Using Open PGP Encryption

(using the gpg4win-2.3.3 installation)

(as of 020317 bkv)

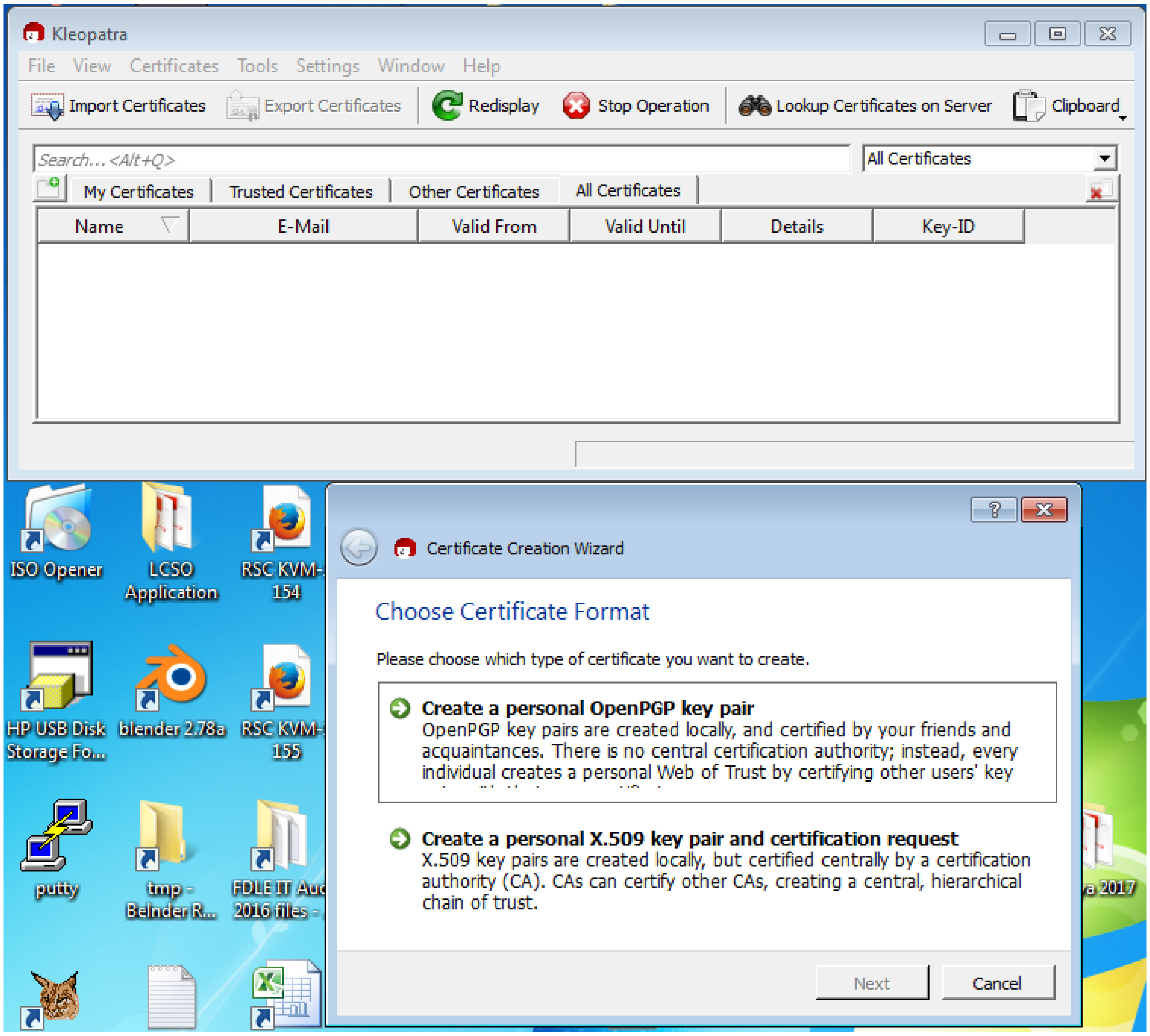
Overview

Upon installation of the software, you will need to 1) create a private certificate for yourself, and 2) export your public certificate so that others can communicate with you. To decrypt a file sent to you by someone else, you will need to have imported their public certificate. Then you can encrypt files (using their public key) and decrypt (using your private key).

Creating a Certificate

Click on File > New Certificate.

Choose “Create a personal OpenPGP key pair”.



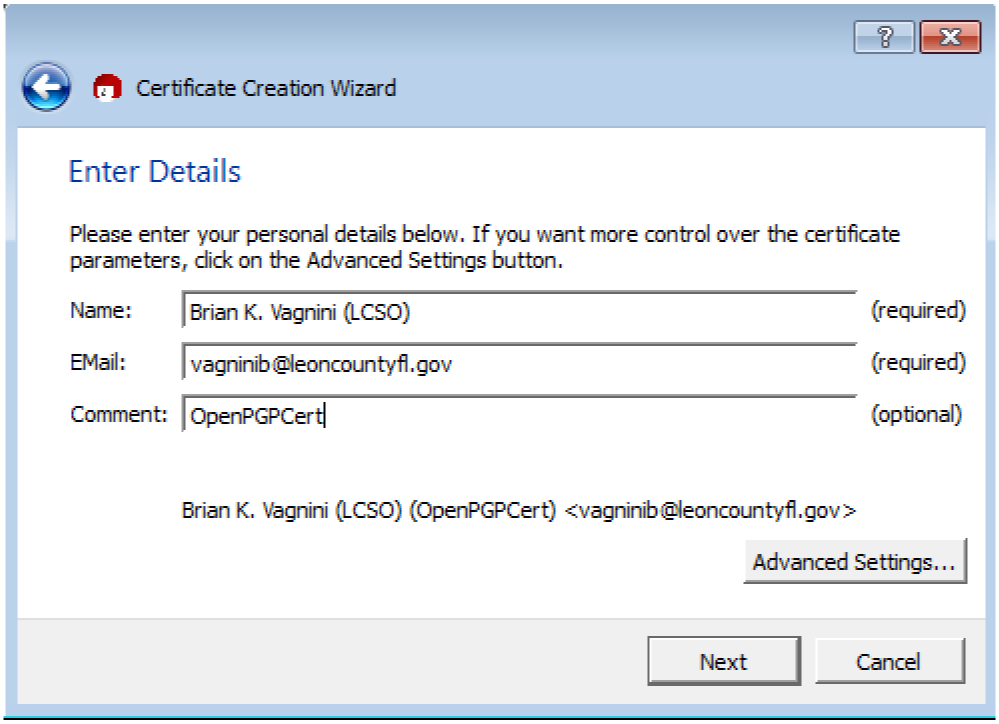
Choose Certificate Format

Please choose which type of certificate you want to create.

Create a personal OpenPGP key pair
OpenPGP key pairs are created locally, and certified by your friends and acquaintances. There is no central certification authority; instead, every individual creates a personal Web of Trust by certifying other users' key

Create a personal X.509 key pair and certification request
X.509 key pairs are created locally, but certified centrally by a certification authority (CA). CAs can certify other CAs, creating a central, hierarchical chain of trust.

Enter your details and click on “Next”.



Certificate Creation Wizard

Enter Details

Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button.

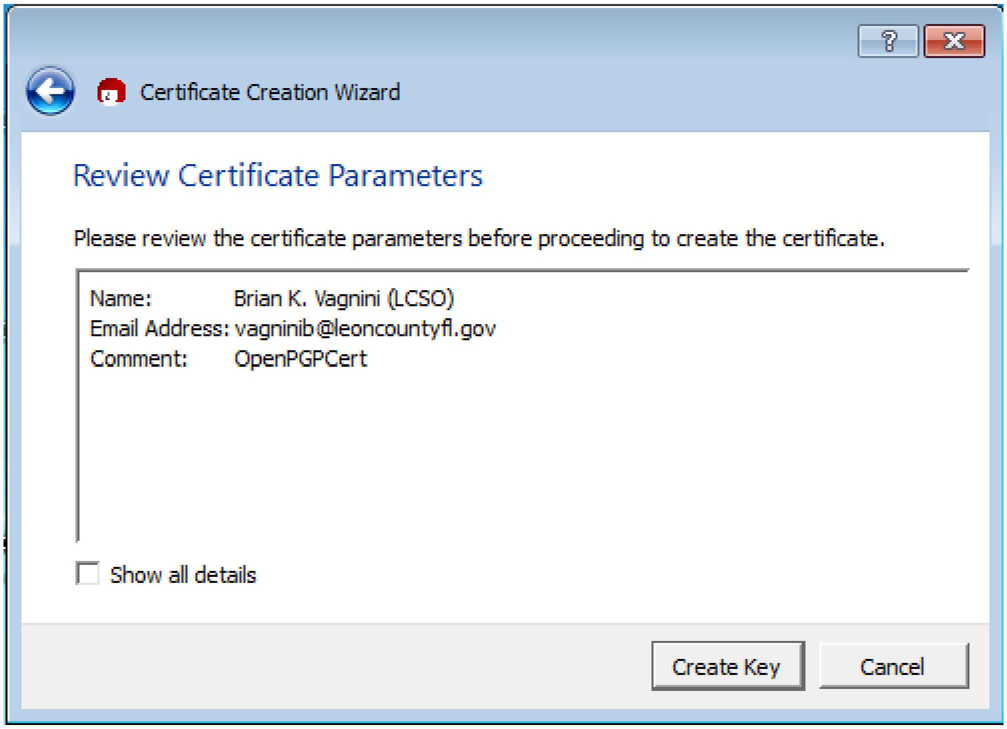
Name: Brian K. Vagnini (LCSO) (required)

EMail: vagninib@leoncountyfl.gov (required)

Comment: OpenPGPCert (optional)

Brian K. Vagnini (LCSO) (OpenPGPCert) <vagninib@leoncountyfl.gov>

Click on “Create Key”.



Certificate Creation Wizard

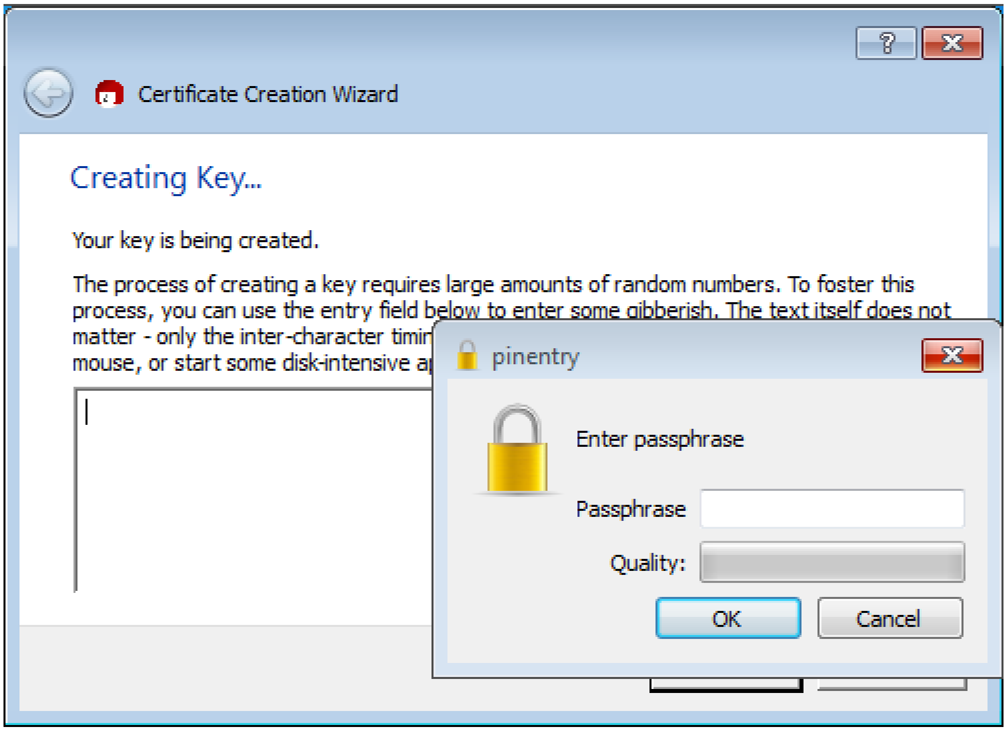
Review Certificate Parameters

Please review the certificate parameters before proceeding to create the certificate.

Name: Brian K. Vagnini (LCSO)
Email Address: vagninib@leoncountyfl.gov
Comment: OpenPGPCert

□ Show all details

Enter your passphrase. It will prompt you for it a second time once you click OK. The passphrase should be long enough to ensure security, yet short enough/memorable enough to be able to enter it each and every time you have to decrypt a file. Usual rules apply regarding UPPER case, lower case, numb3rs, and Spec!@l characters.



Certificate Creation Wizard

Creating Key...

Your key is being created.

The process of creating a key requires large amounts of random numbers. To foster this process, you can use the entry field below to enter some gibberish. The text itself does not matter - only the inter-character timin
mouse, or start some disk-intensive ap

pinentry

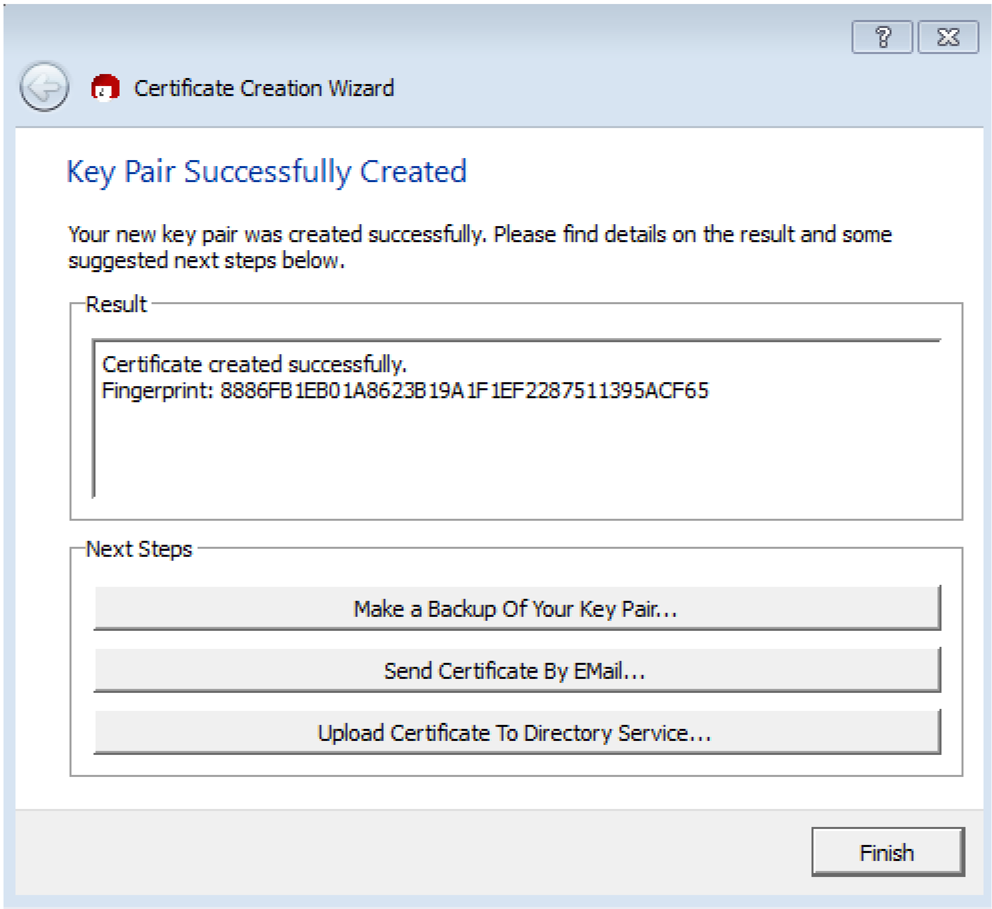
Enter passphrase

Passphrase

Quality:

Your key pairs are created (via the passphrase and moving your mouse around in a random pattern.)

Click on “Make a Backup of Your Key Pair”.


Certificate Creation Wizard

Key Pair Successfully Created

Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

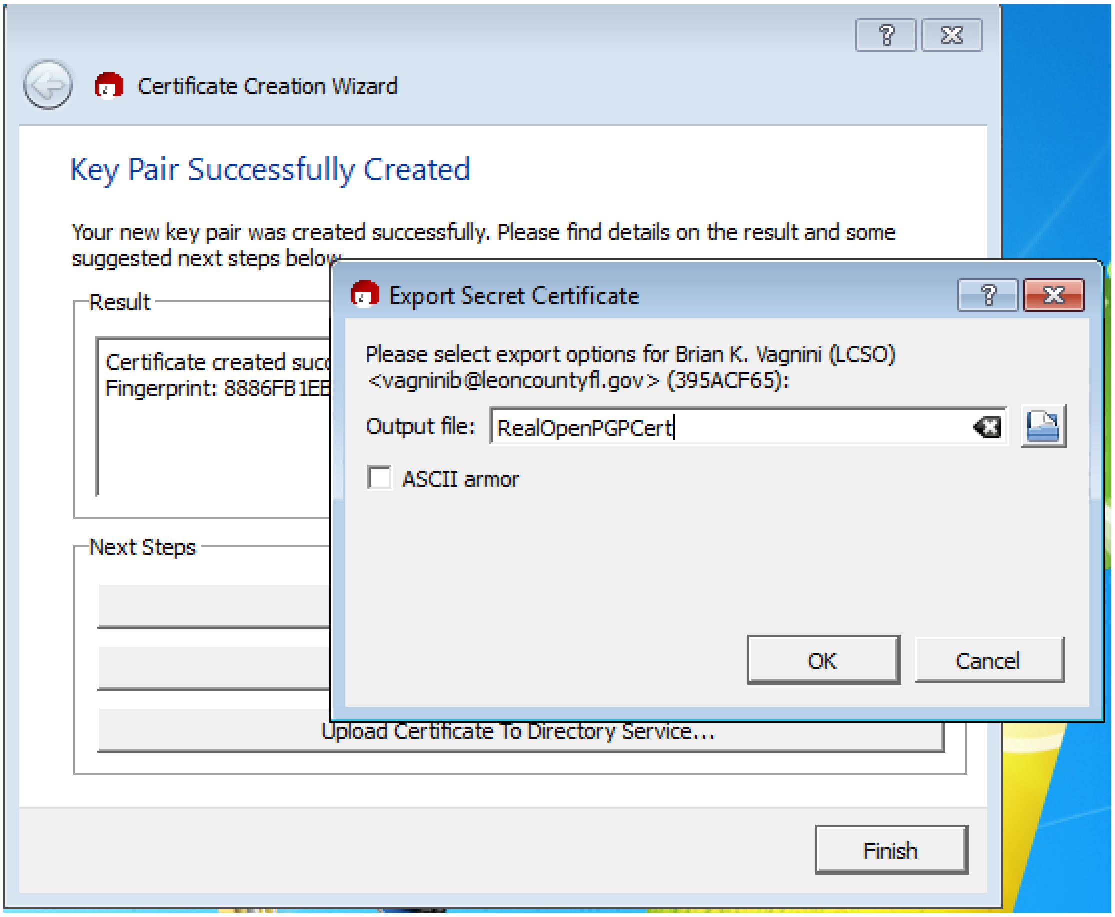
Result

Certificate created successfully.
Fingerprint: 8886FB1EB01A8623B19A1F1EF2287511395ACF65

Next Steps

Make a Backup Of Your Key Pair...
Send Certificate By EMail...
Upload Certificate To Directory Service...
Finish

(This needs some work…Couldn't find where this file lives. It should be ideally stored on removable media and then deleted from the computer, as it contains your Private Key.)



Certificate Creation Wizard

Key Pair Successfully Created

Your new key pair was created successfully. Please find details on the result and some suggested next steps below

Result

Certificate created succ
Fingerprint: 8886FB1EB

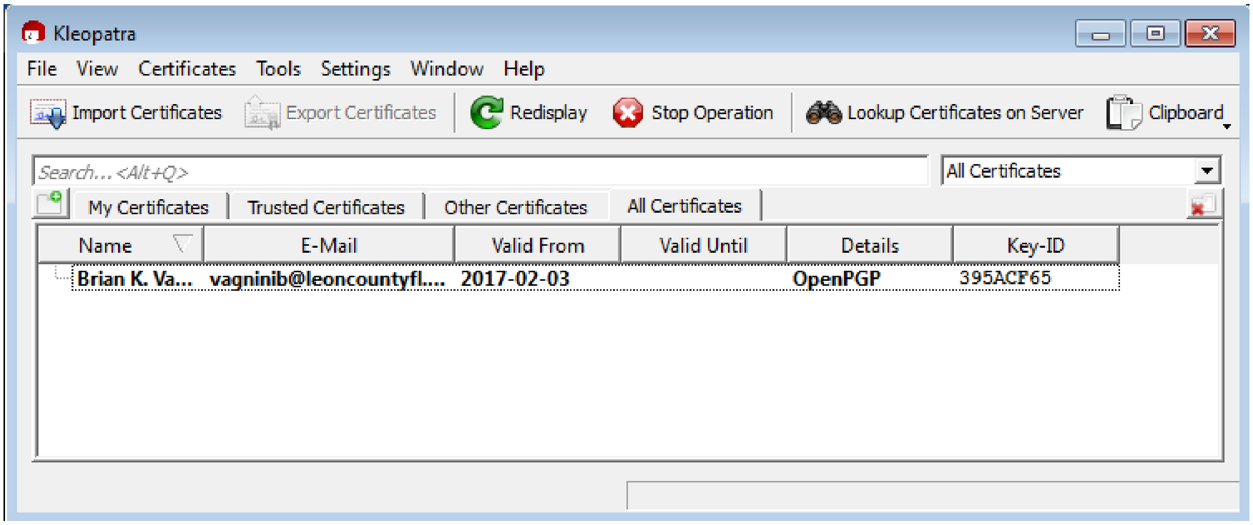
Export Secret Certificate

Please select export options for Brian K. Vagnini (LCSO) <vagninib@leoncountyfl.gov> (395ACF65):

Output file: RealOpenPGPCert

□ ASCII armor

The Kleopatra app (which manages your keys for you), now shows your new OpenPGP certificate.

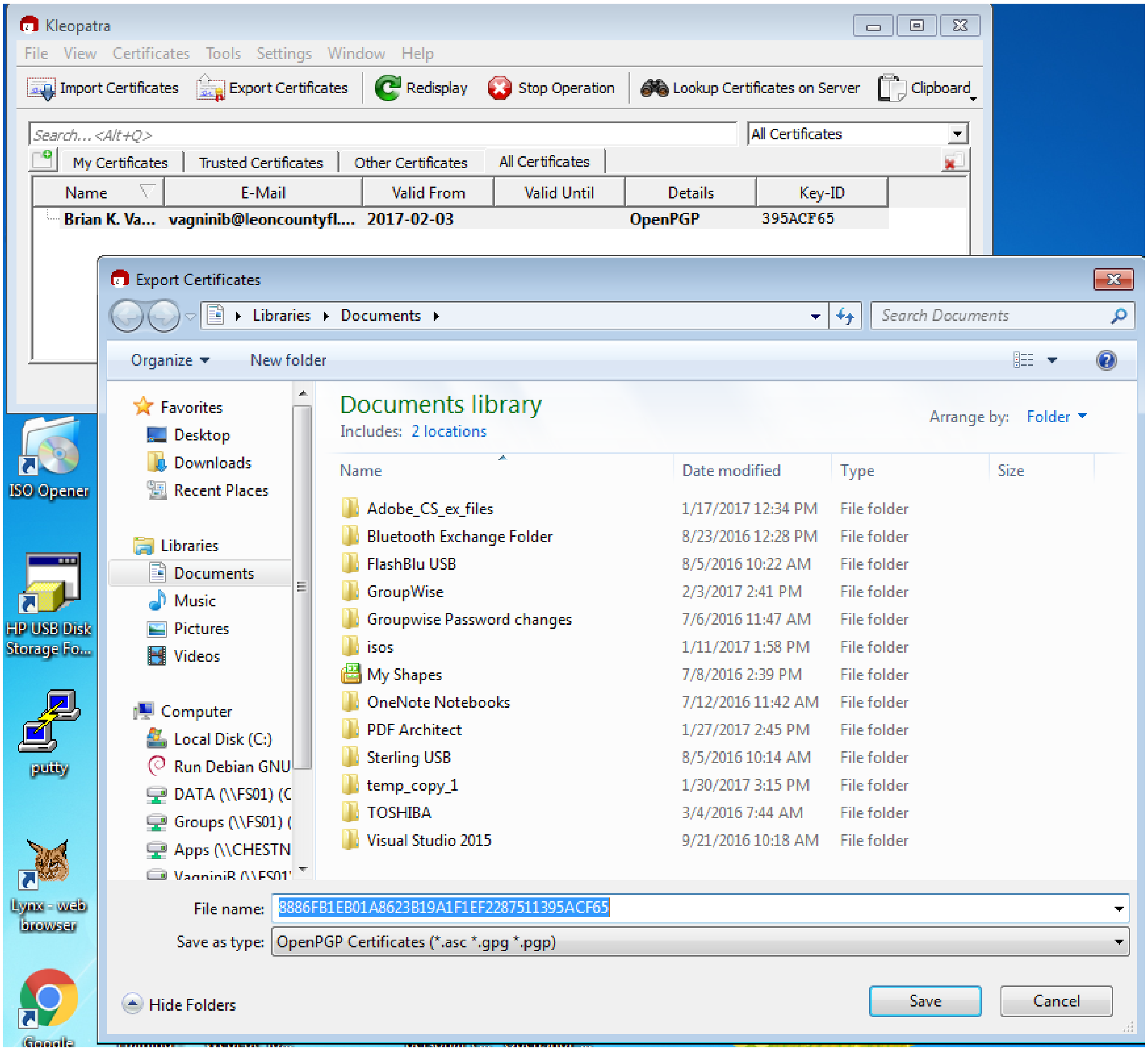


Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Brian K. Va...	vagninib@leoncountyfl....	2017-02-03		OpenPGP	395ACF65

Exporting Your Public Key

Next, you need to export your public key. This can be shared via e-mail, or a text file on a USB drive, or a file share.

Right Click on your Certificate in Kleopatra and choose “Export Certificates”. The name and location can be anything. My advice would be to name it something that you will recognize later, when you need to send your certificate to someone else down the road.



Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Brian K. Va...	vagninib@leoncountyfl....	2017-02-03		OpenPGP	395ACF65

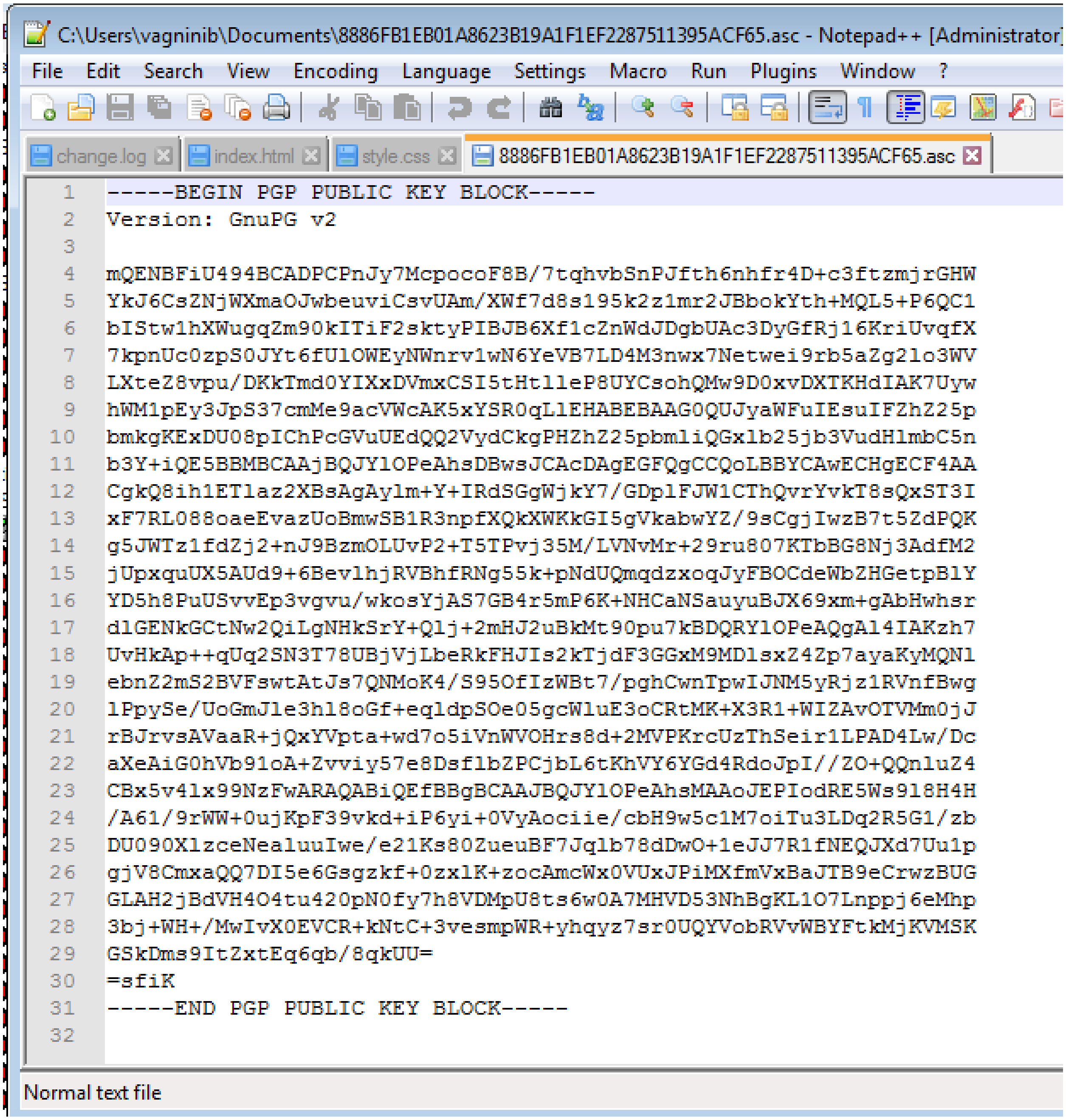
Name	Date modified	Type	Size
Adobe_CS_ex_files	1/17/2017 12:34 PM	File folder	
Bluetooth Exchange Folder	8/23/2016 12:28 PM	File folder	
FlashBlu USB	8/5/2016 10:22 AM	File folder	
GroupWise	2/3/2017 2:41 PM	File folder	
Groupwise Password changes	7/6/2016 11:47 AM	File folder	
isos	1/11/2017 1:58 PM	File folder	
My Shapes	7/8/2016 2:39 PM	File folder	
OneNote Notebooks	7/12/2016 11:42 AM	File folder	
PDF Architect	1/27/2017 2:45 PM	File folder	
Sterling USB	8/5/2016 10:14 AM	File folder	
temp_copy_1	1/30/2017 3:15 PM	File folder	
TOSHIBA	3/4/2016 7:44 AM	File folder	
Visual Studio 2015	9/21/2016 10:18 AM	File folder	

File name: 8886FB1EB01A8623B19A1F1EF2287511395ACF65

Save as type: OpenPGP Certificates (*.asc *.gpg *.pgp)

If you choose to email the public key to the person you wish to encrypt/decrypt files with, open your exported certificate in a text editor. It should look similar to the picture below. IMPORTANT!!

Copy and paste EVERY single part of the text, including the ---BEGIN PGP PUBLIC KEY BLOCK and ---END PGP PUBLIC KEY BLOCK.



C:\Users\vagninib\Documents\8886FB1EB01A8623B19A1F1EF2287511395ACF65.asc - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
change.log
index.html
style.css
8886FB1EB01A8623B19A1F1EF2287511395ACF65.asc

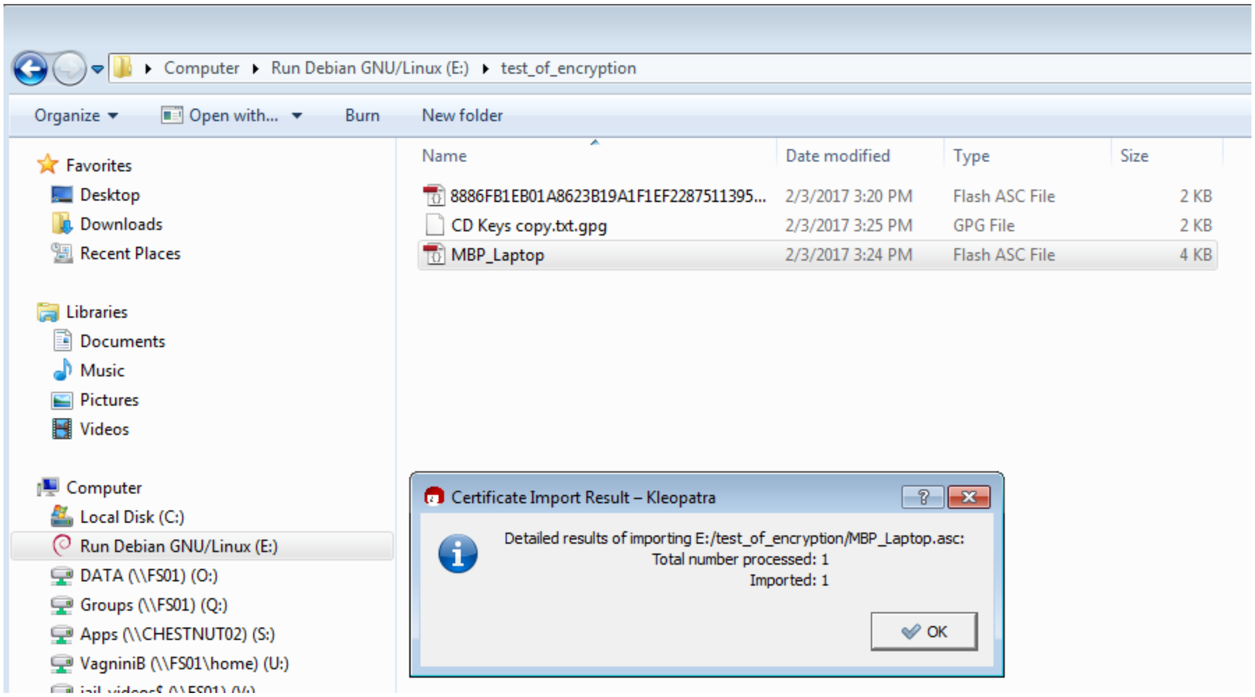
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFiU494BCADPCPnJy7McpocoF8B/7tqhvbSnPJfth6nhfr4D+c3ftzmjrGHW
YkJ6CsZNjWXmaOJwbeuviCsvUAm/XWf7d8s195k2z1mr2JBbokYth+MQL5+P6QC1
bIStw1hXWugqZm90kITiF2sktyPIBJB6Xf1cZnWdJDgbUAc3DyGfRj16KriUvqfX
7kpnUc0zpS0JYt6fU1OWEyNWnrv1wN6YeVB7LD4M3nwx7Netwei9rb5aZg2lo3WV
LXteZ8vpu/DKkTmd0YIXxDVmxCSI5tHtlleP8UYCsohQMw9D0xvDXTKHdIAK7Uyw
hWM1pEy3JpS37cmMe9acVWcAK5xYSR0qLlEHABEBAAG0QUJyaWFuIEsuIFZhZ25p
bmkgKExDU08pIChPcGVuUEdQQ2VydCkgPHZhZ25pbmliQGxlb25jb3VudHlmbC5n
b3Y+iQE5BBMBCAAjBQJY1OPeAhsDBwsJCAcDAgEGFQgCCQoLBBYCAwECHgECF4AA
CgkQ8ih1ETlaz2XBsAgAylm+Y+IRdSGgWjkY7/GDplFJW1CThQvrYvkT8sQxST3I
xF7RL088oaeEvazUoBmwSB1R3npfXQkXWKkGI5gVkabwYZ/9sCgjIwzB7t5ZdPQK
g5JWTz1fdZj2+nJ9BzmOLUvP2+T5TPvj35M/LVNvMr+29ru807KTbBG8Nj3AdfM2
jUpxquUX5AUd9+6Bevlhj RVBhfRNg55k+pNdUQmqdzxoqJyFBOCdeWbZHGetpBlY
YD5h8PuUSvvEp3vgvu/wkosYjAS7GB4r5mP6K+NHCaNSauyuBJX69xm+gAbHwhsr
dlGENkGCtNw2QiLgNHkSrY+Q1j+2mHJ2uBkMt90pu7kBDQRY1OPeAQgAl4IAKzh7
UvHkAp++qUq2SN3T78UBjVjLbeRkFHJIs2kTjdF3GGxM9MDlsxZ4Zp7ayaKyMQNl
ebnZ2mS2BVFswtAtJs7QNMoK4/S95OfIzWBt7/pghCwnTpwIJNM5yRjz1RVnfBwg
1PpySe/UoGmJle3hl8oGf+eqldpSOe05gcWluE3oCRtMK+X3R1+WIZAvOTVMm0jJ
rBJrvsAVaaR+jQxYVpta+wd7o5iVnWVOHrs8d+2MVPKrcUzThSeir1LPAD4Lw/Dc
aXeAiG0hVb91oA+Zvviy57e8DsflbZPCjbL6tKhVY6YGd4RdoJpI//ZO+QQnluZ4
CBx5v4lx99NzFwARAQABiQEfBBgBCAAJBQJY1OPeAhsMAAoJEPIodRE5Ws918H4H
/A61/9rWW+0ujKpF39vkd+iP6yi+0VyAociie/cbH9w5c1M7oiTu3LDq2R5G1/zb
DU090XlzceNealuuIwe/e21Ks80ZueuBF7Jqlb78dDwO+1eJJ7R1fNEQJXd7Uu1p
gjV8CmxaQQ7DI5e6Gsgzkf+0zxlK+zocAmcWx0VUxJPiMXfmVxBaJTB9eCrwzBUG
GLAH2jBdVH4O4tu420pN0fy7h8VDMpU8ts6w0A7MHVD53NhBgKL1O7Lnppj6eMhp
3bj+WH+/MwIvX0EVCR+kNtC+3vesmpWR+yhqyz7sr0UQYVobRVvWBYFtkMjKVMSK
GSkDms9ItZxtEq6qb/8qkUU=
=sfiK
-----END PGP PUBLIC KEY BLOCK-----
```

Importing a Public Key

The person at the other end will be doing the same steps (more or less), and thus, will send you THEIR public key to be imported.

To import a public key, right click the file and select “More GpgEx Options > Import Keys”. It should show the following:

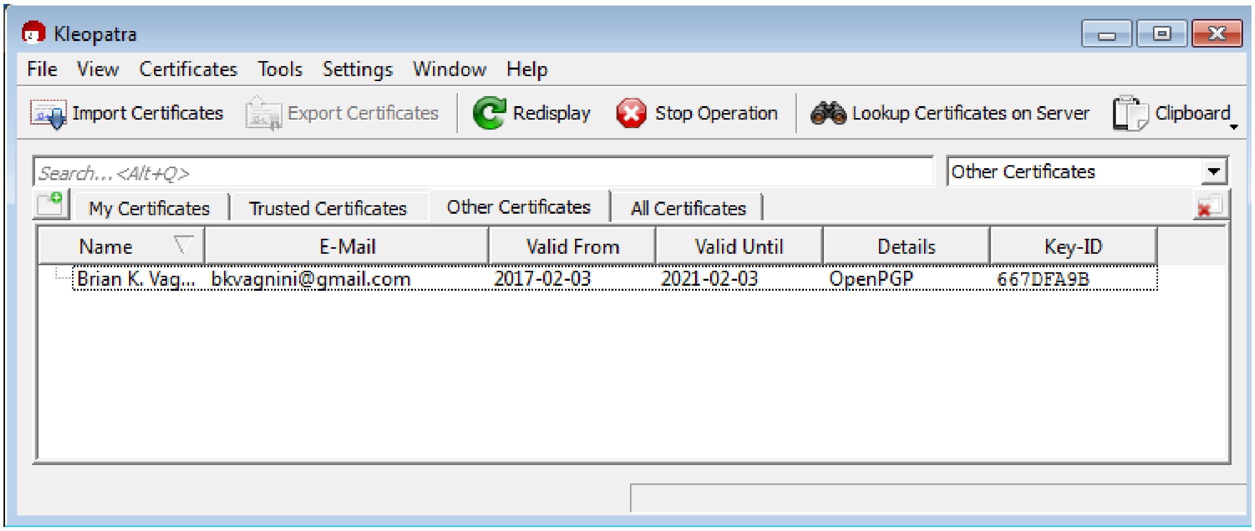


Name	Date modified	Type	Size
8886FB1EB01A8623B19A1F1EF2287511395...	2/3/2017 3:20 PM	Flash ASC File	2 KB
CD Keys copy.txt.gpg	2/3/2017 3:25 PM	GPG File	2 KB
MBP_Laptop	2/3/2017 3:24 PM	Flash ASC File	4 KB

Detailed results of importing E:/test_of_encryption/MBP_Laptop.asc:
Total number processed: 1
Imported: 1

If they emailed their public key, select all the text (in the key- see above re: exporting) and click on “Clipboard” > “Certificate Import”. (This might be a little wonky here.)

If you refresh your view of Kleopatra, it should show an entry under “Other Certificates”.



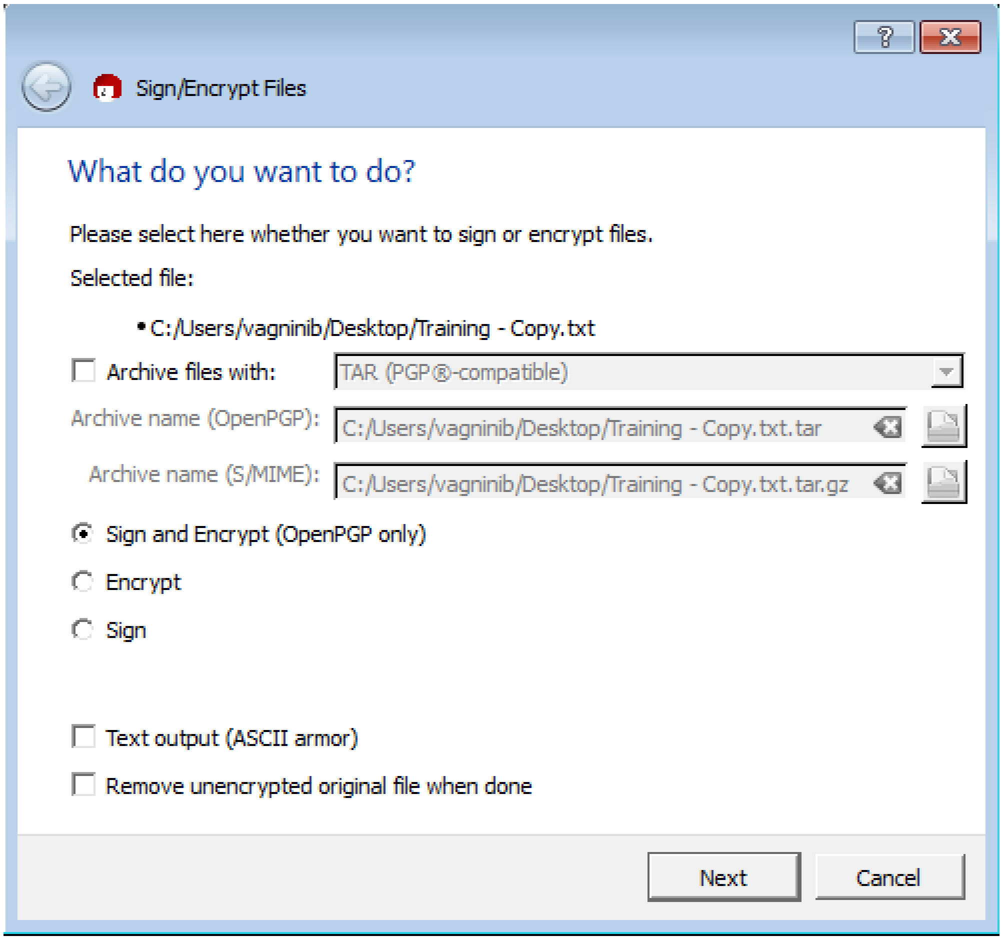
Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Brian K. Vag...	bkvagnini@gmail.com	2017-02-03	2021-02-03	OpenPGP	667DFA9B

YAY! Your initial setup/configuration is complete!

Usage of the OpenPGP system

Encrypting a file

Right Click on a COPY of the file that you want to encrypt and select “Sign and Encrypt”, then choose “Sign and Encrypt”. Click “Next”.



Sign/Encrypt Files

What do you want to do?

Please select here whether you want to sign or encrypt files.

Selected file:

- C:/Users/vagninib/Desktop/Training - Copy.txt

□ Archive files with: TAR (PGP®-compatible)

Archive name (OpenPGP): C:/Users/vagninib/Desktop/Training - Copy.txt.tar

Archive name (S/MIME): C:/Users/vagninib/Desktop/Training - Copy.txt.tar.gz

● Sign and Encrypt (OpenPGP only)

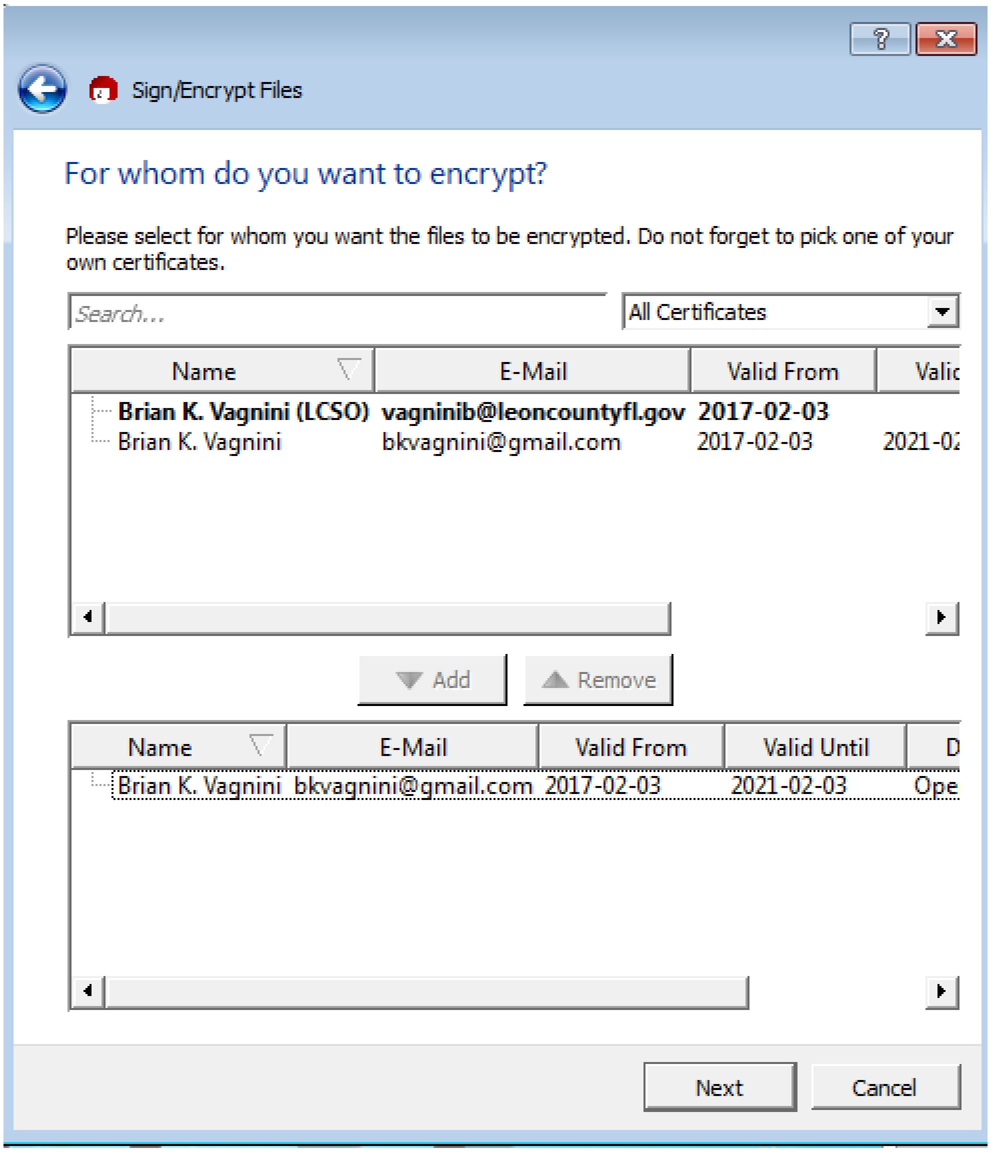
○ Encrypt

○ Sign

□ Text output (ASCII armor)

□ Remove unencrypted original file when done

Choose the recipient's Public Key. Click on "Add", then Next.



For whom do you want to encrypt?

Please select for whom you want the files to be encrypted. Do not forget to pick one of your own certificates.

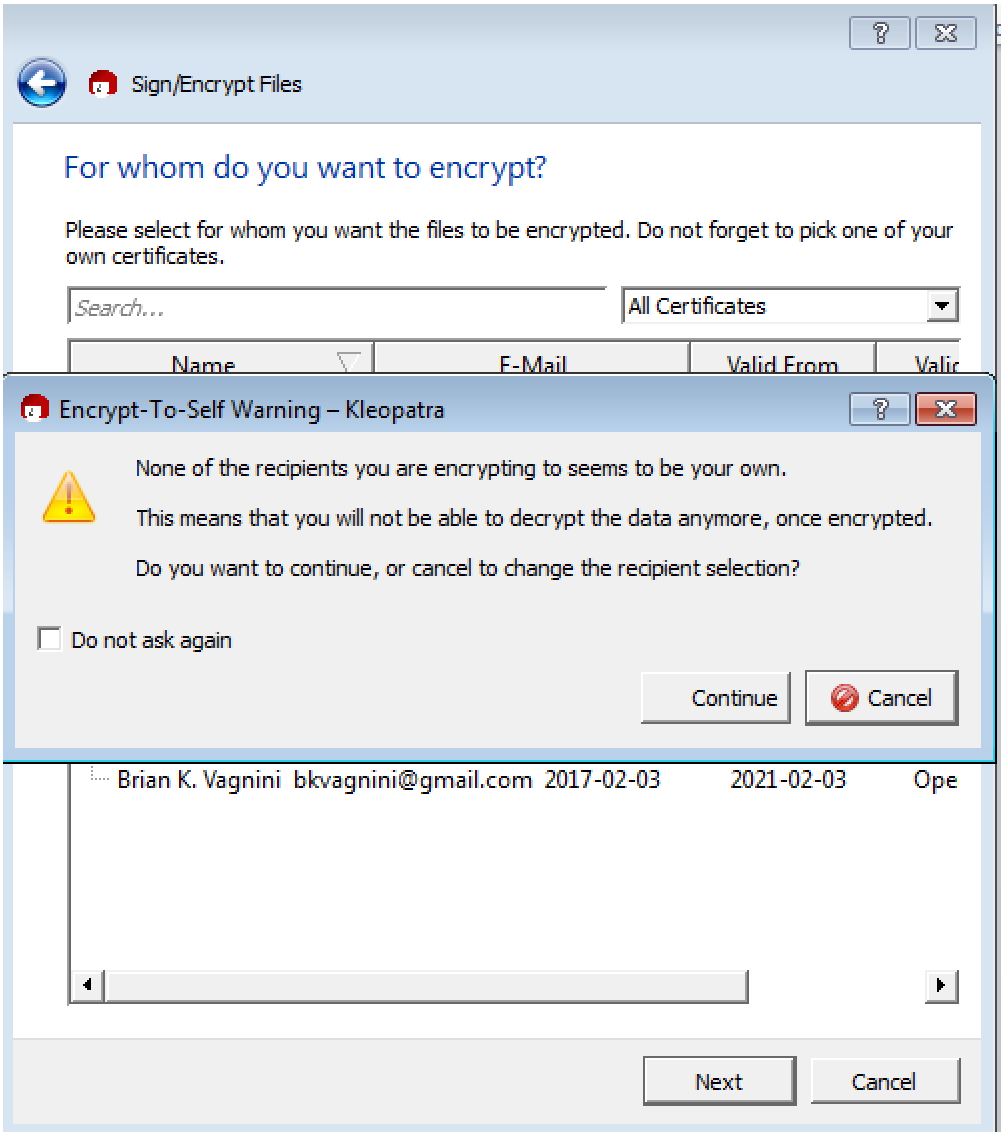
Search...

All Certificates

Name	E-Mail	Valid From	Valic
Brian K. Vagnini (LCSO)	**vagninib@leoncountyfl.gov**	**2017-02-03**	
Brian K. Vagnini	bkvagnini@gmail.com	2017-02-03	2021-0

Name	E-Mail	Valid From	Valid Until	D
Brian K. Vagnini	bkvagnini@gmail.com	2017-02-03	2021-02-03	Ope

It will throw a warning about not being able to decrypt this file. THIS IS WHY WE MADE A COPY FIRST.



For whom do you want to encrypt?

Please select for whom you want the files to be encrypted. Do not forget to pick one of your own certificates.

Encrypt-To-Self Warning – Kleopatra

None of the recipients you are encrypting to seems to be your own.

This means that you will not be able to decrypt the data anymore, once encrypted.

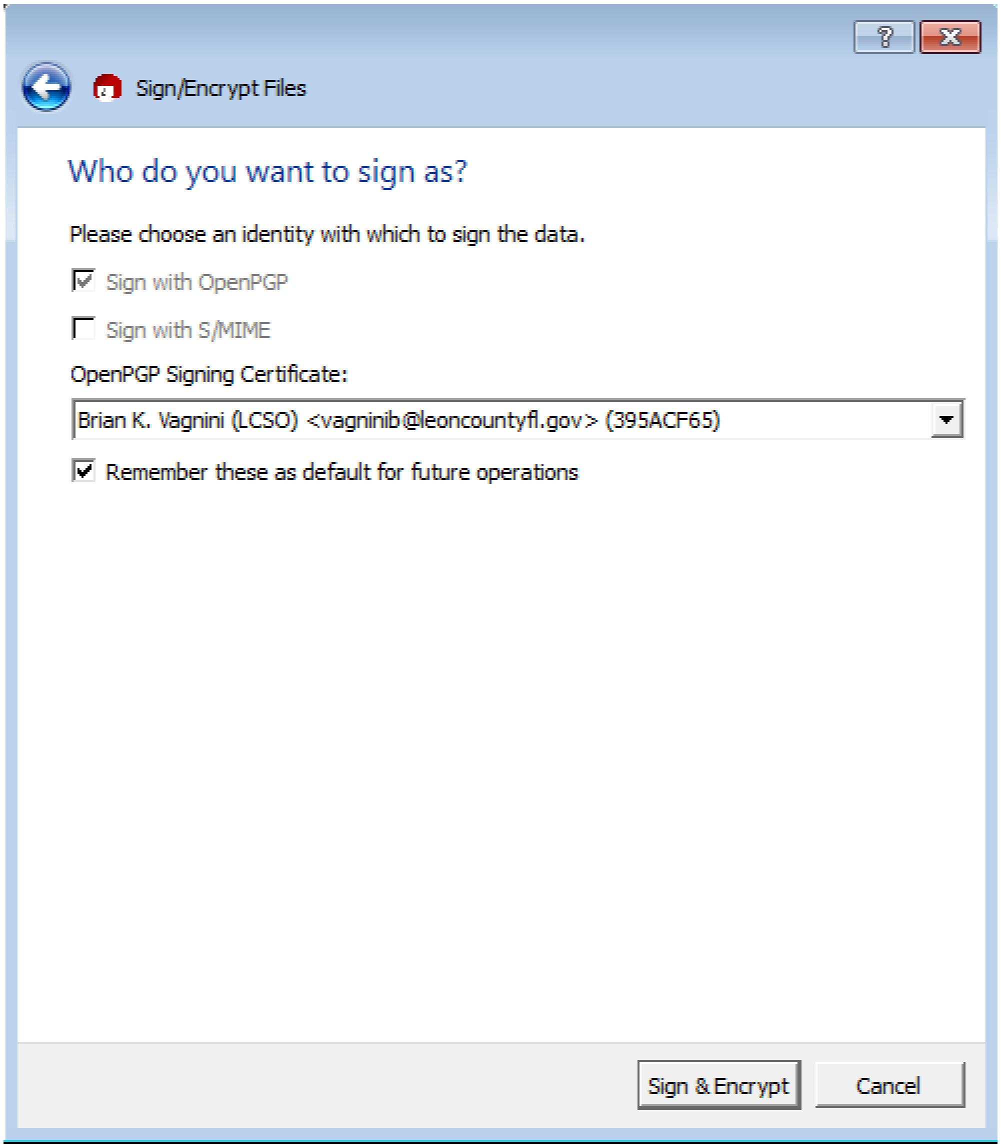
Do you want to continue, or cancel to change the recipient selection?

□ Do not ask again

Name	E-Mail	Valid From	Valic
Brian K. Vagnini	bkvagnini@gmail.com	2017-02-03	2021-02-03 Ope

Click on “Continue”.

Next, it will ask you to choose a signing certificate. Choose YOUR certificate.



Who do you want to sign as?

Please choose an identity with which to sign the data.

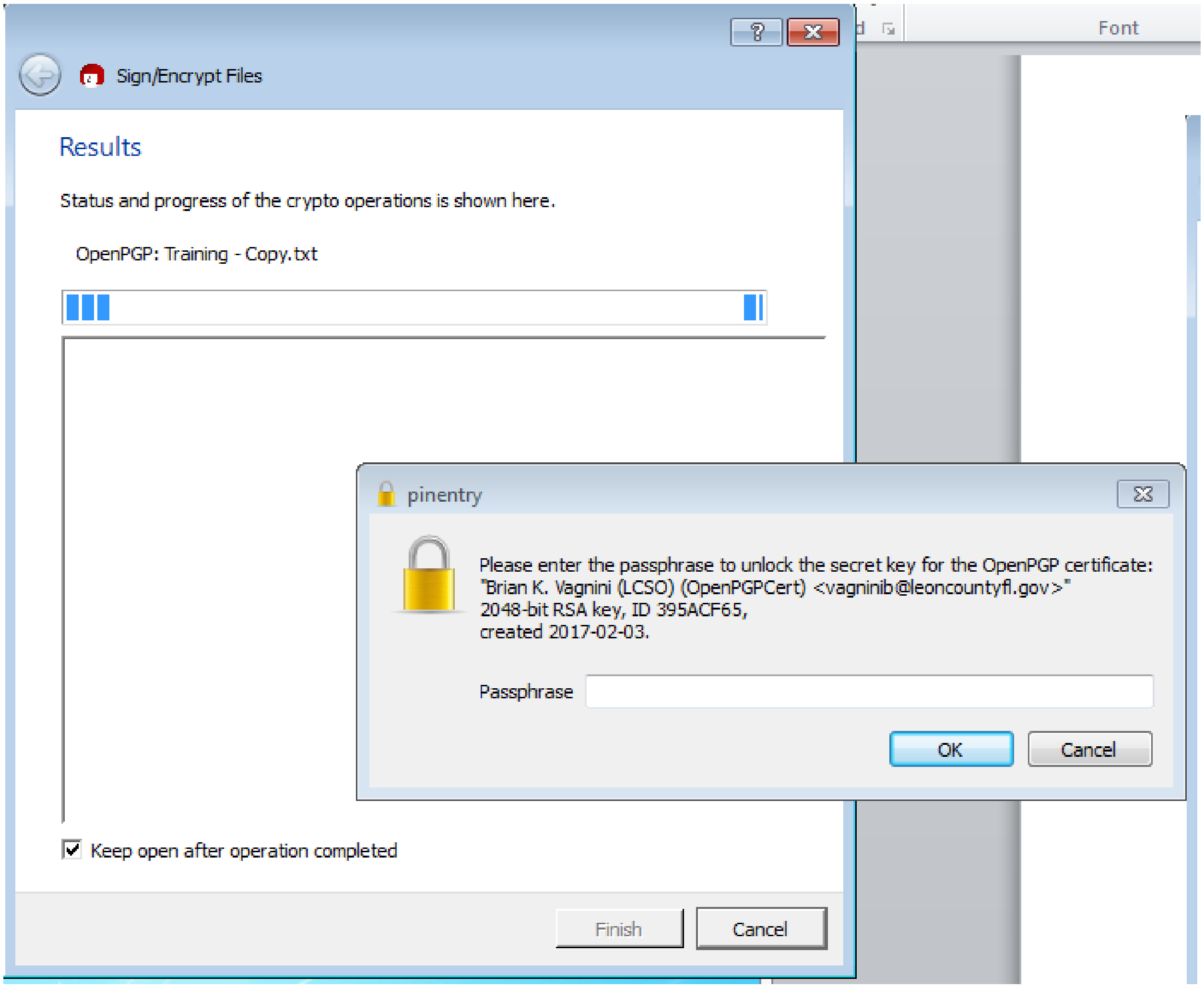
☑ Sign with OpenPGP

□ Sign with S/MIME

OpenPGP Signing Certificate: Brian K. Vagnini (LCSO) <vagninib@leoncountyfl.gov> (395ACF65)

☑ Remember these as default for future operations

Then it will prompt you for your Secret (Private) Key passphrase. This is why I said to keep it short enough that typing it wasn't an issue.



Sign/Encrypt Files

Results

Status and progress of the crypto operations is shown here.

OpenPGP: Training - Copy.txt

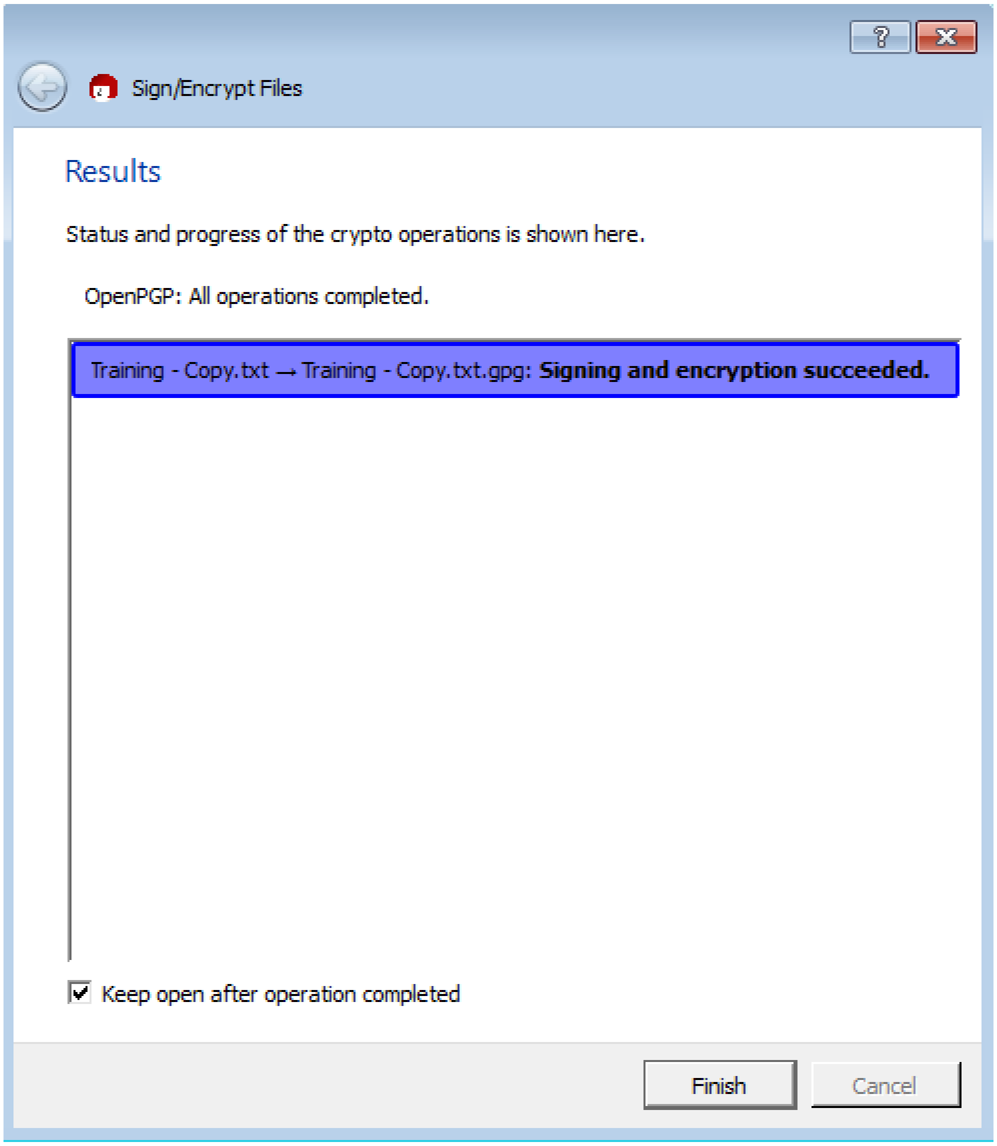
pinentry

Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"Brian K. Vagnini (LCSO) (OpenPGPCert) <vagninib@leoncountyfl.gov>"
2048-bit RSA key, ID 395ACF65,
created 2017-02-03.

Passphrase

☑ Keep open after operation completed

Encryption of your file is complete. Click on “Finish”.



Results

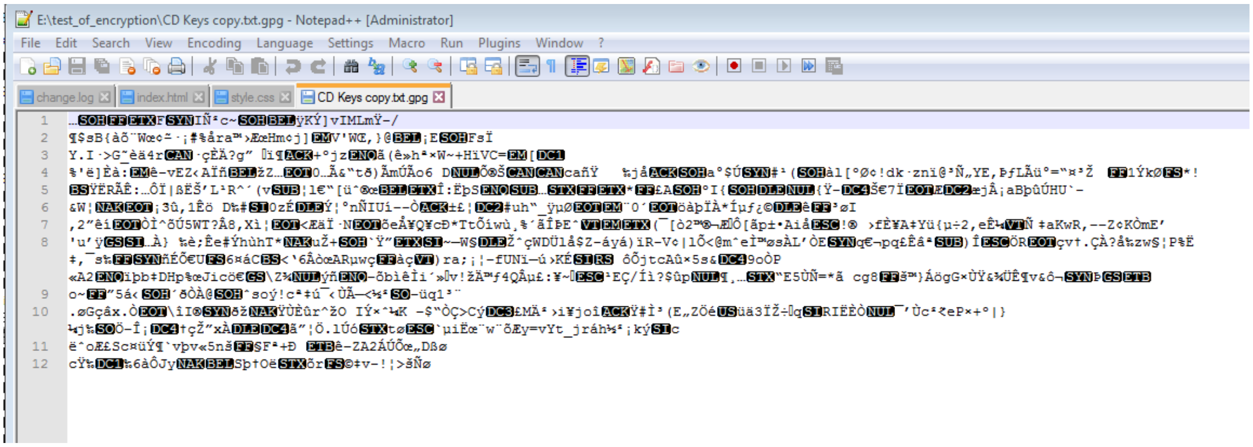
Status and progress of the crypto operations is shown here.

OpenPGP: All operations completed.

Training - Copy.txt → Training - Copy.txt.gpg: **Signing and encryption succeeded.**

☑ Keep open after operation completed

The encrypted file will look this once it’s down (without decryption, that is…”

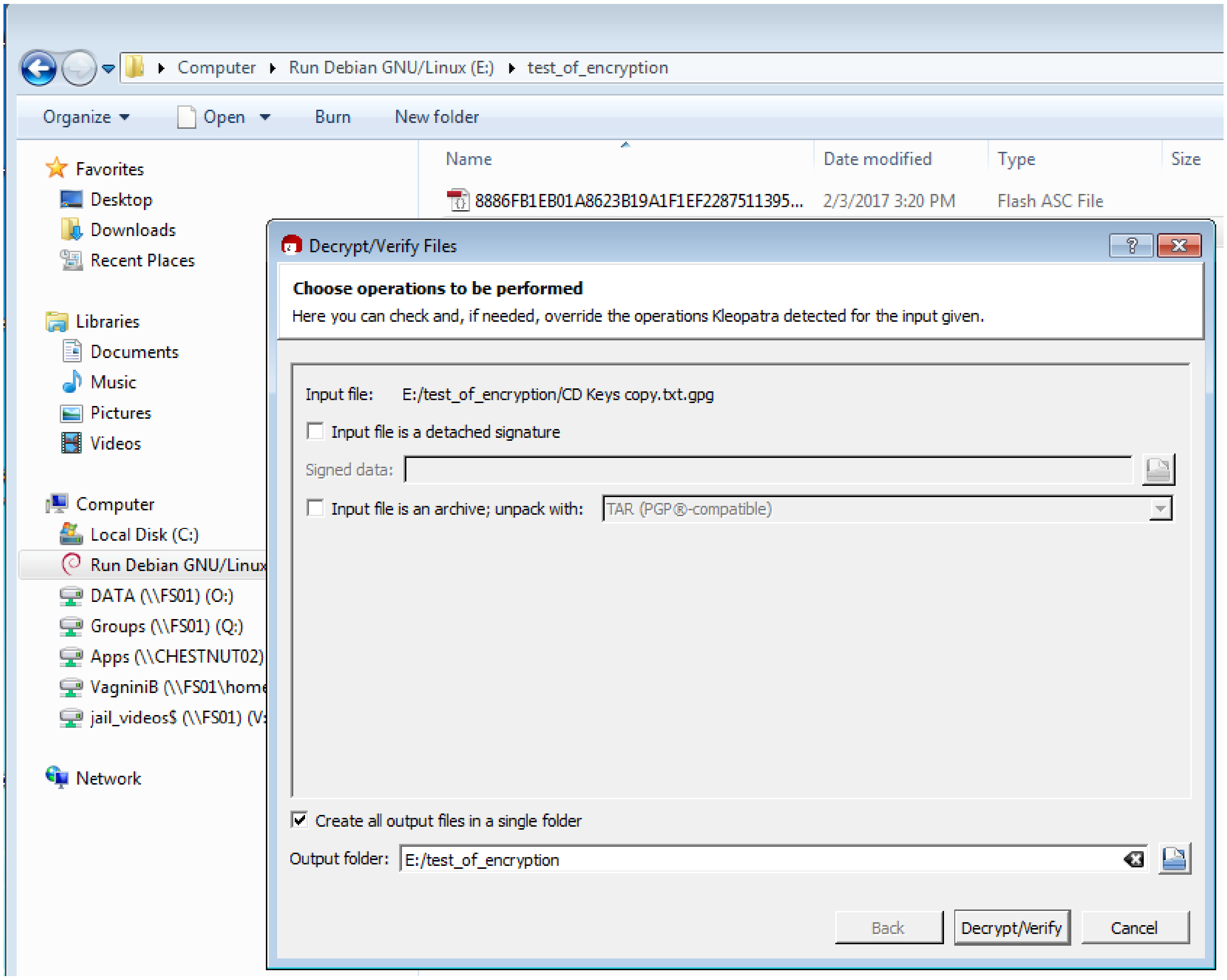

E:\test_of_encryption\CD Keys copy.txt.gpg - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
change.log
index.html
style.css
CD Keys copy.txt.gpg

```
…SOHFFETXFSYNIÑªc~SOHBELÿKÝ]vIMLmŸ-/
¶$sB{àõ¨Wœ¢¯·¡#%åra™›ÆœHm¢j]EMV'WŒ,}@BEL;ESOHFsÏ
Y.I·>G˜èä4rCAN·çÈÄ?g” ▯ï¶ACK+°jzENQã(ê»hª×W~+HïVC=EM[DC1
%'ë]Èà:EMê-vEZ‹AÏñBELžZ…EOT0…Ã&“tð)ÃmÚÃo6 DNULÕ®ŠCANCANcañŸ   ‰jåACKSOHa°$ÚSYN#¹(SOHàl[°Ø¢!dk·znï@³Ñ„YE,ÞƒLÃü°=“¤³Ž  FF1ÝkØFS*!
BSŸËRÃÊ:…ÔÏ|ßËŠ’L¹R^´(vSUB¦1€“[ü^®œBELETXÎ:ËþSENQSUB…STXFFETX*FF£ASOH°I{SOHDLENUL{Ÿ-DC4Š€7ÏEOTÆDC2æjÂ¡aBþûÚHU`-
&W¦NAKEOT¡3û,1Êö D‰#SI0zÉDLEÝ¦°nÑIUí--ÒACK±£¦DC2#uh�``_ÿµØEOTEM¨0´EOTöàþÏÀ*Íµf¿©DLEêFF³øI
,2”êiEOTÒÌ^õÚ5WT?Â8,Xì¦EOT<ÆäÏ·NEOTõeÅ¥Q¥cÐ*TtÕíwù,%´ãÎÞE^VTEMETX(¯[ò2™®¬Æ▯Ô[ãp±•AiåESC!® ›fÈ¥A‡Yü{µ÷2,eÊ¼VTÑ ‡aKwR,--Z¢KÒmE’
'u’ÿGSSI…À} ‰è;Êe#ÝhùhT*NAKuŽ+SOH`Ÿ”ETXSI~—W§DLEŽ^çWDÜ1å$Z-áyá)ïR-V¢|1Õ<@m^eÌ™øsÀL’ÒESYNq€¬pq£Êâª SUB)ÎESCÖREOTçv†.ÇÀ?å‰zw§¦P%Ë
‡,¯s‰FFSYNñÉÕ€UFS6¤áCBS<‘6ÂòœARµwçFFàçVT)ra;¡¦-fUNï—ú›KÉSIRS ôÕjtcAû×5s&DC49oÒP
«A2ENQïþb‡DHp‰œJicö€GS\Z¾NULýñENQ-õbìêÌì´»▯v!žÄ™ƒ4QÂµ£:¥~▯ESC¹EÇ/Íì?$ûpNUL¶,…STX“E5ÙÑ=*ã cg8FFš™}ÁögG×ÙŸ&¾ÜÊ¶v&ô¬SYNÞGSETB
o~FF”5á‹SOH´ðÒÀ@SOH^soý!cª‡ú¯‹ÙÃ—<½ªSO-üq1³¨
.øGçâx.ÒEOT\îI®SYNðžNAKŸÙÈûr^žO IÝ×^¼K -$“ÒÇ>CýDC3£MÄª›i¥joîACKŸ#Ì³(E„ZÖéUSüä3ÏŽ÷▯qSIRIËÈÒNUL¯’Ùcª₹eP×+°|}
¼j‰SOÖ-Î¡DC4†çŽ”xÀDLEDC4ã”¦Ö.1ÚóSTXtøESC`µiËœ¨w¨õÆy=vYt_jráh½ª¡kýSIc
ë^oÆ£Sc¤üÝ¶`vþv«5nšFF§FªÐ ETBê-ZA2ÁÚÕœ„Dßø
cŸ‰DC1‰6àÔJyNAKBELSþ†OëSTXõrFS©‡v-!¦>šÑø
```

Decrypting a file

Once you retrieve your encrypted files from the other person, you will need to decrypt them. They will have used YOUR Public key to encrypt, and you will use your PRIVATE key to decrypt.

Right Click the file to decrypt. Choose “Decrypt and Verify”. It will show the following choices below. Change the output folder (if desired) and click “Decrypt/Verify”.



Choose operations to be performed

Here you can check and, if needed, override the operations Kleopatra detected for the input given.

Input file: E:/test_of_encryption/CD Keys copy.txt.gpg

☐ Input file is a detached signature

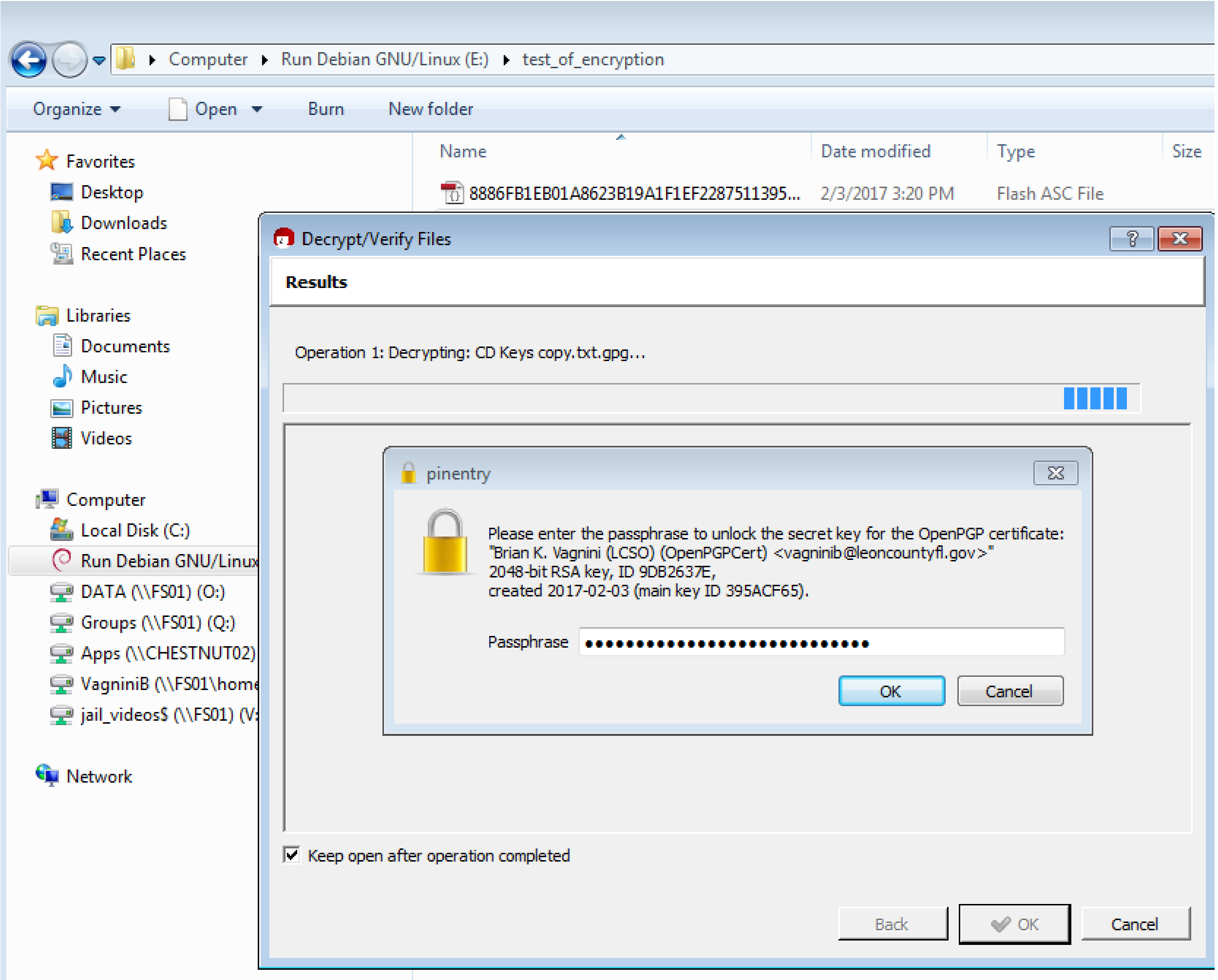
Signed data:

☐ Input file is an archive; unpack with: TAR (PGP®-compatible)

☑ Create all output files in a single folder

Output folder: E:/test_of_encryption

Then it will prompt you for your Secret (Private) Key passphrase. This is why I said to keep it short enough that typing it wasn't an issue.



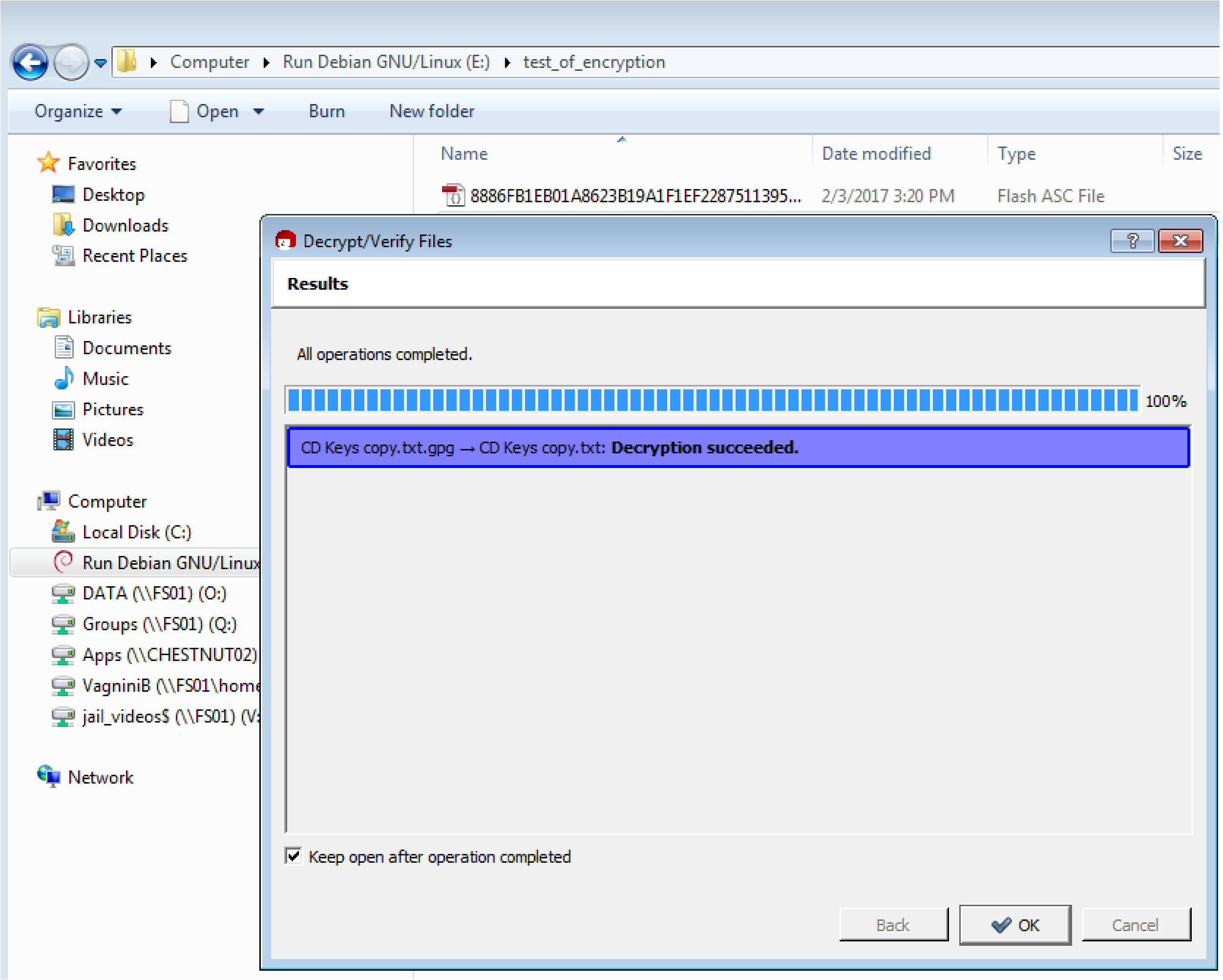
Name	Date modified	Type	Size
8886FB1EB01A8623B19A1F1EF2287511395...	2/3/2017 3:20 PM	Flash ASC File	

Operation 1: Decrypting: CD Keys copy.txt.gpg...

Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"Brian K. Vagnini (LCSO) (OpenPGPCert) <vagninib@leoncountyfl.gov>"
2048-bit RSA key, ID 9DB2637E,
created 2017-02-03 (main key ID 395ACF65).

Passphrase •••••••••••••••••••••••••••••

☑ Keep open after operation completed



Name	Date modified	Type	Size
8886FB1EB01A8623B19A1F1EF2287511395...	2/3/2017 3:20 PM	Flash ASC File	

Decrypt/Verify Files

Results

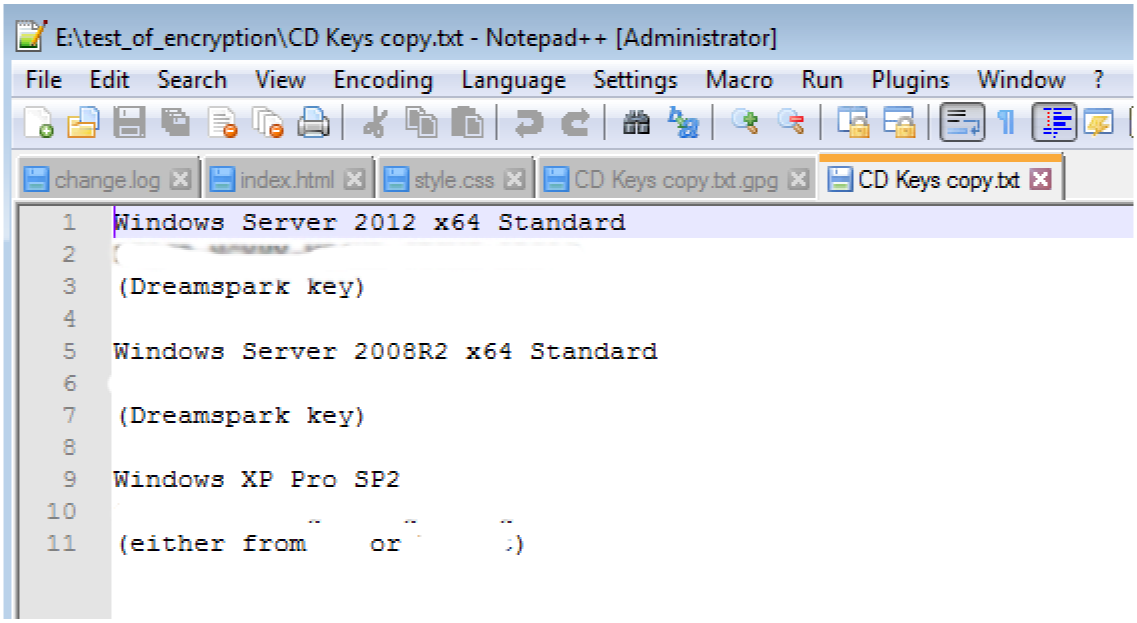
All operations completed.

100%

CD Keys copy.txt.gpg → CD Keys copy.txt: **Decryption succeeded.**

☑ Keep open after operation completed

This is what your decrypted file looks like. (Actual CD Keys removed for security reasons. You get the idea…)


E:\test_of_encryption\CD Keys copy.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
change.log
index.html
style.css
CD Keys copy.txt.gpg
CD Keys copy.txt

```
Windows Server 2012 x64 Standard

(Dreamspark key)

Windows Server 2008R2 x64 Standard

(Dreamspark key)

Windows XP Pro SP2

(either from    or        )
```