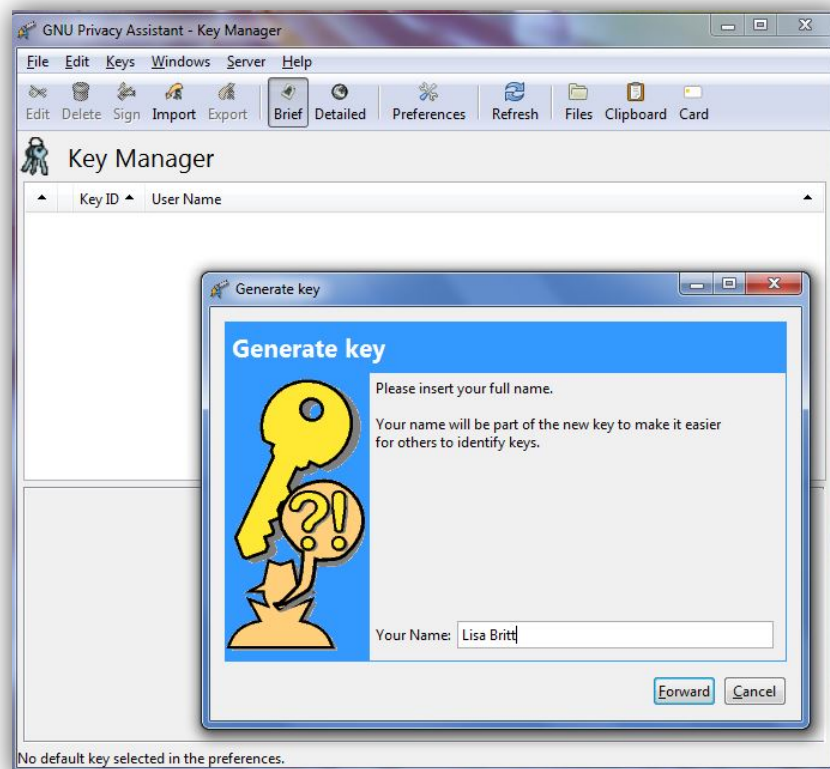
- 12. You should see this icon on your desktop.
Double click the icon to open the GPA program.**



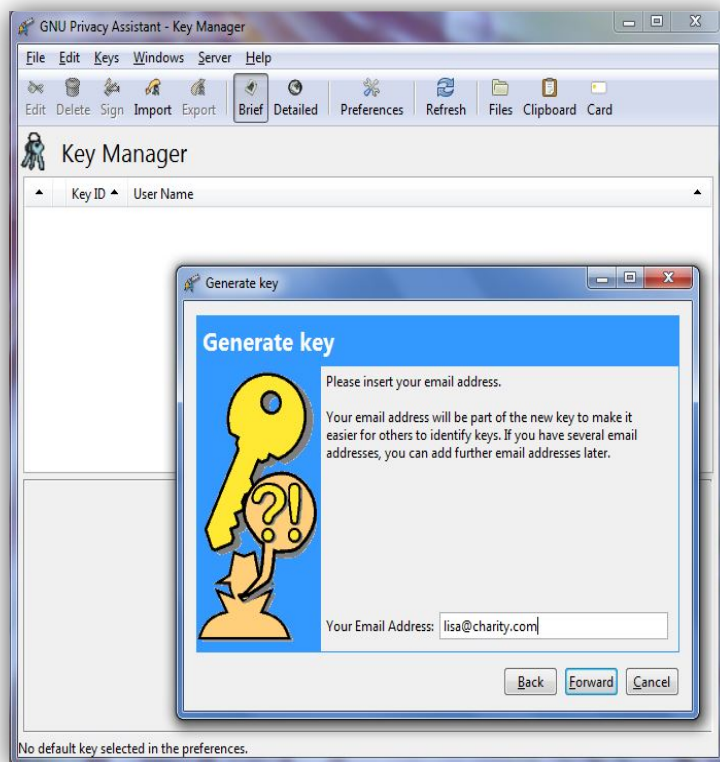
- 13. Assuming you have no keys installed, you will
be asked to generate one.**



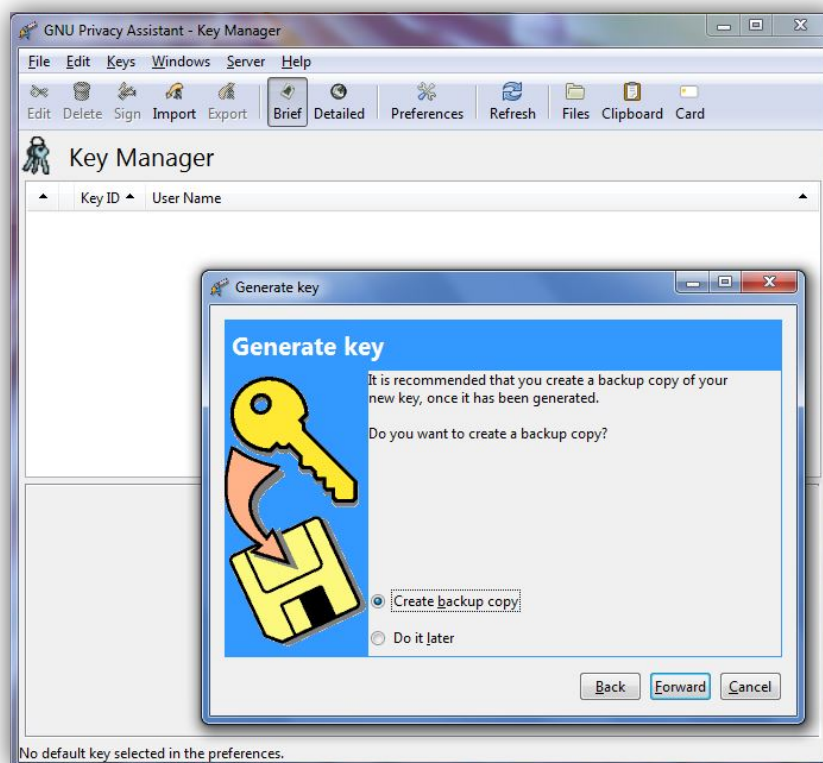
- 14. Type in your full name. This will be used to identify your
public key.**



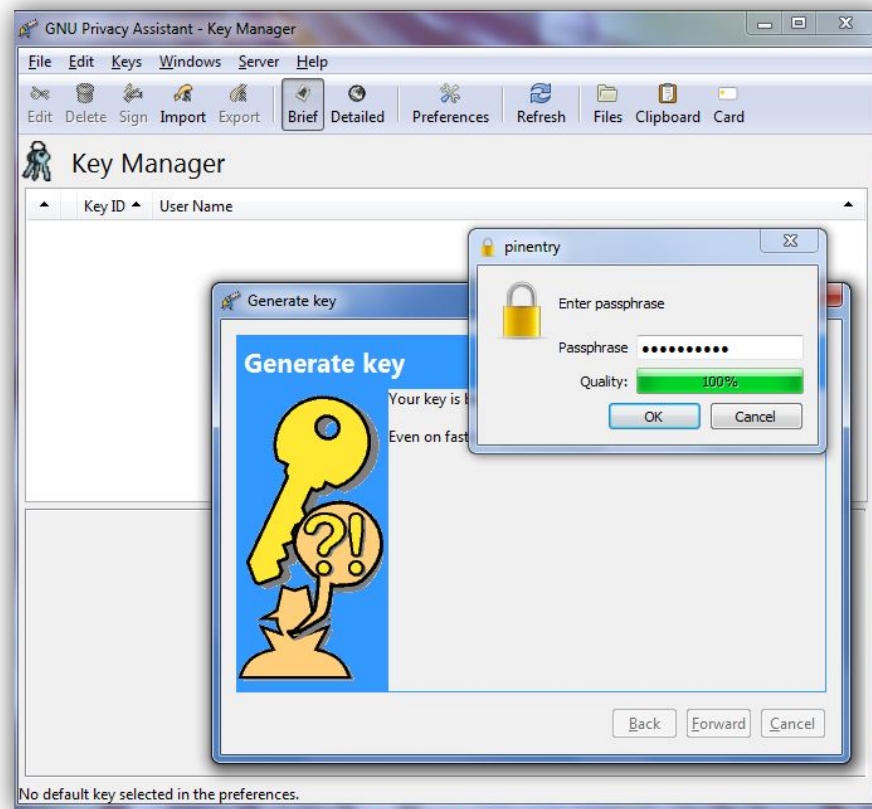
15. And your email address



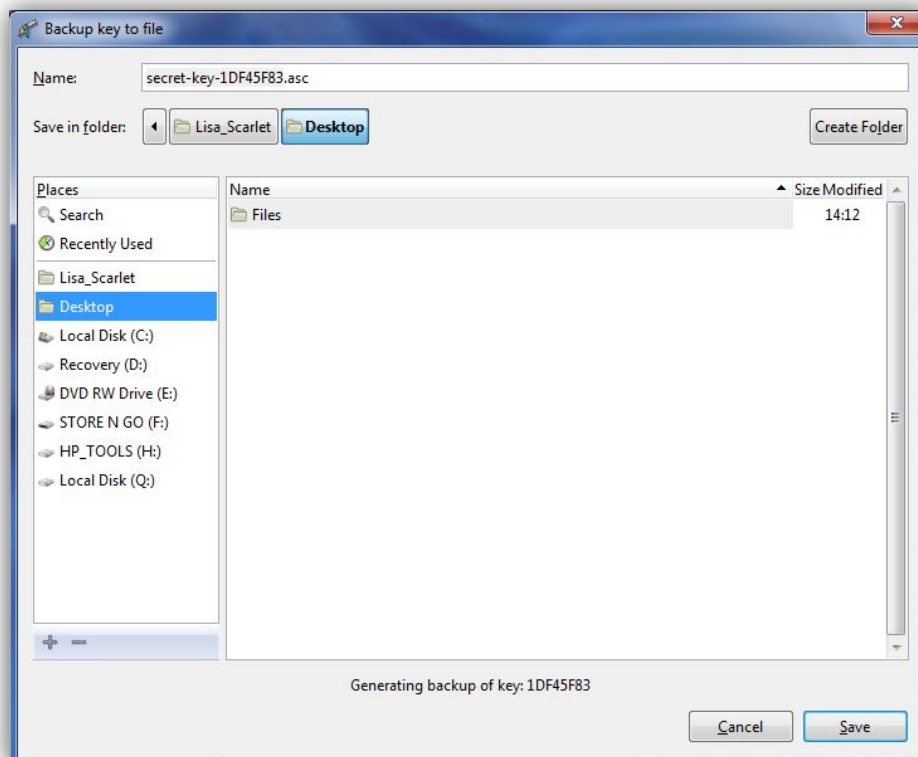
16. Select *Create backup copy* and click *Forward*.



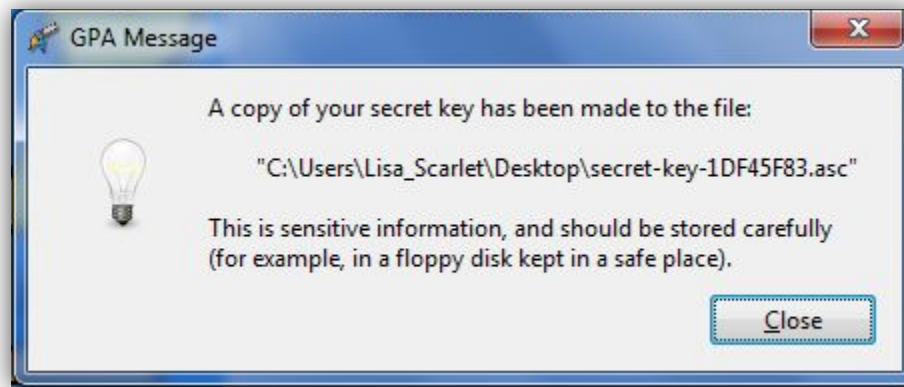
17. Create a passphrase – to enhance security the longer the password is the better. Re-enter the phrase when prompted.



18. Save the key to a safe, retrievable location.

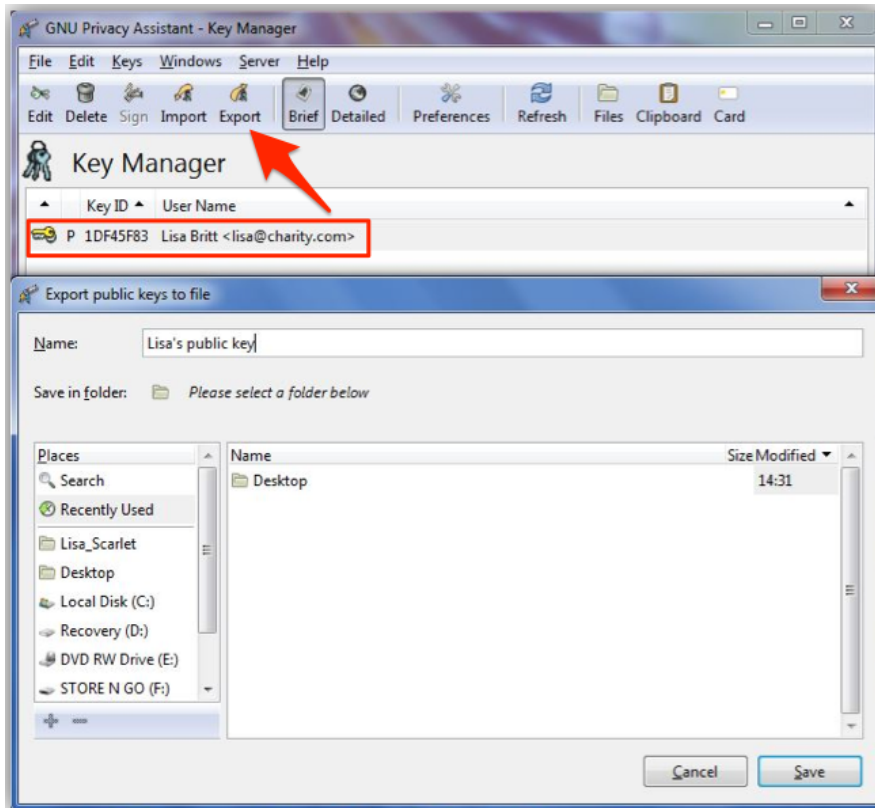


19. You will receive confirmation your key has been saved.



Exporting your public key

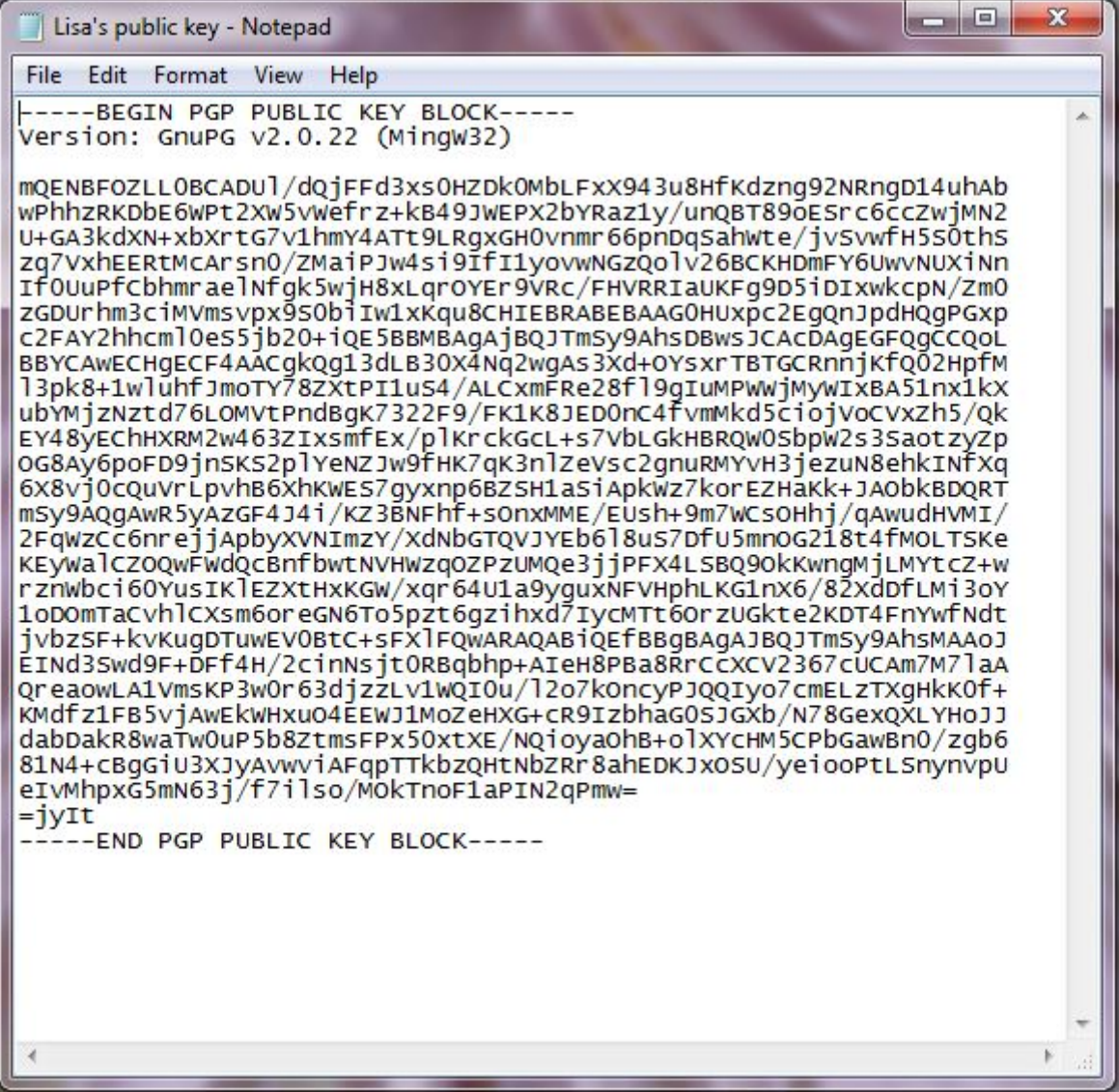
- 20. Congratulations you have created your key and should see it listed under *Key Manager*. Select the key, click *Export*, give the key a name, choose a location and click *Save*.**



- 21. You will then see the Public Key has been saved.**



22. This is what your key should look like if you open it in a text editor like Notepad.



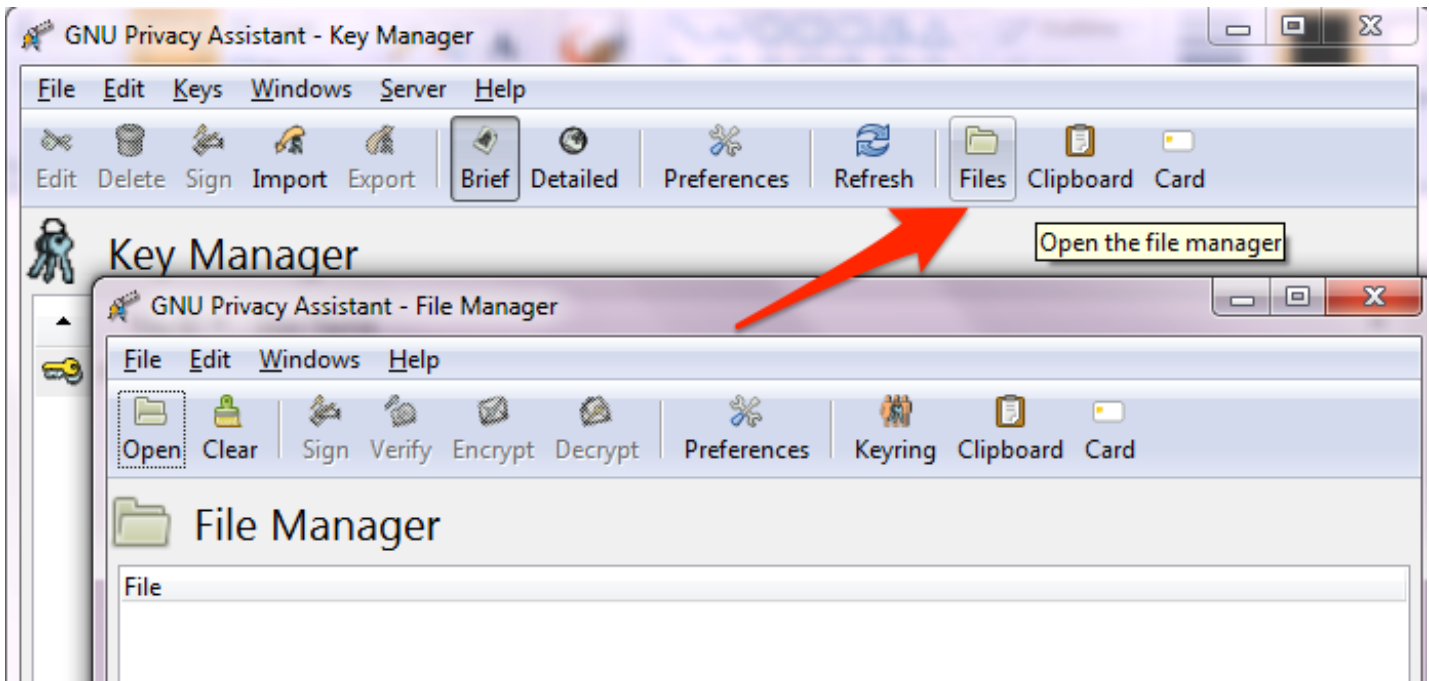
```
File Edit Format View Help
|-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (Mingw32)

mQENBFOZLL0BCADU1/dQjFFd3xs0HZDk0MblFxx943u8HfKdzng92NRngD14uhAb
wPhhzRkDBe6Wpt2Xw5vwefrz+kB49JWEPX2bYRaz1y/unQBT89oESrc6ccZwjMN2
U+GA3kdXN+xbXrtG7v1hmY4Att9LRgxGH0vnmr66pnDqSahwte/jvSvwfH5S0ths
zq7VxhEERTMcArsn0/ZMaIPJw4si9IfI1yovwNGzQo1v26BCKHDMFY6UwvNuxiNn
If0UuPfcbhmr aelNfgk5wjH8xLqroYer9Vrc/FHVRRIauKfg9D5iDIxwkcPn/Zm0
ZGDURhm3ciMvmsvpX9S0biIw1xKqu8CHIEBRABEBAAG0HUxpc2EgQnJpdHQgPGxp
c2FAY2hhcm10es5jb20+iQE5BBMBAGAJBQJTMsy9AhsDBwsJCACDAGEGFQgCCQoL
BBYCAWECHgECF4AACgkQg13dLB30X4Nq2wgAs3Xd+OYsXrTBTGCRnnjKfQ02HpFM
13pk8+1wluhfJmoTY78ZxtPI1uS4/ALCxmFRE28f19gIuMPWwjMywIXBA51nx1kx
ubYMjznZtd76LOMvtPndBgK7322F9/FK1K8JED0nc4fvmMkd5ciojVoCvXzh5/Qk
EY48yECHHXRM2w463ZIxsmfEx/plKrcKGL+s7VbLGkHBRQW0Sbpw2s3SaotzyZp
OG8Ay6poFD9jNSKS2p1YenZJw9fHK7qK3n1Zevsc2gnuRMVvH3jezuN8ehkINFxq
6X8vj0cQuvrLpvhB6xhKwES7gyxnp6BZSH1asiApkwz7korEZHakk+JAObkBDQRT
msy9AQgAWr5yAzGF4J4i/KZ3BNFhf+sOnxMME/Eush+9m7WCsOHhj/qAwudHvMI/
2FqWzCc6nrejjApbyXVNIImZY/XdnBGTQVJYeb6l8uS7DfU5mnOG218t4fMOLTSke
KEYwAlCZOQwFwdQcBnfbwtNVHwzqOZPZUMQe3jjPFX4LSBQ90kKwngmJLMYtCZ+w
rznwbcie60YusIK1EZxtHxKGW/xqr64U1a9yguxNFVHphLKG1nx6/82XdDfLmi3oY
1oDomTaCvhlCXsm6oreGN6To5pzt6gziHxd7IycMTt60rZUGkte2KDT4FnywfnDt
jvbzSF+kvKugDTuEV0BtC+sFXlFQwARAQABiQEfBBgBAGAJBQJTMsy9AhsMAAoJ
EIND3swd9F+Dff4H/2cinnsjt0RBqbhp+AIeH8PBA8RrCCXCV2367cUCAM7M7laA
QreaowLA1VmsKP3w0r63djzLV1wQIOu/12o7koncypJQQIyo7cmELzTXgHkK0f+
KMdfz1FB5vjAwEkWxuo4EEWJ1MoZehXG+CR9IzbhaG0SjGxb/N78GexQXLYHoJJ
dabDakR8waTw0Up5b8ZtmsFPx50xtXE/NQioya0hB+o1XYCHM5CPBgawBn0/zgb6
81N4+CBGgiU3XJyAvwviAFqpTTkbzQhtNbZRR8ahEDKJXOSU/yeiooPtLSnynvpU
eIVMhpxG5mN63j/f7ilso/MokTnoF1aPIN2qPmw=
=jyIt
-----END PGP PUBLIC KEY BLOCK-----
```

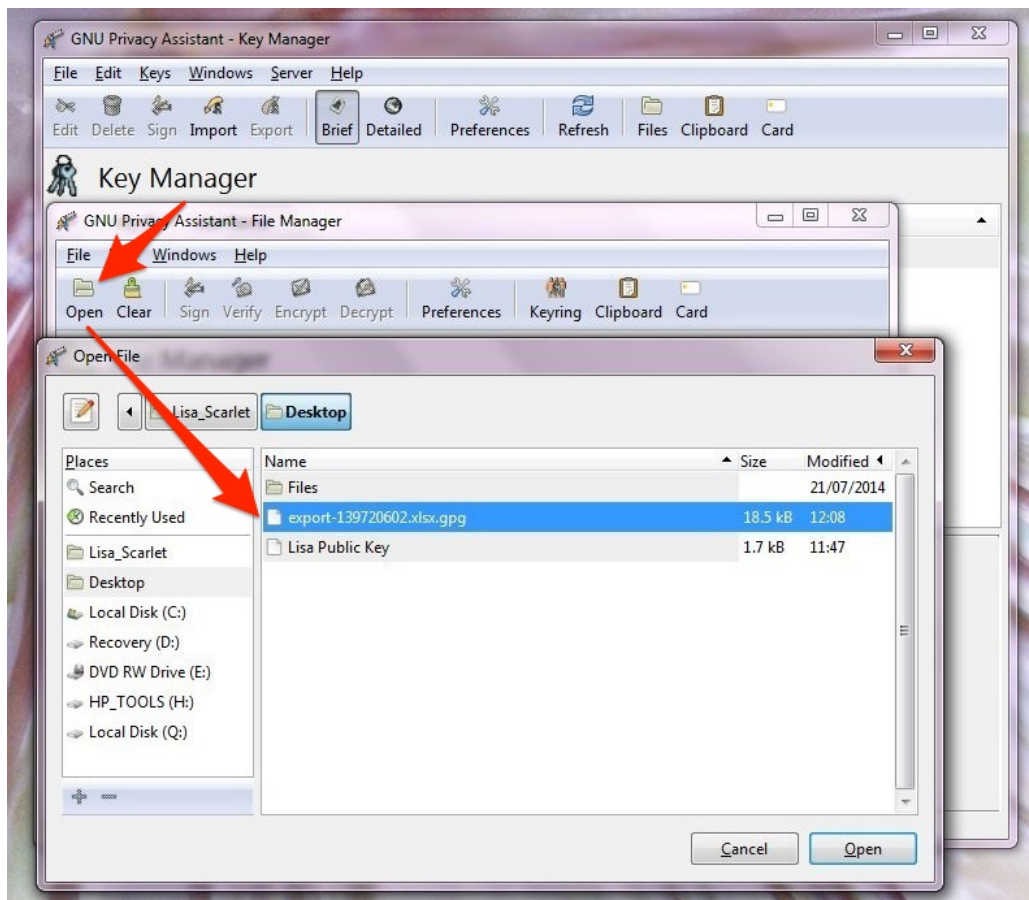
23. Send your key to Waysact securely via HTTPS interface – for example by uploading it to Basecamp. Please do not send via a plain text email.

Decrypting a file

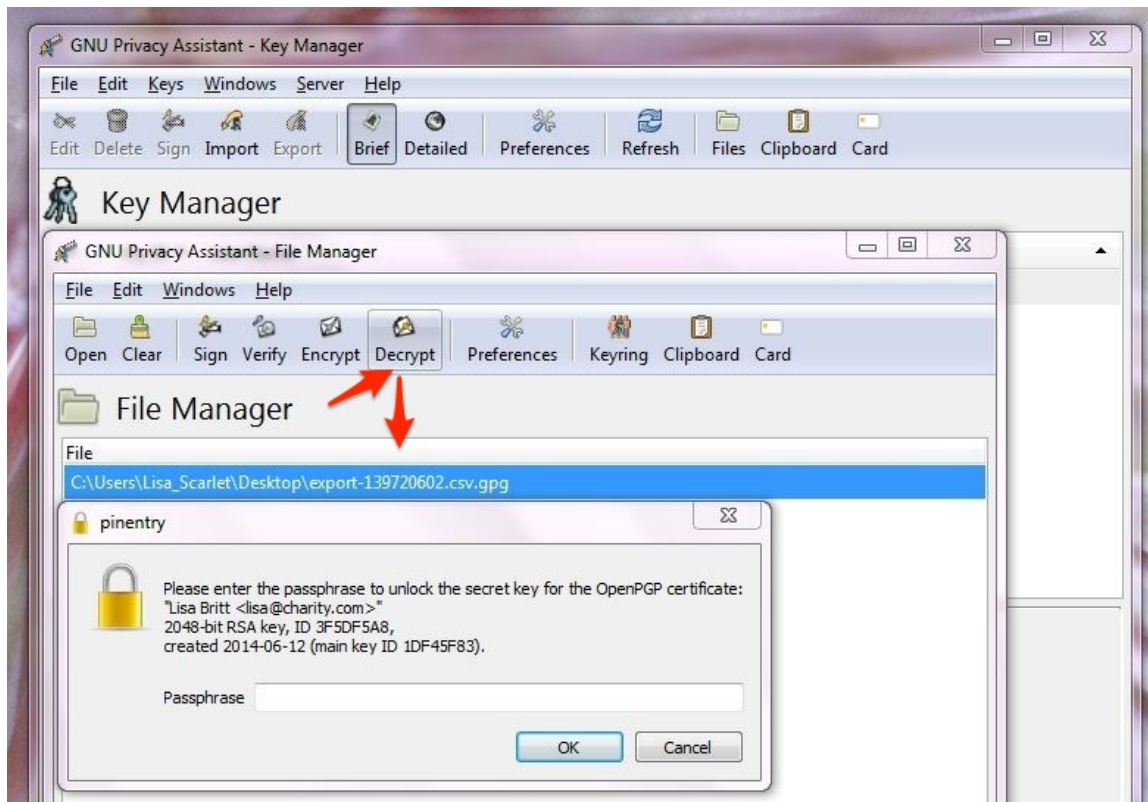
24. In GPA, click on *Files* to open the file manager.



25. Click *Open* to browse for the file you want to decrypt.



26. Select the file (it will end in .gpg) and click *Decrypt*. Enter your passphrase when prompted and click *OK*.



27. That's it! Your decrypted file will be in the same folder as the original file. You can now open the decrypted file.

