1. Introduction

1.2. PGP is a tool for keeping your data safe. It encrypts (scrambles) your data so that if an unauthorized person obtains the file, they are unable to read the information. Only you and Equifax will have access to the decrypted (unscrambled) information. Equifax uses what is called public-key cryptography. Public-key Cryptography uses a key pair for encrypting and decrypting. You will learn to create and apply a public key and a private key. The public key is for encryption, the private key is for decryption.

1.3. To receive encrypted files, you will need to provide a PGP Public key to Equifax. The purpose of this guide is to provide a pathway to empower you on obtaining and implementing the PGP protocol.

1.4. The screenshots are from a computer that has Windows 10 for an operating system and the use of GnuPG software.

1.5. Overview – How It Works
1.5.1. Files Equifax Send – You need to provide a PGP key to the Equifax.
1.5.2. Files Equifax Received – Equifax provides their PGP key to you.

1.6. 1.2. PGP Encryption Specifics:
1.6.1. It's recommended on all Equifax transmission solutions.
1.6.2. PGP key minimum key length is 2048.
1.6.3. Acceptable incoming file name extensions are: *.pgp; *.gpg; and *.asc.
1.6.4. Encrypted files should not contain multiple files.
1.6.5. Encrypted files should not be otherwise compressed

IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

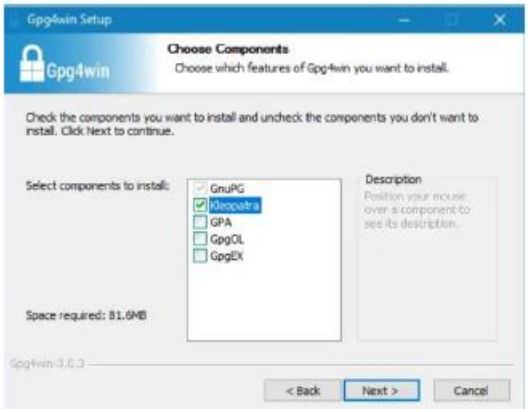
2. Installation

2.1. Download GPG4WIN from https://www.gpg4win.org/download.html , then run the install.

2.2. Once you run the install file, you will see this screen:

Select your language then click OK.

2.3. When you see the screen shown below, check the 'Kleopatra' box. You can uncheck the other boxes if you wish.



Click Next> then click Install.

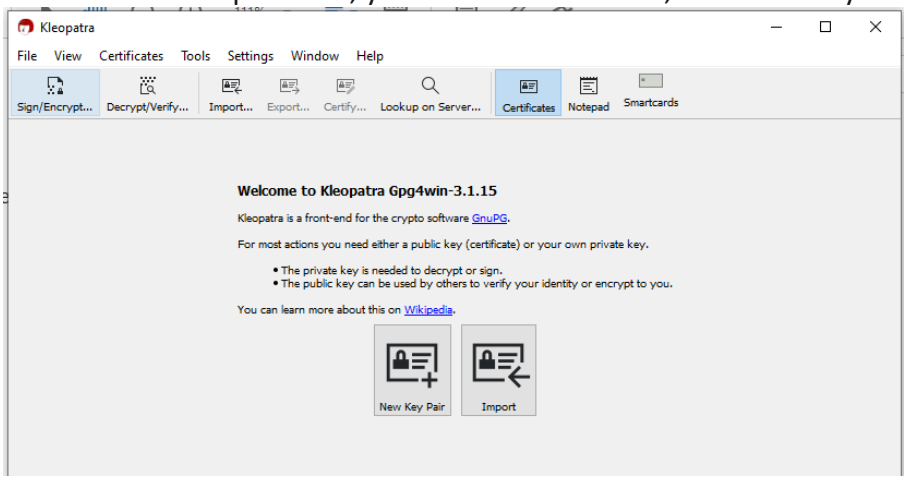
2.4. Once setup is done, check the 'Run Kleopatra' box.

Click Finish.

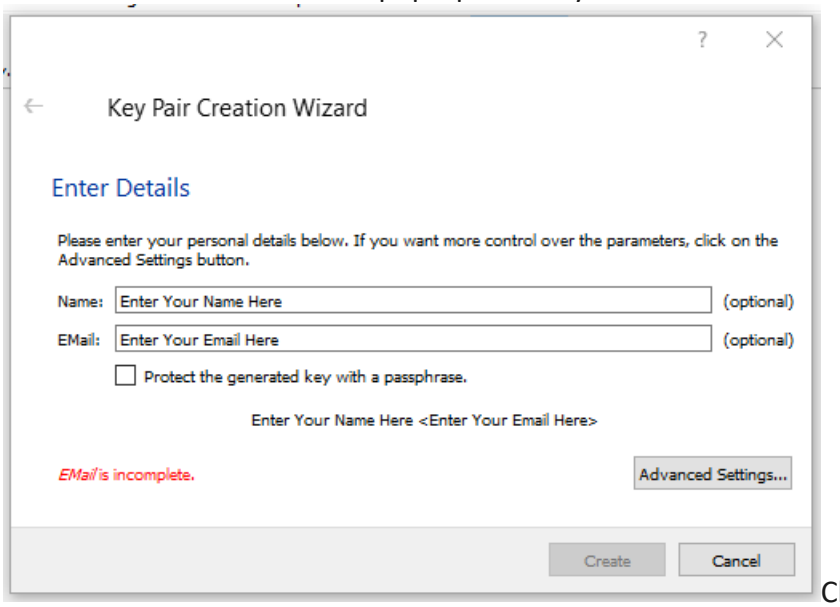
IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

3. Generating Your PGP Key Pair

3.1. Once the setup is done, you will see this screen, click New Key Pair.



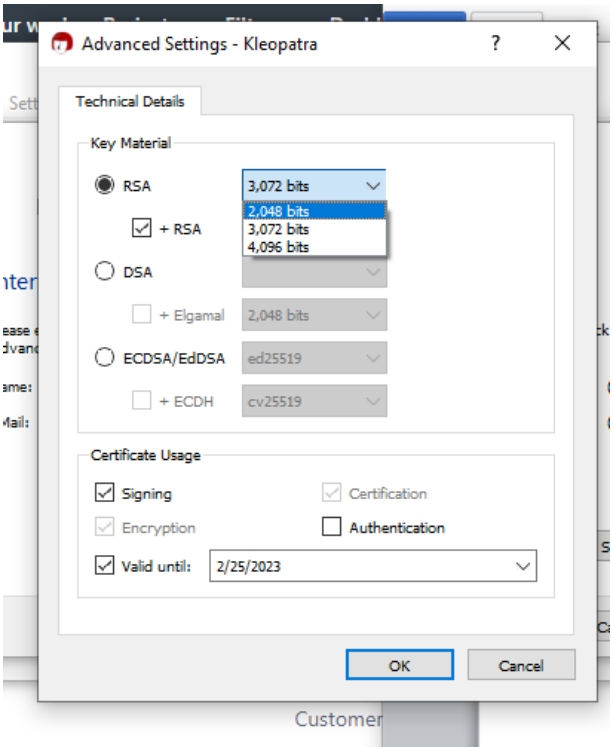
3.2. Screen shown below will pop-up. Enter your name and email.



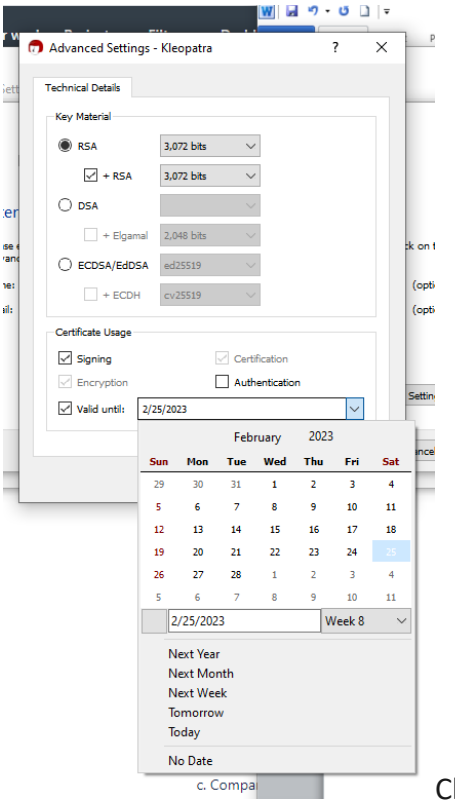
Click Advanced Settings.

3.3. Select 2048 bit under RSA

IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

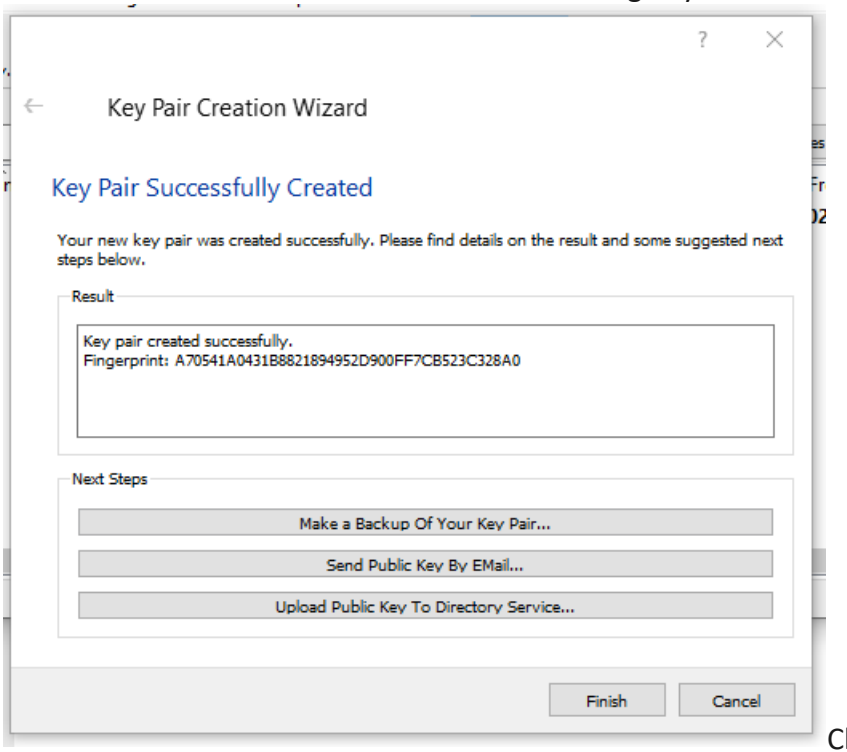


3.4. Change the Valid Until date to ensure it aligns with your company's internal policies.



Click Ok then click Create.

3.5. You should receive the below screen showing Key Pair Successfully Created.

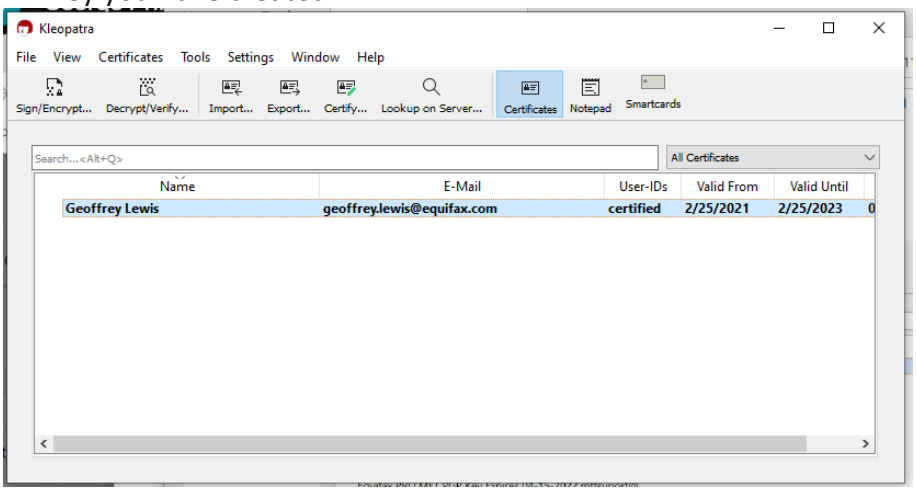


Click Finish.

IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

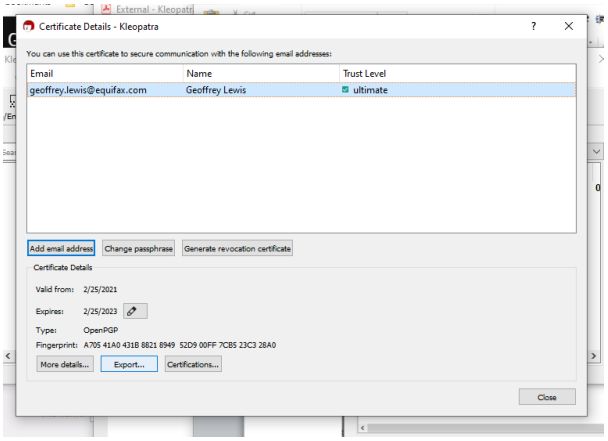
4. Locating and exporting Public Key.

4.1. Once you finish creation of keys, you will see this screen with an entry name of the key you have created.



Double click it.

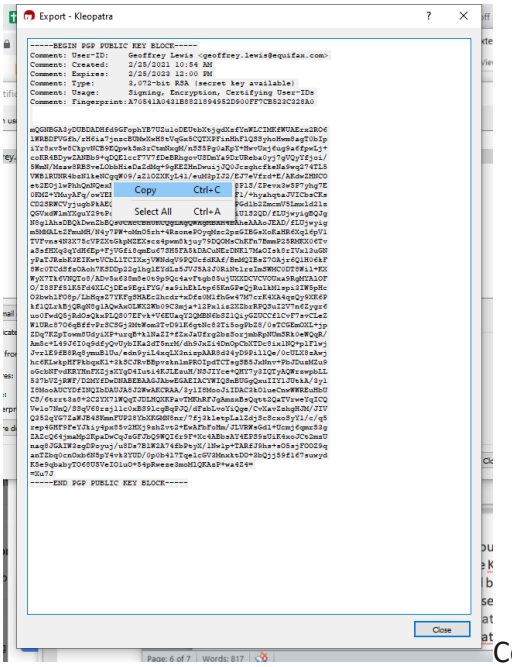
4.2. You will see the screen shown below.



Click Export.

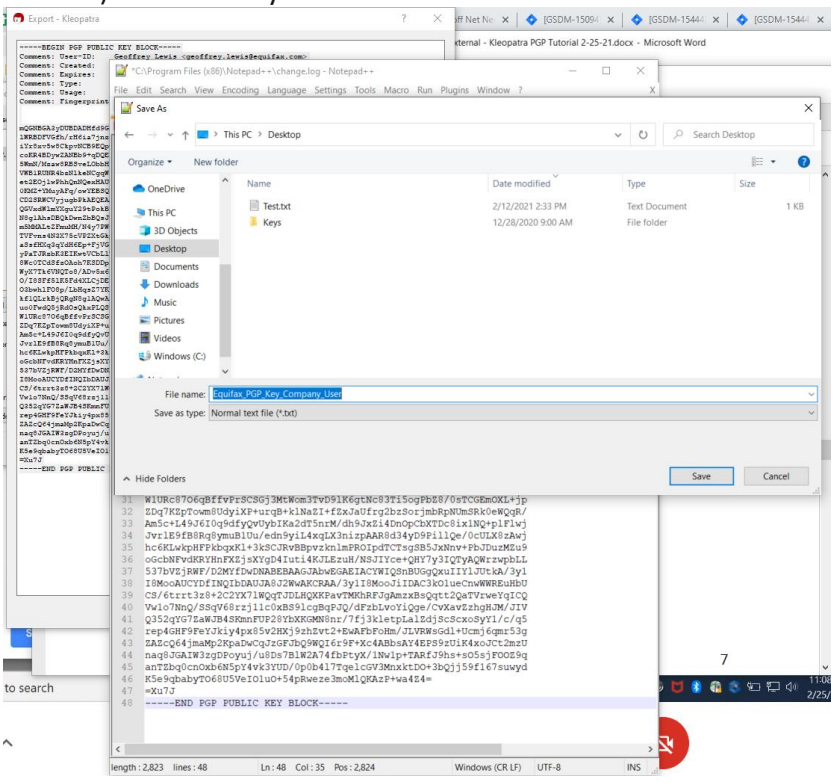
4.3. You should be able to see your public key.

IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.



Copy the entire PGP Key Block.

4.4. Paste the PGP Key Block into any document editor (NotePad++, Word, Wordpad, etc.) that allows you to Save As a .txt file.



Save as a .txt file using a file naming convention that includes your company name and, if applicable, username.

IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

4.5. Forward the key to your Equifax MFT point of contact as an email attachment.

4.6. Go back to Kleopatra and close the open screen.

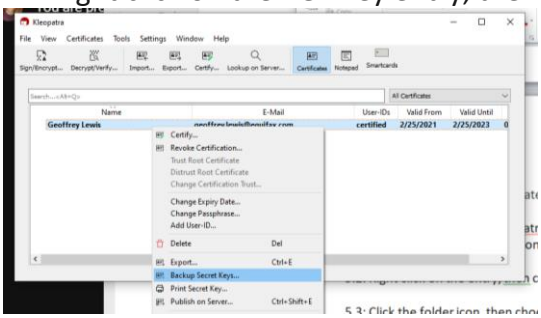
IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

5. Exporting and backing up private key

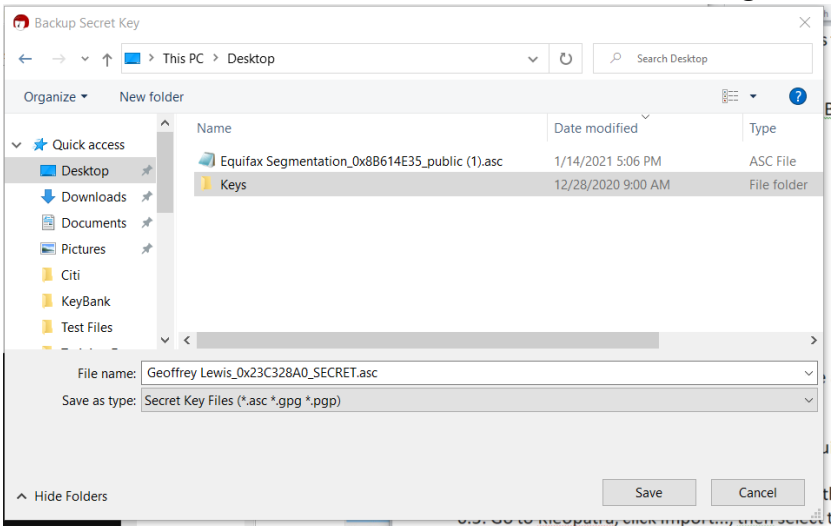
NOTE: Keep your private key secret, NEVER share a private key!!!

5.1. It's recommended by Kleopatra developers to back up your private key, in case of computer failure, theft or accidental deletion.

5.2. Right click on the PGP key entry, then click Backup Secret Keys…



5.3. Click the folder icon, then choose file name and saving location.

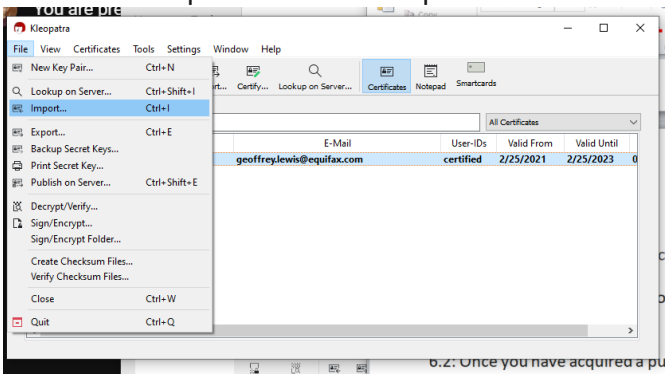


IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

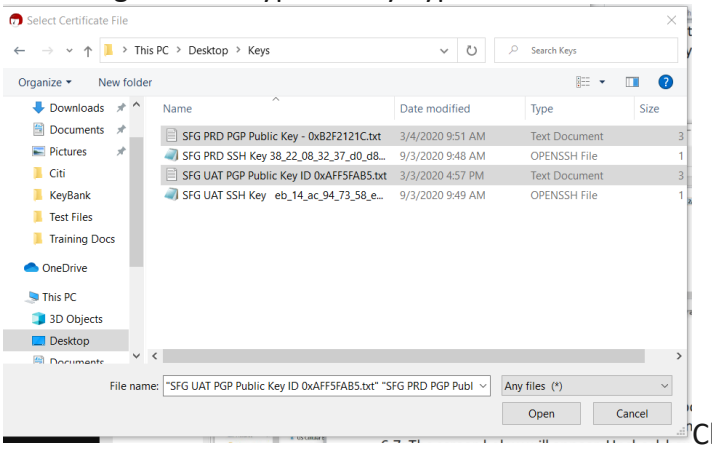
6. Importing a public key

6.1. To send Equifax an encrypted file, you must import and certify both the Equifax SFG UAT PGP Key and SFG PRD PGP Key. Equifax should provide you the keys as email attachments. Download both keys from your email and save ion your local drive.

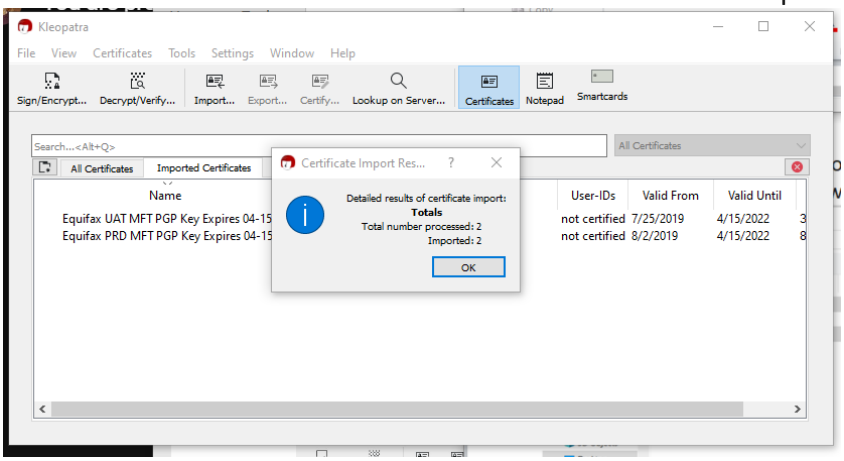
6.2. Go to Kleopatra → File → Import...



6.3. Go to the directory where you saved the keys and select them. You may need to change the file type to Any Type in order to view the keys.



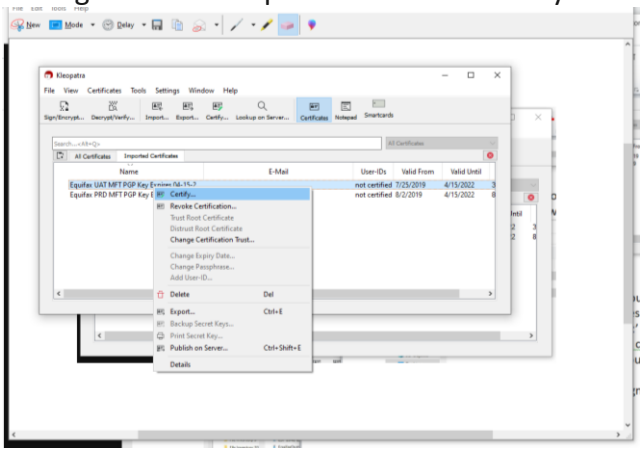
Click Open.



Click Ok.

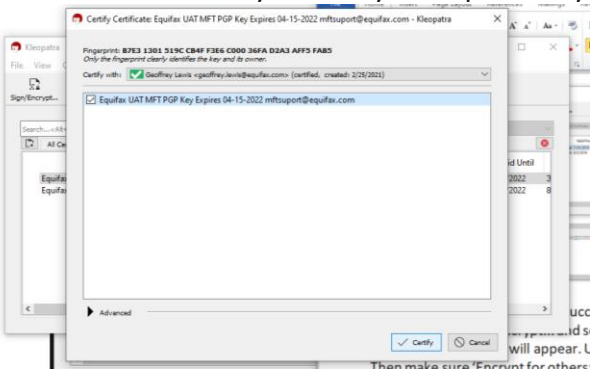
IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

6.4. Right click the Equifax SFG UAT PGP key.



Click Certify.

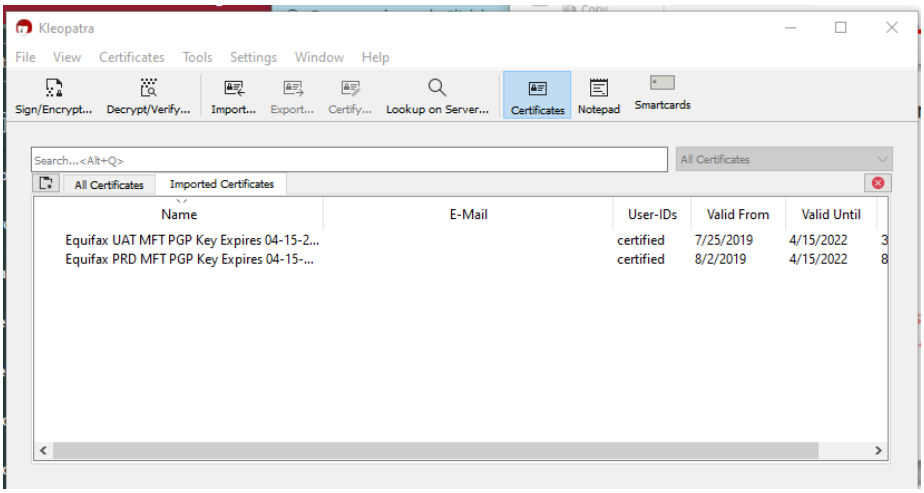
6.5. Make sure Certify With is your Equifax key entry.



Click on the Equifax PGP key. Click Certify.

6.6. Repeat steps 6.4 and 6.5 for the Equifax SFG PRD PGP Key.

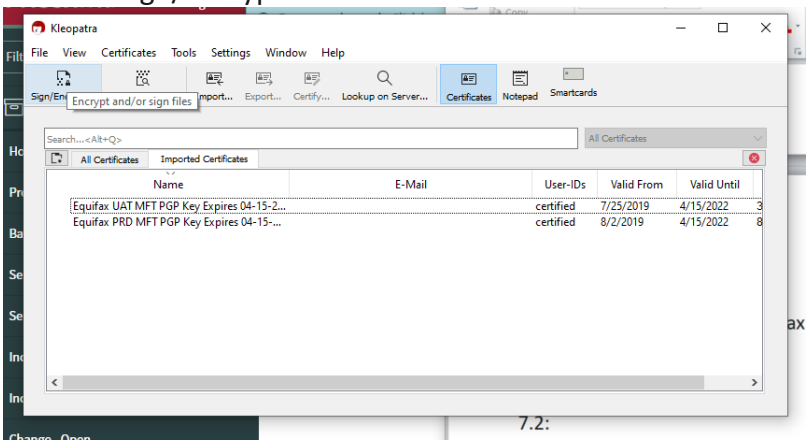
6.7. Both keys should not show as Certified.



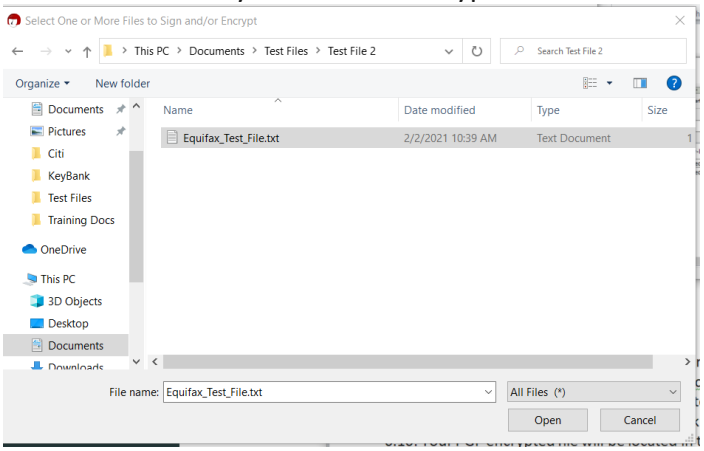
IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

7. Encrypting Files Sent to Equifax

7.1. Click Sign/Encrypt….



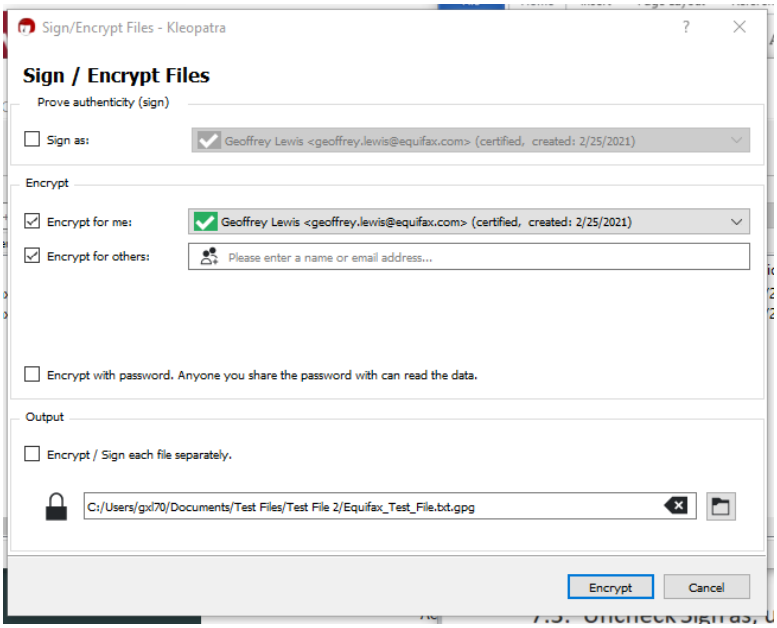
7.2. Select the file you want to encrypt.



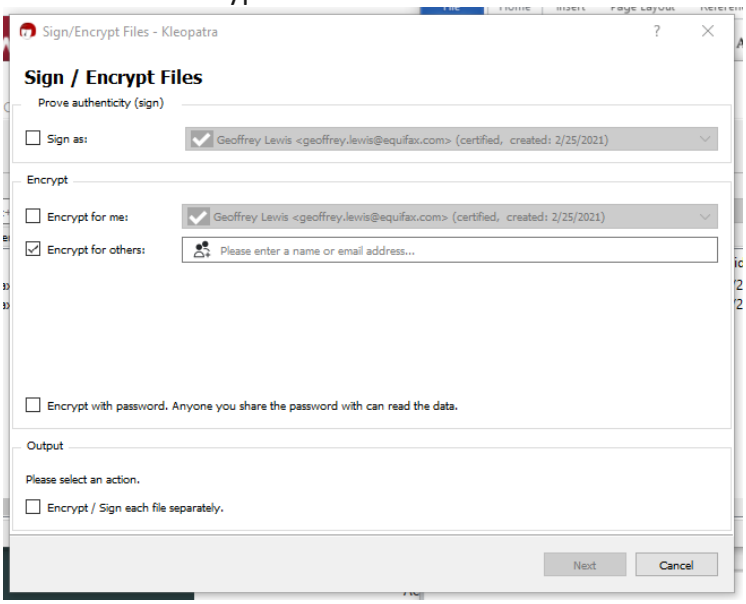
Click Open.

7.3. Uncheck Sign as, unless you had Equifax configure a PGP signing requirement. If so, leave it checked and make sure your Equifax PGP key entry is selected.

IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

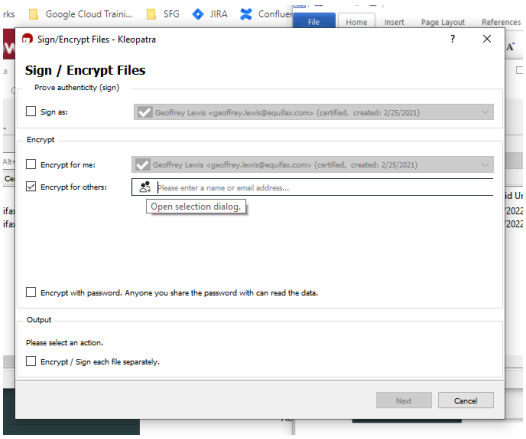


7.4. Uncheck Encrypt for me:

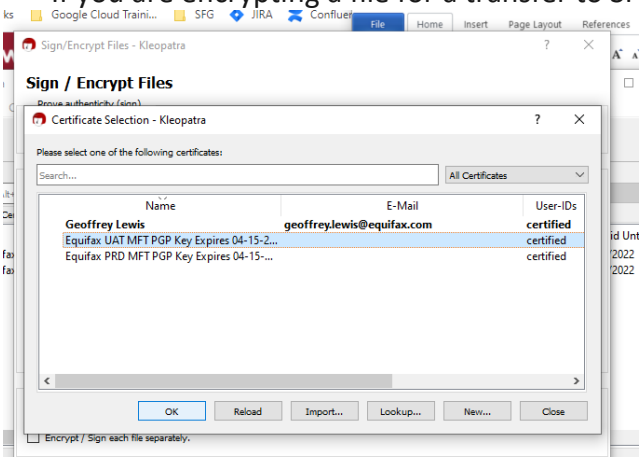


7.5. Click the Encrypt for others → Open Selection Dialogue

IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

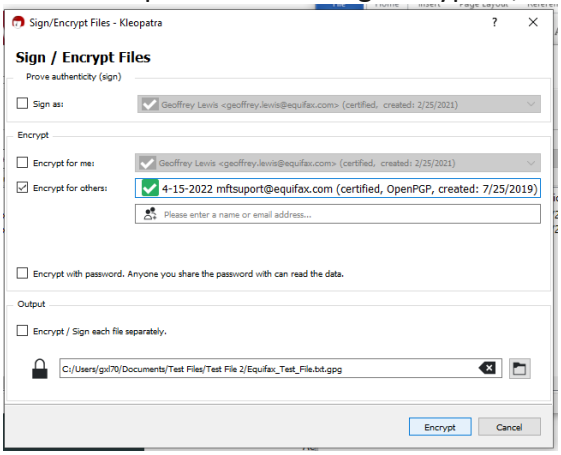


7.6. If you are encrypting a file for a transfer to SFG UAT, select the Equifax UAT PGP Key. If you are encrypting a file for a transfer to SFG PRD, select the Equifax PRD PGP Key.



Click Ok.

7.7. Output should show the full directory path where you want the encrypted file saved. If multiple files are being encrypted, Encrypt/Sign each file separately.

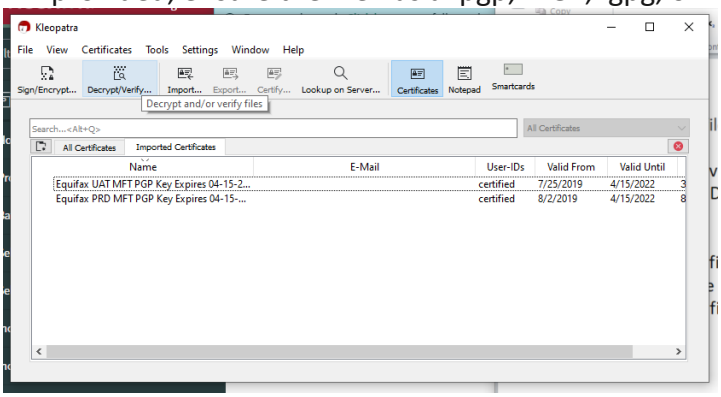


Click Encrypt.

IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

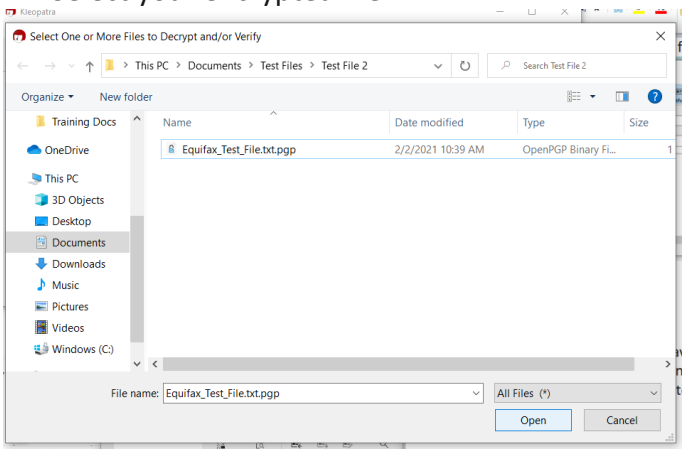
8. Decrypting PGP files

8.1. Once you received the file that Equifax encrypted with the public PGP key you provided, ensure the file has a .pgp, .PGP, .gpg, or .GPG file extension.



Go to Kleopatra. Click Decrypt/Verify...

8.2. Select your encrypted file.



8.3. You will see the success screen below. Click Save All.

8.4. The decrypted file will be located in the designated folder where the original file was saved.

IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.